The 24th Network Security Conference -Korea

# NetSec-KR 2018

## 제24회 정보통신망 정보보호 컨퍼런스

2018
4. 12 Thu.
— 13 Fri.

COEX
Seoul, Korea

## 4차 산업혁명시대의 사이버보안

**주 관** 한국정보보호학회(KIISC)

**주 최** 한국인터넷진흥원(KISA)

**후 원** 과학기술정보통신부(MSIT), 행정안전부(MOIS)

**기관후원** 국가보안기술연구소(NSR), 한국전자통신연구원(ETRI), 금융보안원(FSI)

**대학후원** KAIST 사이버보안연구센터, 고려대학교 정보보호대학원, 국민대학교 정보보안암호수학과·차세대 암호연구센터, 부산대학교 사물인터넷연구센터, 순천향대학교 IoT보안연구센터·정보보호학과, 숭실대학교 사이버보안연구센터, 아주대학교 사이버보안학과, 연세대학교 정보보호연구실, 중앙대학교 BK21·인간중심보안경영연구팀, 중앙대학교 산업보안연구센터, 충남대학교 운영체제안전성연구단·핀테크보안연구센터

**기업후원**

*Platinum Sponsor*
라온시큐어, 시큐브, 안랩, 코나아이

*Gold Sponsor*
네이버, 드림시큐리티, 마이크로소프트, 에스지에이솔루션즈, 윈스, 지란지교시큐리티, 한국통신인터넷기술

*Silver sponsor*
LG 히다찌, 이글루시큐리티, 지니언스, 케이사인, 포멀웍스

*Bronze sponsor*
소만사, 온시큐리티, 이니텍

한국정보보호학회
Korea Institute of Information Security & Cryptology

# 프로그램

## 4. 12

| | 301 | 401 | 402 |
|---|---|---|---|
| 09:00~10:00 | | 등록 | |
| 10:00~12:00 | **Tutorial 1**<br>**소프트웨어 보안** | **Tutorial 2**<br>**블록체인** | **Tutorial 3**<br>**차량보안** |
| | 좌장 : **류연승** 명지대 교수 | 좌장 : **조규민** 금융보안원 팀장 | 좌장 : **이은덕** 교통안전공단 박사 |
| | IoT SW보안 취약점 자동분석 기술<br>**이희조** 고려대 교수 | Private 블록체인 기반의<br>상품 거래 시스템 구현 시연<br>**공무제** IBM 에반젤리스트 | 스마트카 보안의 현안과 기술 방향<br>**심상규** 펜타시큐리티 소장 |
| 12:00~13:30 | | Lunch Break | |
| 13:30~15:00 | **Session 1**<br>**소프트웨어 보안** | **Session 2**<br>**블록체인 I** | **Session 3**<br>**인공지능 보안** |
| | 좌장 : **이동근** KISA 단장 | 좌장 : **맹영재** NSR 박사 | 좌장 : **강필용** KISA 센터장 |
| | Semantic Transformation을 이용한<br>사용자의 패스워드 보안과 취약점분석<br>**우사이먼** 한국뉴욕주립대학교 수 | 비트코인 시스템의 이해<br>**김형식** 성균관대 교수 | SPAI (Secure and Private AI)<br>**윤성로** 서울대 교수 |
| | 최근 랜섬웨어 동향 및 전망<br>**김병재** KISA 선임 | 프라이빗/컨소시움<br>블록체인 vs 퍼블릭 블록체인<br>**양대헌** 인하대 교수 | 딥러닝을 이용한 악성코드 분석 연구<br>**윤명근** 국민대 교수 |
| | 브라우저 보안의 진화<br>**박세준** 티오리 대표 | 블록체인 프라이버시 보호 기술 동향<br>**조남수** ETRI 선임 | 딥러닝 기반 이상징후<br>탐지시스템 실적용 사례<br>**유경식** 인피니그루 대표 |
| 15:00~15:30 | | Coffee Break | |
| 15:30~17:30 | **Session 4**<br>**차세대 인증** | **Session 5**<br>**블록체인 II** | **Session 6**<br>**제어시스템 보안** |
| | 좌장 : **정병호** ETRI 박사 | 좌장 : **임을규** 한양대 교수 | 좌장 : **서정택** 순천향대 교수 |
| | 생체신호를 이용한 차세대 인증기술<br>**김재성** KISA 연구위원 | 다크웹 및 불법 암호화폐 거래 분석 기술<br>**허준범** 고려대 교수 | 제어시스템 보안 기술 동향<br>**민병길** NSR 선임 |
| | 상황인지 기반의 범용 인증기술<br>**김승현** ETRI 선임 | 블록체인 취약점 연구 동향<br>**김용대** KAIST 교수 | Is it ICS Malware or No-malware?<br>**손태식** 아주대 교수 |
| | 인공지능기반 차세대 인증<br>패러다임 변화 방향<br>**박정현** 금융결제원 팀장 | 스마트 컨트랙트와 보안<br>**이종협** 가천대 교수 | 발전제어시스템 이상징후 탐지를 위한<br>화이트리스트 개발 및 현장적용 사례<br>**강형구** 온시큐리티 대표 |
| | 딥러닝을 적용한<br>서명행위 기반의 생체인증<br>**한승호** 시큐브 연구소장 | 암호화폐 거래소 보안 전략<br>**이은준** 라온시큐어 이사 | 전력제어 사이버보안 기술 동향<br>**김진철** 한전KDN 팀장 |
| 17:30~17:40 | | 경품 추첨(401호) | |

# 프로그램

## 4. 13

| | 301 | 401 | 402 |
|---|---|---|---|
| 09:00~09:30 | 등록 | | |
| 09:30~11:30 | **초청강연**(401호) / 좌장 : **강병훈** KAIST 교수<br>Keynote 1 **"암호화폐 거래소의 보안 현황" / 이석우** ㈜두나무 대표<br>Keynote 2 **"Driving Behavior Identification via Ubiquitous Sensing" / 신강근** 미, 미시간대 석좌교수 | | |
| 11:30~12:00 | **개회식** / 사회 : **서정택** 순천향대 교수<br>**개회사** 한국정보보호학회 **홍만표** 회장<br>**환영사** 한국인터넷진흥원 **김석환** 원장<br>**축사** 과학기술정보통신부 **김정삼** 정보보호정책관<br>**축사** 행정안전부 **김혜영** 정보기반보호정책관<br>**과학기술정보통신부 장관표창 시상**<br>**행정안전부 장관표창 시상**<br>**한국인터넷진흥원 원장상 시상**<br>경품추첨 | | |
| 12:00~13:30 | Lunch Break | | |
| 13:30~15:00 | **Session 7**<br>**클라우드 보안**<br>좌장 : **이문규** 인하대 교수<br>클라우드 가상화 환경에서의 보안위협: 캐시 기반 은닉 채널<br>**신영주** 광운대 교수<br>다양한 클라우드 서비스를 활용한 보안 빅데이터 분석 시스템<br>**이경용** 국민대 교수<br>I'm listening to your location inferring user location with acoustic side channel<br>**윤지원** 고려대 교수 | **Session 8**<br>**차량보안**<br>좌장 : **신재곤** 교통안전공단 처장<br>이더넷 기반의 커넥티드 자동차 보안<br>**권혁찬** ETRI 책임<br>자동차 해킹사례와 방어기법<br>**이유식** ESCRYPT 부장<br>자동차 보안 표준화 동향<br>**박승욱** 현대자동차 파트장 | **Session 9**<br>**IoT 보안**<br>좌장 : **김인중** NSR 부소장<br>IoT 디바이스 하드웨어 취약성 및 보안기술<br>**김호원** 부산대 교수<br>IoT용 디바이스를 위한 보안 SoC의 활용 방안<br>**김동규** 한양대 교수<br>IoT환경에 적합한 자율형 보안기술<br>**최두호** ETRI 실장 |
| 15:00~15:20 | Coffee Break | | |
| 15:20~16:50 | **Session 10**<br>**오픈소스 보안**<br>좌장 : **나중찬** ETRI 그룹장<br>악성코드 분석 오픈 플랫폼<br>**최원혁** 누리랩 대표<br>오픈소스 보안 글로벌 동향 및 보안 인텔리전스 관리 방안<br>**기태현** 영남이공대 교수<br>바이너리 코드에 기반한 오픈소스 정보 및 관련된 취약점 분석 기술<br>**김영곤** 인사이너리 팀장 | **Session 11**<br>**데이터 분석**<br>좌장 : **문종철** NSR 실장<br>국내 대상 위협 인텔리전스<br>**곽경주** 금융보안원 과장<br>KOSIGN : 대용량 악성파일의 자동화 분석 플랫폼과 분석 대응 기술<br>**조학수** 윈스 전무<br>2017 정보보호 R&D 데이터 챌린지를 통해 살펴본 data-driven security<br>**김휘강** 고려대 교수 | **Session 12**<br>**모바일 보안**<br>좌장 : **황성운** 홍익대 교수<br>블랙마켓 CC Crawling 결과 및 시사점<br>**신동휘** 스틸리언 이사<br>CDR 기술 기반의 모바일 웹 콘텐츠 보안 구현<br>**이상준** 지란지교시큐리티 연구소장<br>5G 이동통신 인증프레임워크<br>**유일선** 순천향대 교수 |
| 17:00~18:00 | [패널토론] **4차산업혁명 시대의 암호화폐 정책 방향**(401호)<br>사회 : **김승주** 고려대 교수<br>토론자 : **김형식** 성균관대 교수 / **구태언** 테크앤로 대표변호사 / **주용완** KISA 본부장 / **이한상** 고려대 교수 / **김종환** 블로코 대표 | | |
| 18:00~18:10 | 경품추첨(401호) 및 폐막 | | |

The 24th Network Security Conference -Korea

# 암호화폐 거래소 보안의 현황

**이석우** (주)두나무 대표

### 학력 및 경력사항

| | |
|---|---|
| 1988.02 | 서울대 인문대학 동양사학과 학사 |
| 1991.08 | University of Hawaii at Manoa 역사학 석사 (Master of Arts) |
| 1997.05 | Lewis & Clark College Law School 법학 박사 (Juris Doctor) |
| 1992 ~ 1994 | 중앙일보 편집국 기자 |
| 1999 ~ 2004 | 한국IBM 사내변호사 |
| 2004 ~ 2011 | 엔에이치엔 주식회사 법무이사, 경영정책 부사장, 미국법인장 |
| 2011 ~ 2015 | 주식회사 카카오 공동대표이사 |
| 2015 ~ 2017 | 중앙일보 조인스 공동대표이사 겸 디지털 총괄 |
| 2017 ~ 현재 | 두나무 주식회사 대표이사 |

### 강연요약

작년 한해동안 암호화폐에 대한 사회적 관심이 뜨거워지면서 암호화폐 거래 환경, 특히 보안성에 대한 우려들이 지속적으로 제기되었다. 실제로 해외에서는 2014년 일본의 암호화폐 거래소인 마운트 곡스의 사고로부터 올해초 일본의 암호화폐 거래소인 코인체크의 해킹사고까지 가상화폐 거래소들의 보안에 대한 우려가 끊이지 않았으며, 국내에서도 작년말 가암호화폐 거래소인 유빗의 보안사고로 인하여 국내의 투자자들도 안전하지 않다는 인식이 존재한다. 본 강연에서는 이전에 발생한 암호화폐 거래소들의 보안사고의 원인을 분석하고 암호화폐 거래소들이 취해야 할 기본적인 보안조치들에 대한 기준을 제시하고자 한다.

# 두나무
# 암호화폐 거래소의 보안

*두나무 대표이사*
이 석 우

## 목차

I. 두나무 - 업비트 현황

II. 암호화폐 거래소 사고사례

III. 암호화폐 거래소 보안

IV. Compliance

# I. 두나무 - 업비트 현황

## 두나무 현황

kakao

QUALCOMM VENTURES

CUBE VENTURES

Atinum INVESTMENT

우리기술투자(주)
WOORI TECHNOLOGY INVESTMENT CO., LTD.

## 두나무 현황

**Chairman 송치형**

서울대학교
컴퓨터공학, 경제학

- 다날에서 차이나모바일 전자 결제 시스템 개발
- Develop Innomove에서 신규 사업 기획 및 개발

**CEO 이석우**

서울대학교
동양사학과

- 전 카카오 CEO
- 전 중앙일보 디지털 총괄실장

**CSO 김형년**

서울대학교
농경제학과

- 다날에서 전자결제 시스템 개발
- 증권 솔루션 회사 10년 경영

**CFO 남승현**

서울대학교
통계학과

- 한국공인회계사
- 삼정 KPMG 내부통제 컨설팅
- 삼성증권 컴플라이언스

**CTO 김광수**

서울대학교
컴퓨터공학

- 카카오 서비스 개발
- 삼성전자 서비스 개발

**CISO 차종현**

경북대학교
전기전자공학

- 삼성SDS 증권매매시스템 개발
- 삼성증권 보안 담당

**CPO 송세정**

연세대학교
문헌정보학

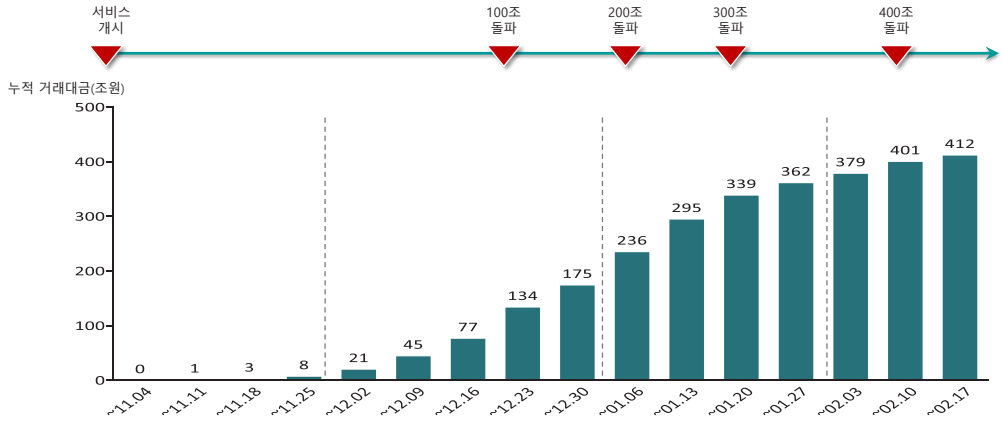
- 카카오에서 서비스 전략
- 다음에서 검색, 소셜 등 서비스 본부장

**CIO 이강준**

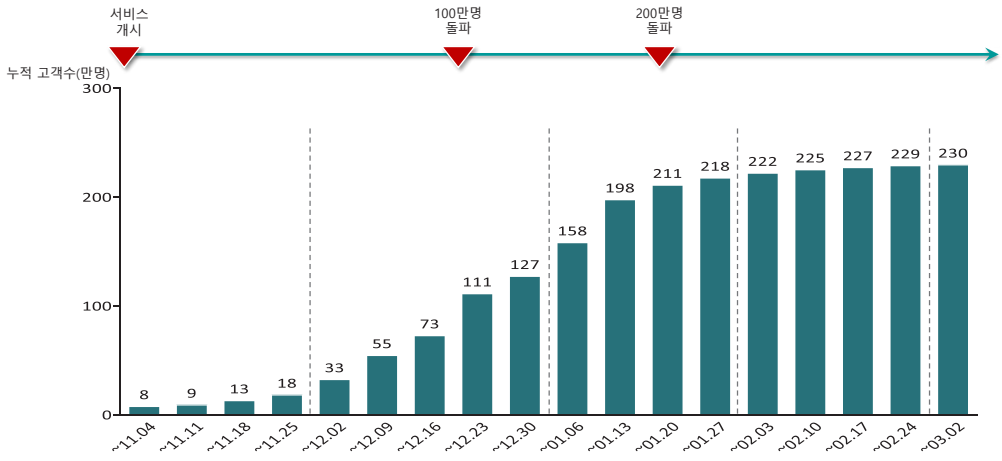
서울대학교 Wharton MBA
컴퓨터공학

- 티몬 여행 총괄, SVP
- 소프트뱅크 벤쳐스, 파트너
- 맥킨지, 컨설턴트

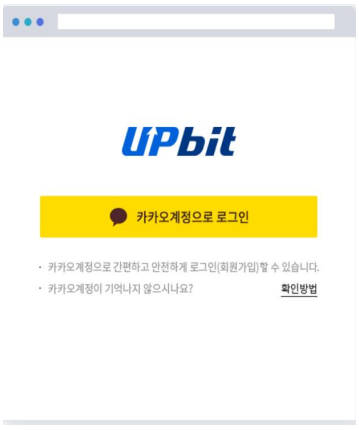
## 업비트 현황 – 누적 거래 대금



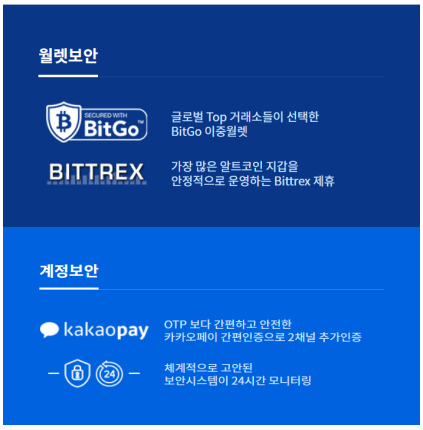
## 업비트 현황 – 누적 고객수




## 업비트 현황 – 보안 경쟁력




<카카오계정 로그인 화면>



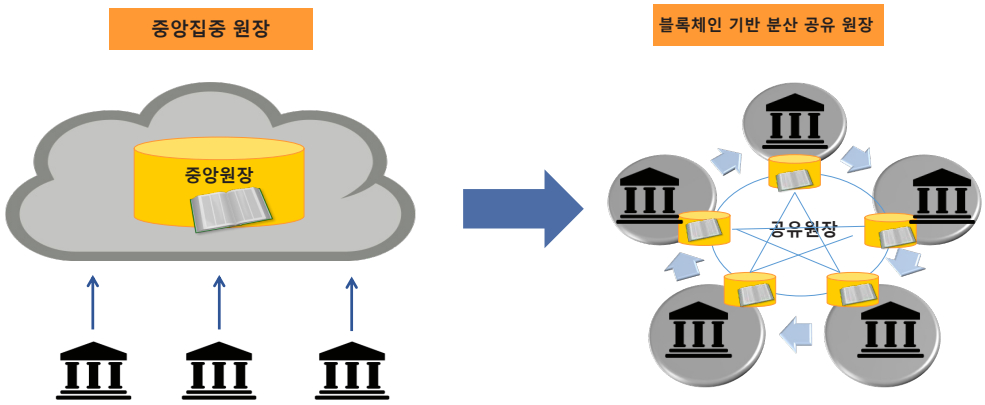

<보안체계 파트너>

## 주요 개념

### 암호화폐

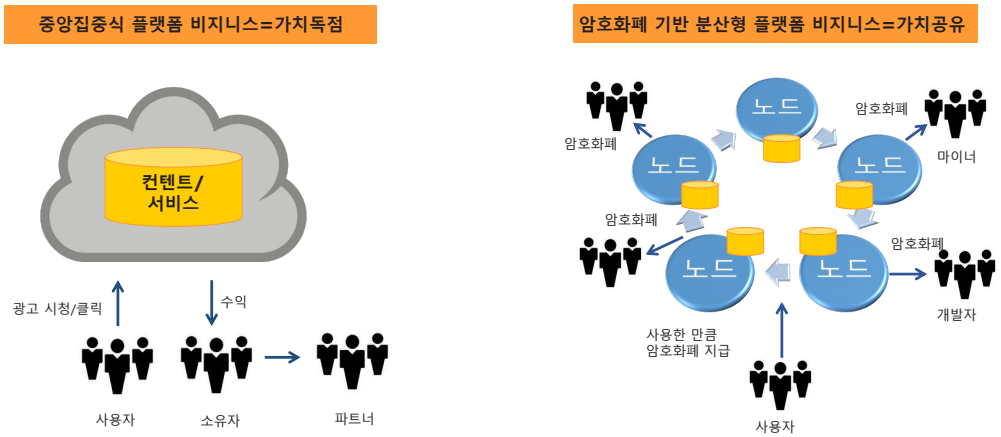
▶ **블록체인** 기술로 암호화되어 네트워크상에서 사용될 수 있는 **디지털자산**

ex) 비트코인, 이더리움, 리플 등



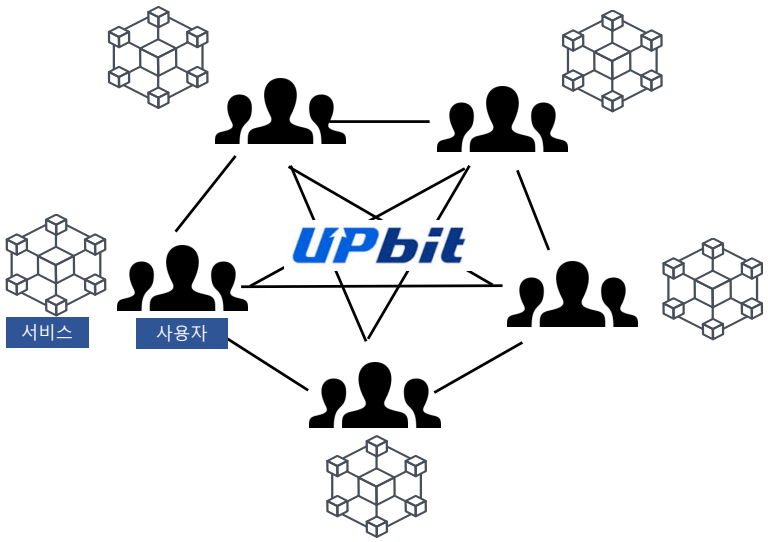

출처 : '코어 이더리움' 강의 교재

## 주요 개념 – 블록체인 기반 분산형 가치 모델




출처 : '코어 이더리움' 강의 교재

## 주요 개념 – 거래소의 역할




## 주요 개념 – 암호화폐 wallet

### 핫월렛(hot wallet)

- 인터넷에 접근 가능한 전자주소
- 출금이 쉽고 빠름
- 해킹에 취약함
- 소액 보관에 용이

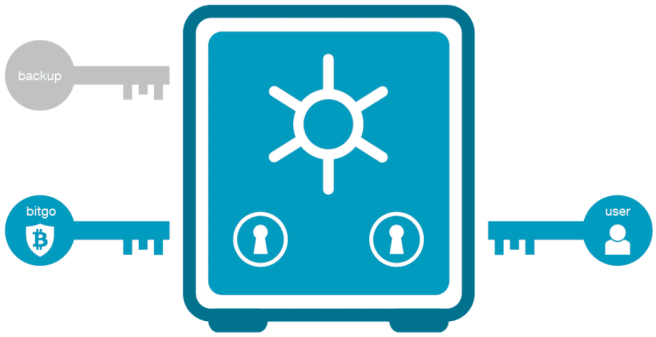
### 콜드월렛(cold wallet)

- 인터넷에 접근 불가능한 전자주소
- 출금이 번거로움
- 상대적으로 해킹에 안전함
- 거액 보관에 용이

## 주요 개념 – 멀티시그(multisig)

### 멀티시그(multisig)

- ▶ 다중 서명 보안
- ▶ 트렌젝션을 위해 2개 이상의 서명(key)을 해야 전송하는 방식
- ▶ 거래소, 보안회사, 오프라인상으로 보관하여 해킹으로부터 안정성을 높이는 방법




출처 : 경록김의 뷰티풀 프로그래밍

# Ⅱ. 암호화폐 거래소 사고사례

## 암호화폐 거래소 사고사례

### 사건 개요

▶ **(1차사고)** 거래소 핫월렛에서 보관중인 Private-Key가 유출되어 전체 자산의 37%에 해당하는 비트코인 탈취당함
- 직원의 개인PC가 악성코드에 감염되어 있었고, 분석결과 북한 소행으로 추정
- 이후 고객의 자산에서 37%를 일괄적으로 차감 후 사명을 변경하여 영업재개

▶ **(2차사고)** 거래소에 보관중인 암호화폐 자산 17%가 해킹으로 탈취당했다고 발표 후 파산 선언
- 사고발생 18일전 사이버종합보험(30억원) 가입에 따른 자작극 논란
- 피해 보상이 완료되지 않은 상태에서 소유권 매각 후 영업재개

### 시사점

▶ 콜드월렛, 멀티시그 기술 적용 등 거래소 지갑에 대한 보안 강화 필요
▶ 국내 암호화폐 거래소 해킹 중 가장 이슈화가 된 사례로 사고 이후 대응도 미흡하여 업계 신뢰도 하락

| 사고년월 | 피해 | 피해액 | 비고 |
|---|---|---|---|
| **2017**년 **4**월 | 비트코인 **3,831**개 | **55**억원 | 개인자산 **37%** 차감 |
| **2017**년 **12**월 | 암호화폐 자산 **17%** 손실 | **170**억원 | 파산 선언 |

출처 : 가상화폐 거래소 `유빗` 해킹에 파산, 조선일보, 2017.12.20

## 암호화폐 거래소 사고사례

### 사건 개요

▶ 스피어피싱 메일을 통해 협력업체 직원 PC가 악성코드에 감염, 개인정보가 포함된 파일 탈취
▶ 유출된 파일을 바탕으로 해커가 3500개의 IP에서 약 200만번의 사전대입공격을 수행
▶ 이중 5000개 계정은 로그인에 성공하여 사용자 계정 탈취, 266개 계정은 로그인 성공 후 암호화폐 출금
▶ 과징금, 과태료, 책임자 징계권고, 재발방지대책 수립 등 행정처분

### 시사점

▶ 개인정보 파일을 암호화 하지 않고 개인용 컴퓨터에 저장
▶ 개인정보 유출 시도 탐지 부재

| 사고년월 | 피해 | 피해액 | 비고 |
|---|---|---|---|
| **2017**년 **6**월 | 개인정보 **36,000**건 | - | 과징금 **4,350**만원<br>과태료 **1,500**만원 |

출처 : 방송통신위원회 보도자료, 2017.12.12

## 암호화폐 거래소 사고사례

### 사건 개요

▶ 코인** ICO을 3분 후 해커가 공식 웹사이트를 해킹, 토큰을 구입하기 위해 돈을 송금하는 이더리움 지갑의 주소를 변경
▶ 코인**는 실수를 인정하고 해커의 지갑으로 이더리움을 송금한 사용자에게도 토큰을 부여
▶ 그러나 해커는 탈취한 이더리움 43,400개 중 2회에 걸쳐 30,000개의 이더리움을 반환
▶ 돌려준 이유는 알 수 없으나 해커의 지갑 주소가 블랙리스트에 등록되어 현금화가 어려웠을 것으로 추정

### 시사점

▶ 암호화폐 거래시스템이 아닌 단순 홈페이지 해킹만으로 암호화폐 탈취가 가능

| 사고년월 | 피해 | 피해액 | 비고 |
|---|---|---|---|
| **2017**년 **7**월 | 이더리움 **43,400**개 | **85**억원 **(**사고시점 기준**)** | **17**년 **9**월 **10,000 ETH** 반환 **18**년 **1**월 **20,000 ETH** 반환 |

출처 : 이더리움 훔쳤다가 되돌려준 해커, 보안뉴스, 2018.2.28

## 암호화폐 거래소 사고사례

### 사건 개요

▶ 해커가 인터넷에 연결된 지갑에 접근하여 보관중인 NEM을 전량 탈취, 580억 엔 인출
▶ 암호화폐 이체, 인출이 8시간에 걸쳐 이루어졌으나, 최초 이체로부터 11시간이 지난 후 해킹 사실 확인
▶ 코인**는 암호화폐에 태그를 붙여 해커가 현금화 하는 것이 쉽지 않을 것이라 주장했으나, 최근 이유를 알리지 않은 채 추적을 중단함
▶ 익명사이트를 거쳐 중국, 캐나다 등 전세계의 타인 계좌로 보내진 뒤 이미 돈세탁이 끝난 것으로 추정

### 시사점

▶ 암호화폐를 핫월렛에 전량 보관하고 멀티시그 보안방식을 적용하지 않아 해킹 위험에 노출
▶ 지갑 이상징후 모니터링을 통한 해킹 등 침해사고 대응 및 피해 방지 필요

| 사고년월 | 피해 | 피해액 | 비고 |
|---|---|---|---|
| **2018**년 **1**월 | **5**억 **2,300**만 **NEM** | **5700**억원 | 역대 최대 피해 금액 |

출처 : 해커, 훔친 `코인` 현금화 시도.. NEM재단 `꼬리표` 붙여 추적, 동아일보, 2018.2.2

## 암호화폐 거래소 사고사례

### 주요 거래소 해킹 사건

| 사고 년월 | 국가 | 피해 | 피해금액 | 공격유형 | 비고 |
|---|---|---|---|---|---|
| 18년 2월 | 이탈리아 | 1,700만 Nano | 1,700억원 | 핫월렛 해킹 | |
| 18년 1월 | 일본 | 5억 2,300만 NEM | 5,700억원 | 핫월렛 해킹 | 피해자 26만명 |
| 17년 12월 | 한국 | 전체 자산의 17% | 170억원 | 핫월렛 해킹 | 파산 선언 |
| 17년 9월 | 한국 | 508 BTC | 21억원 | 핫월렛 해킹 | |
| 17년 7월 | - | 43,400 ETH | 85억원 | 홈페이지 해킹 | 해커가 30,000 ETH 반환 |
| 17년 6월 | 한국 | 개인정보 36,000건 | - | 내부자 공격 | 과징금 4,350 만원<br>과태료 1,500 만원 |
| 17년 4월 | 한국 | 3,831 BTC | 55억원 | 핫월렛 해킹 | 모든 개인 자산을 37% 차감 |
| 16년 8월 | 홍콩 | 119,756 BTC | 700억원 | 핫월렛 해킹 | 모든 개인 자산을 36% 차감 |
| 15년 1월 | 슬로베니아 | 18,866 BTC | 55억원 | 내부자 공격 | 투자자 손실 없음 |
| 14년 2월 | 일본 | 850,000 BTC | 4500억원 | 내부자 공격 | 파산 |

## 암호화폐 거래소 사고사례

### 해킹 사고 유형

| 사고 유형 | 유형 설명 |
|---|---|
| Wallet Vulnerability | •전자지갑과 Hot Wallet(Hot wallet)에서 투자자들의 개인키를 훔쳐 암호화폐를 다른 전자지갑으로 이체하여 탈취하는 유형 |
| Application Vulnerability | •웹이나 App의 코드 상 취약점을 이용하여 해킹을 시도하는 유형<br>•대부분 개발자의 백도어나 버그가 원인 |
| Insider Vulnerability | •내부자의 부주의에 의한 해킹사고 유형<br>•인터넷에 연결된 내부자의 PC 등을 이용하여 개인정보, 해킹시도 하기 위해 필요한 정보를 탈취하는 유형 |

***"궁극적으로 Wallet의 Private Key를 얻어서 암호화폐를 탈취할 목적을 가지고 접근"***

## 암호화폐 거래소 사고사례

### 암호화폐 거래소 해킹 발생 이유?

▶ **구체적인 대상**
- 암호화폐는 실체가 없으므로, 거래소라는 구체적인 대상이 해킹의 타겟이 됨

▶ **중앙집중식 시스템**
- 증권거래소 형식의 중앙집중식 거래 방식
- 고객들의 코인을 거래소의 전자지갑에 보관하는 방식

▶ **풍부한 유동성**
- 3월 기준 상위 두 거래소(업비트, 빗썸)거래 금액 약 10조원

▶ **새로운 비즈니스 모델**
- 새로운 비즈니스 모델에 따른 새로운 해킹형태
- 그만큼 방어와 예방에 더 많은 시간과 노력이 필요함

## 암호화폐 거래소 사고사례

### ROOT CAUSE ESTIMATES

*"구조적 보안, Application 보안적 문제로 사고가 발생"*

*"Cloud 시스템을 이용하여 서비스를 제공하는 경우가 많아 Cloud 보안이 대두"*

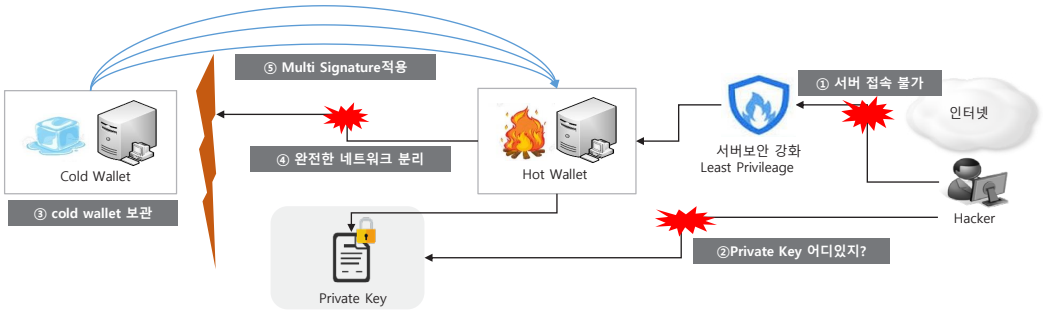
출처 : BLOCKCHAIN GRAVEYARD

# Ⅲ. 암호화폐 거래소 보안

## 암호화폐 거래소 보안 – wallet 보안

### Wallet 보안 5단계

| 서버 보안 강화 | Private Key 관리 | Cold Wallet 구성 | Cold & Hot Wallet 네트워크 분리 | Multi Signature |
|---|---|---|---|---|
| • 서버접근제어 강화<br>• 최소권한의 원칙<br>• 감사로그 점검 | • 서버가 공격 당하더라도 Hot Wallet의 Private Key를 찾지 못하면 이체 시킬 수 없다 | • Cold Wallet을 구성하여 반드시 70% 이상의 금액은 Cold Wallet에 보관(권고) | • Cold & Hot Wallet의 네트워크를 완전하게 분리하여 통신할 수 없도록 처리 | • Private Key 2개 이상이 승인해야 Cold Wallet에서 Hot Wallet으로 송금 가능<br>• Private Key 백업하여 분리<br>• Cold Wallet 관련 모니터링 강화 |



## 암호화폐 거래소 보안 – 모니터링 체계 구축

**이상금융거래 모니터링**

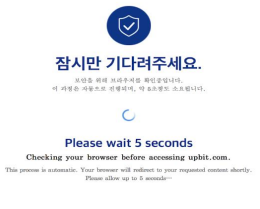
- ▶ 보이스피싱
- ▶ 의심스러운 입출금
- ▶ 암호화폐 다단계 사기

**Hot wallet 이상징후**

- ▶ 핫월렛 출금 상시 모니터링
- ▶ 이상징후 발견 즉시 출금 정지
- ▶ 핫월렛 비중 최소화

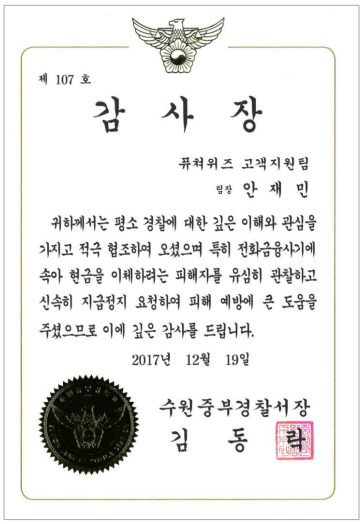
**침해사고 모니터링**

- ▶ DDoS 공격 대응체계 구축
- ▶ 악성코드 이메일 등 APT공격 대응
- ▶ 웹/모바일 취약점 공격 대응




## 암호화폐 거래소 보안 – 모니터링 체계 구축

### 업비트 자체 모니터링 성과



제 107 호

감 사 장

퓨쳐위즈 고객지원팀
팀장 안 재 민

귀하께서는 평소 경찰에 대한 깊은 이해와 관심을 가지고 적극 협조하여 오셨으며 특히 전화금융사기에 속아 현금을 이체하려는 피해자를 유심히 관찰하고 신속히 지급정지 요청하여 피해 예방에 큰 도움을 주셨으므로 이에 깊은 감사를 드립니다.

2017년 12월 19일

수원중부경찰서장
김 동 락

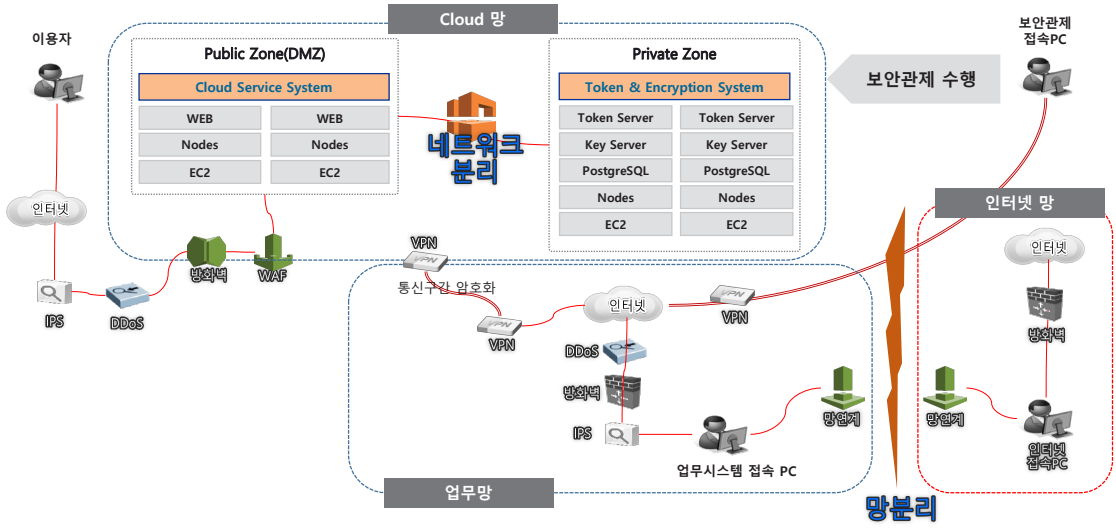
보이스피싱 당해 암호화폐 투자했다가 횡재한 피해자

[중앙포토]

보이스피싱으로 털린 재산이 암호화폐에 투자돼 오히려 더 많은 돈을 벌게 된 사연이 뒤늦게 알려졌다. 피해자는 보이스피싱범을 가리켜 '귀인'이라고 칭했다.

## 암호화폐 거래소 보안 – 망분리 구축

### 망분리를 통한 안전성 확보




## 암호화폐 거래소 보안 – Cloud 보안

| Cloud 관리적 보안 | |
|---|---|
| Cloud Asset | ▪ 가상머신 자산 정보 수집<br>▪ 가상머신 자산 회수<br>▪ 가상머신 모니터링 |
| Cloud Server | ▪ 공개용 서버 보안<br>▪ 악성코드 방지 프로그램 |
| Application | ▪ 인터페이스 보안<br>▪ Software 설치 시 보안 |
| Database | ▪ 데이터 이관 시 보안 |
| Monitoring | ▪ 이상징후 탐지<br>▪ 24시 보안관제 |
| SCM | ▪ Secure Coding<br>▪ 개발과 운영 분리<br>▪ 변경관리 |

| Cloud 기술적 보안 | |
|---|---|
| Access Control | ▪ 비 인가자 접근 통제<br>▪ 접근 기록 모니터링 |
| IAM | ▪ 사용자 관리<br>▪ 사용자 그룹 역할 정의<br>▪ 사용자 패스워드 관리 |
| Authentication | ▪ Cloud 접속 시 강화된 인증<br>▪ 외부에서 접속 시 추가 인증 |
| Database | ▪ 데이터 위.변조 방지<br>▪ 데이터 저장소의 무결성<br>▪ 데이터 추적성 |
| Network | ▪ DDoS 공격으로부터 방어<br>▪ 네트워크 보호장비 구축<br>▪ 서비스별 네트워크 분리 |
| Encryption | ▪ 암호키 Life Cycle 관리 |

| 침해사고 대응 |
|---|
| ▪ Cloud Region DR 구축 |
| ▪ 주요정보 타 Region 백업 |
| ▪ Cloud 환경의 재해 복구 계획 수립 |
| ▪ Cloud 서비스 공급자 보안 인증 |
| ▪ Cloud CDN 서비스 운영 |
| ▪ Cloud Console 모니터링 |
| ▪ Cloud 인증서 관리 |
| ▪ Cloud API 통제 |

*"주요 암호화폐거래소의 시스템은 Cloud 기반에서 운영 중이고, Cloud에 맞는 보안 체계 구축이 필요하다."*

## 암호화폐 거래소 보안 – 내부 보안 교육

### 내부 직원 교육

- ▶ 국내외 사고 사례에 대한 꾸준한 관심과 점검
- ▶ 내/외부 Compliance 주기적 교육
- ▶ 보안의 날 등 정기적 보안점검 활동 체계화
- ▶ 보안 뉴스레터, 웹툰, 캠페인 등 상시 보안교육

### 고객 보안의식 향상

- ▶ 개인정보(ID/패스워드, 계좌정보, 입출금주소 등) 관리 교육
- ▶ 보이스피싱, 거래소를 사칭한 계정 탈취 등 유행하는 보안사고 공지
- ▶ 거래서비스에 필요한 보안프로그램 설치 및 업데이트에 관한 교육
- ▶ 보안관련 범죄에 대한 처벌 및 보상관련 규정 공지

## 암호화폐 거래소 보안 – 보안 수준 단계

### 보안 수준 단계

# IV. Compliance

## Compliance

### 암호화폐 거래소 주요 보안 취약점

▶ **암호화폐 지갑관리 미흡**
- 지갑에 대한 접근통제 및 사용절차, 접속단말기 지정 등 보안통제절차 수립

▶ **망분리 및 시스템 접근통제 관리 미흡**
- 주요 단말기 지정 및 망분리 구성

▶ **정보보호시스템 구축 미흡**
- 방화벽, IPS 등 부재

▶ **외부 개인PC에서 인터넷망을 통해 내부시스템 접근 가능**
- 원격 접근통제 미흡

▶ **관리자PC 설치프로그램에 대한 보안관리 미흡**
- 유해사이트 차단 미흡

▶ **침해사고 대응 절차, 지침 부재**

▶ **주요 데이터 백업관리 체계 미흡**

## Compliance

### 한국블록체인협회 자율규제안

▶ **투자자 예치자산 보호 장치 마련**
- 원화 예치금은 100% 금융기관 예치
- 암호화폐 예치금은 콜드월렛 70% 이상 의무화

▶ **신규 코인 상장 프로세스 강화 · 투명성 제고**
- 신규 코인 상장 평가 정보 공개

▶ **본인 계좌 확인 강화 · 1인 1계좌 입출금 관리**
- 금융기관이 제공하는 시스템을 통해 본인확인 후 입출금

▶ **오프라인 민원센터 운영 의무화**
- 공정한 민원처리와 구제절차 마련

▶ **거래소 회원 요건 강화**
- 20억 이상 자기자본 보유
- 금융업자에 준하는 정보보안시스템, 내부프로세스 및 정보보호인력 조직 운영

▶ **임직원 윤리 강화**
- 거래소 임직원의 미공개 정보 이용, 시세조종, 부정거래행위 등 일체 금지

## Compliance - 암호화폐 거래소의 Compliance

### 현재 Compliance

### 제도화 후

## 이상적인 암호화폐 거래환경

▶ 암호화폐 거래소의 보안 수준을 끌어 올리지 않으면, 국내.외 해킹 사건과 같은 사고로 인하여 투자 피해에 대해서 감당할 수 없다.

▶ 암호화폐 거래소를 선택하는 필수 조건은 보안이 될 것이다.

▶ 해킹 등 침해 사고로부터 암호화폐 거래소가 안전해져야 암호화폐의 가치가 올라간다.

▶ 암호화폐 거래소는 해킹으로부터 안전하게 보호하여 안전한 거래 환경을 조성해야 할 의무가 있다.

감 사 합 니 다

두나무

The 24th Network Security Conference -Korea

# Driving Behavior Identification via Ubiquitous Sensing

**신강근** 미시간대 교수

### 학력 및 경력사항

He received the B.S. degree in Electronics Engineering from Seoul National University, Seoul, Korea in1970, and both the M.S. and Ph.D. degrees in Electrical Engineering from Cornell University, Ithaca, New York in 1976 and 1978, respectively.

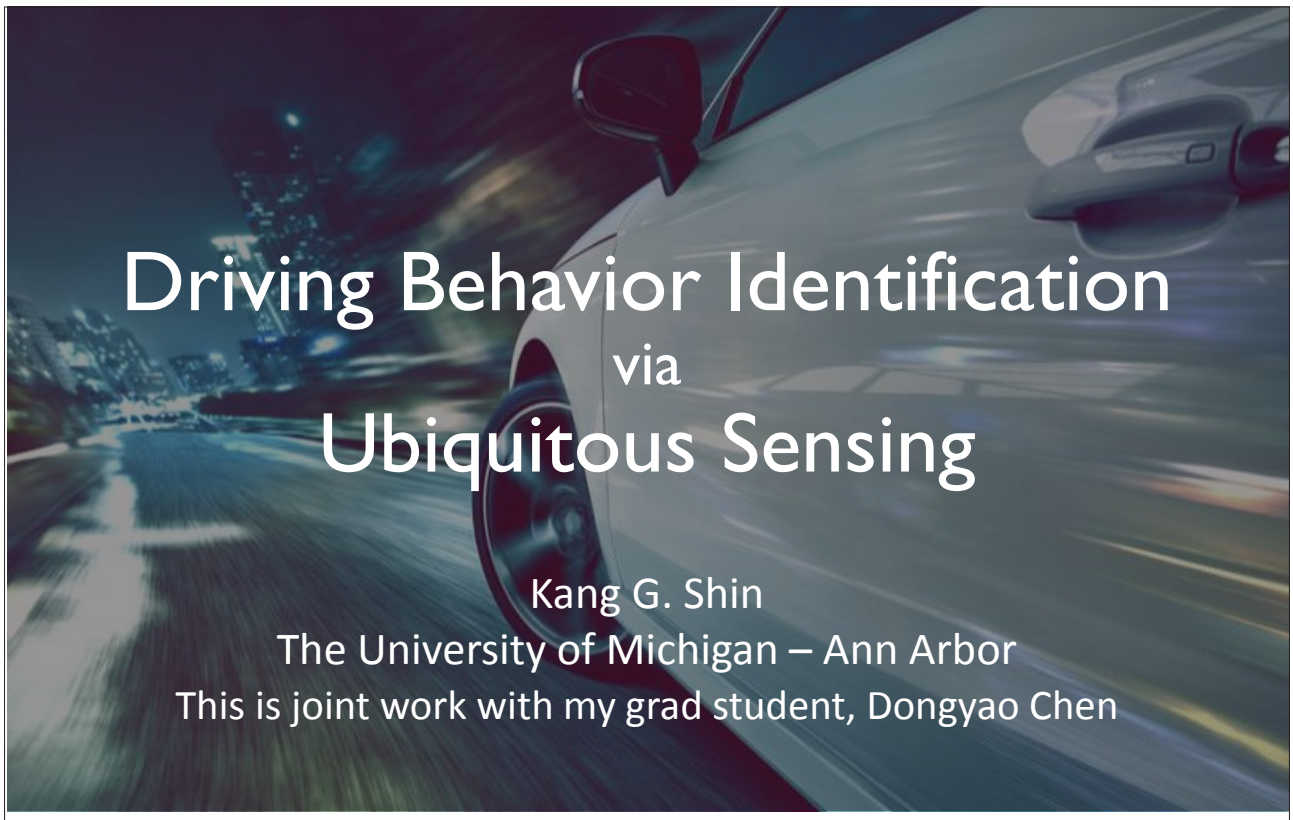
He has held visiting positions at the U.S. Airforce Flight Dynamics Laboratory, AT&T Bell Laboratories, Computer Science Division within the Department of Electrical Engineering and Computer Science at UC Berkeley, and International Computer Science Institute, Berkeley, CA, IBM T.J. Watson Research Center, Carnegie Mellon University, HP Research Laboratories, Hong Kong University of Science and Technology, Ewha Womans University in Korea, and Ecole Polytechnique Federale de Lausanne (EPFL) in Switzerland.

### 강연요약

As vehicle maneuver data becomes abundant for assisted or autonomous driving, their implication of privacy invasion/leakage has become an increasing concern. In particular, the surface for fingerprinting a driver will expand significantly if the driver's identity can be linked with the data collected from his mobile or wearable devices which are widely deployed world–wide and have increasing sensing capabilities.

In line with this trend, I will first review fast emerging driving data collection efforts with focus on driver's privacy implications. I will then show that such privacy threats can be materialized via any mobile device with IMUs (e.g., gyroscope and accelerometer). I will finally present Driver Fingerprint (Dri–Fi), a driving data analytic engine that can fingerprint the driver with vehicle turn(s). Dri–Fi achieves this based on IMUs data taken only during the vehicle's turn(s). Such an approach expands the attack surface significantly compared to existing driver fingerprinting schemes. An adversary or beneficial user equipped with Dri–Fi on his/her smartphone is shown to be able to correctly fingerprint the driver within just one turn with 74.1%, 83.5%, and 90.8% accuracy across 12, 8, and 5 drivers — typical of an immediate family or close–friends circle — respectively. Moreover, with measurements on more than one turn, s/he can achieve up to 95.3%, 95.4%, and 96.6% accuracy across 12, 8, and 5 drivers, respectively.

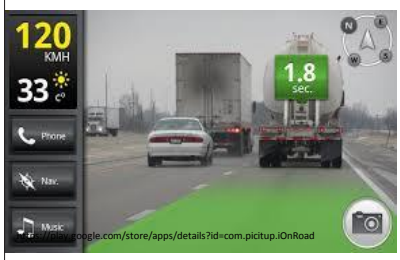
This is joint work with my PhD students, Dongyao Chen, Kyong–Tak Cho, and Mert Pesé


Driving Behavior Identification
via
Ubiquitous Sensing
Kang G. Shin
The University of Michigan – Ann Arbor
This is joint work with my grad student, Dongyao Chen

Driving Behavior Identification
• For human-driven cars
• Driving assistance system
• Detect dangerous driving maneuvers
• Lane change without turn signal
• Anti-theft
Essential for achieving safer and more enjoyable transportation
• For autonomous cars
• Detect anomalies (e.g., software bugs, hardware failure)
Google

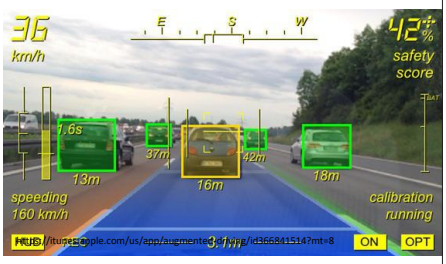
# State-of-the-Art

- Over-reliance on camera and image data

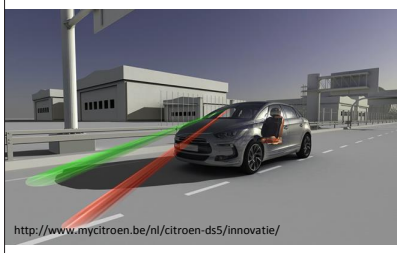



iOnRoad app

BlackSensor app

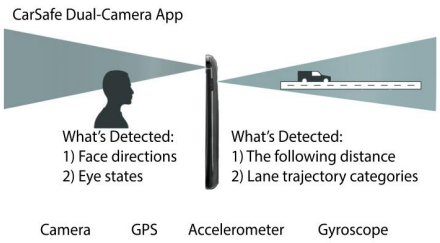



Augmented Driving app




Citroën DS5 LDW System

Volvo CX90 LDW System

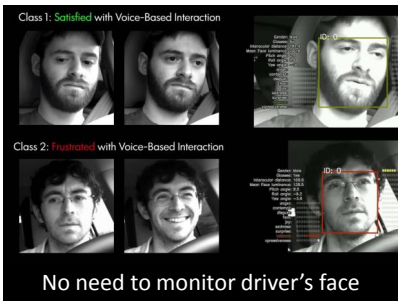



CarSafe app

# Advantages of Ubiquitous Sensing

Usability, practicability, scalability

Light-weight

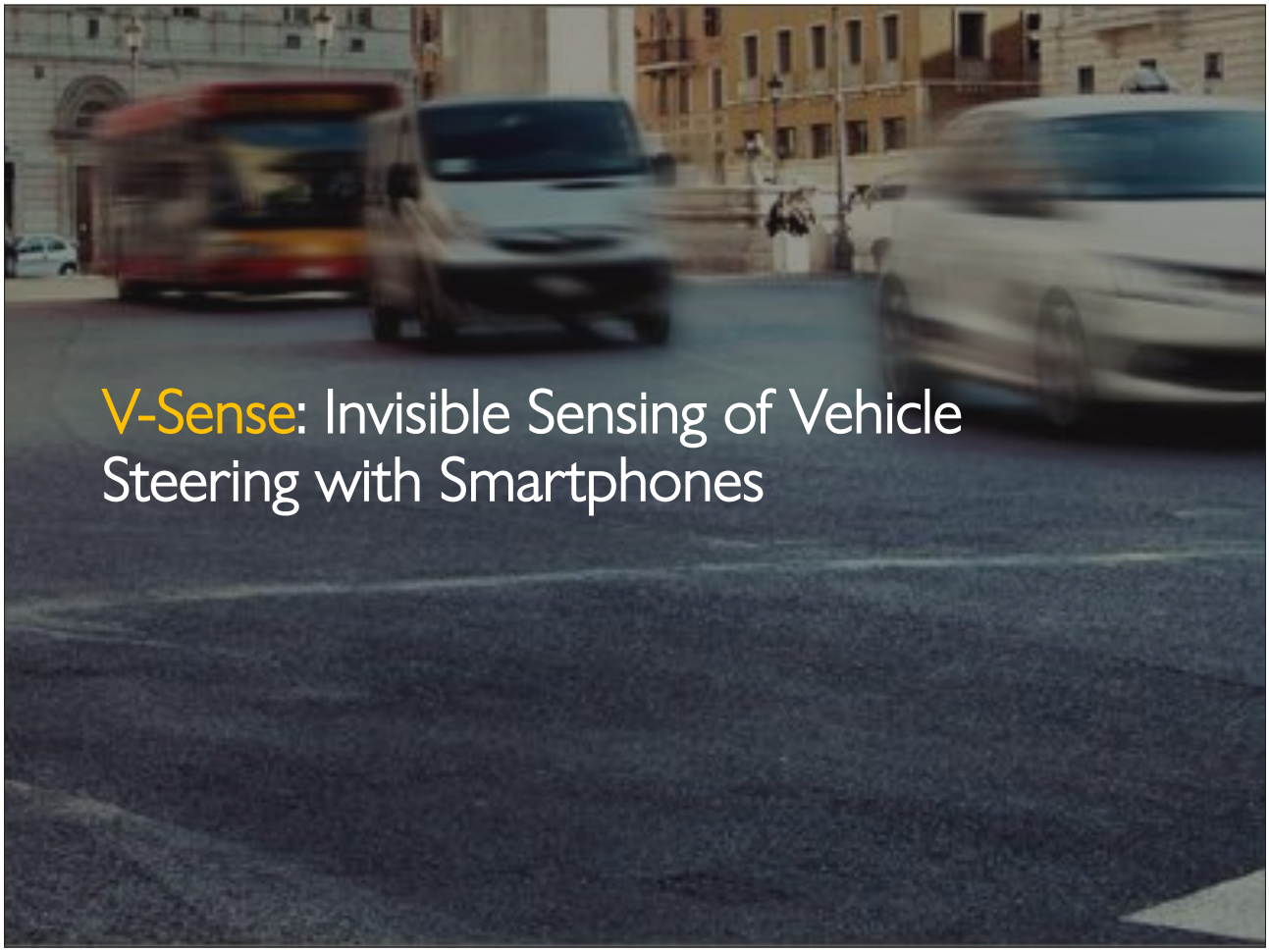


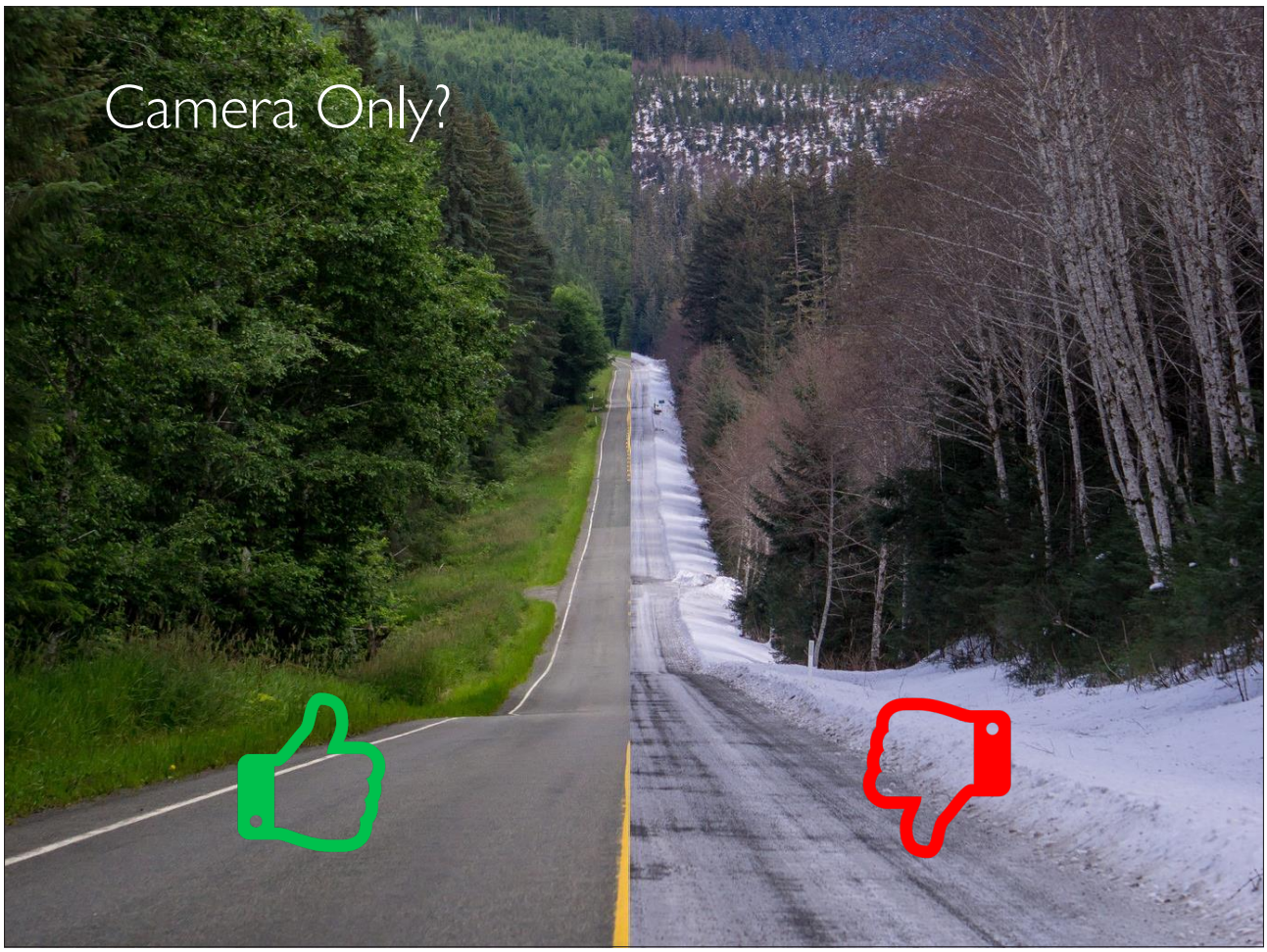

No need to monitor driver's face

- Usability, practicability, scalability:
  - Applicable for all road/weather conditions and various real-world apps
  - Scalable to billions
- Efficiency:
  - Does not require an additional/dedicated sensing platform
  - Detect events/behaviors using time-series sensor data
- Privacy-preserving
  - Detect/identify driving behavior without taking images

# This Talk Covers

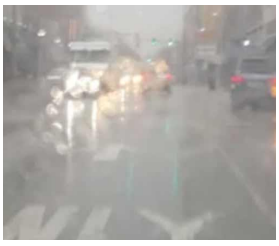
- Two essential enablers for driving behavior identification:
  - Understand vehicle movement (V-Sense)
  - Fingerprint a driver (Dri-Fi)






# Using camera only is not effective!

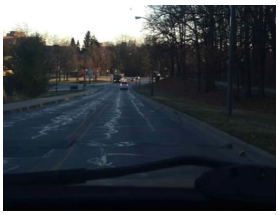
Lighting


Weather

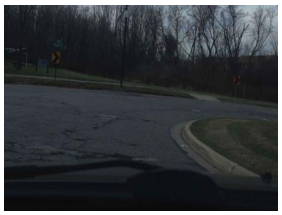
Pavement

Placement

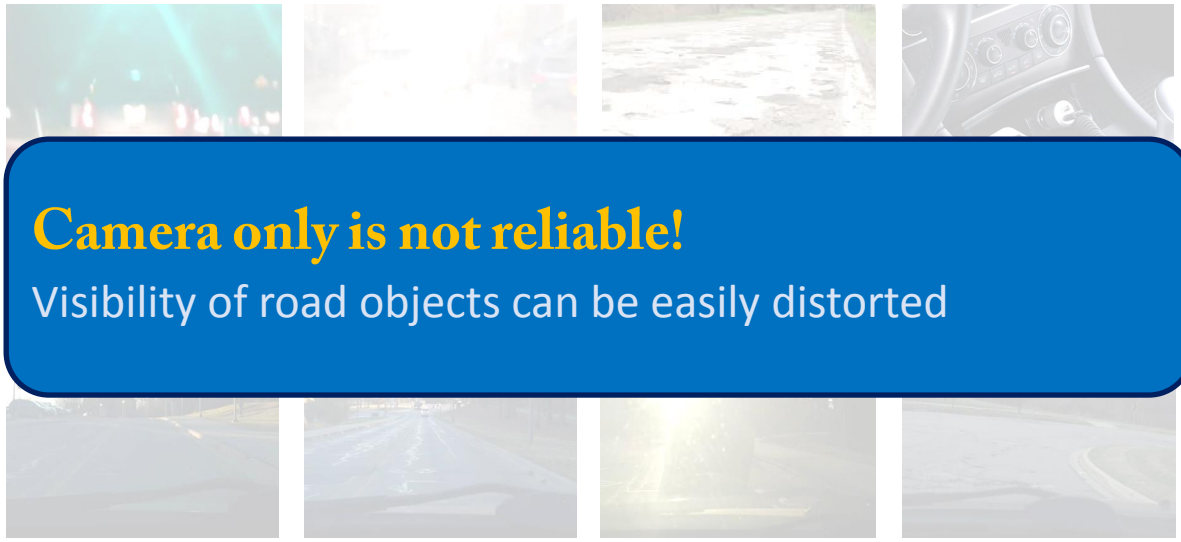
Heavy Shadow


Missing Lane

Sunlight Reflection


Sharp Turn

# Ineffectiveness of Camera Only



**Camera only is not reliable!**

Visibility of road objects can be easily distorted

Heavy Shadow | Missing Lane | Sunlight Reflection | Sharp Turn

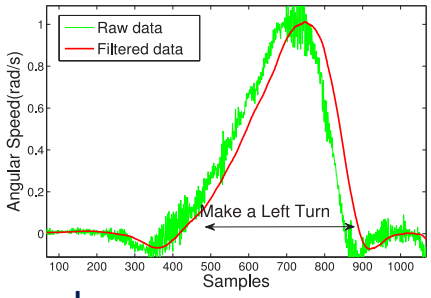
# Detection/Identification of Driving Behavior

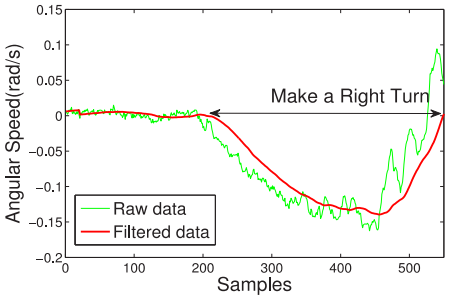
V SENSE

- Reliable
  - Robust to lighting, weather, and pavement conditions
- Accurate
  - In a variety of scenarios
- Easily Accessible
  - As a smartphone app

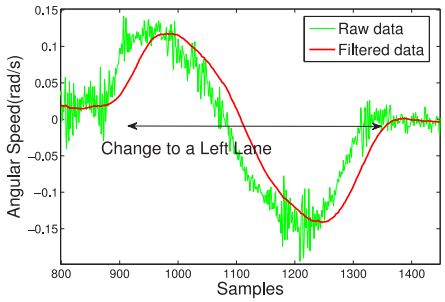
# "Signatures" of Vehicle Steering

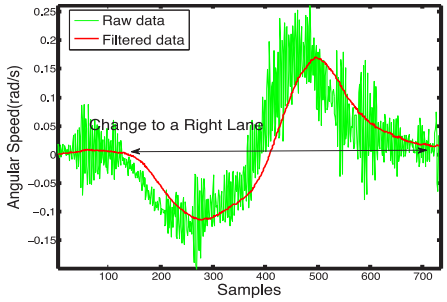
- Gyroscope readings in left & right turns



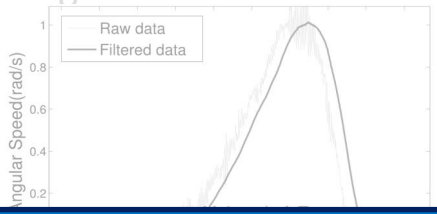

- Lane changes



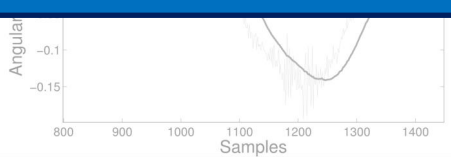

# "Signatures" of Vehicle Steering

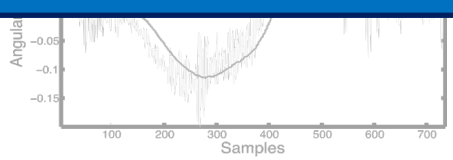
- Left & right turns



**Utilize the signatures in gyroscope readings**

- How to detect these signatures?
- How to differentiate them?

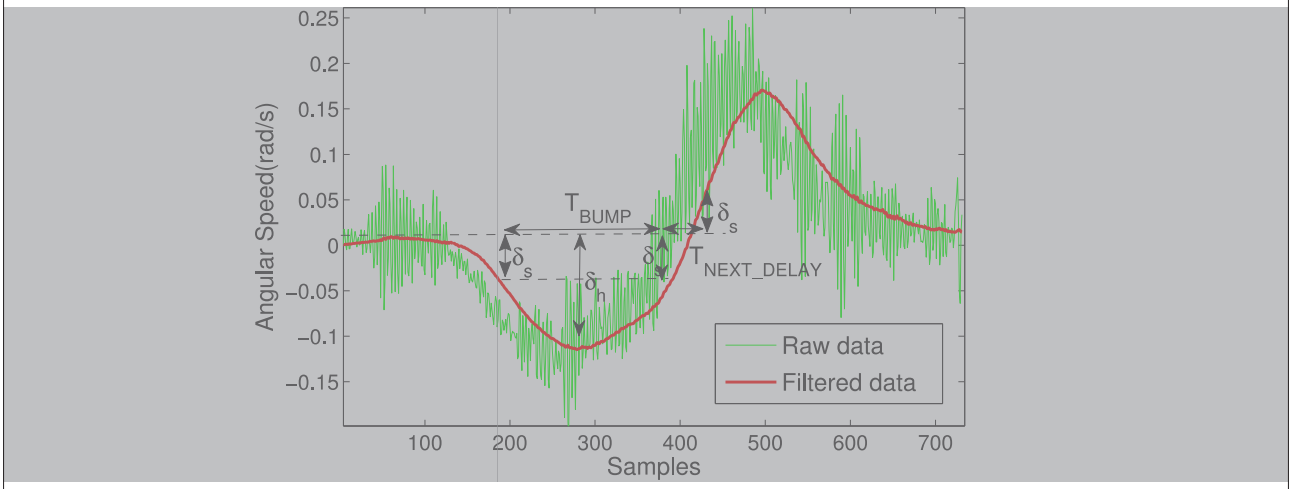


# Bump Detection

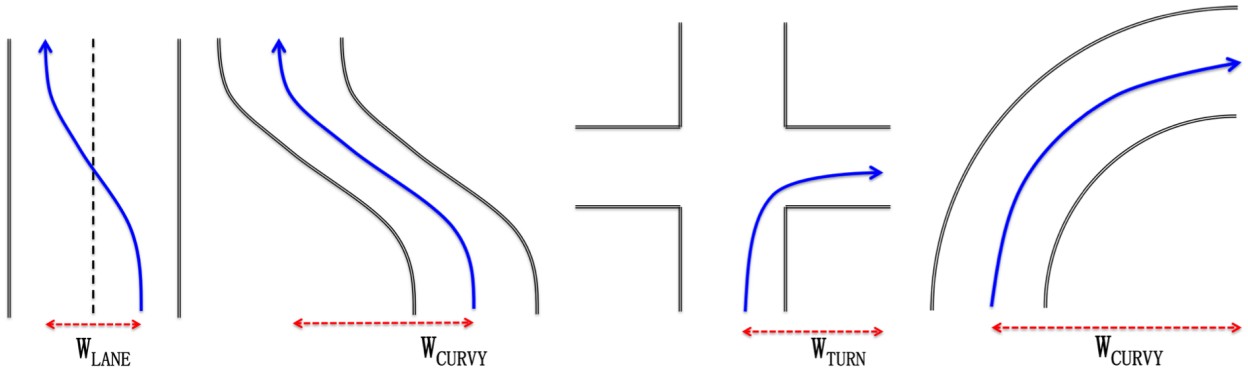
- Three states

No bump → One bump → Wait for another bump




$$\delta_h = 0.07 \qquad T_{BUMP} = 1.5 \text{ seconds}$$
$$\delta_s = 0.05 \qquad T_{NEXT\_DELAY} = 3 \text{ seconds}$$

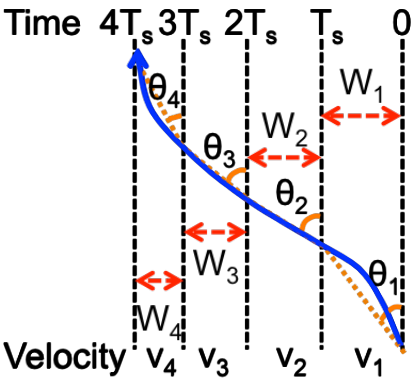
# Horizontal Displacement




(a) Lane change (b) A S-shaped curvy road (c) Turning (d) A L-shaped curvy road

Integrate horizontal displacements over all samples

# Differentiation of Maneuvers




Calculation of horizontal displacement

$$\theta_n = \theta_{n-1} + Y_{avg}T_s \approx \theta_{n-1} + Y_nT_s,$$

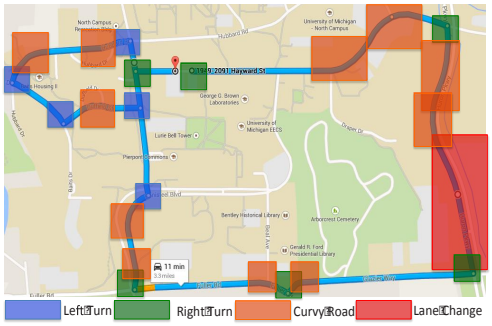
$$W_n = v_nT_s sin(\theta_n).$$

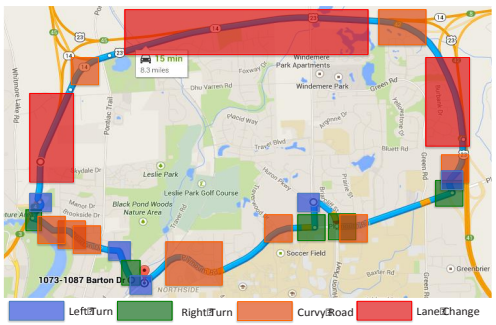
$$W_{final} = \sum_{n=1}^{N} W_n = \sum_{n=1}^{N} v_nT_s sin(\theta_n) = \sum_{n=1}^{N} v_nT_s sin(\sum_{k=1}^{n} Y_kT_s)$$

# Evaluation

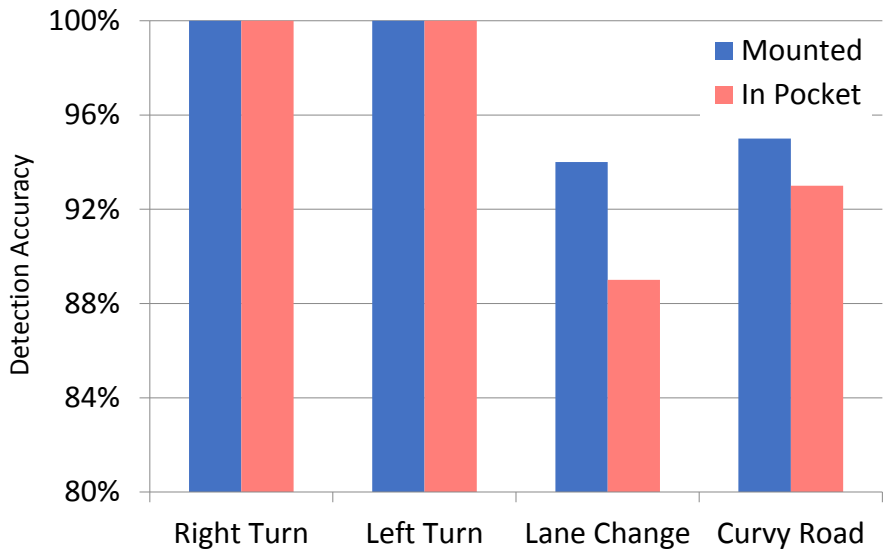
- Implemented V-Sense on Samsung Galaxy S4 and S3
- Test Environments
  - On both local road and freeway
- More than 40 hours on-road test

| # of mobile devices | 2 models of Android phones |
|---|---|
| # of cars | 2 |
| # of participant drivers | 9M, 3F |



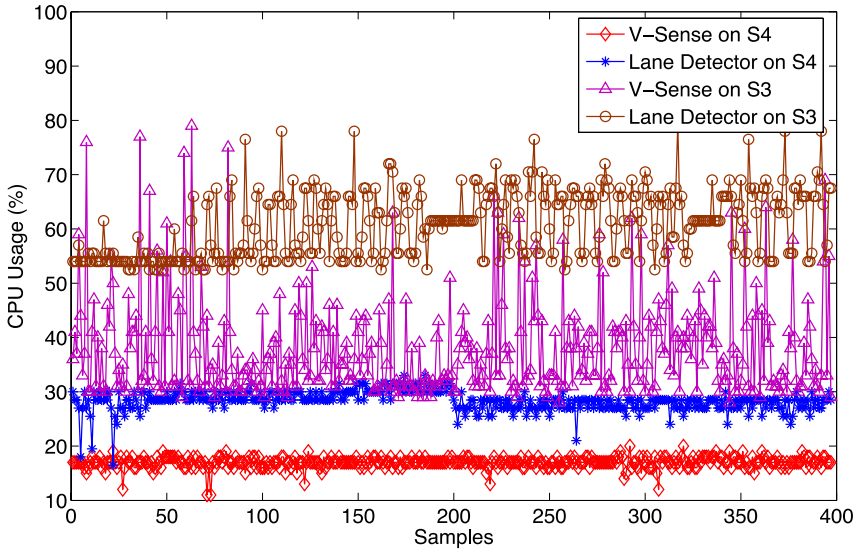



# Evaluations: Accuracy

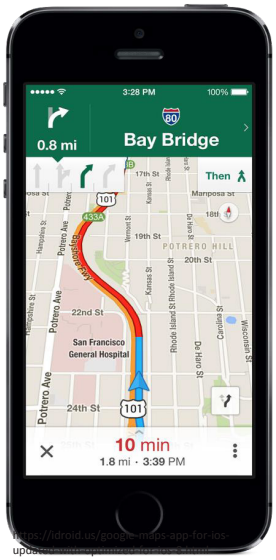



V-Sense can achieve high detection accuracy in various smartphone posture

# Evaluation: CPU Usage

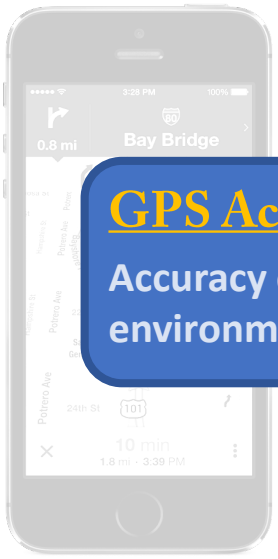


# Application: Fine-grained Lane Guidance



http://365stagandhenweekends.co.uk/blog/

# Application: Fine-grained Lane Guidance

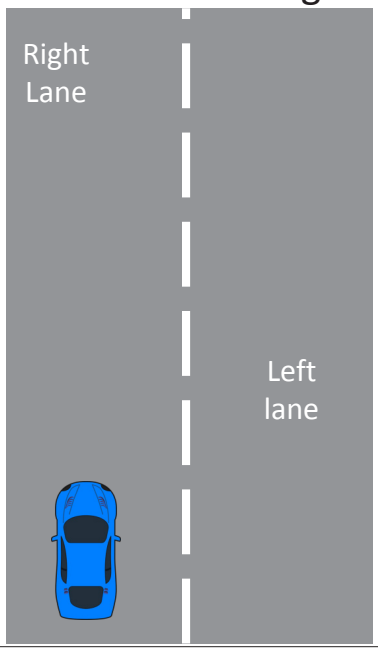


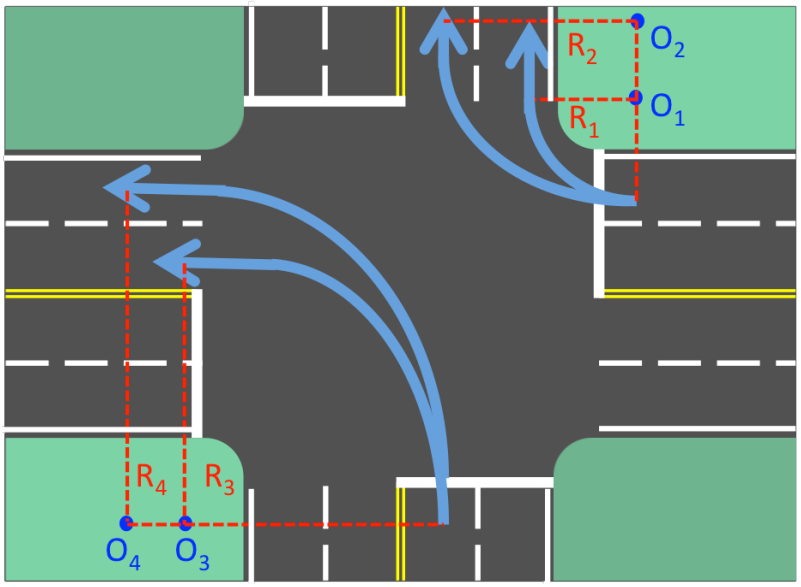
**GPS Accuracy**

**Accuracy of GPS is unstable and varies a lot with environment**

# Application: Fine-grained Lane Guidance

- Lane tracking on straight road
- Lane tracking at intersection



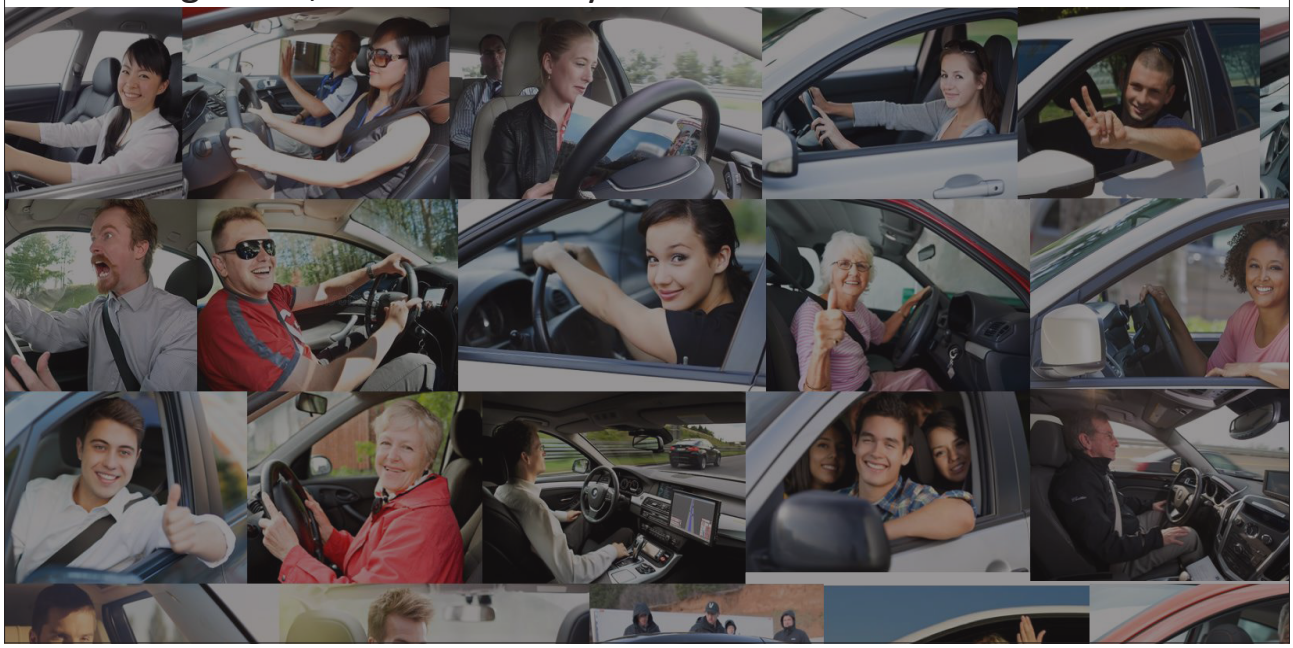




# Summary of V-Sense

- V-Sense
  - An reliable, accurate and easy accessible system for detecting steering maneuvers
  - Capable of recognizing various maneuvers: left/right lane change, left/right turning, U-turn, driving on curvy road, and abrupt acceleration/brake
- Proof-of-concept application
  - Fin-grained Lane Guidance

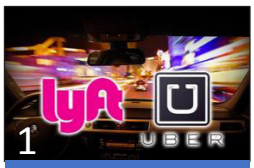
## Everyone Drives Differently

- Different drivers maneuver their vehicles differently
- In general, driver's identity shouldn't be disclosed



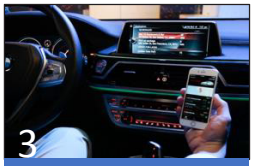
# Driver Fingerprinting

- Smart driving assistance system

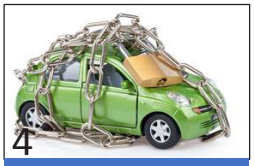



Identify driver for ride-hailing services

Verifies insuree's identity




Adjusts vehicle settings for different drivers




Warns possible vehicle theft

- Fingerprinting drivers using in-vehicle data
  - Limitations
    - installation of an OBD-II dongle
    - reverse engineering of CAN data to understand its meaning
  - Poor accuracy due to various car models and road conditions

# Challenges of Sensing via Mobile IMU

- Limited amount of data to use
  - Limited # of data types, c.f., OBD-II dongle has > 36 data types
  - Small amount

Can gyroscope and accelerometer still capture driving behaviors?

- Difficult to derive useful features
  - IMU data stream is noisy due to hardware limitation/imperfection

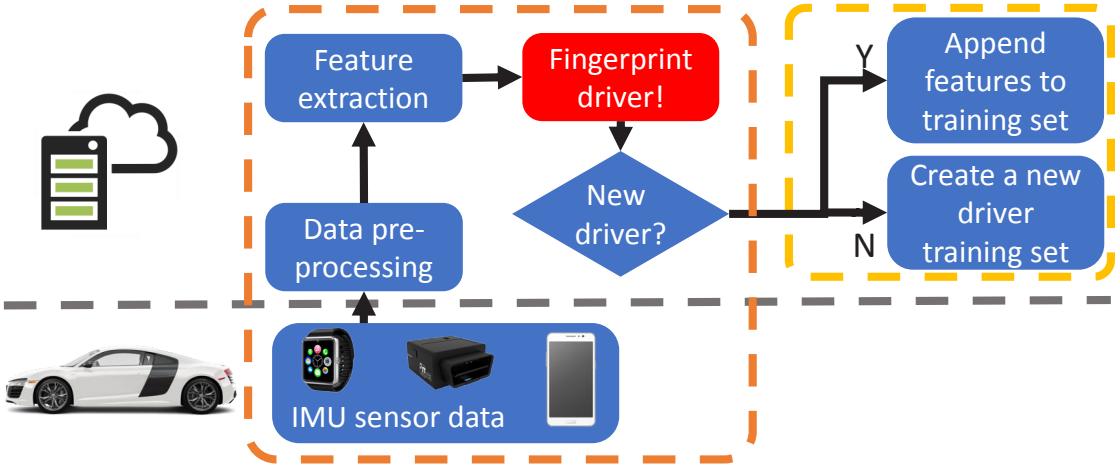
# Our Solution: Driver-Fingerprinting (Dri-Fi)

**Dri-Fi**

- Only requires IMU sensor data
  - Ease-to-access IMU sensors (gyroscope, accelerometer)
  - Available on most mobile & wearable devices
- Fast & accurate driver fingerprinting
  - Exploits feature vector only related to driving style

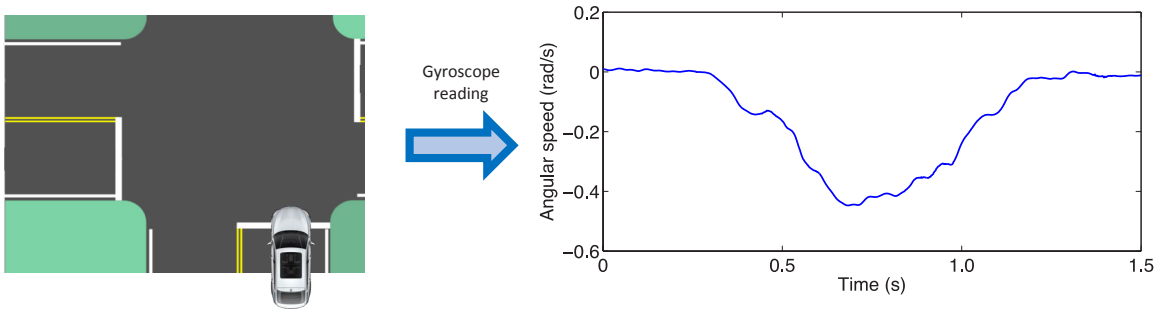
27

# System Overview




28

# Scrutinizing Left/Right Turns

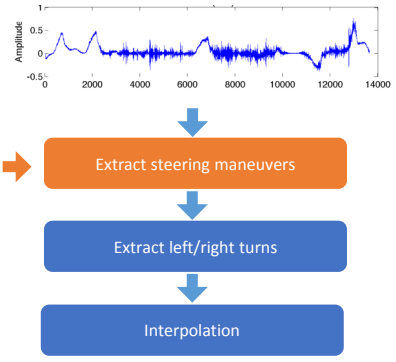


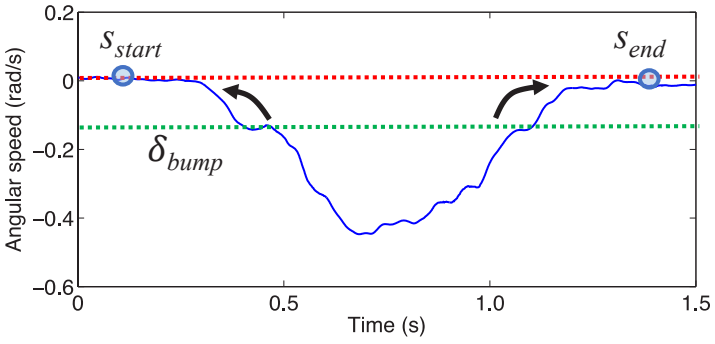

- Driver's left/right turns contain unique driving-style information
- Turns can be captured from *gyroscope* data



# Data Pre-processing

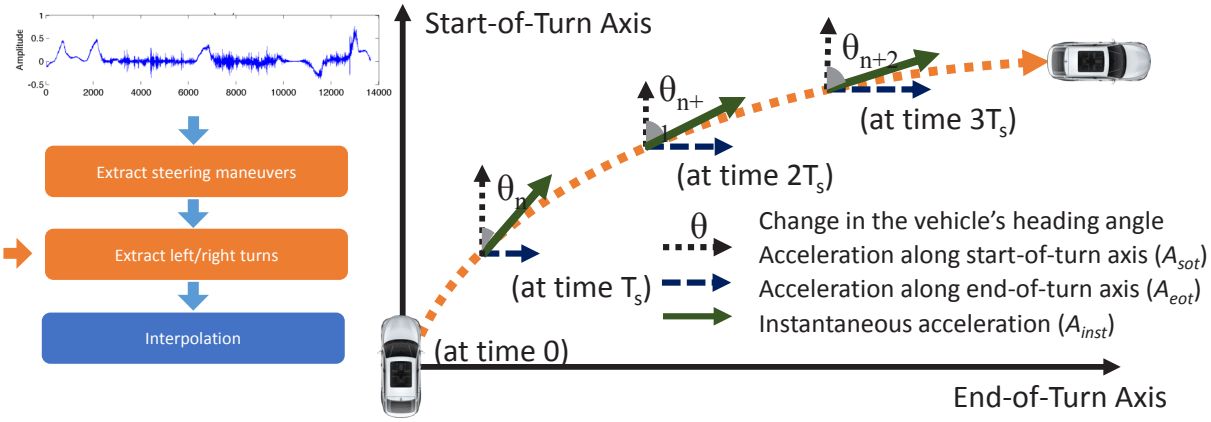
- Extract steering maneuver via *bump* detection [V-Sense]



# Data Pre-processing

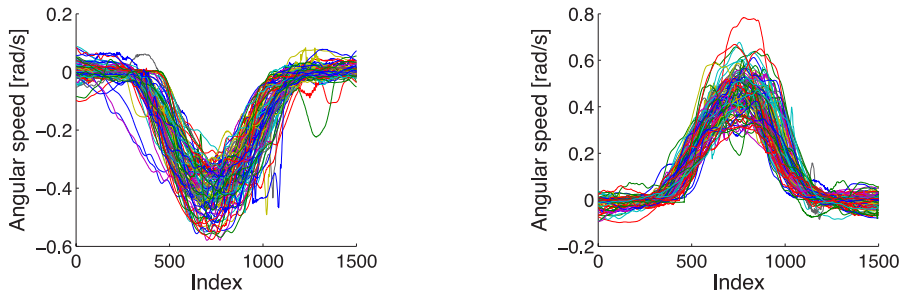
- Retain only left/right turn maneuvers
  - Filter out other steering maneuvers (U-turn, etc.) by deriving steering angles






# Data Pre-processing

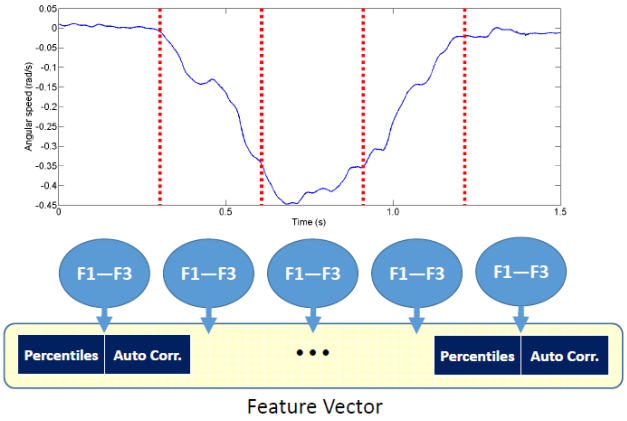
- Interpolation: form route-independent data, showing consistent morphology feature




>140 left/right turns by 12 drivers

# Maneuver-based Driver Fingerprinting

- Proposed features for driver fingerprinting:
  - F1: Acceleration along the end-of-turn (eot) axis ($A_{eot}$): *indep of road geometry*
  - F2: Rate of $A_{eot}$: aggressiveness of acceleration
  - F3: Rate of yaw rate: aggressiveness of turning steering wheel
- Construct feature vector:
  - Percentiles and autocorrelations of F1—F3 in each stage of turns




33

# Maneuver-based Driver Fingerprinting

Use the constructed Feature Vector as inputs to classifiers (e.g., naïve Bayes, Random Forest, SVM)

**Maneuver-based fingerprinting:**
Dri-Fi can fingerprint the driver within a SINGLE left/right turn

34

# Trip-based Driver Fingerprinting

- Use naïve Bayes classifier to enhance the accuracy with more turns
  - $N$ different drivers, $D_1, \ldots, D_N$
  - Each driver makes $n$ different turns, $T_1, \ldots, T_n$
- With more turns, Dri-Fi can estimate the maximum posterior probability (MAP) and predict the driver to be $D_{pref}$:

$$D_{pref} = arg \max_{k \in \{1,\ldots,N\}} p(D_k) \prod_{i=1}^{n} p(T_i|D_k)$$

With more drivers, Dri-Fi needs more turns to be accurate!

35

# Evaluation Setup

- Data collection over 3 months, obtaining ~20 hours of driving data
- Road tests in:
  - Suburban area with less traffic
  - Metropolitan area with heavy traffic
- Settings

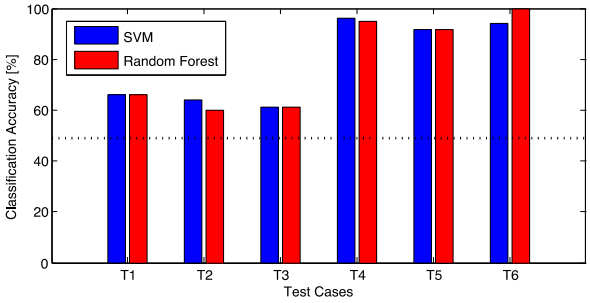
| # of mobile devices | 4 models of Android phones |
|---|---|
| # of cars | 10 |
| # of car models | 7 |
| # of participant drivers | 9M, 3F |

36

# Evaluation: Driver-Dependent Features

- Dri-Fi's feature vector is shown to be independent of routes and cars

| Change | Driver | Car | Route | Acc. |
|---|---|---|---|---|
| T1. Car | = | ≠ | = | Low |
| T2. Route | = | = | ≠ | Low |
| T3. Car, route | = | ≠ | ≠ | Low |
| T4. Driver | ≠ | = | = | High |
| T5. Driver, car | ≠ | ≠ | = | High |
| T6. Driver, route | ≠ | = | ≠ | High |
| T7. Driver, car, route | ≠ | ≠ | ≠ | High |

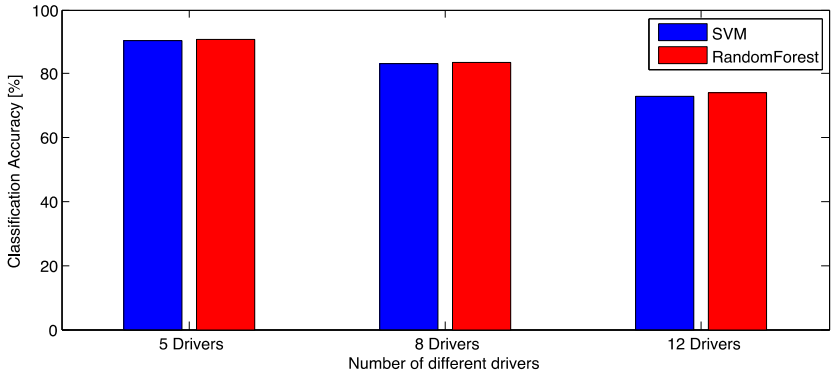



Our feature vector depends only on *driver!*

37

# Evaluation: w/ 2 Machine Learning Algs

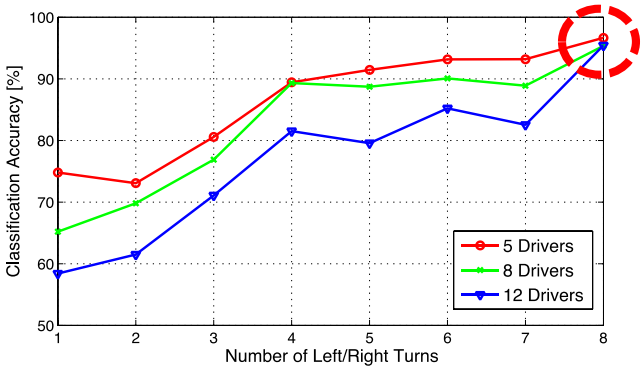
- Dri-Fi's accuracy of single-turn-based approach with different machine learning algorithms




38

# Evaluation: Trip-based Approach

- Dri-Fi's accuracy of trip-based approach (using Naïve Bayes classifier)




Dri-Fi achieves 96.6% accuracy (despite different # of drivers) with up to 8 turns!

39

# Summary of Dri-Fi

**Dri-Fi**

- Only requires IMU sensor data
  - Easy-to-access IMU sensors (gyroscope, accelerometer)
  - Available on most mobile & wearable devices
- Fast & accurate driver fingerprinting
  - Exploits feature vector only related to driving style
  - **90.8%** accuracy with just 1 turn for up to 5 drivers
  - > **96.6%** accuracy with >1 turn

40

# More Apps

- Construction of detailed maps, including potholes, speed bumps, obstacles, etc.
- Usage-based insurance (UBI)
- Ride-hailing services
- Anti-theft
- Adaptive vehicle settings
- Enhancing driving safety

Thank you!
• Q & A

The 24th Network Security Conference -Korea

# IoT SW보안 취약점 자동분석 기술

**이희조** 고려대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2004 ~ 현재 | 고려대학교 정보대학 컴퓨터학과 교수 |
| 2015 ~ 현재 | IoT 소프트웨어보안 국제공동연구센터 센터장 |
| 2017 ~ 현재 | 대통령직속 4차산업혁명위원회 민간위원 |
| 2010 ~ 2011 | 미국 CMU CyLab 방문교수 |
| 2001 ~ 2003 | 안랩 CTO |
| 2000 ~ 2001 | 미국 Purdue CERIAS 박사후연구원 |
| 1989 ~ 2000 | POSTECH 컴퓨터공학과 학사/석사/박사 |

### 강연요약

IoT기기는 우리 생활의 많은 분야에서 이용이 증가되고 있으며, 보안사고가 생명의 위협이 되는 경우가 있어 보안성(security)과 안전성(safety)이 보장되어야 하는 특성을 지니게 된다. 본 튜토리얼에서는 개발단계 또는 도입단계에서 활용할 수 있는 보안 취약점 자동분석 기술을 소개한다.

– 오픈소스의 CVE취약점을 탐지하는 정적분석기술
– 잠재적 취약점 검증을 위한 자동 설정 콘콜릭테스팅기술
– WiFi, Bluetooth등 네트워크 프로토콜 퍼징기술
– SSL/TLS 취약점 자동 점검 기술

특히, 미국, 영국, 스위스와 국제공동연구를 통해 개발중인 IoTcube의 데모 및 실습을 통해 관련 기술의 이해를 돕는다. 또한, 오픈소스를 분석한 사례를 통해 최신 버전의 오픈소스도 CVE 취약점을 다수 지니고 있어 보안 취약점 관리 체계가 필요함을 보인다.

# IoT SW보안 취약점 자동분석 기술

고려대학교

이 희 조

2018년 4월 12일 (목)

## [발표자] 이희조 교수

- **2017~현재 4차산업혁명위원회(대통령직속) 민간위원**
- 2007~현재 대검찰청 디지털포렌식 자문위원
- 2007~현재 Journal of Communications and Networks 편집위원
- 2006~현재 국가 Cyber Security 정책 자문위원
  (필리핀, 우즈베키스탄, 베트남, 미얀마, 코스타리카, 캄보디아 등)
- 2004~현재 한국인터넷진흥원(KISA) 자문위원

- **2015~현재 IoT 소프트웨어보안 국제공동연구센터 센터장**
- **2004~현재 고려대학교 정보대학 컴퓨터학과 교수**
- 2010~2011 미국 카네기멜론 대학 CyLab 방문교수
- 2001~2003 안랩 최고기술책임자 (CTO)
- 2000~2001 미국 Purdue University CERIAS 박사후연구원
- 1989~2000 POSTECH 컴퓨터공학과 학사/석사/박사

- **2016년 ISC² ISLA Award 아시아태평양 정보보안 최고상 (Community Service Star)**
- 2016년 행정자치부 장관 표창 (국립과학수사연구원 협력 공로)

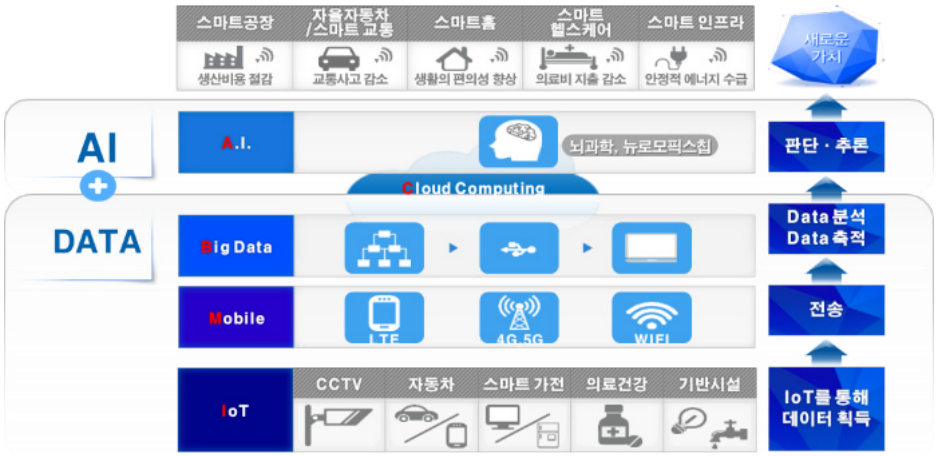
# 목차

- 개요
- 취약점 자동분석 기술
  1. 오픈 소스 CVE 취약점 탐지 기술
  2. 코드 유사도 분석 기술
  3. 잠재 취약점 검증을 위한 자동 설정 콘콜릭테스팅 기술
  4. 무선 네트워크 프로토콜 구현 오류 자동탐지 기술
  5. SSL/TLS 취약점 자동 점검 기술
- IoTcube 실습
- 활용 사례 및 향후 계획
- 맺음말
- Q & A



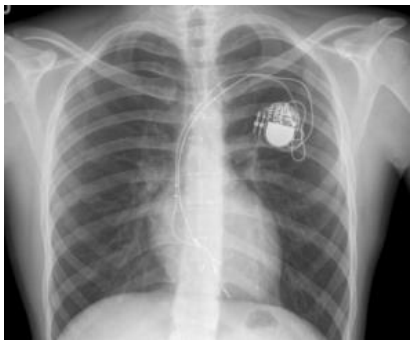
# 4차 산업혁명 핵심 기술

- **데이터 활용 기술**
  - 4차 산업의 동인은 "데이터 확보와 활용" – ***데이터를 가치로 변환 하기***
  - 가상공간 데이터(구글, 아마존)와 현실공간 데이터(건강, 교통, 공장 등)
- **인공지능 기술**
  - 인간의 고차원적 정보처리 활용(인지·학습·추론) 구현



# IoT시대 보안 패러다임

- **IoT security = Cybersecurity + CPS security**
  - 사이버 물리 시스템 (CPS)은 센서와 작동장치가 네트워크로 연결되어 시스템을 원격 제어 가능 하도록 함 (사이버+물리적 특성)
  - 보안 (security)외에도 안전 (safety) 요구사항이 추가됨
- **보안과 안전의 상호 연관성 정의 (Boehm'78)**
  - 보안(security) 이란? the world must not harm the system
  - 안전(safety) 이란? the system must not harm the world



Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

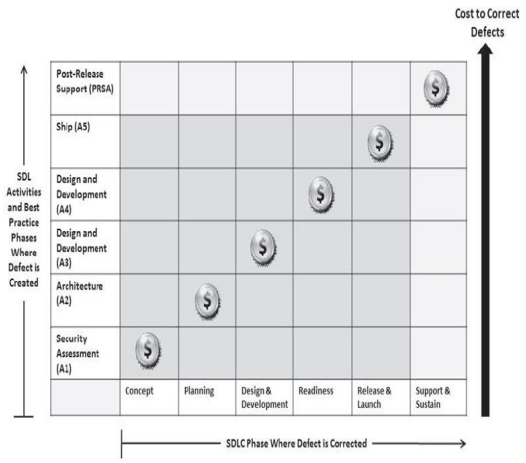
FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

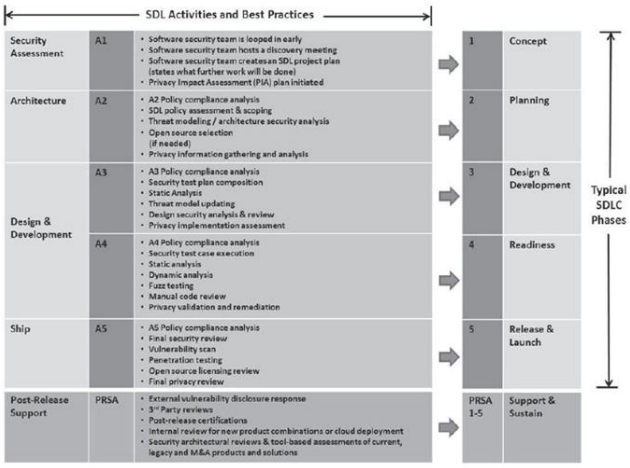
# 4차 산업혁명과 보안기술의 역할 제고

- **보안 = 정보사회의 주춧돌**
  - **보안은 4차 산업혁명에 있어 가장 중요한 기반**
  - **아무리 편리한 도구도 보안이 담보되지 않으면 흉기**
  - **4차 산업혁명의 결과물을 안전하게 향유할 수 있으려면 보안이 필수**

# 개발단계의 보안 내재화

- Security development lifecycle (SDL)
  - Microsoft, OWASP, Cisco 그리고..
  - 사람과 도구 (SW security team, static/dynamic analysis, fuzzing tools)






# SW보안 국제공동연구센터(CSSA) 설립

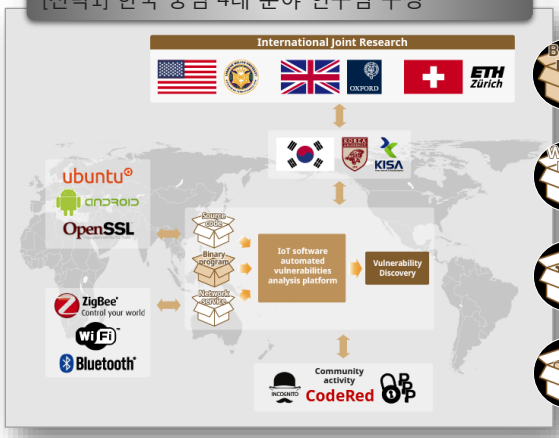
- **CSSA (Center for Software Security and Assurance)**
  - 동시 4개국 화상회의 등 국제 연구, IoTcube 개발 중심
  - 서울 고려대학교 자연계 캠퍼스내 설립 (2015년 6월)

- **기술 교류 및 세미나**
  - 공동연구 정기 워크숍 및 자문회의
  - SW보안 아이디어 공모전 및 IoT Security 컨퍼런스 개최
  - 해외 정부 관계자 기술 교육 (모로코, 캄보디아, 아제르바이잔)
  - 기술 세미나 (워싱턴大, UC Berkeley, Ford, RedHat, THEORI社 등)

# SW보안 국제공동연구 추진 개요

※ 세계 TOP 10 대학中 3개 참여

## [전략1] 한국 중심 4대 분야 연구팀 구성




## [전략2] 글로벌 리딩* 그룹과 IoTcube 공동 개발

美 카네기멜론대학교 David Brumley 교수
세계 최고 SW 취약점 자동분석 기술 보유

英 옥스퍼드대학교 Sam Staton 교수
세계 최고 시스템 SW 오류 자동검증 기술 보유

스위스 취리히연방공과대 Adrian Perrig 교수
세계 최고 네트워크 프로토콜 보안 기술 보유

한국 인터넷진흥원(KISA) 김환국 팀장
국가 취약점 DB 활용 및 검증 기술 보유

고려대학교 정보대학 이희조 교수
보안 취약점 탐지 및 검증 기술 보유

고려대학교 정보대학 오학주 교수
정적 분석 및 기호실행 분야 전문가

고려대학교 정보대학 허준범 교수
무선 네트워크 보안 표준 전문가

고려대학교 정보대학 김정현 교수
정보 가시화 및 UI/UX 처리기술 보유

## [전략3] 보안 실무 전문가 그룹 연계

- 보안 취약점 분석 실무 전문가 그룹 참여
  - ✓ 세계최고 해킹팀 CMU PPP, 국내 해킹그룹 CodeRed
  - ✓ 국내 12개 대학 정보보호 동아리 연합 인코그니토(Inc0gnito)
- R&D 자문위원단 운영
  - ✓ ETRI, 포항공대, 충남대, CONCERT, 김앤장, 스틸리언, 아이넷캅 등



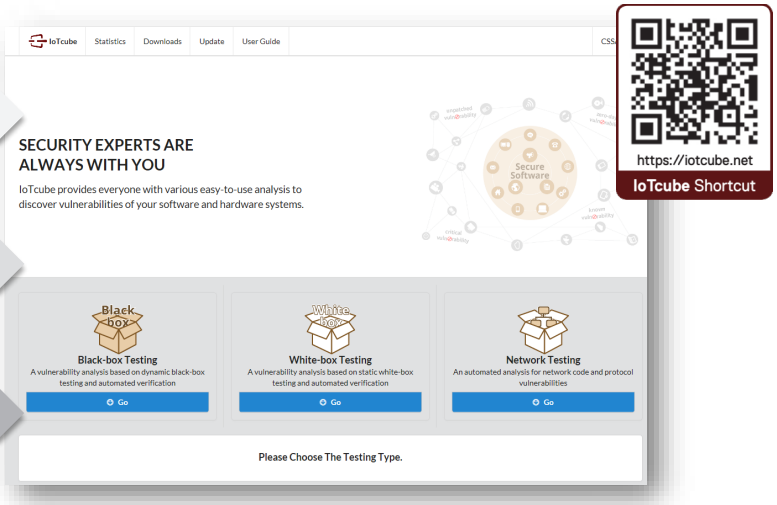
# 보안 취약점 자동분석 플랫폼

(https://iotcube.net)

**Automation**
Finding known and unknown vulnerabilities automatically

**Easy-to-use**
Easily operated even by non-security experts

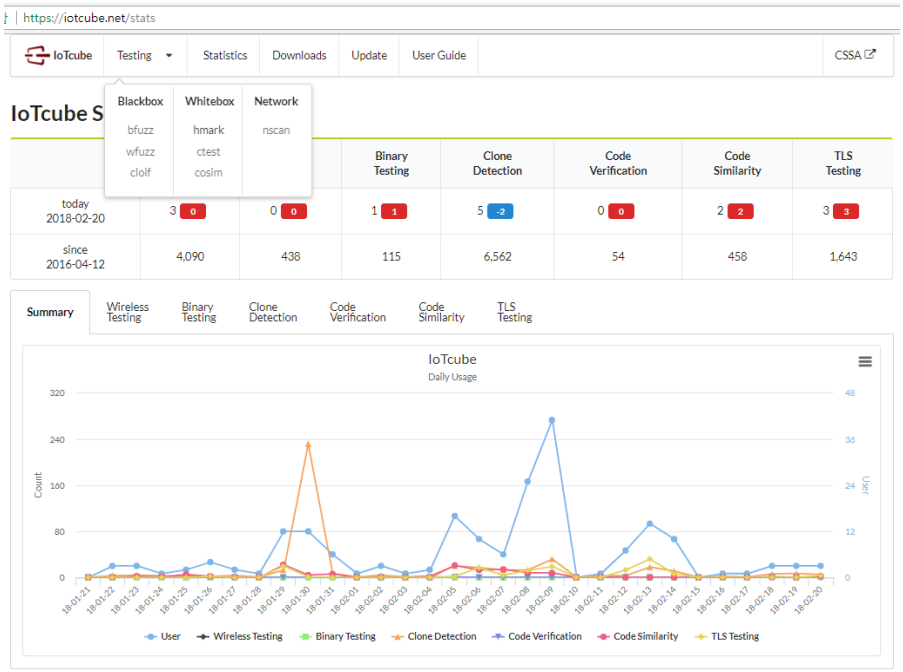
**Scalability**
Applicable scalability to OSS




- 2016년 4월 서비스 공개 이후 4,000명 이상 사용 (2018년 2월 현재)
  - 100여종의 디바이스로 부터 500여개 Unique Crash 패킷 확보
  - 200억 라인의 소스코드로부터 취약한 복제코드(VCC) 30만 여개 검출
- 2017년 2월 1차 컨퍼런스 이후 추가된 기능
  - 2017년 4월, 화이트박스테스팅 ctest 모듈 추가 (취약코드 검증기능)
  - 2017년 8월, 화이트박스테스팅 cosim 모듈 추가 (유사 취약점)

# 7개의 자동 분석 기능 제공

- 블랙박스 (3), 화이트박스 (3), 네트워크 (1) 테스팅 도구로 구성






# 오픈 소스 CVE 취약점 탐지 기술 (HMARK)

- Seulbae Kim, Seunghoon Woo, Heejo Lee, Hakjoo Oh, "VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery", IEEE Symposium on Security and Privacy, May 22 2017.
- Seulbae Kim, Heejo Lee, "Software systems at risk: an empirical study of cloned vulnerabilities in practice", Computers & Security, Feb. 27 2018.

# 코드 클론?

- 정의
  - 복제된 코드 (Ctrl + C, Ctrl + V)
  - 복제 후 약간 수정된 코드도 포함

- Example
  - 오픈 소스 라이브러리를 사용한 프로그램
  - 리눅스 커널을 기반으로 만든 운영체제
  - 이전에 개발한 소스 코드를 재활용

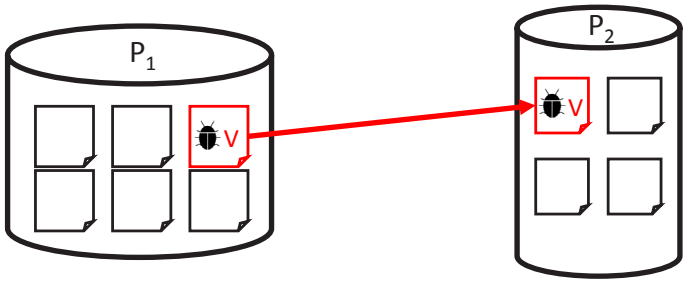


# 코드 클론?

- 코드 클론의 종류
  - ★Type-1: Exact clone
    - 원본과 클론이 정확히 일치
  - ★Type-2: Renamed clone
    - 클론에서 자료형, 변수명, 식별자, 주석, 탭/스페이스 등이 바뀔 수 있음
  - Type-3: Restructured clone
    - 클론에 구조적 변형(문장의 삽입/삭제/재배치 등)이 가해짐
  - Type-4: Semantic clone
    - 원본과 클론이 기능적으로 동일하나 다른 구문(syntax)을 가짐

# 코드 클론을 활용한 취약점 탐지

- 원리
  - 프로그램 P1 내부에 **취약 코드 V**가 존재할 때,
  - 프로그램 P2 에도 같은 코드 **V**가 존재한다면
  - 프로그램 P2 역시 취약할 확률이 매우 높음

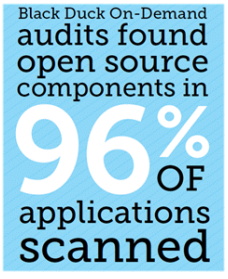




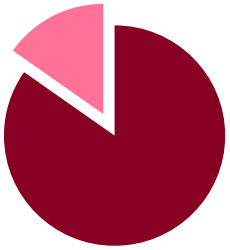

# 취약 코드 클론 탐지의 필요성

- 오픈 소스 소프트웨어의 증가에 따른 코드 클론의 자연스러운 증가
  - Black Duck Openhub에 등록된 소프트웨어의 **96%**는 하나 이상의 오픈 소스를 사용 중

    **(2017 Open source security & Risk analysis, Blackduck Software)**



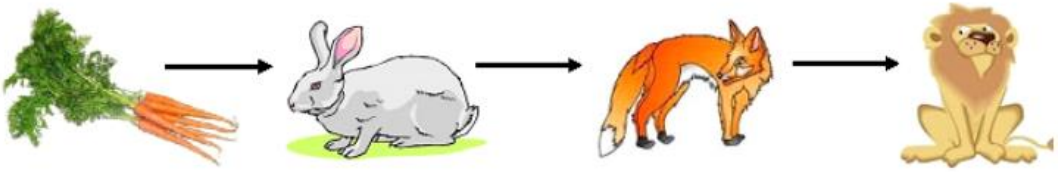

  - 2,600개 오픈 소스 프로젝트 중 **2,202개**에서 코드 클론 발견
    - 2000 Top-rated C/C++ projects from GitHub
    - 600 most popular C/C++ projects from SourceForge



**84.7 %** 프로젝트에 코드 클론 존재

# 취약 코드 클론 탐지의 필요성

- 오픈 소스 소프트웨어의 증가에 따른 코드 클론의 자연스러운 증가
  - 신뢰도 높은 코드의 사용
  - 개발 시간 단축
  - 비용 절감

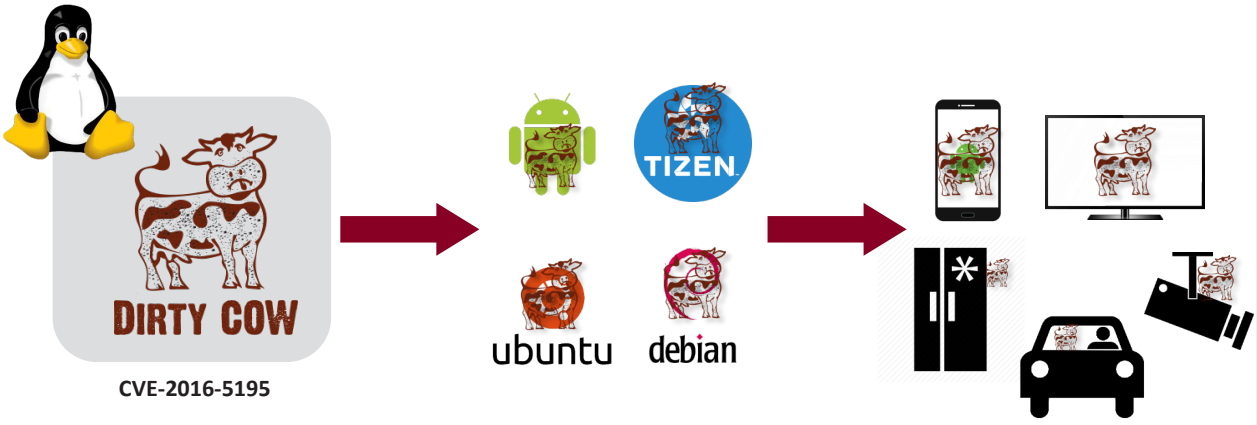


라이브러리 | 소/대규모 소프트웨어 (e.g., 리눅스 커널) | 운영체제 | IoT 디바이스



# 취약 코드 클론 탐지의 필요성

- 취약 코드가 확산되기에 매우 적합한 오픈 소스 생태계!

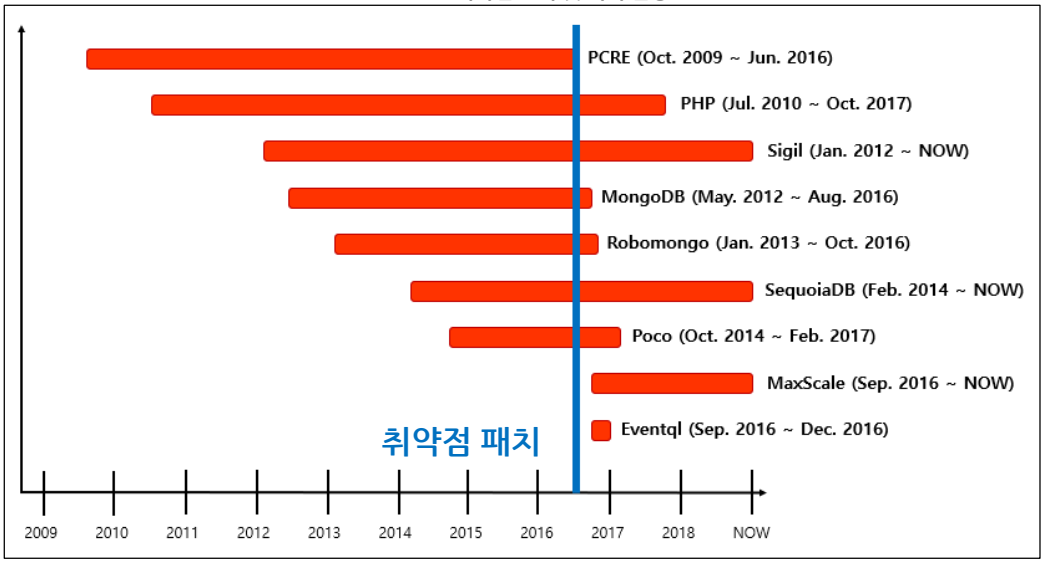



CVE-2016-5195

# 취약 코드 클론 탐지의 필요성

- 일반적으로 취약점이 발견된 소프트웨어 내에서 오랜 기간동안 존재하고, 심지어 패치가 이루어지더라도 여전히 다른 소프트웨어에 남아있는 경우가 많음

<오픈소스 취약점 전파 및 패치 현황>






# 코드 클론을 활용한 취약점 탐지

- Q) 어떻게 빠르고 정확하게 취약 코드 클론을 찾을까?
  - Growing size of software
    - Linux kernel – 15 Million Lines of Code (LoC)
  - Everyone hates false alarm
    - Tool X – 2,000개 취약 코드클론 탐지 BUT 1,800개**(90%)**가 false alarm
- A) Solution: **VUDDY**
  - Scalable and accurate **VU**lnerable co**D**e clone **D**iscover**Y**
  - 함수 단위로 클론 탐지
  - 함수의 바디 길이와 해시로 fingerprinting
  - 정규화 & 추상화 적용하여 Type-2 clone 탐지

# VUDDY

- Preprocessing

```
void avg (float arr[], int len) {
  static float sum = 0;
  unsigned int i; // counter
  for (i = 0; i < len; i++)
    sum += arr[i];
  printf("%f %d", sum/len, check(sum));
}
```

↓ 추상화

```
void avg (float arr[], int len) {
  DTYPE LVAR = 0;
  unsigned DTYPE LVAR; //counter
  for (LVAR = 0; LVAR < FPARAM; LVAR ++)
    LVAR += FPARAM[LVAR];
  FUNCCALL("%f %d", LVAR/FPARAM, FUNCCALL(LVAR));
}
```

↓ 정규화

```
DTYPELVAR=0;unsignedDTYPELVAR;for(LVAR=0;LVAR<FPARAM;LVAR++)LVAR+=FPARAM[LVAR];FUNCCALL("%f%d",LVAR/FPARAM,FUNCCALL(LVAR));
```

↓ 길이, 해시 계산

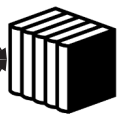
```
length: 123
hash   : 589612034a29029f95b35957212d00b3
```



# VUDDY

- Length-indexed dictionary

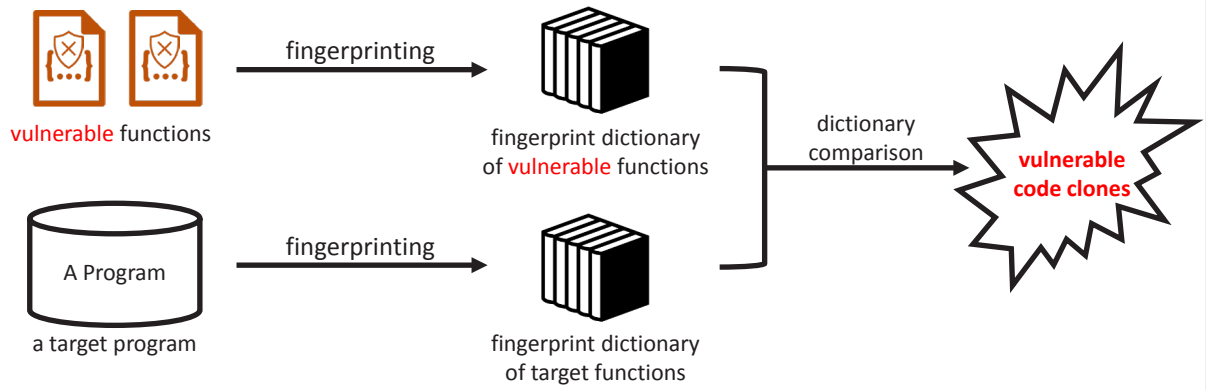
```
length: 123
hash   : 589612034a29029f95b35957212d00b3

length: 38
hash   : 9a45e4a15c928699afe867e97fe839d0

length: 42
hash   : d6e77882a5c55c67f45f5fd84e1d616b

length: 123
hash   : c94d99100e084297ddbf383830f655d1
```



```
38: {
   9a45e4a15c928699afe867e97fe839d0
}

42: {
   d6e77882a5c55c67f45f5fd84e1d616b
}
123: {
   589612034a29029f95b35957212d00b3,
   c94d99100e084297ddbf383830f655d1
}
```

# VUDDY & IoTcube

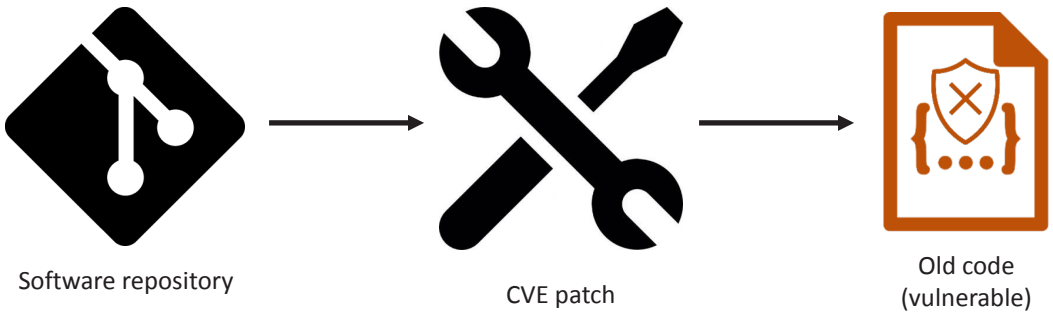
- System overview





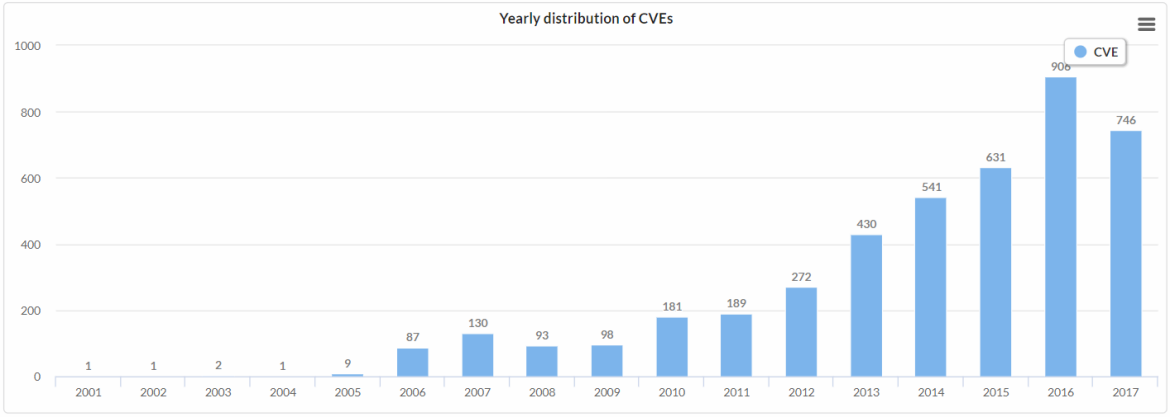

# 취약 함수 수집 과정

- 취약점 패치 정보를 이용하여 취약 함수 복원



# 취약 함수 수집 과정

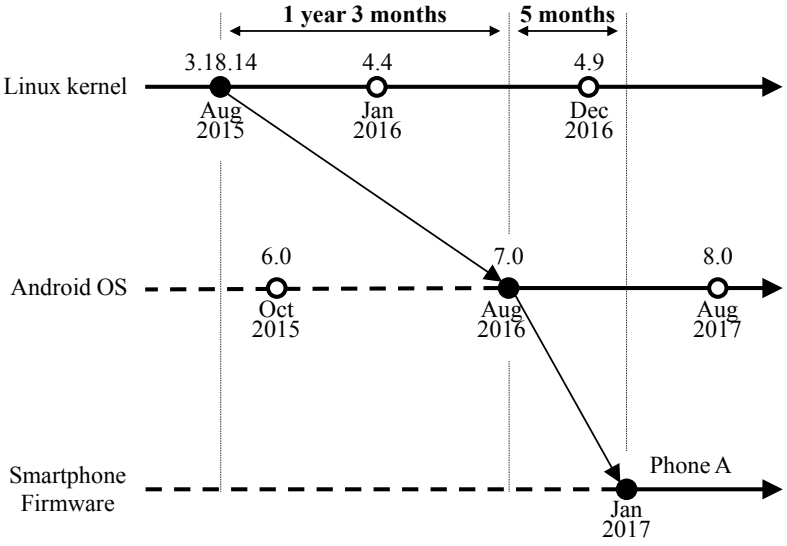
- 자동화된 솔루션을 통해 일괄 수집
  - 2018년 1월 20일 기준 (매 분기 정기 업데이트)
    - 39개 오픈 소스 REPO
    - 4,319개 CVE 패치
    - 13,553개 취약 함수





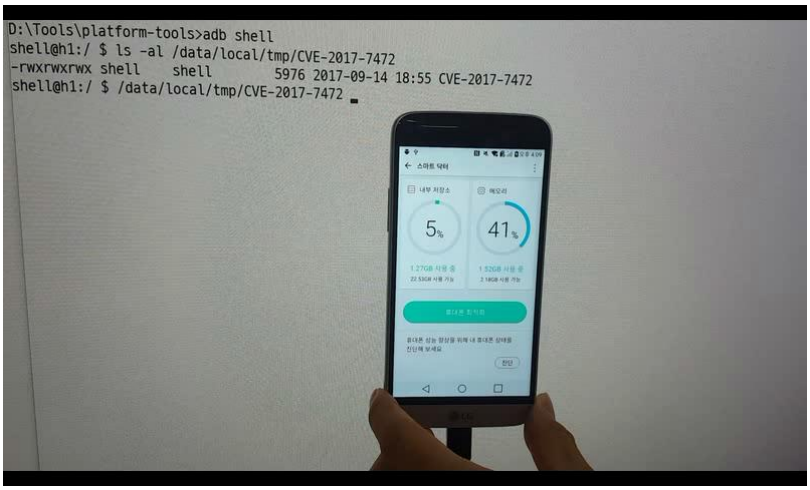

# 코드 클론 취약점 사례 (1)

- 코드 클론과 패치 지연으로 인한 attack surface
  - 리눅스 커널 취약점이 **1년 8개월** 뒤에 출시되는 스마트폰에서 발견됨



# 코드 클론 취약점 사례 (1)

- CVE-2017-7472 Exploit DEMO video
  - A memory vulnerability in Linux kernel before 4.10.13
  - PoC available at https://www.exploit-db.com/exploits/42136/






# 코드 클론 취약점 사례 (2)

- Zero-day in Apache HTTPD 2.4.23
  - Clone chain: Expat library → Apache Portable Runtime (APR) → Apache HTTPD
    - vulnerable to CVE-2012-0876
  - Hash DoS attack triggered by sending a crafted packet!

```
// Vulnerable function in httpd/srclib/apr-
util/xml/expat/lib/xmlparse.c
for (i = 0; i < table->size; i++){
  if (table->v[i]) {
    unsigned long newHash = hash(table->v[i]->name);
    size_t j = newHash & newMask;
    step = 0;
```

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4730 | daemon | 20 | 0 | 435504 | 8968 | 2952 | S | 100.1 | 0.2 | 0:04.92 | httpd |
| 634 | root | 20 | 0 | 191960 | 10648 | 9444 | S | 0.3 | 0.3 | 0:02.54 | vmtoolsd |
| 1442 | unused | 20 | 0 | 1571620 | 114444 | 68224 | S | 0.3 | 2.8 | 0:26.20 | compiz |
| 1 | root | 20 | 0 | 119676 | 5800 | 3944 | S | 0.0 | 0.1 | 0:01.86 | systemd |
| 2 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.01 | kthreadd |
| 3 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.03 | ksoftirqd/0 |
| 5 | root | 0 | -20 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kworker/0:0H |

# 코드 클론 취약점 사례 (3)

- 최신 리눅스 커널(4.11.1)에서 발견된 신규 취약점

**Original patch for CVE-2008-3528 targeting ext2 file system**

```
1   struct ext2_dir_entry_2 * ext2_dotdot (struct inode *dir, struct page **p)
2   {
3 -   struct page *page = ext2_get_page(dir, 0);
4 +   struct page *page = ext2_get_page(dir, 0, 0);
5     ext2_dirent *de = NULL;
6
7     if (!IS_ERR(page)) {
```

Could trigger "printk flood" & DoS in CentOS 7, and Ubuntu 14.04

**Patched function in ext2 file system**

```
1  struct ext2_dir_entry *ext2_dotdot (struct
                  inode * dir, struct page **p)
2  {
3    struct page *page = ext2_get_page(dir, 0,
0);
4    struct ext2_dir_entry *de = NULL;
5
6    if (!IS_ERR(page)) {
```

ext2 파일 시스템에 적용된 패치

**Vulnerable function in nilfs2 file system**

```
1  struct nilfs_dir_entry *nilfs_dotdot (struct
                  inode * dir, struct page **p)
2  {
3    struct page *page = nilfs_get_page(dir, 0);
4    struct nilfs_dir_entry *de = NULL;
5
6    if (!IS_ERR(page)) {
```

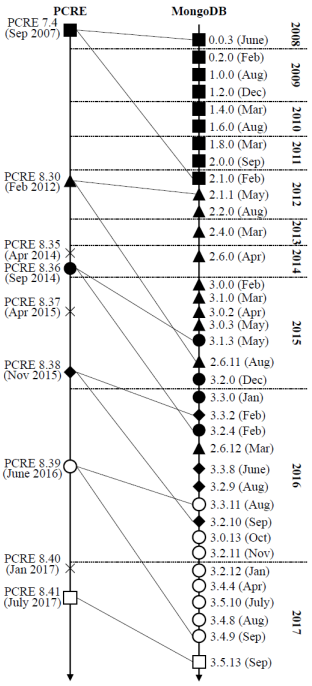
nilfs2 파일 시스템은 패치 되지 않음



# 코드 클론 취약점 사례 (4)

- CVE-2016-3191 in MongoDB
  - A vulnerability in PCRE (before 8.39) that allows an remote code execution via a crafted regular expression
- Patching procedure
  - 16년 2월 PCRE 개발 트리에 패치 적용됨
  - 16년 6월 패치된 PCRE (8.39) 정식 배포
  - 16년 11월 MongoDB 3.2에 PCRE 8.39 적용

취약점 패치가 발견되고 업데이트 되기까지 9개월 소요



# 코드 유사도 분석 기술

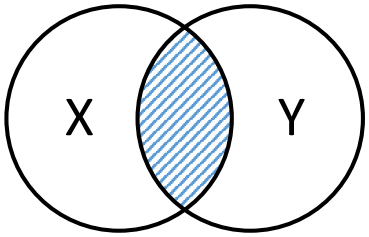
# (COSIM)



## 코드 유사도 분석

- **코드 유사도 분석(COSIM)의 정의**
  - 두 소프트웨어의 소스코드가 얼마나 유사한지를 분석
    - 소프트웨어의 소스코드를 함수단위로 나눈 후, 공통으로 사용하는 함수의 비율을 확인

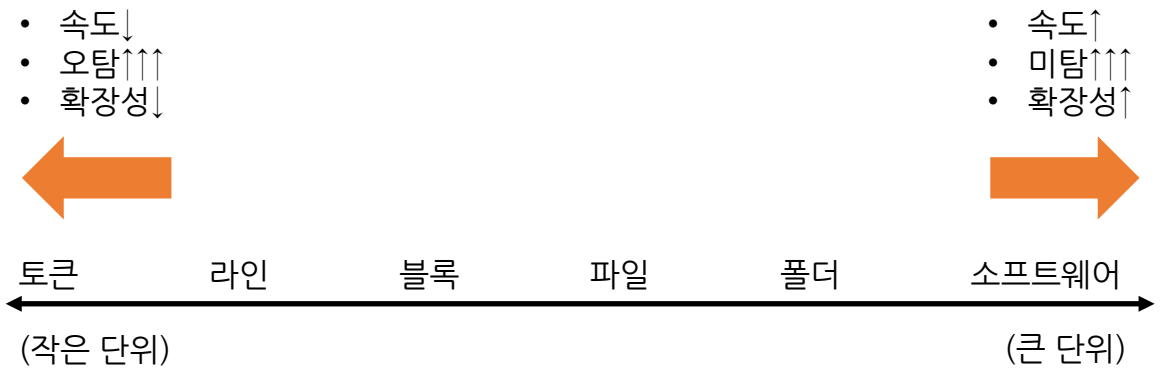
- **소스코드 유사도**
  - 공통적으로 사용하는 함수의 개수를 각 소프트웨어에 존재하는 전체 함수의 개수로 나눈 값




- Y에 대한 **X의 유사도**
  = n(X∩Y) / **n(X)**
- X에 대한 **Y의 유사도**
  = n(Y∩X) / **n(Y)**

# 코드 유사도 분석

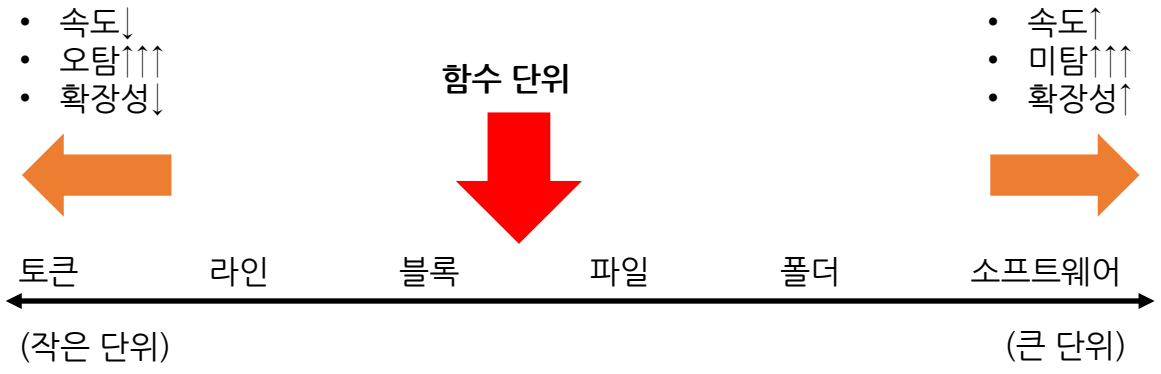
- **함수단위 선정**
  - 한쪽으로 치우친 단위는 장점이 명확한 반면 단점도 뚜렷함
    - 예) 라인 단위는 더 세세한 변화를 보여줄 수 있지만, 오탐이 굉장히 많고 속도 및 확장성이 떨어짐






# 코드 유사도 분석

- **함수단위 선정**
  - 따라서 독립적인 의미를 가지는 중간 단위인 함수로 선정
    - Length-based filtering 을 통한 속도 및 확장성 극대화
    - 오탐이 거의 없고, 일부 미탐 발생가능성 존재
      - File level grouping 을 통해 해결하고자 연구 중



# 코드 유사도 분석

- **예제 1)** 같은 종류의 제품, 다른 제조사
  - **S사 스마트TV** 와 **L사 스마트 TV** (모두 2017년 제조된 모델)
    - 각 회사의 opensource 사이트에 공개된 소스코드
    - S사 스마트 TV 소스코드의 **약 70%,** L사 스마트 TV 소스코드의 **약 37%** 가 서로 일치함

Calculate code similarity of two projects

* Total functions
S_TV : 562481 functions
L_TV : 1088702 functions

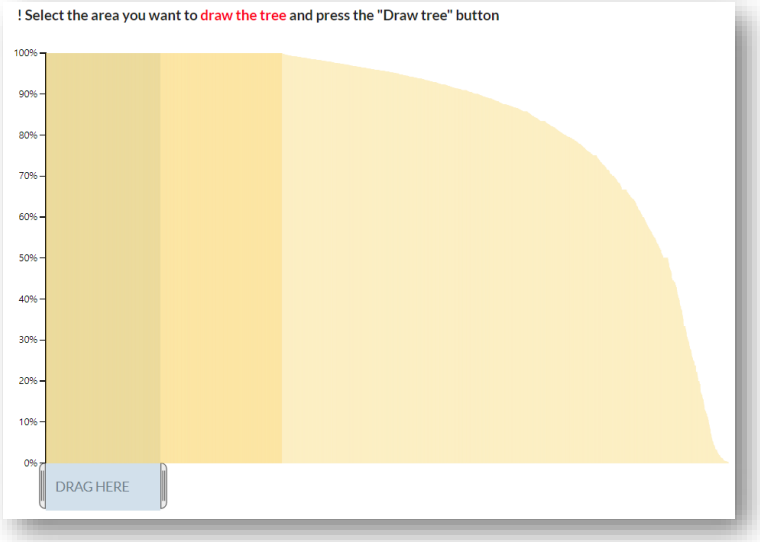
* First project A = S_TV
* Second project B = L_TV

* Similarity of First project
( A ∩ B ) / A = 70.51% (396624 / 562481)
* Similarity of Second project
( B ∩ A ) / B = 37.56% (408963 / 1088702)



# 코드 유사도 분석

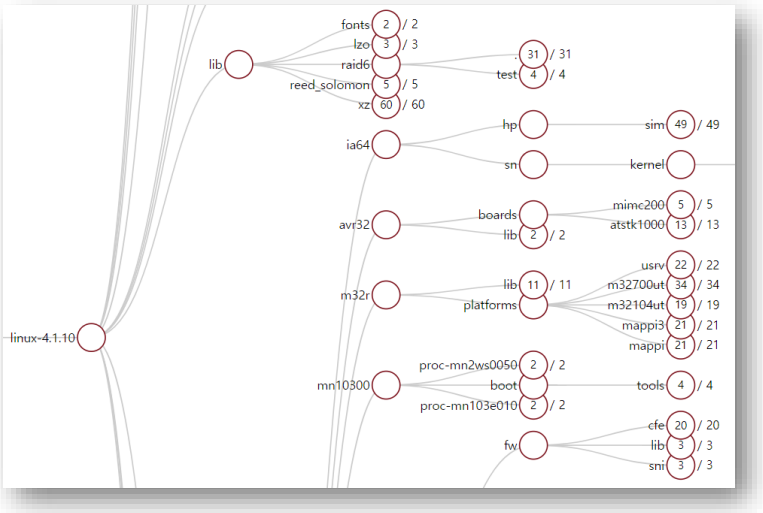
- **예제 1)** 같은 종류의 제품, 다른 제조사




- X축: C/C++ 파일을 **하나 이상 포함하고 있는 디렉토리**
- Y축: (X축 디렉토리 내의) 공통 함수 개수 / 전체 함수 개수

# 코드 유사도 분석

- **예제 1)** 같은 종류의 제품, 다른 제조사




- Linux kernel 에서 많은 부분이 매칭, 기타 공통으로 사용중인 라이브러리에서도 많은 매칭이 발생



# 코드 유사도 분석

- **활용 방안**
  1. 자체적으로 **보유하고 있는 취약점**이 특정 소프트웨어 내에 존재하는지 탐지 가능
     - 자체적으로 보유한 **취약점의 해시 인덱스 파일**과, **검사를 원하는 소프트웨어의 해시 인덱스 파일**을 생성한 후 유사도를 측정
  2. 특정 소프트웨어 내에 **사용중인 오픈소스 소프트웨어**들에 대한 탐지 가능
     - 어떤 오픈소스의 어떤 버전을, 얼마나 사용중인지에 대한 정보
     - **업데이트가 필요한 오픈 소스 라이브러리에 대한 대응** 가능

# 잠재적 취약점 검증을 위한 자동 설정 콘콜릭테스팅기술

# (CTEST)

Computer & Communication Security Lab., Korea University

## 취약점 탐지 및 검증 방법론

### 정적 분석 (Static Analysis)

- 프로그램 실행 없이 프로그램에서 발생할 수 있는 오류를 검출하는 기법
- 비교적 적은 시간이 소요되나, 프로그램 실행 경로와 상태를 추상화하기 때문에 높은 False Positive 발생

### 동적 분석 (Dynamic Analysis)

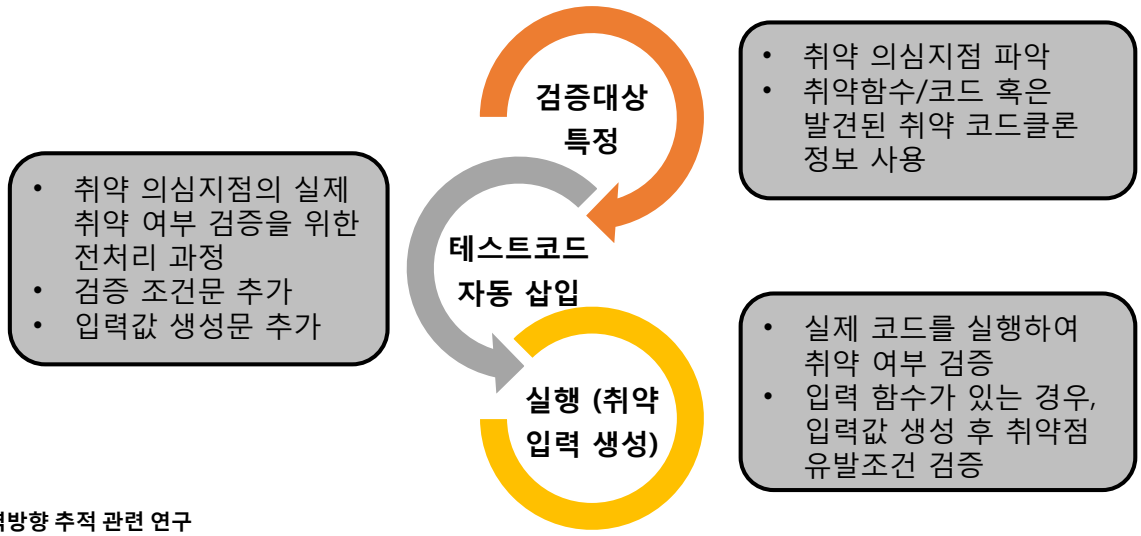
- 다양한 입력값으로 프로그램을 실제 실행해 프로그램 오류를 검출하는 기법
- 검증 대상과 무의미한 분석을 할 수 있어 비교적 많은 시간 소요

### 기호 실행 (Symbolic Execution)

- 동적 분석 시, 프로그램의 다양한 실행 경로를 분석하기 위해 입력값을 기호화된 값으로 변환하여 실행하는 기법
- 자동화된 취약점 검증에 사용되는 콘콜릭테스팅 기술은 기호실행의 일종

# CTest: 자동화된 취약점 검증 도구

- **자동화된 취약점 검증 기법을 위해 필요한 기술**




*** 역방향 추적 관련 연구**

- Hongzhe Li, Hyuckmin Kwon, Jonghoon Kwon, Heejo Lee, "A Scalable Approach for Vulnerability Discovery Based on Security Patches", Applications and Techniques in Information Security (ATIS), pp. 109-122, Nov. 28. 2014. **(Best Paper Award)**
- Hongzhe Li, Jaesang Oh, Hakjoo Oh, Heejo Lee, "Automated Source Code Instrumentation for Verifying Potential Vulnerabilities", IFIP Int'l Conf. on ICT Systems Security and Privacy Protection (IFIP SEC), Vol. 471, pp. 211-226, May. 11. 2016.



# CTest 검증 절차 – 1

## 1. 검증 대상이 되는 취약 의심지점 파악

- 현재는 모든 취약 의심지점에 대해 검증 수행

| 취약 의심지점 (예시) | 취약 의심지점 검증 조건문 (예시) |
|---|---|
| **strcpy(dst,src)** | dst.space > src.strlen |
| **strncpy(dst,src,n)** | (dst.space ≥ n) ^ (n ≥ 0) |
| **strcat(dst,src)** | dst.space > dst.strlen + src.strlen |
| **buf[i] = expr** | buf.space > i |

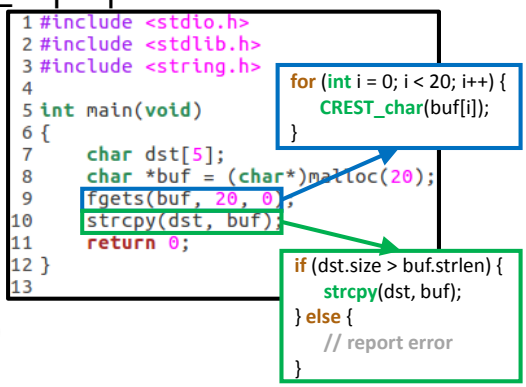
(x.space: x의 크기, y.strlen: y(문자열)의 길이)

- 대상(dst) 버퍼가 동적 할당된 경우, 크기 정보를 위해 별도의 자료구조에 동적 할당된 버퍼의 크기 기록

2. 취약 의심지점 검증을 위한 Test Code 자동 삽입
3. 실행(취약 유발 입력값 생성)

# CTest 검증 절차 – 2 (1)

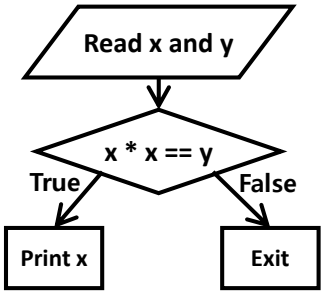
1. 검증 대상이 되는 취약 의심지점 파악
2. **취약 의심지점 검증을 위한 Test Code 자동 삽입**
   - 취약 의심지점에 대한 입력 위치 역방향 추적
   - 취약 의심지점에 검증 조건문 추가
   - 입력 위치에 기호 입력값 생성문 추가
   - Buffer Overflow 예시 코드
     - 9번 줄에서 입력을 받은 뒤
     - 10번 줄에서 BOF 취약점 발생
       - 크기가 5인 버퍼에 크기가 5를 넘는 입력값 복사
3. 실행(취약 유발 입력값 생성)





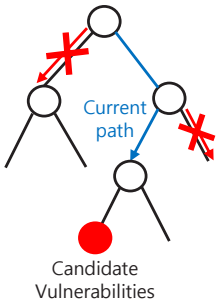

# CTest 검증 절차 – 2 (2) : 고려 사항

1. 분기문 제약 조건 해결 방법
   - 기존 기호화 실행 기법에서는 비선형 제약 조건을 해결하지 못함
     - ex) x * x == y에서 x, y 값을 정할 때
       - 기호 실행으로는 x, y값 특정 불가
       - Concolic Testing에서는 비선형 값 (x * x)에 따라 y값을 정함
   - 비선형 제약 조건 문제 해결을 위해 Concolic Testing 기법 사용



# CTest 검증 절차 – 2 (3) : 고려 사항

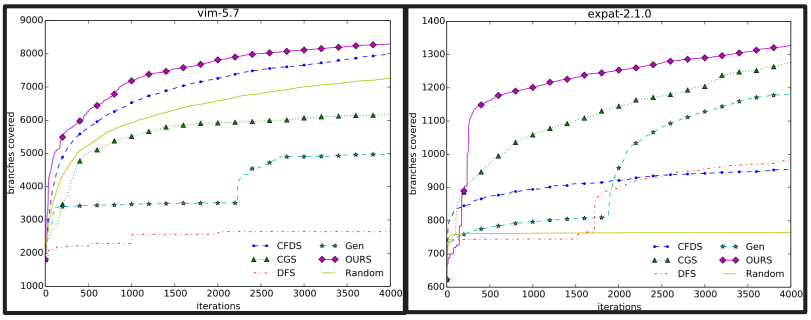
2. 검증 대상에 빠르게 도달하는 방법
   - Code Coverage 확대 연구 수행
     - **Automatically Generating Search Heuristics for Concolic Testing (ICSE'18)**
     - 프로그램에 따른 최적화된 탐색 전략 도출
     - 기존 탐색전략 대비 높은 Code Coverage 달성



**Input: C programs**
(e.g., grep-2.2 , vim-5.7)

$S_{grep}$
$S_{vim}$

**Output: Search Heuristic**
(e.g., $S_{grep}$, $S_{vim}$)






# CTest 검증 절차 – 2 (4) : 삽입 결과

- 원본 코드에 대한 Test Code 자동 삽입 결과
  - CTest 도구 중간 생성 파일
    - 검증 완료 후 자동 삭제

```
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4
5 int main(void)
6 {
7     char dst[5];
8     char *buf = (char*)malloc(20);
9     fgets(buf, 20, 0);
10    strcpy(dst, buf);
11    return 0;
12 }
13
```

```
52 #line 8
53   tmp = malloc(20);
54 #line 8
55   __cil_tmp5 = (int )tmp;
56 #line 8
57   mysizeof_store(__cil_tmp5, 20, 1, 1);
```

동적 할당된 버퍼의 크기 정보 저장

```
83   while (__cil_tmp20 < 20) {
84     CREST_char(buf[__cil_tmp20]);
85     mysizeof_filedesc_write_one("%02x ", buf[__cil_tmp20] & 255);
86     __cil_tmp20 ++;
87   }
```

<취약 유발 입력값 생성문 추가>

```
 98 #line 10
 99   __cil_tmp12 = buf;
100 #line 10
101   __cil_tmp13 = buf;
102 #line 10
103   __cil_tmp11 = mysizeof_getspace((char *)__cil_tmp12, (char *)__cil_tmp13, 0);
104 #line 10
105   __cil_tmp14 = strlen(buf);
106 #line 10
107   if (__cil_tmp11 > 0) {
108 #line 10
109     if (sizeof(dst) > __cil_tmp14) {
110 #line 10
111       strcpy(dst, buf);
112     } else {
113 #line 10
114       mysizeof_filedesc_write_zero("\n-hl:10\n-hf:sample.c\n-hc: Call(@strcpy(S
```

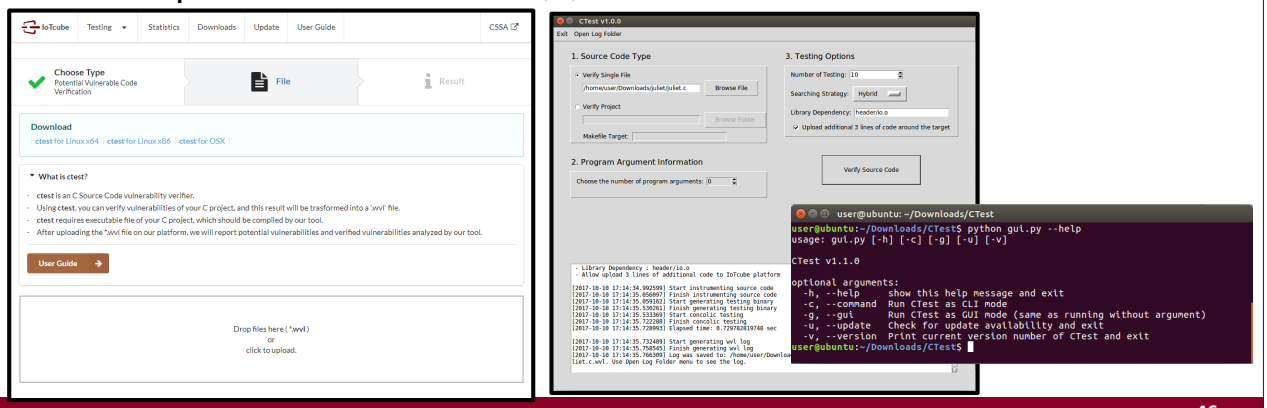
취약 지점에 대한 검증 조건문 추가

앞서 저장된 동적 할당 버퍼의 크기 정보 획득 부분

검증 조건문을 만족하지 않으면 해당 취약점 보고

# CTest 검증 절차 – 3 (1)

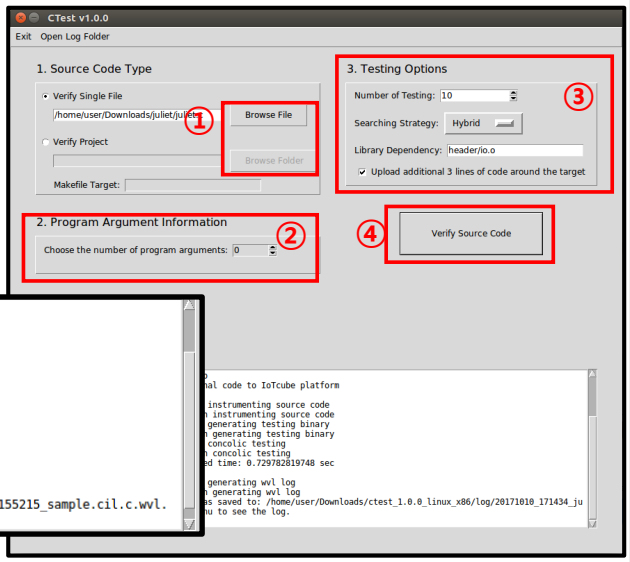
1. 검증 대상이 되는 취약 의심지점 파악
2. 취약 의심지점 검증을 위한 Test Code 자동 삽입
3. **실행(취약 유발 입력값 생성)**
   - CTest를 이용한 검증
   - https://iotcube.net 플랫폼 활용



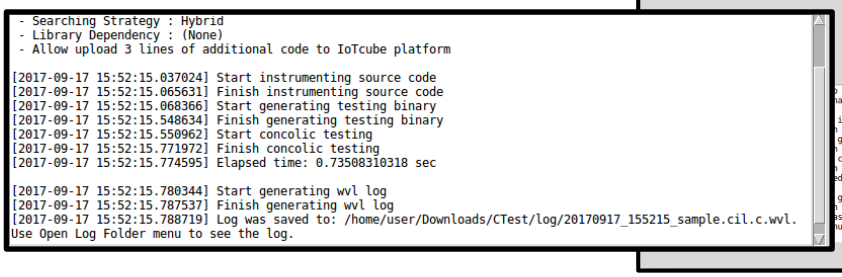



# CTest 수행 방법 (1)

- CTest를 이용한 검증 수행
  1. 파일 (프로젝트 폴더) 선택
  2. 프로그램 인자정보
     - 본 예제에서는 해당 없음
  3. 테스트 옵션 선택
  4. 검증 시작

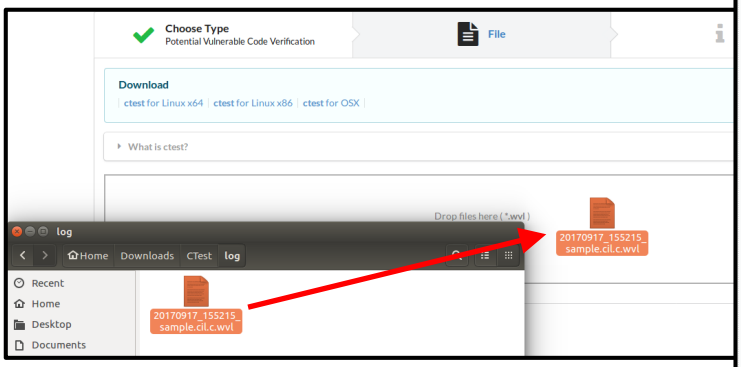



↓ 검증 진행 과정 Message



# CTest 수행 방법 (2)

- 생성된 Log 파일 업로드



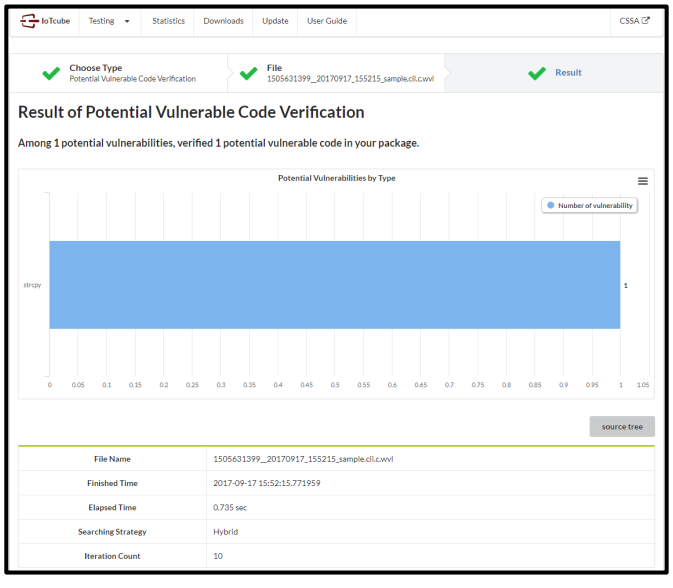


```
{
    "BitType": "86",
    "OsType": "linux",
    "hotspot_all": {
        "0": {
            "file": "sample.c",
            "line_num": 10,
            "source_sliced": "ICAgIGNoYXIgZHN0WzVdOwogICAgY2hhciAqYnVmID0gKGNoYXIq
            wKTsKICAgIHN0cmNweShkc3QsIGJ1Zik7CiAgICByZXR1cm4gMDsKfQoK",
            "vulntype": "strcpy"
        }
    },
    "hotspot_verified": {
        "0": {
            "verif_cond": "SizeOfE(dst)>__cil_tmp14"
        }
    },
    "overall_time_elapsed": 0.735083,
    "overall_time_end": "2017-09-17 15:52:15.771959",
    "overall_time_start": "2017-09-17 15:52:15.036876",
    "strategy": "Hybrid",
    "test_count": 10,
    "toolVer": "1.0.0",
    "tree_json": {
        "children": [
            {
                "children": [],
                "hotspot_all_idx": [
                    0
                ],
                "hotspot_verified_idx": [
                    0
                ],
                "line_count": 13,
                "name": "sample.c"
            }
        ],
        "name": "testcode"
    },
    "triggering_info": [
        {
            "iteration_count": 1,
            "time_end": "2017-09-17 15:52:15.596433",
            "time_start": "2017-09-17 15:52:15.596376",
            "triggering_hotspot": [
                0
            ],
            "triggering_value": {
                "0": "67 79 44 99 30 89 65 97 0f eb 60 3e fc 15 7e d5 ed 32 f6 b0"
            }
        },
```




# CTest 수행 방법 (3)

- IoTcube 업로드 결과



# CTest 활용 범위

- Single File 취약점 검증 가능 (예: Juliet Test Suite)
  - Juliet Test Suite 내 Pointer 사용과 관련된 6종 취약점 (총 9,959개 샘플) 중 92% (9,162개) 샘플 검증 가능

| 취약점 종류 | 전체 | 성공 | 실패 |
|---|---|---|---|
| Stack Based Buffer Overflow | 4,009 | 3,898 (97.23%) | 111 (2.77%) |
| Heap Based Buffer Overflow | 2,339 | 2,144 (91.66%) | 195 (8.34%) |
| Buffer Overread | 924 | 748 (80.95%) | 176 (19.05%) |
| Buffer Underwrite | 1,246 | 1,090 (87.48%) | 156 (12.52%) |
| Buffer Underread | 1,246 | 1,087 (87.24%) | 159 (12.76%) |
| Double Free | 195 | 195 (100%) | 0 (0%) |
| **합계** | **9,959** | **9,162 (92.00%)** | **797 (8.00%)** |

- 소규모 패키지 취약점 검증 가능
  - Zitser-bug (Sendmail, bind, wu-ftpd), Coreutils 등

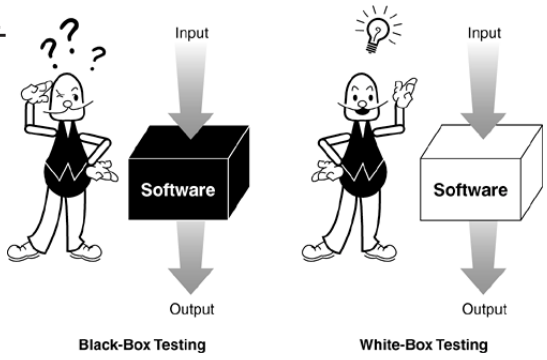


# 무선 네트워크 프로토콜 구현 오류 자동탐지 기술

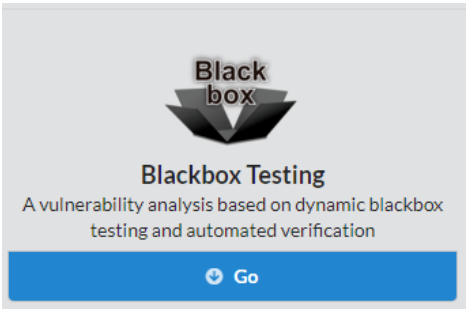
# (BFUZZ/WFUZZ)

# IoTcube의 블랙박스 테스팅

- 소프트웨어 테스팅의 한 종류
  - 소프트웨어 소스코드 없이 테스트하는 기법
    - 입력값과 결과값을 가지고 테스트
    - 내부 소스 분석 없이 진행



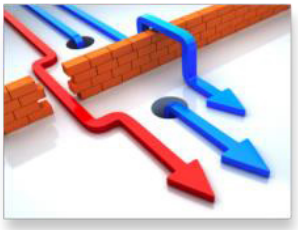

- IoTcube 내 테스팅 도구
  - bfuzz
    - Bluetooth 프로토콜 (L2CAP, OBEX, RFCOMM, SDP)
  - wfuzz
    - Wi-Fi 프로토콜 (802.11)
  - cloif
    - 바이너리 입력값 추론 도구






# 퍼징을 통한 취약점 탐지

- 임의 혹은 사전 정의된 입력값을 순차 전송
  - 비정상적 응답이나 크래시 유발 목적



- “Fuzzing” in the Wikipedia
  - An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

- Valid한 입력값을 찾는 것이 이슈
  - 임의로 생성된 입력값들은 대부분 Non-acceptable

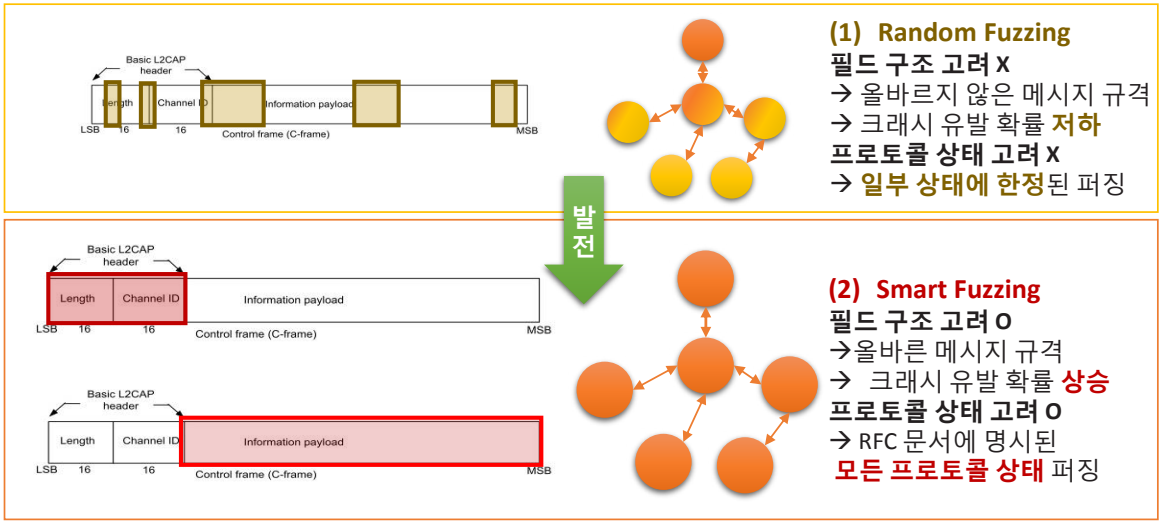
- 퍼징 연구에서의 주안점
  - ‘그럴듯한’ 입력값을 생성하는 알고리즘과 전략
  - 효율적인 전송을 통해 속도 극대화

# 자동 무선 퍼징의 필요성

- 대상 기기의 소스코드 없이도 테스팅이 가능!
- IoT 시스템의 성격
  - 다양한 인터페이스 및 프로토콜
    ex) Bluetooth / Wi-Fi / ZigBee / 6LowPan / …
  - 각 프로토콜 마다 다양한 implementation
    - Manual 하게 테스팅하는 것은 Time-consuming
  - 프로토콜, SW 다양성으로 인해 자동 분석 필요성 증대

# Smart & Stateful 퍼징

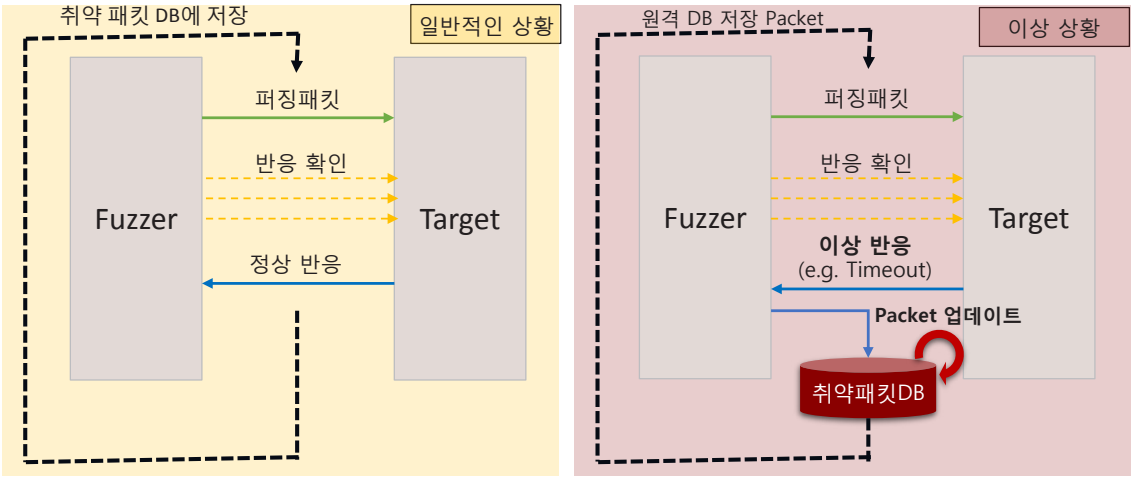
- **상태기반 스마트 퍼징**
  - 프로토콜 상태별 패킷 구조를 따르는 시드값 기반 필드값 변조




- **실제 유효 크래시 여부 판별**
  - 퍼징 중 Instrumentation 을 통한 실제 크래시 유효성 확인

# 피드백 기반 퍼징

- Instrumentation - 퍼징 과정 중, 상대 기기의 “Keep Alive” 상태 확인
  - BT : 상대 기기에 Ping 을 보냄으로써 확인
  - WiFi : 상대 기기 (AP) 의 Beacon Frame 송신 여부 확인
- 의심스러운 반응이 나타날 경우 “취약 의심 패킷“ 으로 간주



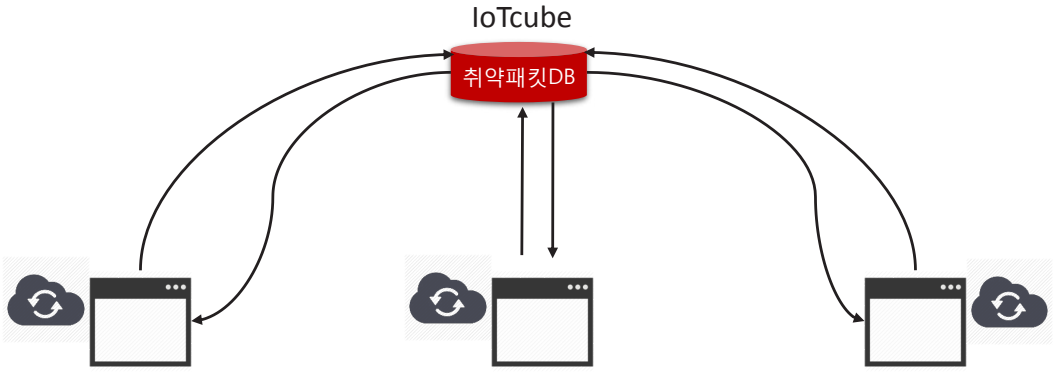



# 효과적인 Fuzz Test Case 생성

- Smart & Stateful 퍼징은 Random 퍼징 보다 효과적
  - 그러나, 여전히 취약 패킷 생성에 많은 시간 소요
- 상용 퍼징 도구
  - 필드 및 상태를 고려하여 수많은 퍼징 테스트 케이스 사전 정의
  - 그러나, 실제 퍼징 수행시 효과적이지 않은 결과
    - 수많은 미탐 및 오탐
- ‘실제로’ Crash 를 일으킨 패킷을 다시 활용한다면?
  - A에서 발견된 취약 패킷이 B기기에서도 동일하게 크래시 발생가능
- 취약 패킷을 Seed 로 Mutation 한다면?
  - 훨씬 효과적인 Test case 생성 가능

# 취약 의심패킷 DB와 REPLAY

- 사용자들이 찾아낸 취약 의심패킷을 데이터베이스화
  - 전세계 어디서나 도구 실행시 취약 패킷 실시간 동기화
  - 현재 110개 이상의 기기에서 발견된 530개 이상의 취약 패킷 보유

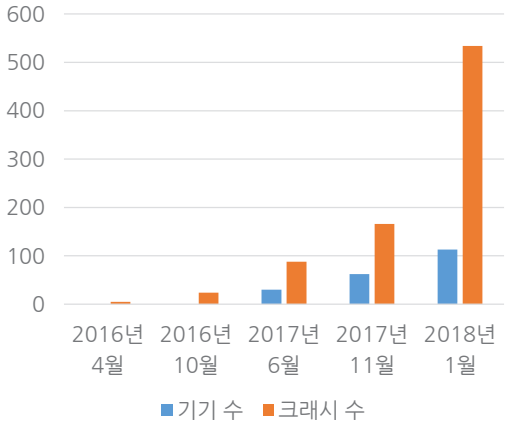



- 취약 의심 패킷 REPLAY 기능
  - 원격 DB에 저장된 패킷들을 선택하여 주변 기기에 전송
  - A 기기에서 발생된 크래시를 B 기기에서도 테스트 가능!



# IoTcube Fuzz Testing 통계

- bfuzz & wfuzz (2018.04.02)
  - Fuzzing 결과 분석 **341 회**
  - 수집된 Unique 패킷 **534 개**
  - 테스팅 된 Unique 기기 **113 대**
    - 기기 예시
      - Samsung Galaxy series (S5, S6, …)
      - Samsung Note series (Note 3, 4 …)
      - Smart TVs
      - LG G series (G3, G5, …)
      - Google Nexus series (Nexus 5, 7, …)
      - ipTime APs




취약 패킷 보유 현황

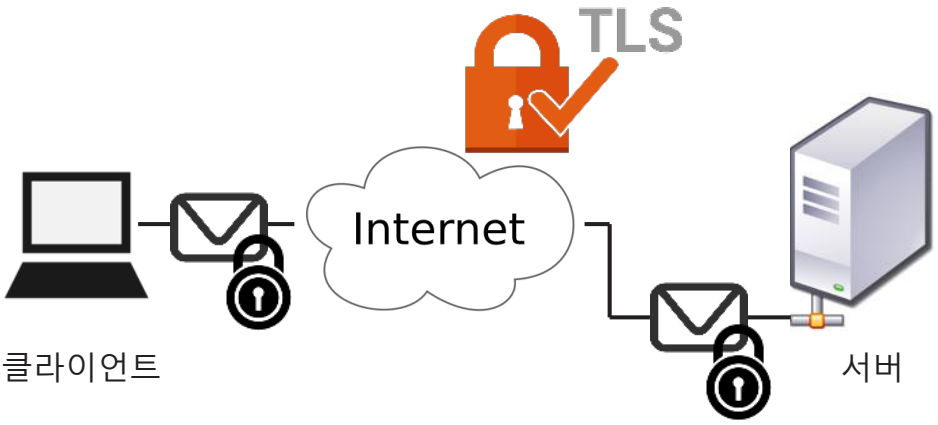
| Rank | Protocol | # Crash |
|---|---|---|
| 1 | OBEX | 188 |
| 2 | RFCOMM | 184 |
| 3 | L2CAP | 84 |
| 4 | 802.11 AP | 71 |
| 5 | SDP | 9 |

# SSL/TLS 취약점 자동 점검 기술 (NSCAN)

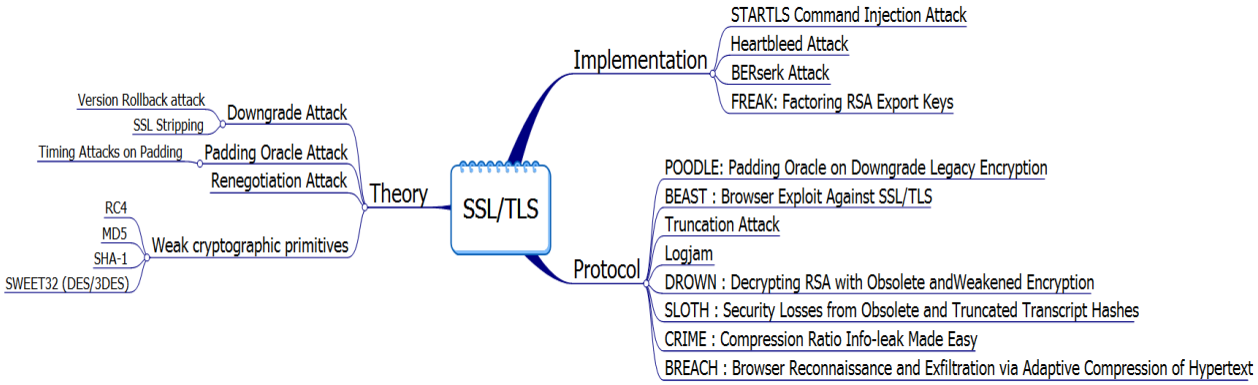


## SSL/TLS 란?

- 인터넷을 통해 클라이언트와 서버가 통신할 때, 통신 내용을 안전하게 보호하는 기법
- 서버 인증, 클라이언트 인증, 데이터 암호화 기능 제공



# TLS 취약점 분류





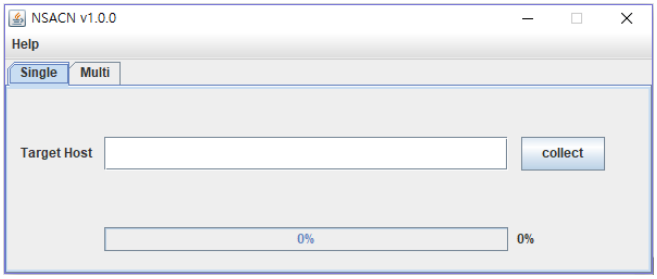

# TLS 취약점 보고

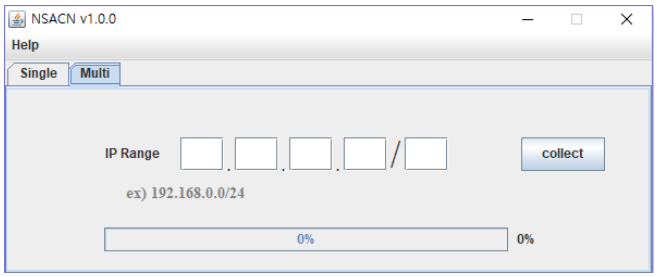
- Heartbleed 공격 - 2014년 04월
- FREAK 공격 - 2015년 01월
- SLOTH 공격 - 2015년 09월
- DROWN 공격 - 2015년 12월
- Sweet32 공격 - 2016년 01월
- Ticketbleed 공격 - 2016년 11월

⋮ ⋮

# NSCAN (1)

- **N**etwork **S**ecurity s**C**anner with **A**utomatic detectio**N**




– 싱글/멀티 도메인 취약점 탐지 지원

– 탐지 가능 취약점 12개

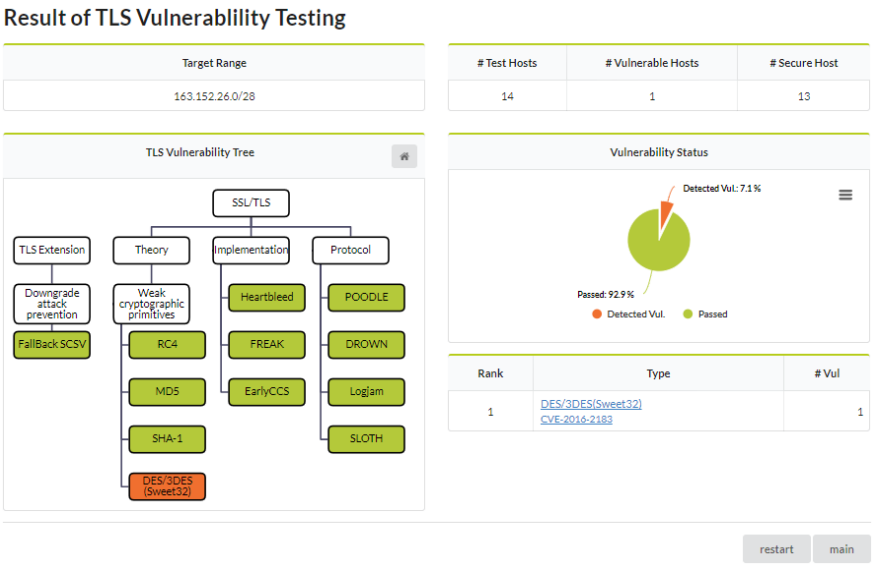


# NSCAN (2)

- NSCAN – Single Search

# NSCAN (3)

- NSCAN – Multi Search






# 조사 대상

Alexa

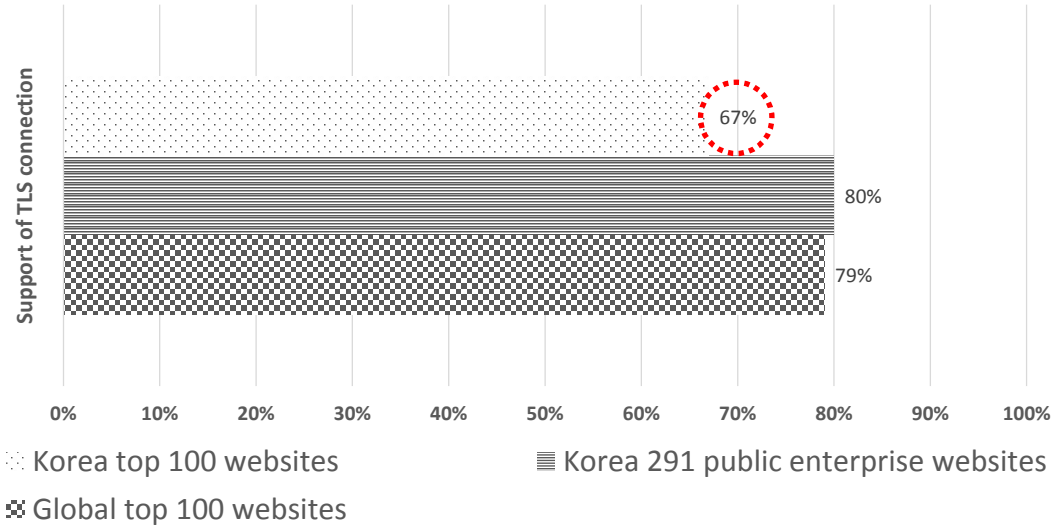
1. Alexa Top 500 기준 국내 100대 웹사이트
2. 국내 주요 291개 공기업 웹사이트
   - 정부기관, 국립병원 등*
3. Alexa Top 100 Global 웹사이트

*** 관련 연구**

- Jongmin Jeong, Hyunsoo Kwon, Hyungjune Shin, Junbeom Hur, "A Practical Analysis of TLS Vulnerabilities in Korea Web Environment", International Workshop on Information Security Applications (WISA), pp. 112-123, March. 30. 2017.

# TLS 지원 현황

- 국내 100대 웹사이트의 33%가 TLS를 지원하지 않음

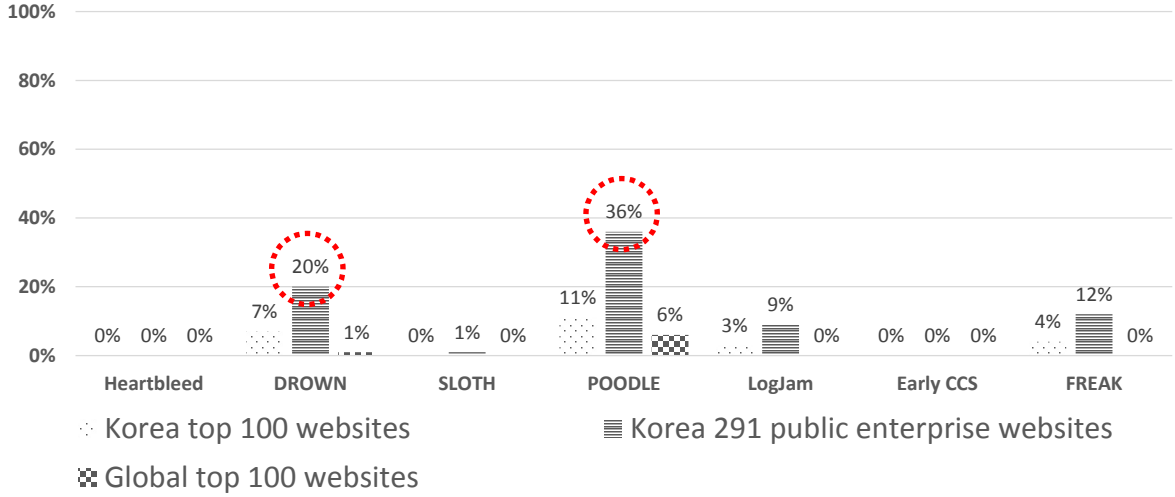



(2018년 02월 기준)



# TLS 취약점 현황 (1)

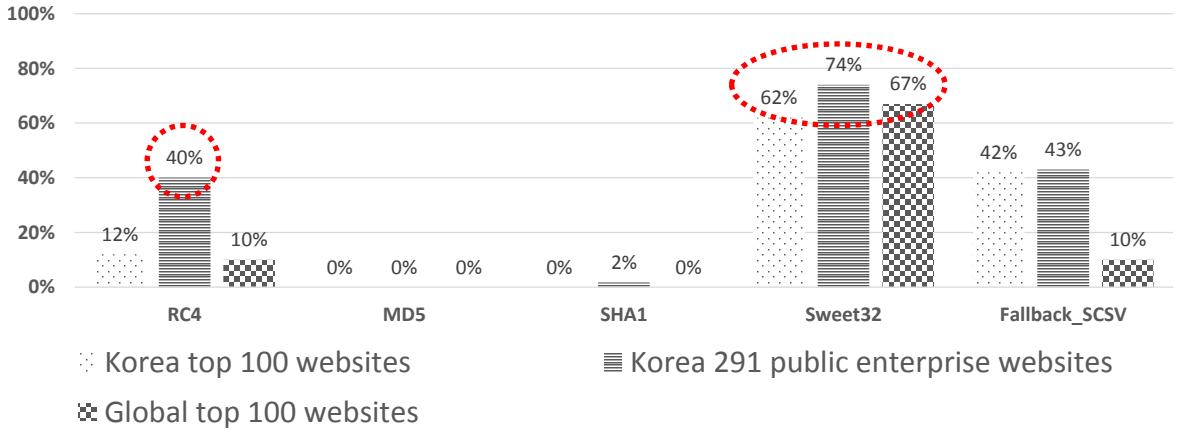
- 취약한 국내 291개 공기업 웹사이트
  - 약 36%가 POODLE 공격에 취약
  - 약 20%가 DROWN 공격에 취약




(2018년 02월 기준)

# TLS 취약점 현황 (2)

- 국내 291개 공기업 웹사이트의 약 40%가 RC4 공격에 취약
- 다수의 웹사이트가 Sweet32 공격에 취약




(2018년 02월 기준)



# NSCAN 확장 방향

- 인증서 신뢰 검증 기능 지원 주력
  - 기존 CA 기반 인증서 검증 기법
  - 최신 인증서 투명성(certificate transparency, CT) 기반 인증서 검증 기법

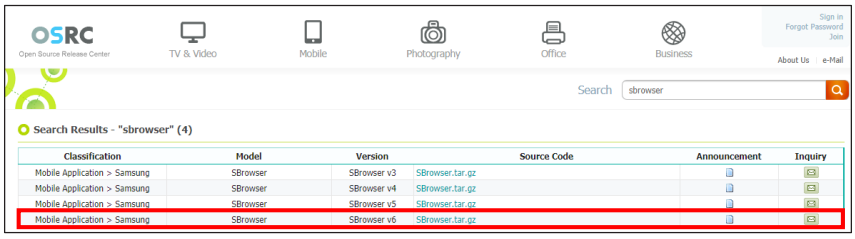
# IoTcube 실습

# 코드 클론 취약점 탐지 실습

# 코드 클론 취약점 탐지 과정

# Step 1. 타겟 선정 및 코드 다운로드

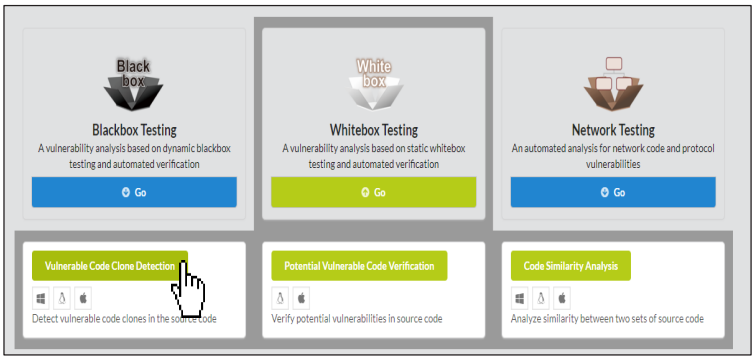
- 브라우저 소스코드 다운로드
  http://opensource.samsung.com/reception/receptionSub.do?method=sub&sub=F&searchValue=sbrowser




- 실습용 소스코드 (저용량) :
  https://ccs.korea.ac.kr/netsec.zip

# Step 2. Vulnerable Code Clone Detection

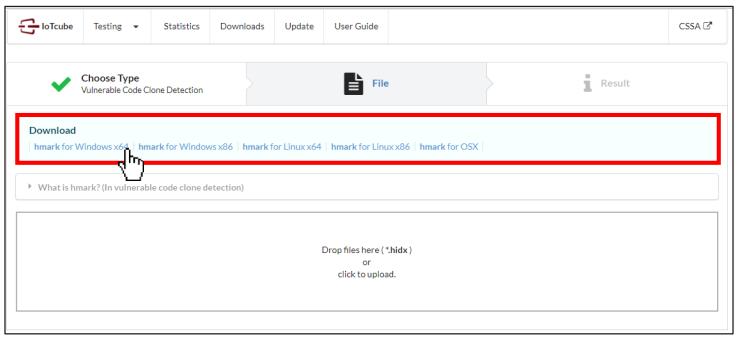
- IoTcube의 Whitebox Testing을 이용하여 취약한 코드 클론이 존재하는지 분석
- Iotcube.net 접속 후
  Vulnerable Code Clone Detection으로 이동
  https://iotcube.net/process/type/wf1





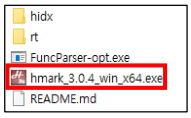

# Step 2. Vulnerable Code Clone Detection

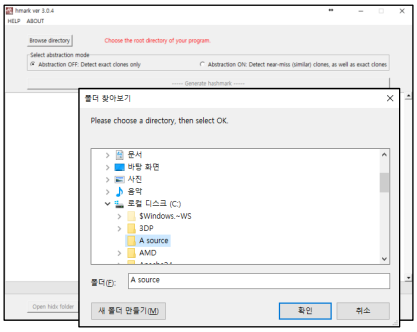
- Vulnerable Code Clone Detection 도구인 hmark를 본인의 플랫폼에 맞게 다운로드

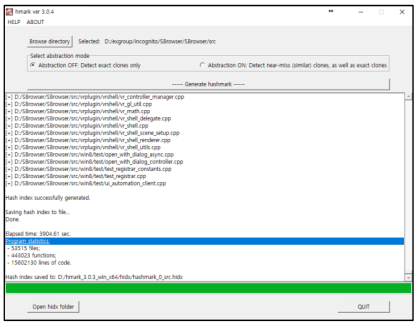


# Step 2. Vulnerable Code Clone Detection

- hmark를 통해 소스코드로 부터 hidx 생성
- GUI뿐 아니라 CLI도 지원
  https://iotcube.net/userguide/hmark.pdf



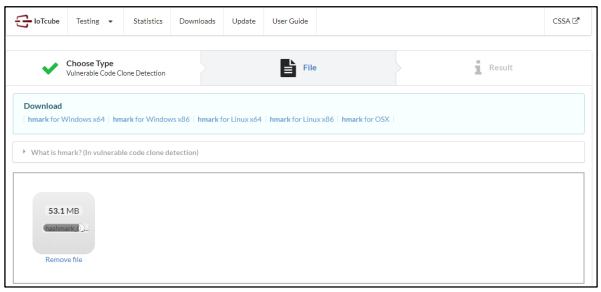





# Step 2. Vulnerable Code Clone Detection

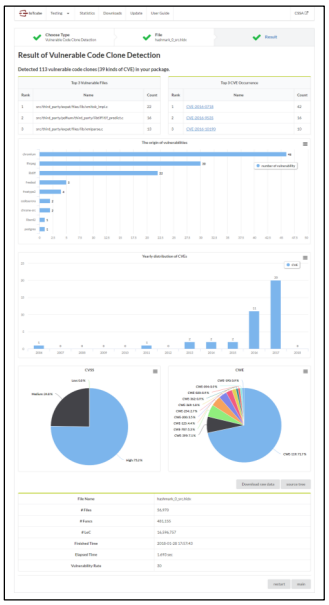
- 생성된 hidx를 iotcube에 업로드
  https://iotcube.net/process/type/wf1

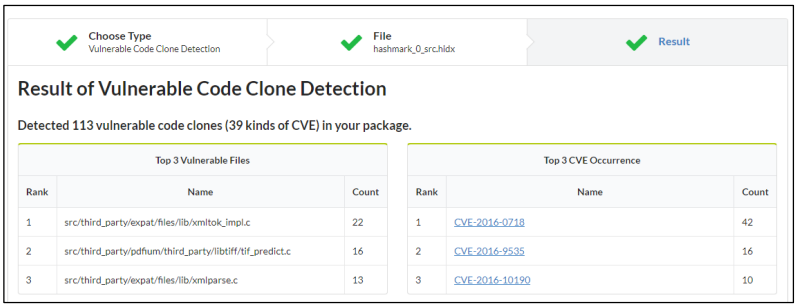



- 실습용 hidx:
  https://ccs.korea.ac.kr/netsec.zip

# Step 3. 결과 보고서 및 코드 분석

- 결과 보고서





Choose Type
Vulnerable Code Clone Detection

File
hashmark_0_src.hldx

Result

**Result of Vulnerable Code Clone Detection**

Detected 113 vulnerable code clones (39 kinds of CVE) in your package.

Top 3 Vulnerable Files

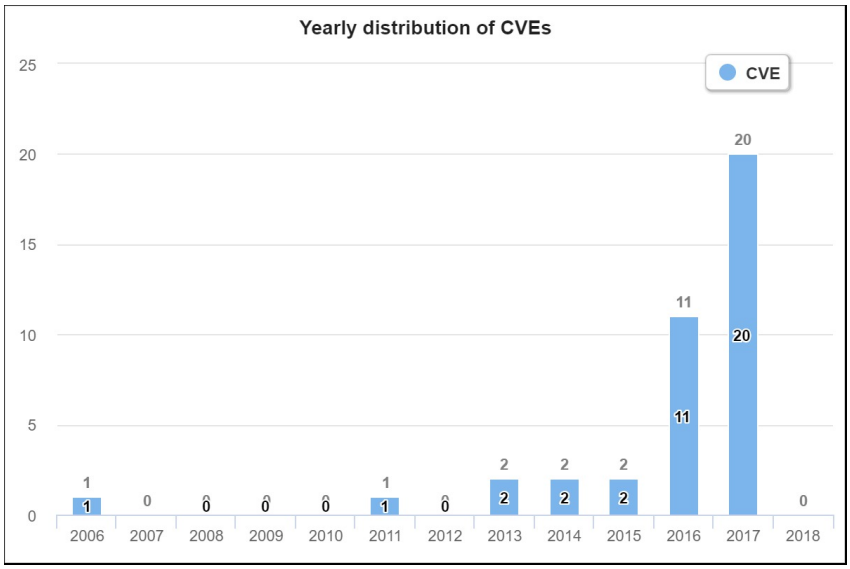
| Rank | Name | Count |
|---|---|---|
| 1 | src/third_party/expat/files/lib/xmltok_impl.c | 22 |
| 2 | src/third_party/pdfium/third_party/libtiff/tif_predict.c | 16 |
| 3 | src/third_party/expat/files/lib/xmlparse.c | 13 |

Top 3 CVE Occurrence

| Rank | Name | Count |
|---|---|---|
| 1 | CVE-2016-0718 | 42 |
| 2 | CVE-2016-9535 | 16 |
| 3 | CVE-2016-10190 | 10 |

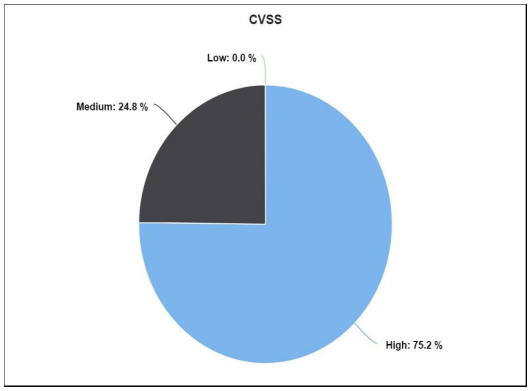


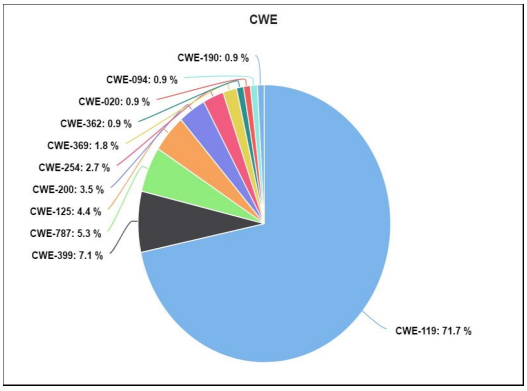
# Step 3. 결과 보고서 및 코드 분석




- 연도별 CVE 확인

# Step 3. 결과 보고서 및 코드 분석

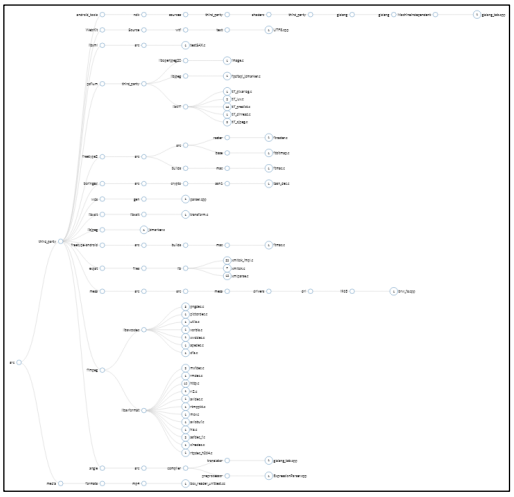


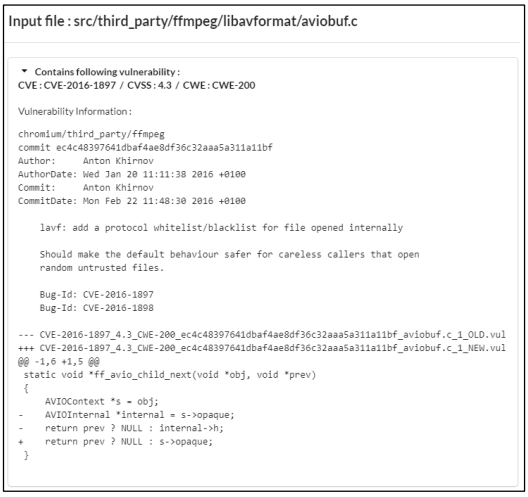




- CVSS 분류별(High, Medium, Low) 분포 확인
- CWE 별 분포 확인



# Step 3. 결과 보고서 및 코드 분석






- 소스 트리에서 파일 클릭 후
  코드 클론에서의 취약점 탐지정보 확인

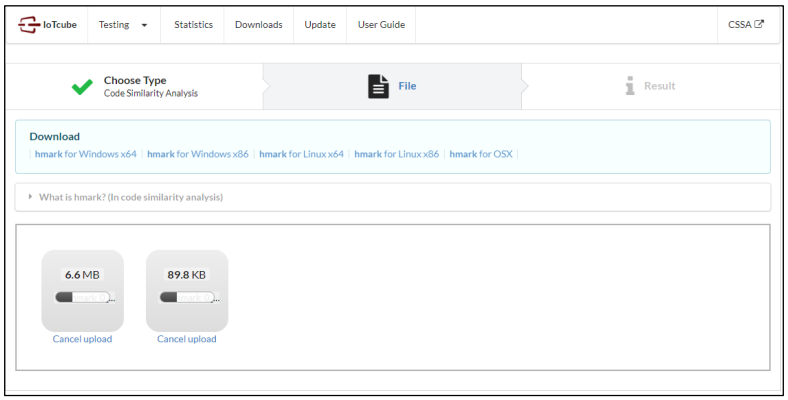
# 코드 유사도 분석 실습

# 코드 유사도 분석

- **사용 방법**
  - https://iotcube.net/ -> Whitebox Testing -> **Code Similarity Analysis** 에 접속
  - 자신의 운영체제에 맞는 Hmark 툴 다운로드
  - Hmark 툴을 통해 비교를 원하는 **두 소프트웨어의 해시 인덱스 파일(.hidx)** 생성
    - 해시 인덱스 파일
      - 소프트웨어를 함수단위로 나누어, 각 함수의 해시 값을 저장한 파일
      - 함수의 길이또한 기록하여, 함수 비교 시 시간 복잡도를 줄일 수 있음
  - 두 개의 hidx 파일을 업로드 후 **결과 확인 및 분석**

# Step 1. Code Similarity Analysis

- 생성된 2개의 hidx를 iotcube에 업로드
  https://iotcube.net/process/type/wf3

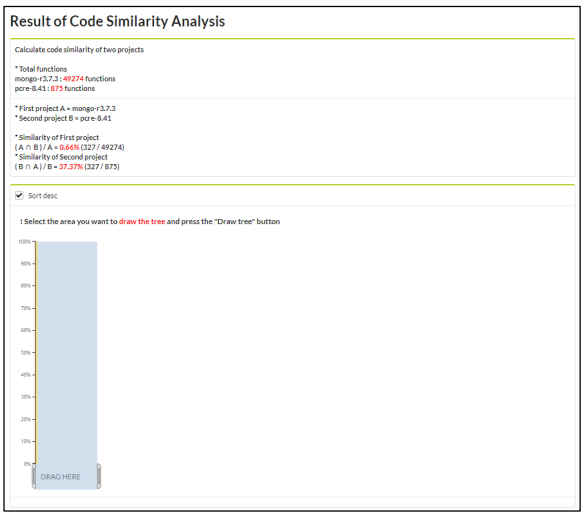



- 실습용 hidx:
  https://ccs.korea.ac.kr/cosim.zip (LargeHidx 와 SmallHidx 로 구성)



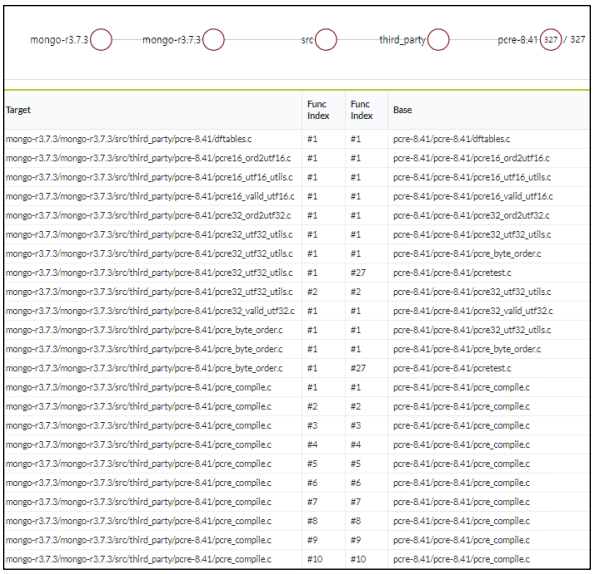
# Step 2. 결과 보고서 및 코드 분석

- 결과 보고서
  - SmallHidx 의 결과



# Step 2. 결과 보고서 및 코드 분석

- 트리의 리프노드 클릭 후 자세한 path 정보 확인




| Target | Func Index | Func Index | Base |
|---|---|---|---|
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/dftables.c | #1 | #1 | pcre-8.41/pcre-8.41/dftables.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre16_ord2utf16.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre16_ord2utf16.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre16_utf16_utils.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre16_utf16_utils.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre16_valid_utf16.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre16_valid_utf16.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_ord2utf32.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre32_ord2utf32.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_utf32_utils.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre32_utf32_utils.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_utf32_utils.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre_byte_order.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_utf32_utils.c | #1 | #27 | pcre-8.41/pcre-8.41/pcretest.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_utf32_utils.c | #2 | #2 | pcre-8.41/pcre-8.41/pcre32_utf32_utils.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre32_valid_utf32.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre32_valid_utf32.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_byte_order.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre32_utf32_utils.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_byte_order.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre_byte_order.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_byte_order.c | #1 | #27 | pcre-8.41/pcre-8.41/pcretest.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #1 | #1 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #2 | #2 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #3 | #3 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #4 | #4 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #5 | #5 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #6 | #6 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #7 | #7 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #8 | #8 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #9 | #9 | pcre-8.41/pcre-8.41/pcre_compile.c |
| mongo-r3.7.3/mongo-r3.7.3/src/third_party/pcre-8.41/pcre_compile.c | #10 | #10 | pcre-8.41/pcre-8.41/pcre_compile.c |

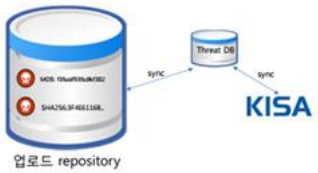


# IoTcube 활용 사례 및 계획

# 국·내외 IoTcube 활용 사례

## C-TAS 정보 연계 (KISA)

KISA에서 운영중인 사이버 위협정보 분석·공유시스템 (C-TAS)와 보안 취약점 정보 공유 (데이터베이스 연계)



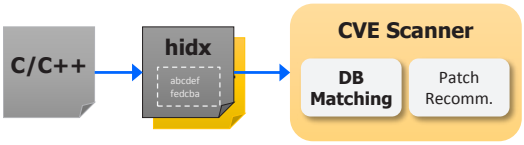

## I³ 컨소시엄* 보안성 점검

美 Intelligent IOT Integrator (I³) 시스템의 오픈소스 보안성 점검 절차로 IoTcube 활용 ('17년 11월 창립)

** 美 LA시와 USC가 주도하는 IoT 테스트베드 사업*

## S전자 보안 내재화

IoTcube와 연동하여 오픈소스 코드 내에 보안 취약점(CVE) 자동 검사 및 패치 정보 제공




## RedHat 요구기술 적용

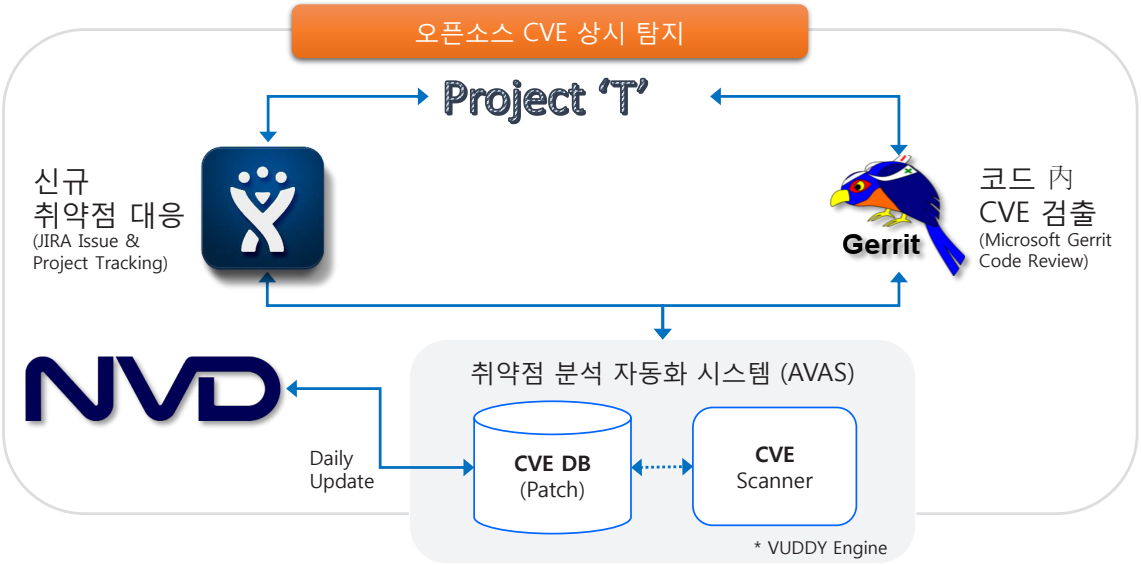
Code Similarity 기반 보안 취약점 탐지 기술 (COSIM) 개발 및 관련 정보 교류

redhat



# IoTcube 기술 적용 사례 (국내)

- **S전자 보안 내재화** (Security by Design)
  - AVAS (Automated Vulnerability Analysis System) 시스템內 기술 이전
  - S전자 SDL (Security Development Lifecycle) 상의 코드 리뷰 절차에 적용



# IoTcube 기술 적용 사례 (국외)

- **I³ Consortium** (Intelligent IoT Integrator) **& Security Verification**
  - 美 LA시와 USC*가 주도하는 스마트시티 구축 공동체 (창립 멤버 참여)
    - 도시 규모 IoT 테스트 환경 구축, 기업이 제품 개발이나 테스트에 활용하도록 데이터 흐름을 통합 '데이터 강 (Data Rivers)' 형태로 제공하는데 목적
    - I³ 시스템은 오픈 소스를 기반으로 하며, IoT 장비 등 관련 소프트웨어의 보안성을 자동으로 검증하는 절차로 IoTcube가 참여함

※ 서든캘리포니아대학 (University of Southern California)

  - 주요 멤버

# 2018년도 IoTcube 계획

- **블랙박스 테스팅 기능 IoTcube 추가** 2018.04 예정
  - "zfuzz" 개발 중 (ZigBee, Z-wave 대상 테스팅 도구)

- **화이트박스 테스팅 Ctest 엔진기술 논문 발표** 2018.05 예정
  - SW공학 분야 최우수학회인 ICSE 2018에 논문 발표 예정

  - Title : **Automatically Generating Search Heuristics for Concolic Testing**

연중 계획

- **KISA IoT보안 테스트베드 및 인증에 IoTcube 기술 도입**
  - 블랙박스 테스팅 zfuzz (ZigBee, Z-wave) 개발 이후 관련 기술 이전
  - KISA IoT 혁신센터 內 IoTcube 상시 전시 예정

# 맺음말

- **CVE 취약점에 대한 전반적인 보안성 점검이 필요함**
  - 취약 코드 클론등을 통해 취약점이 복제되는 경우가 많음
  - 취약점이 패치되지 않고 그대로 존재하는 경우도 빈번함
- **최신버전의 오픈소스 소프트웨어도 안전하지 않음**
  - 실제 패치 적용이 지연되는 경우가 존재
  - 지속적인 관리와 점검이 필요함
- **IoT기기 보안성 점검의 중요성 대두**
  - 시장에 존재하는 다양하고 많은 IoT 기기에 대한 보안성 점검이 필요
  - 출시 이후 뿐 아니라 기기 소프트웨어 개발단계 및 기술적용단계의 보안성 점검 또한 필요함



# Q & A

- **IoTcube**
  - https://iotcube.net
- **고려대학교 컴퓨터보안연구실**
  - Computer & Communication Security Laboratory (CCS Lab)
  - 307B, Woojung Hall of Informatics, Korea University, Anam Campus
  - 02-3290-3638
  - https://ccs.korea.ac.kr/
- **CSSA**
  - IoT 소프트웨어 보안 국제공동연구센터
  - Center for Software Security and Assurance(CSSA)
  - Room 106A, Science Building Annex, Korea University, Anam Campus
  - 02-3290-4816
  - https://cssa.korea.ac.kr

The 24th Network Security Conference -Korea

# Private 블록체인 기반의 상품 거래 시스템 구현 시연

**공무제** IBM 에반젤리스트

### 학력 및 경력사항

| | |
|---|---|
| 2016 ~ | 블록체인 에반젤리스트, IBM Korea |
| 2016 | 소프트웨어 엔지니어, IBM Korea |
| 2012 ~ 2015 | 하이브리드 클라우드 아키텍트, IBM Korea |

### 강연요약

본 강의는 다양한 산업군에서 적용을 검토하고 있는 블록체인의 개념에 대한 설명을 하고 오픈소스 기반 Private 블록체인 서비스를 이용하여 상품거래 플랫폼 개발 과정을 시연합니다.

1. 블록체인 기본 개념 및 Hyperledger Fabric v1.0 소개
2. Private 블록체인 네트워크 구성
3. 상품 거래를 위한 어플리케이션 구현

## 블록체인 기술

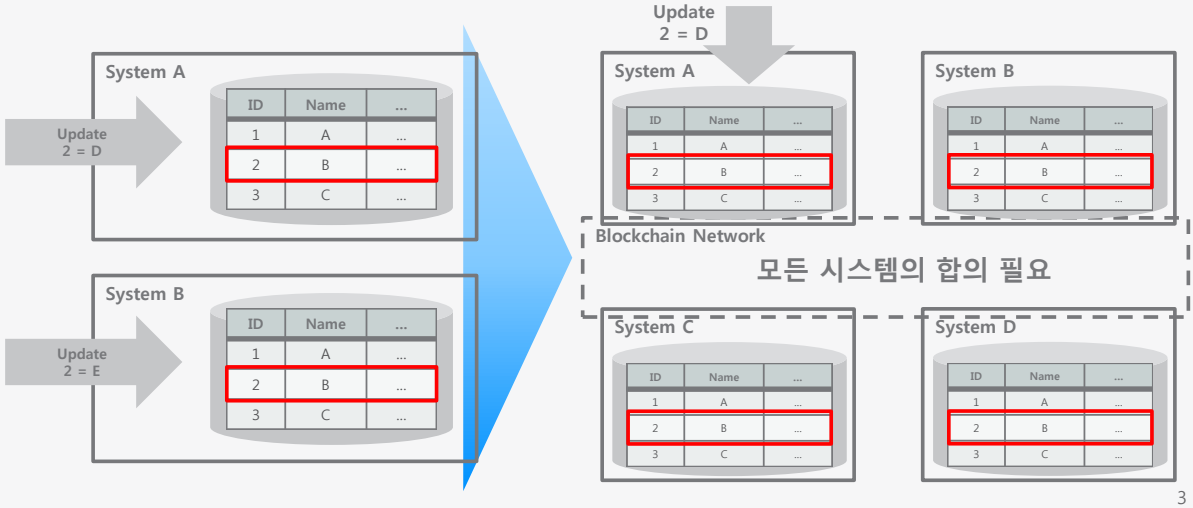
비즈니스 네트워크(Business Network)의 모든 참여자들이
원장(Ledger)을 볼 수 있도록 해주는
**공유 원장 기술**
**(shared ledger technology)**

비즈니스 프로세스를 간소화하면서
신뢰와 투명성을 확립하는
**차세대 트랜잭션 애플리케이션**을
구축하기위한 토대

2

# 분산원장

참여하고 있는 모든 시스템이 각자 원장 데이터를 보유하고 항상 동기화를 하는 것




3

# 블록체인의 시작 - 비트코인

블록체인은 비트코인을 구현하기 위해 만들어 졌음.

- 2008년 11월 사토시 나카모토의 논문에의해 알려짐
- P2P 네트워크 상에서 구현한 최초의 가상화폐
- 2009년 1월 비트코인 소프트웨어 배포되어 운영
- 2009년 1월 3일 최초의 블록(genesis block)이 만들어진 이후 지금까지 가동되고 있음.

4

# 비트코인의 목적

사토시 나카모토의 논문 중...

"A purely peer -to -peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution ."

"전자 화폐를 순수 P2P (Peer to Peer)로 만들 수 있다면 금융 기관의 개입 없이 사용자끼리 직접 온라인으로 지불할 수 있게 된다."

**온라인에서 사용자간 거래를 위한 기술적 해결해야 할 점**

- 본인 보증, 부인 방지
- 제삼자 기간의 보증 대체
- 원장 데이터에 대한 위/변조 위험
- P2P 네트워크상에서의 비잔티움 장군 문제
- 등등

**해결 방법**

- 전자 서명
- 블록체인
- 해답 인센티브
- PoW

5

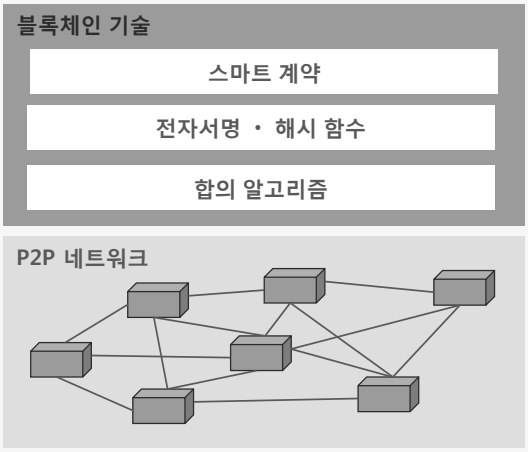
# 블록체인의 기술요소 구성

**피어 투 피어(P2P) 네트워크**
컴퓨터끼리 같은 목적으로 연결해 네트워크를 형성하는 방식이다. 어떤 컴퓨터도 같은 처리를 할 수 있기 때문에 1대가 정지해도 시스템 전체에는 영향을 주지 않는 특징을 가진다.

**합의 알고리즘**
P2P 네트워크와 같은 분산 네트워크에서 합의 형성을 수행하기 위한 알고리즘이다. 블록체인을 여러노드에서 공유하기 위한 가장 중요한 구조라고 할 수 있다.

**전자 서명·해시 함수**
트랜잭션(거래)을 발생시킨 사람의 정당성을 보증하거나 거래·블록체인 변조 방지, 암호화 등 보안과 관련된 기능이다.

**스마트 계약**
블록체인 네트워크에서 동작하는 프로그램을 가리킨다. 블록체인 기반 기술 중에서 가장 자유도가 높은 프로그램을 만들 수 있다.




6

# 블록체인 기반 기술의 분류

| | 공용(Public) 형 | 컨소시엄형<br>(여러 조직에서 운영) | 개인(Private)형<br>(단일 조직에서 운영) |
|---|---|---|---|
| (마이닝)<br>노드형 | 제한 없음 | 제한 가능 | 제안 가능 |
| 블록체인 검색 | 제한 없음 | 제한 가능 | 제한 가능 |
| 블록 생성시 | 높은 난이도 필요 | 임의 | 임의 |
| 마이닝 보수 | 필요 | 임의 | 임의 |

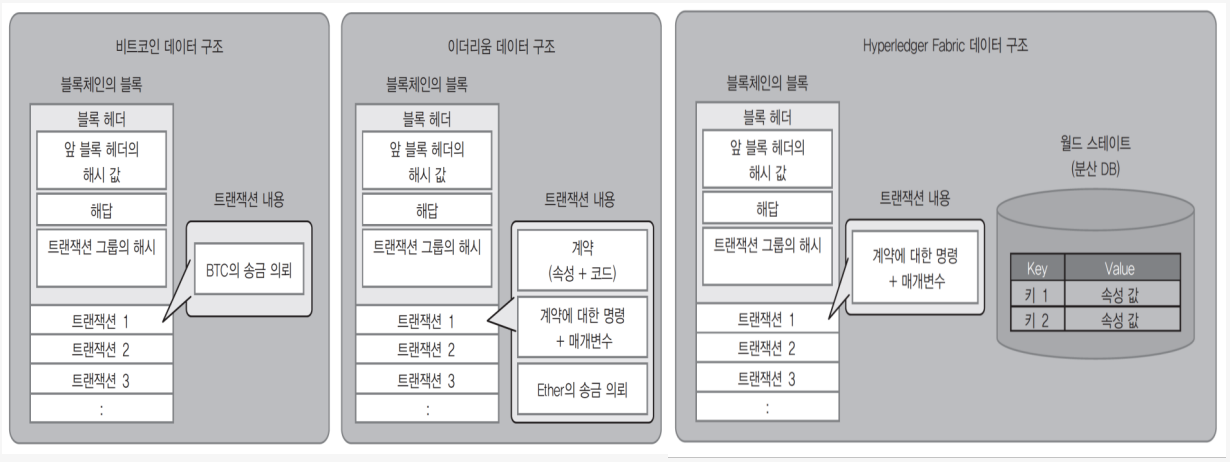
7

# 블록체인 기반 기술 비교

| 분류 | 하이퍼레저<br>(Hyperledger) | 이더리움<br>(Ethereum) | 리플<br>(Ripple) | 비트코인<br>(Bitcoin) |
|---|---|---|---|---|
| **소개** | 모든 산업에서 사용할 수 있는 Blockchain 기술의 표준화 | 일반적인 사용을 위한 Blockchain | 페이먼트 Blockchain | 페이먼트 Blockchain |
| **거버넌스** | 리눅스 재단 | 이더리움 개발자 | 리플 랩(Ripple Labs) | 비트코인 개발자 |
| **합의 네트워크** | 플러거블 : PBFT (Practical Byzantine Fault Tolerance) | 마이닝 | 리플 프로토콜 | 마이닝 |
| **네트워크** | 프라이빗 또는 퍼블릭 | 퍼블릭 또는 프라이빗 | 퍼블릭 | 퍼블릭 |
| **프라이버시<br>(Privacy)** | 오픈 원장 부터 사설 원장 지원 | 오픈 원장 | 오픈 원장 | 오픈 원장 |
| **스마트 컨트랙<br>(Smart Contracts)** | 멀티 프로그래밍 언어<br>(Go, Java, Node.js) | 'Solidity' 프로그래밍 언어 | 없음 | 가능하지만 분명하지 않음 |
| **통화** | 통화기반이 아님(UTXO API 활용하여 구현 가능) | Ether | XRP | BTC |
| **마이닝 보상** | 관련없음 | 있음 | 없음 | 있음 |
| **State** | 키-밸류 데이터베이스 | 계좌(Account) 데이터 | 없음 | 거래(Transaction) 데이터 |

8

# 블록체인 데이터 모델 비교




9

# Hyperledger 소개

**오픈소스**
전 산업에 적용가능한
**블록체인 기술**을 위한
공동의 노력

**The Linux Foundation**에
의해 관리,
리눅스 재단의 역사상
가장 빠른 성장

금융, 은행, IoT, 공급망,
의료, 제조, 기술 등을
포괄하는
**글로벌 협업**

10

# 공유 원장 데이터베이스

**블록체인은 여러 다양한 참여기관이 공통의 데이터에 대해서 안전하게 상호작용할 수 있게 합니다.**

### 금융

간소화 된 결제, 유동성 개선, 투명성 강화 및 신제품 / 시장

### 헬스케어

이기종 프로세스 통합, 데이터 흐름 및 유동성 증가, 비용 절감, 환자 경험 및 결과 개선

### 공급망

부품 및 서비스 출처를 추적하고, 제품의 신뢰성을 보장하고, 위조품을 차단하고, 충돌을 줄입니다.

11

# Hyperledger 목표

**비즈니스 블록체인 기술의 시스템 개발을 위해 다양한 접근을 시도하는 오픈소스 프로젝트**

비즈니스 트랜잭션을 지원하기 위한

**엔터프라이즈 레벨, 오픈소스, 분산원장 프레임워크 와 코드베이스**

기술 및 비즈니스 거버전스 지원을 통해

**중립적이고 개방적인 커뮤니티 기반의 인프라 확보**

블록체인 및 공유원장 PoC , 유즈케이스, 파일럿 및 실 업무 적용을 통해

**테크니컬 커뮤니티 구축**

블록체인 기술에 대한 시장의 기회 등

**공개 교육**

수많은 플랫폼과 프레임워크와 함께 툴킷화 함으로

**커뮤니티 영역 확장**

12

# Hyperledger 모듈러 우산 방식

**인프라스트럭처**
**기술, 법, 마케팅, 조직적**
개방형 개발 환경과 상업적 채택을 위한 에코시스템

THE LINUX FOUNDATION

Cloud Foundry | Node.js | **Hyperledger** | Open Container Initiative

**프레임워크**
커뮤니티 공동체에 의해 개발된 비즈니스 블록체인 프레임워크에 대한 차별화된 접근

Hyperledger **Indy** | Hyperledger **Fabric** | Hyperledger **Iroha** | Hyperledger **Sawtooth** | Hyperledger **Burrow**

**도구들**
일반적으로 단일 프로젝트를 위해 개발되었다가 공동 라이센스 및 커뮤니티 공동체 접근 방식에 의해 다른 프레임워크로 포팅

Hyperledger **Quilt** | Hyperledger **Composer** | Hyperledger **Explorer** | Hyperledger **Cello**

13

# Hyperledger 비즈니스 블록체인 프레임워크

- **Hyperledger Fabric**: 모듈형 아키텍처로 응용 프로그램 또는 솔루션을 개발하기위한 토대가되는 Hyperledger Fabric은 합의 및 멤버쉽 서비스와 같은 구성 요소를 플러그 앤 플레이 방식으로 지원
- **Hyperledger Iroha**: 분산 원장 기술을 필요로하는 인프라 프로젝트에 간단하고 쉽게 통합 할 수 있도록 설계된 비즈니스 블록 체인 프레임 워크.
- **Hyperledger Sawtooth**: 분산 원장을 구축,배포,실행하기위한 모듈 방식의 플랫폼. Hyperledger Sawtooth 자원을 최소한으로 소비하면서 대규모로 분산된 합의 노드위 환경을 대상으로하는 합의 알고리즘인 Proof of Elapsed Time(PoET)를 포함
- **Hyperledger Burrow**: 허가형 스마트 컨트랙트 머신. 2014년 12월 최초 릴리즈, Ethereum Virtual Machine(EVM)의 명세를 해석하는 허가형 스마트 컨트랙트와 모듈 방식의 블록체인 클라이언트 제공
- **Hyperledger Indy**: 블록 도메인 또는 다른 분산 원장을 기반으로하는 디지털 ID를 제공하기위한 도구, 라이브러리 및 재사용 가능한 구성으로, 관리 도메인, 응용 프로그램 및 기타 모든 블록체인 프레임워크에서 상호 운용 가능

14

# Hyperledger 기술적 범위

| Out of Scope | 커스텀 애플리케이션 | 애플리케이션 레이어 |
|---|---|---|
| In Scope | API 라이브러리와 GUIs<br>합의 알고리즘<br>멤버쉽 정책<br>게이트웨어<br>운영 대시보드 | 부가 기능 |
| | Core APIs | Core APIs |
| | 코드 실행 환경<br>원장 데이터 구조<br>모듈방식의 합의 알고리즘<br>모듈 방식의 인증 서비스<br>블록체인 노드(피어) | 공유 원장 |

15

# Hyperledger 모멘텀

**190+**
멤버
(30+ 이상이 중국)

**9**
Hyperledger
프로젝트

**1**
제품 릴리즈
**Hyperledger Fabric v1.0**

**3.6M+**
코드 라인수

**49K+**
첫번째 Edx 과정
등록자

Hosted the most popular webinar in history of The Linux Foundation on Hyperledger Fabric v1.0

**91**
밋업

**25K+**
밋업 참여자

**35K+**
트위터 팔로워

**1.5K+**
매스컴에 의해
소개된 평균 횟수
(2017)

16

# Hyperledger 멤버

Premier

Source: https://www.hyperledger.org/members
Updated: 26 January 2018

General

General

Associate

7

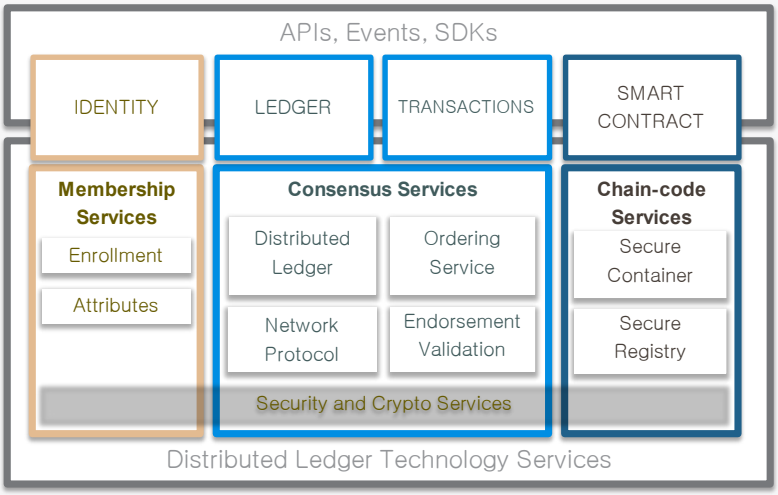
# Hyperledger Fabric

Business Blockchain Framework

- Hyperledger 에 기부된 첫번째 프로젝트
- Digital Asset 과 IBM에 의해 기부
- Golang(v1.1 부터 자바스크립트 지원)으로 작성되는 "체인코드라고 부르는 스마트 계약과 보안이 확보된 도커 컨테이너에서 구동되는 환경
- 트랜잭션에 포함된 참여자들만 거래 가능한 채널 지원

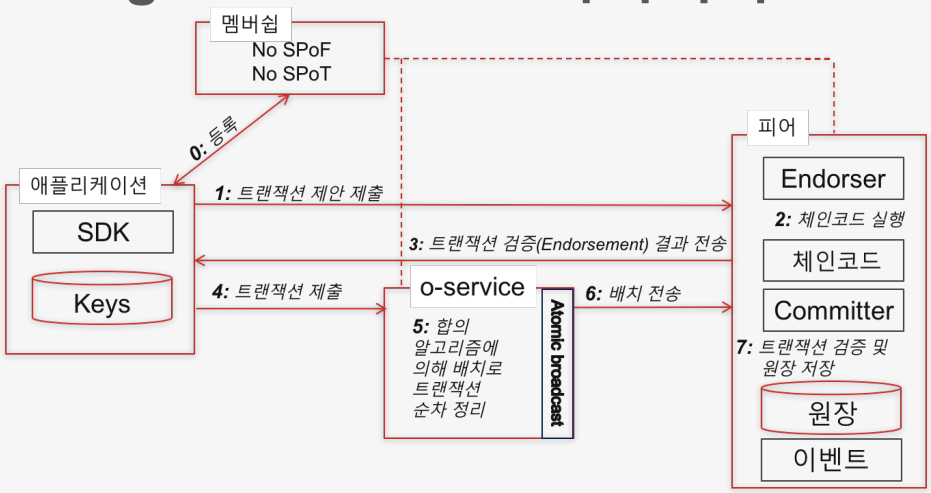
18

# Hyperledger Fabric 아키텍처




19

# Hyperledger Fabric v1.0 아키텍처




20

# 감사합니다.

21

The 24th Network Security Conference -Korea

# 스마트카 보안의 현안과 기술 방향

**심상규** 펜타시큐리티 소장

### 학력 및 경력사항

| | |
|---|---|
| 1996 | 포항공과대학교(POSTECH) 전자전기공학과 학사 |
| 1998 | 포항공과대학교(POSTECH) 전자전기공학과 석사 |
| 2004 | 포항공과대학교(POSTECH) 전자전기공학과 박사 |
| 2004.01 ~ 2005.01 | 펜타시큐리티시스템 과장 |
| 2005.02 ~ 2008.04 | 삼성전자 SW연구소 책임연구원 |
| 2008.06 ~ 2010.08 | 위디랩(WIDI Lab.) 수석연구원 |
| 2010.10 ~ 2011.05 | 하우스컨설팅(How's Consulting) 이사 |
| 2011.06 ~ 2011.11 | 넥스토모(nextomo) 이사 |
| 2012.01 ~ 현재 | 펜타시큐리티시스템 이사 |
| 2014.03 ~ 2016.02 | 순천향대학교 융합서비스보안학과 겸임교수 |
| 2016.03 ~ 2017.02 | 동덕여자대학교 컴퓨터학과 겸임교수 |
| 2015.04 ~ 현재 | 펜타시큐리티시스템 IoT융합보안연구소 소장 |

### 강연요약

자동차가 점차 지능화되어 Smart Car로 변화해 가는 것은 자동차가 Connected Car로서 외부통신 연결 기능을 갖는다는 것에서 시작된다. 자동차가 외부통신 기능을 갖기 시작하면서 자동차는 다양한 보안 문제에 직면하고 있으며, 기존 IT환경과는 달리 자동차에서의 보안 문제는 탑승자의 생명을 위협하는 문제이기 때문에 매우 중요하다. 본 강연에서는 안전한 connected car 환경의 확보를 위해 고려되어야 하는 보안 위협과 이에 대응하는 보안기술들을 다양한 시각에서 살펴 본다.

Penta SECURITY

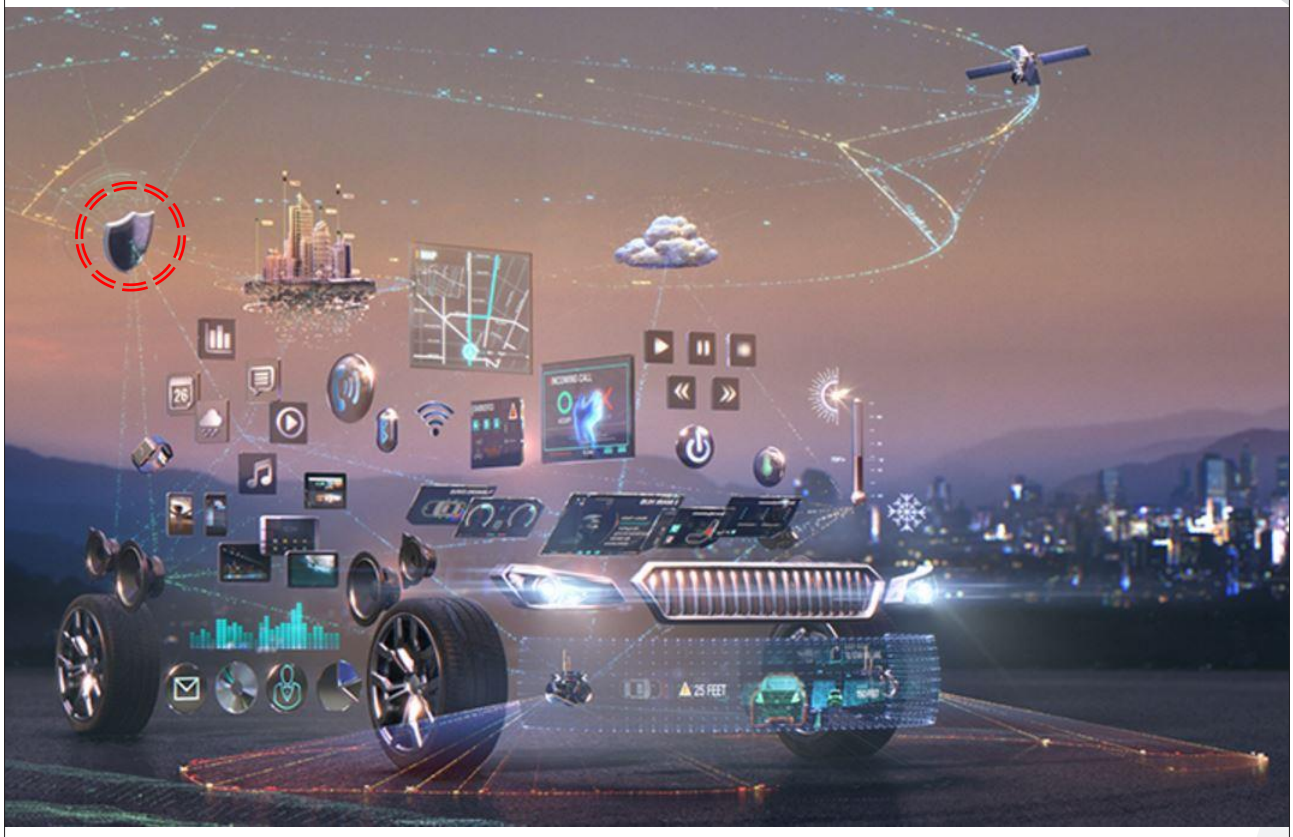
Penta SECURITY
cloud · iot · enterprise

# 스마트카 보안의 현안과 기술 방향

April 12, 2018

SangGyoo SIM, Ph.D
(sgsim@pentasecurity.com)
Head of Penta IoT Convergence Lab.

5 Public

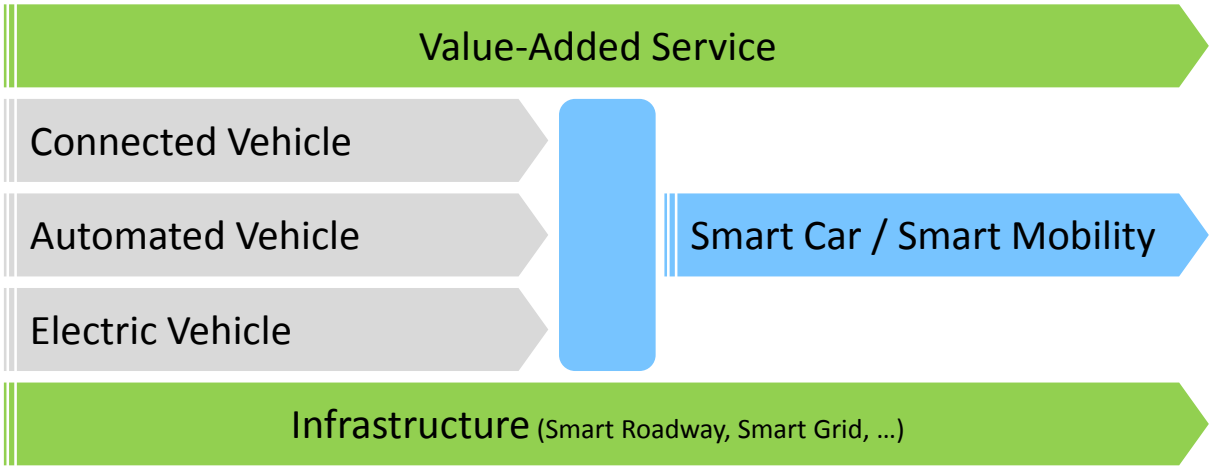


http://www.rcrwireless.com/connected-cars-2/harman-connected-car-services-trends-tag6-tag99



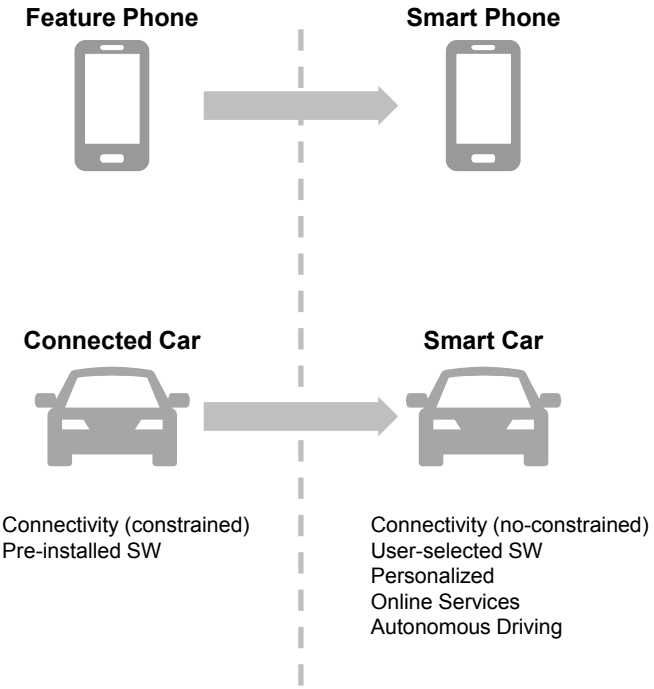
5 Public

## Evolution toward Smart Car

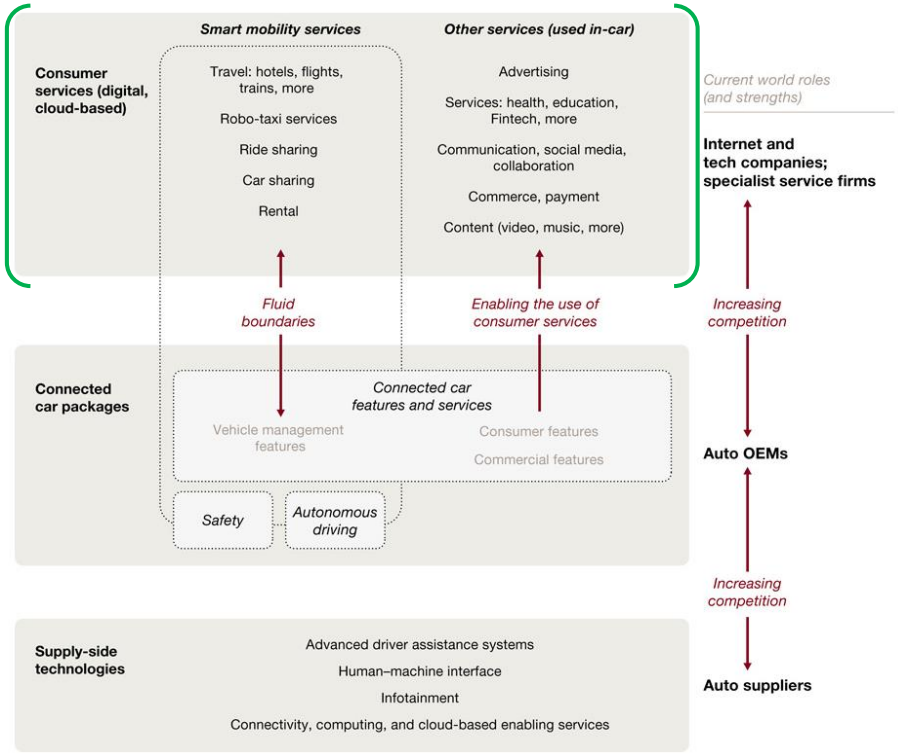





## "Cars are mobile devices."



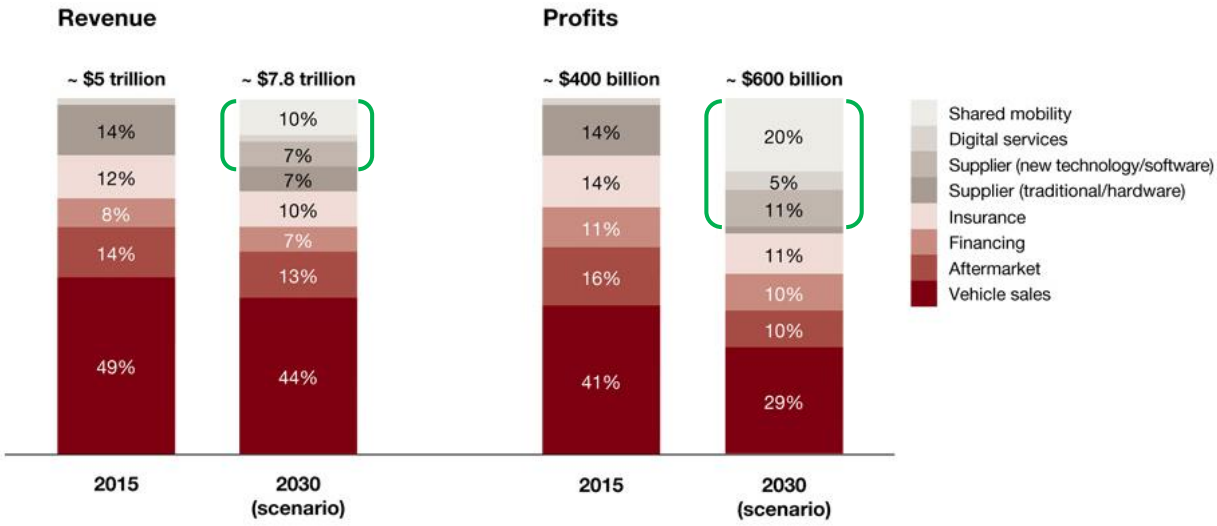
## Connected Car Technologies & Services




https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)



## Value Shifts in the Auto Industry, 2015-2030




Share addressable by today's OEM model declining to less than 70%

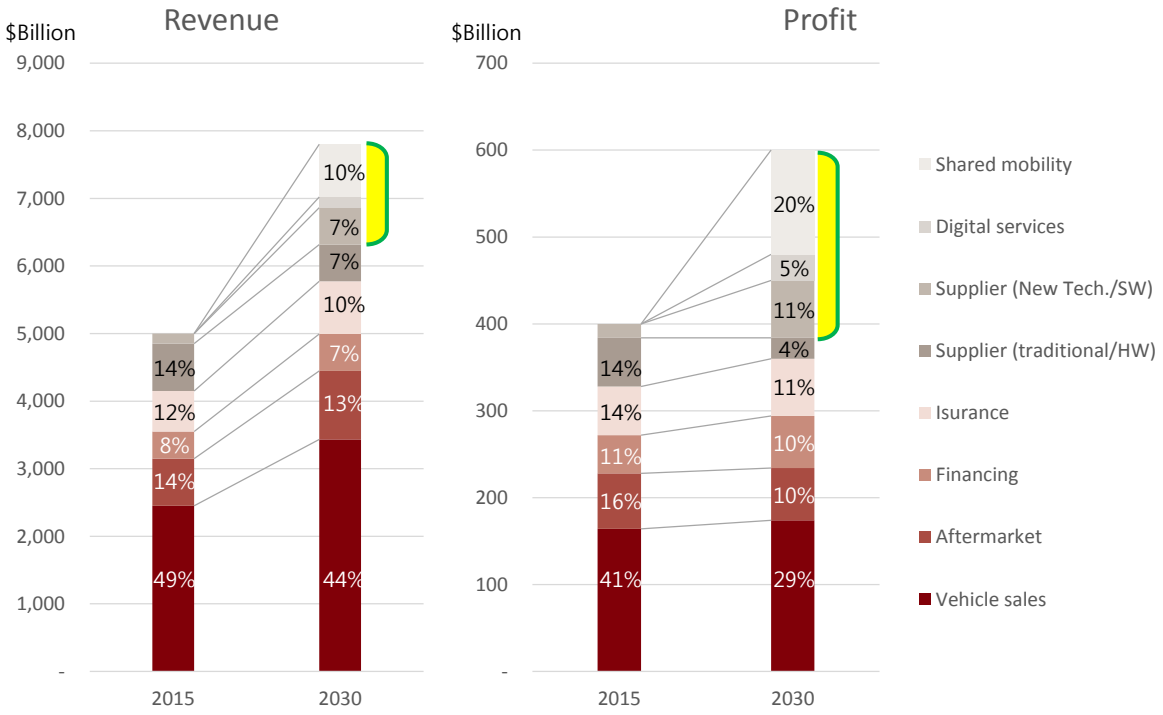
Share addressable by new entrants (digital services, mobility, new technology supply, Fintech, startup EV players) growing to more than 45% or $3.5 trillion

Share addressable by OEM declining from ~70% to less than 50%

Share that can be captured by new entrants growing to 60% or $360 billion

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)

## Value Shifts in the Auto Industry, 2015-2030

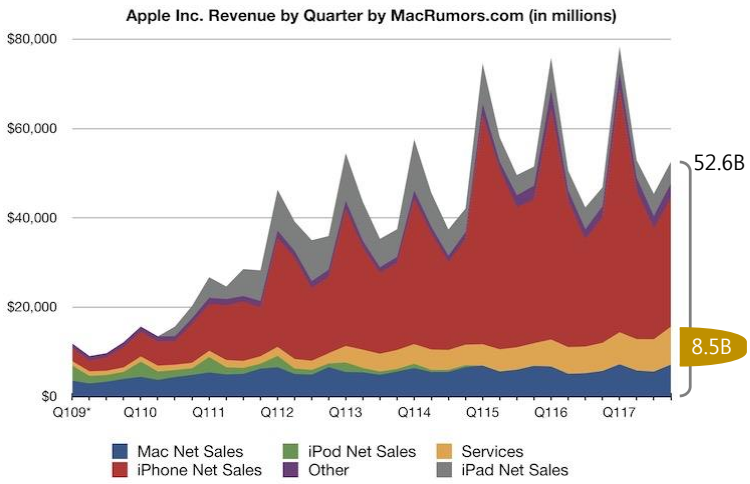


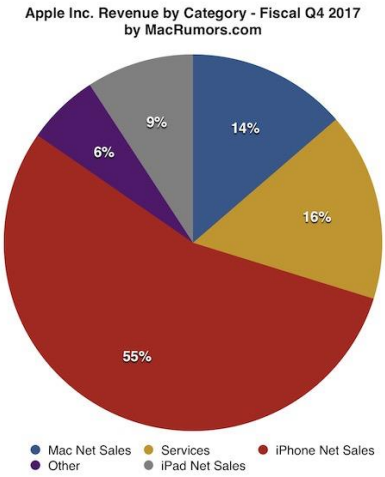

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)



Public

## Service Business : The Case of Apple



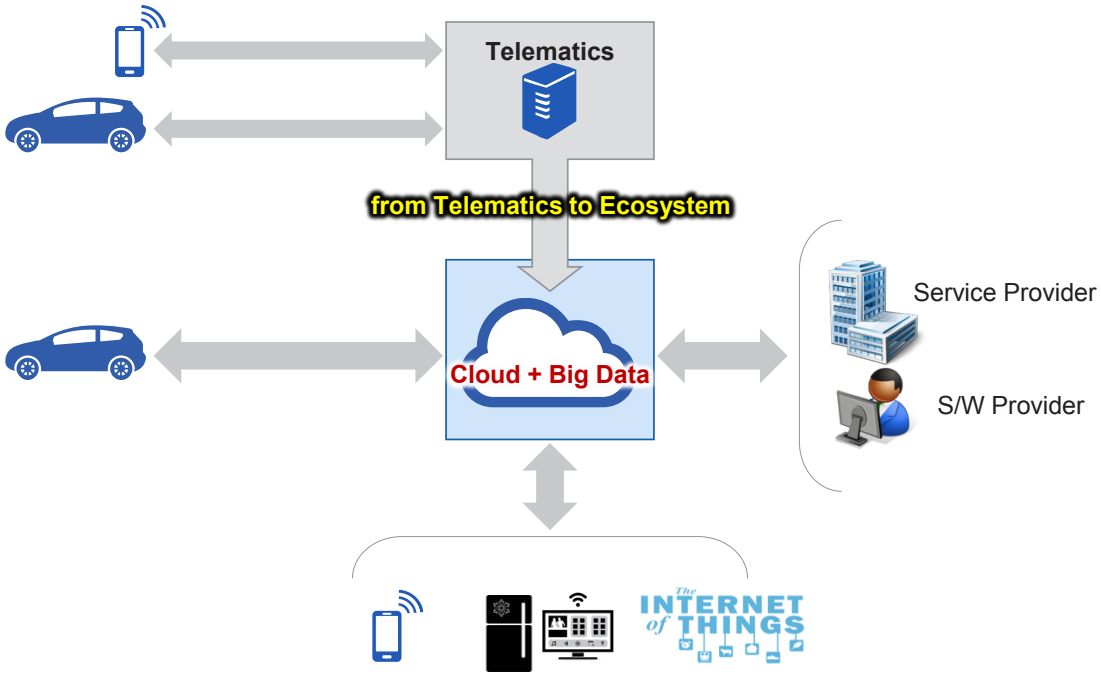




https://www.macrumors.com/2017/11/02/earnings-4q-2017/



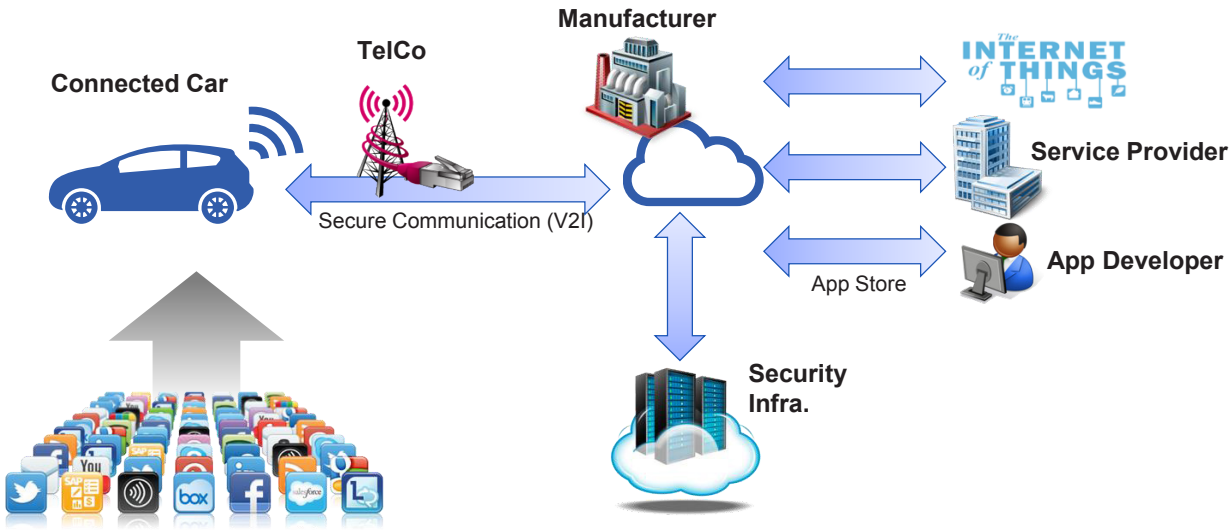
Public

## Viewpoint of Manufacturers

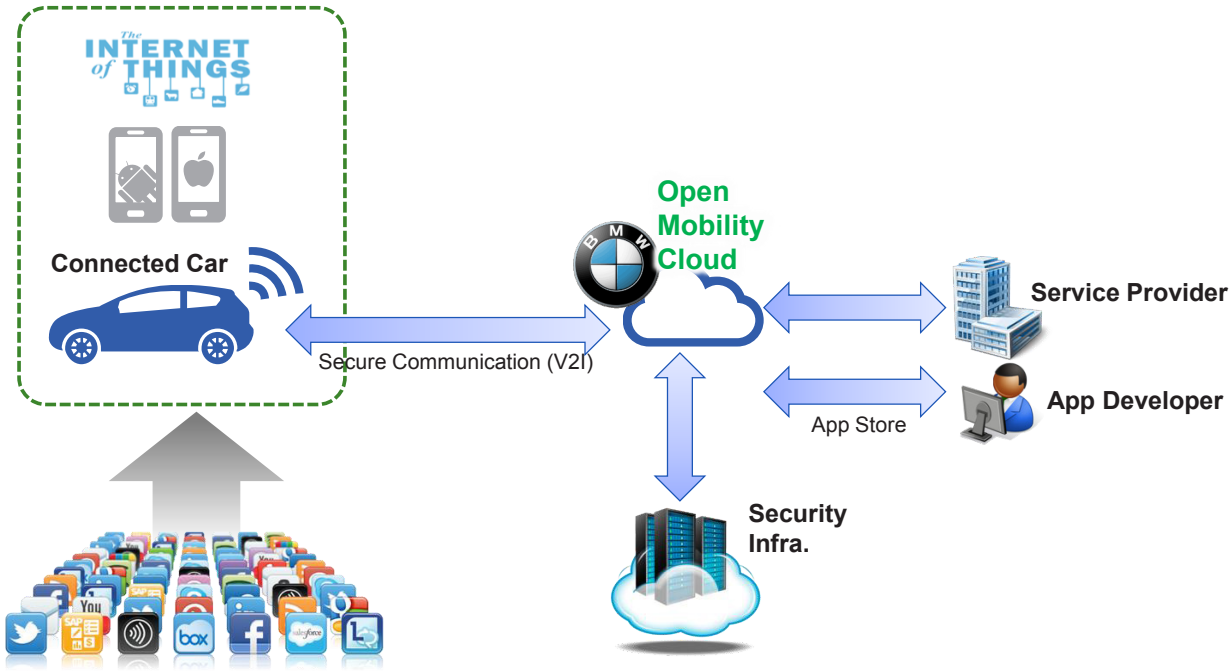





## Future Biz of Manufacturers

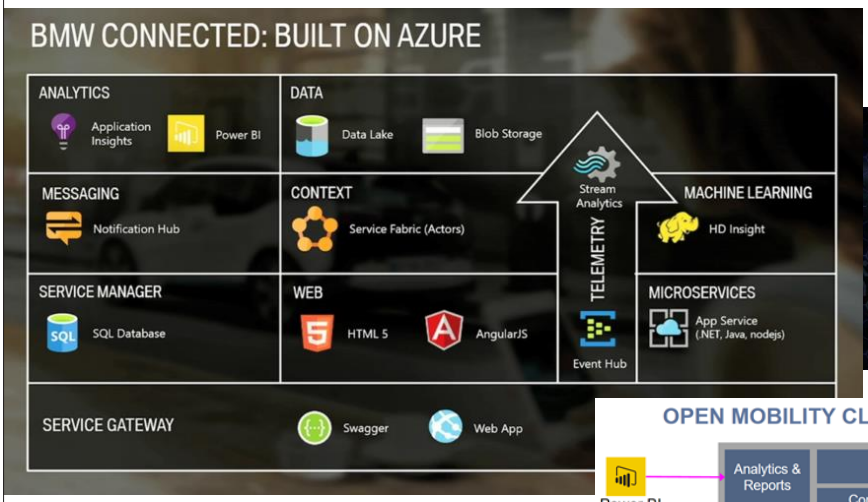


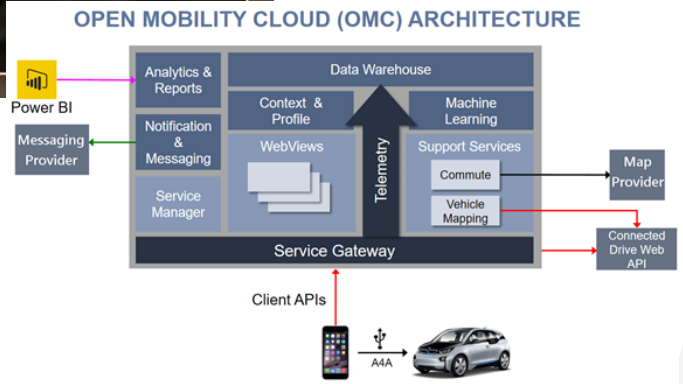
## Future Biz of Manufacturers - BMW





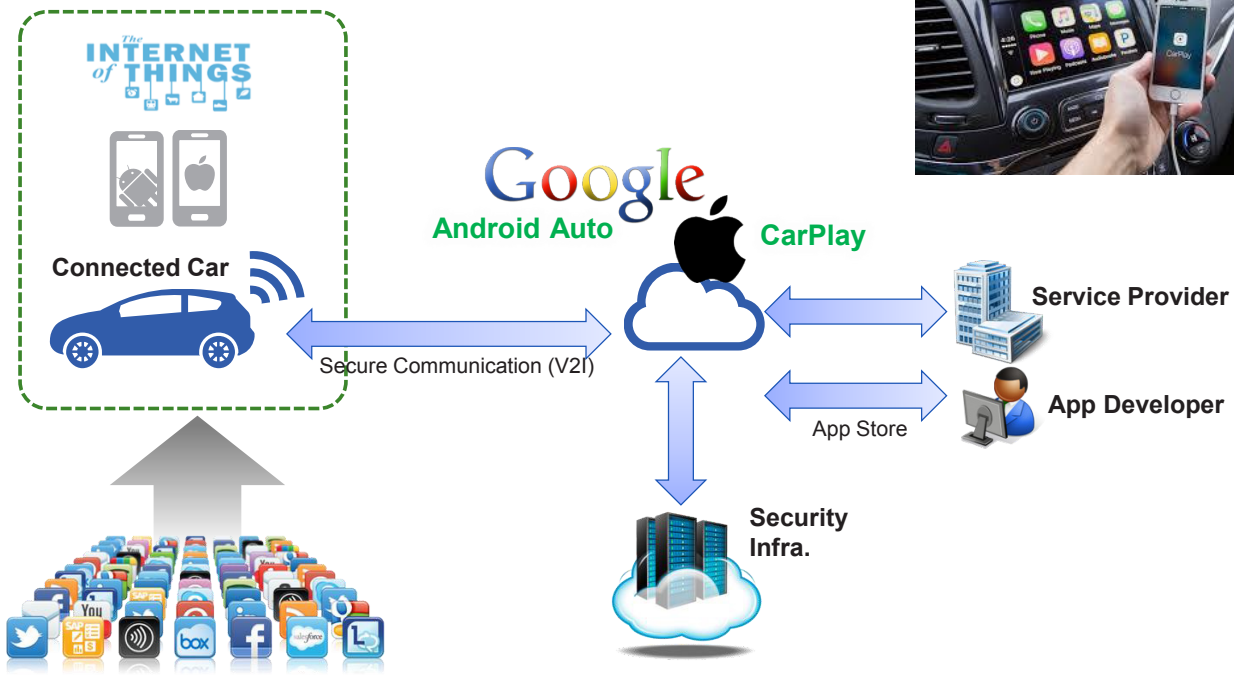

## Future Biz of Manufacturers - BMW






https://www.infoq.com/news/2016/04/Azure-Service-Fabric-GA
https://blogs.msdn.microsoft.com/azureservicefabric/2016/08/24/service-fabric-customer-profile-bmw-technology-corporation/

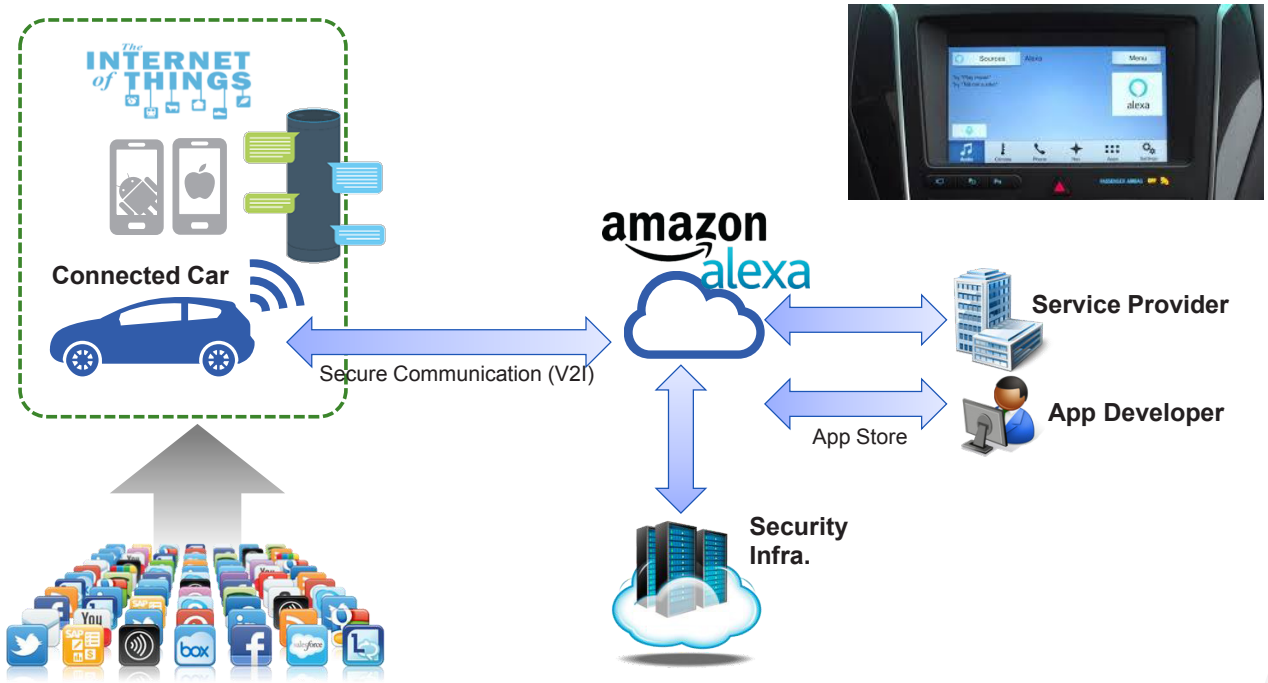
## View from Platform Venders



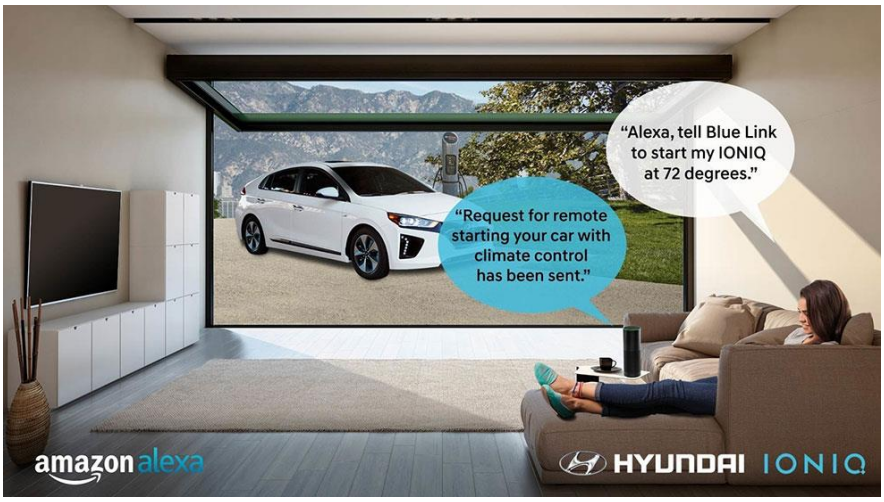



## View from Platform Venders





## Amazon Alexa



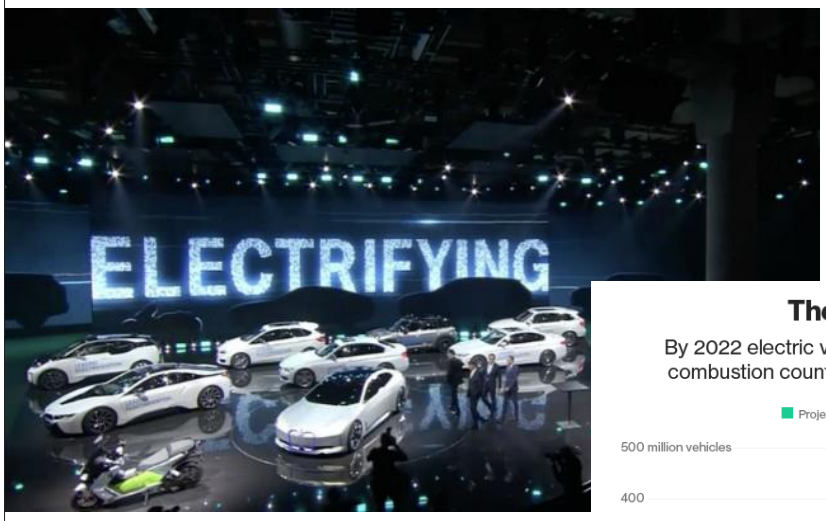

https://www.slashgear.com/hyundai-ioniq-blue-link-supports-amazon-alexa-voice-commands-17464449/



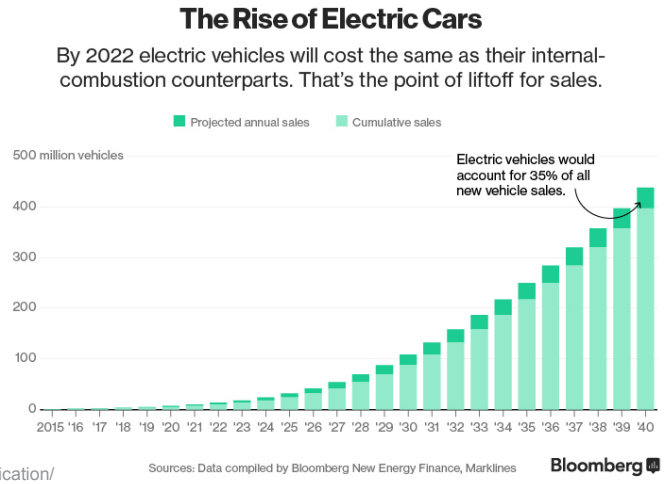
## Trend Keywords for Smart Cars

https://www.csis.org/analysis/implications-ultra-low-cost-access-space

## Trend Keywords : Electrification



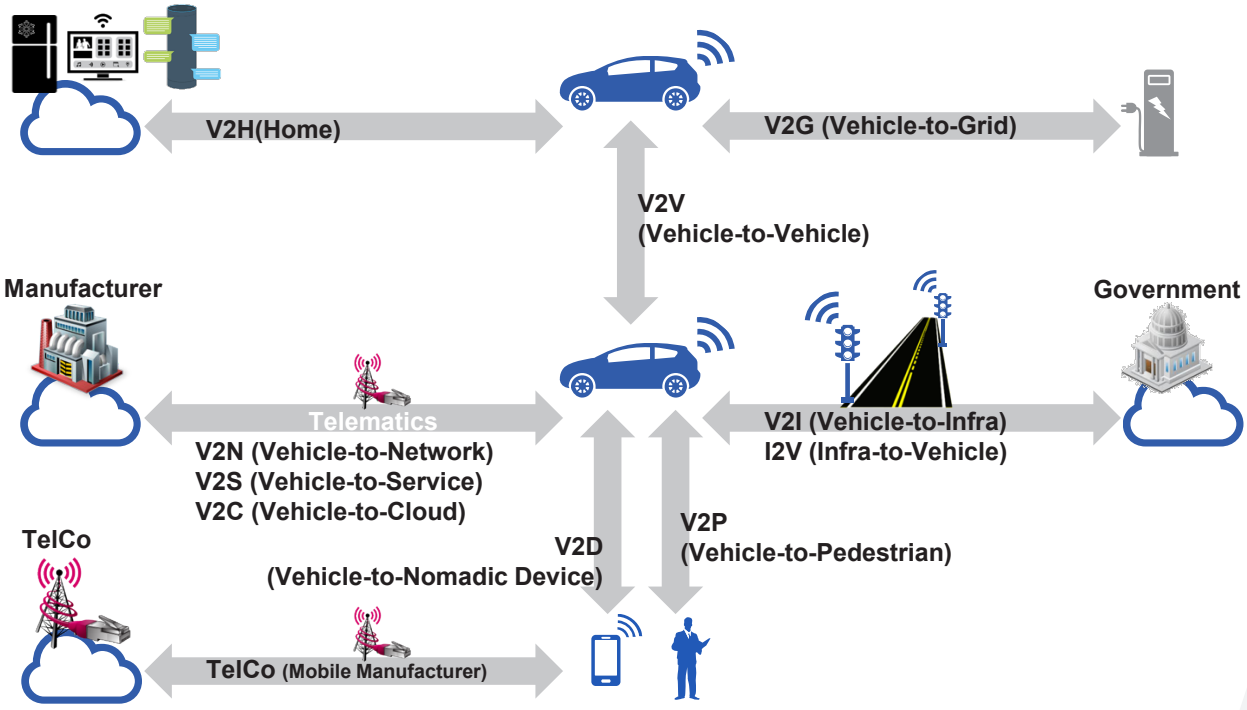

Electric vehicles would account for **35%** of all new vehicle sales.




https://www.carmudi.com.ph/journal/carmakers-brace-mass-vehicle-electrification/
https://www.bloomberg.com/features/2016-ev-oil-crisis/

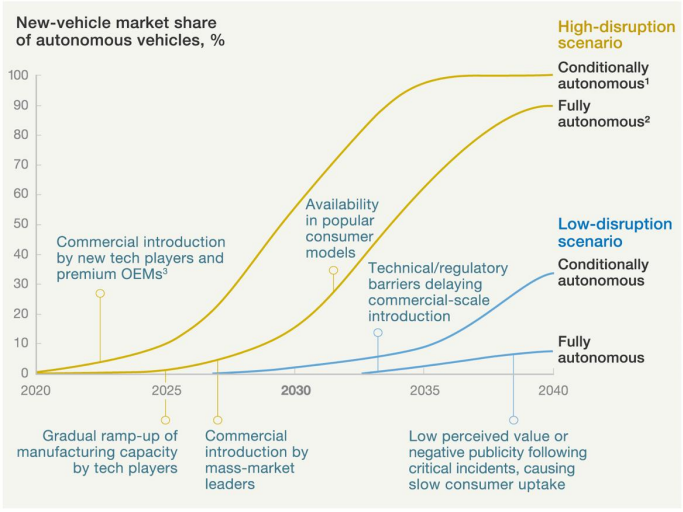


## Trend Keywords : Connectivity



## Trend Keywords : Autonomous

How many new cars may be fully autonomous by 2030?




| Factors in disruption scenarios | High disruption | Low disruption |
|---|---|---|
| Regulatory challenges | Fast | Gradual |
| Safe, reliable technical solutions | Comprehensive | Incomplete |
| Consumer acceptance, willingness to pay | Enthusiastic | Limited |

[1]Conditionally autonomous car: the driver may take occasional control.
[2]Fully autonomous car: the vehicle is in full control.
[3]Original-equipment manufacturers.

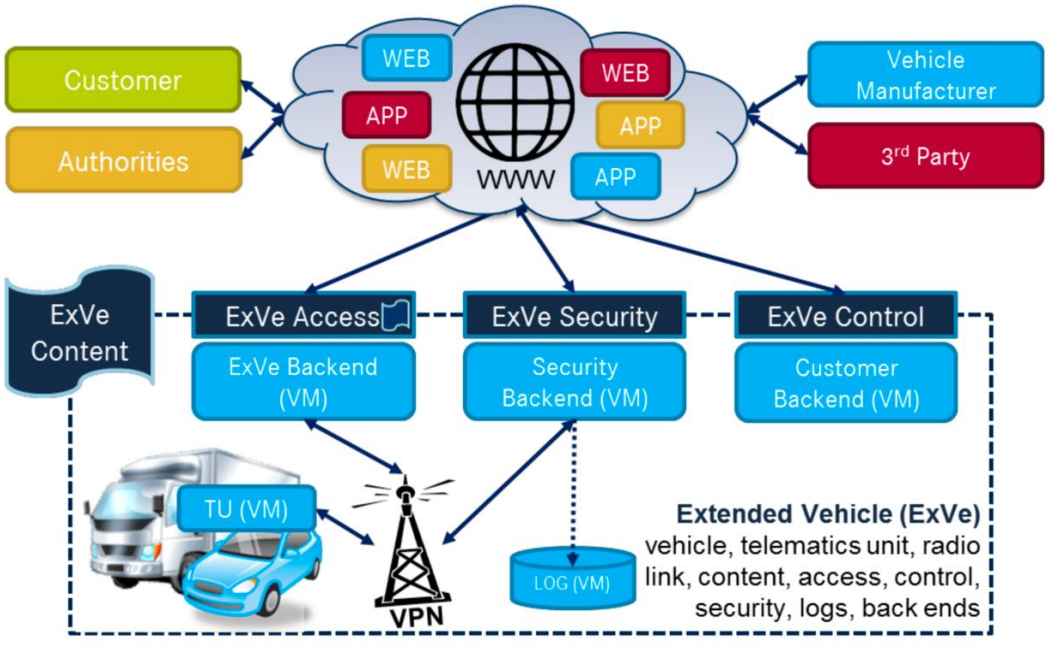
McKinsey&Company

https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry



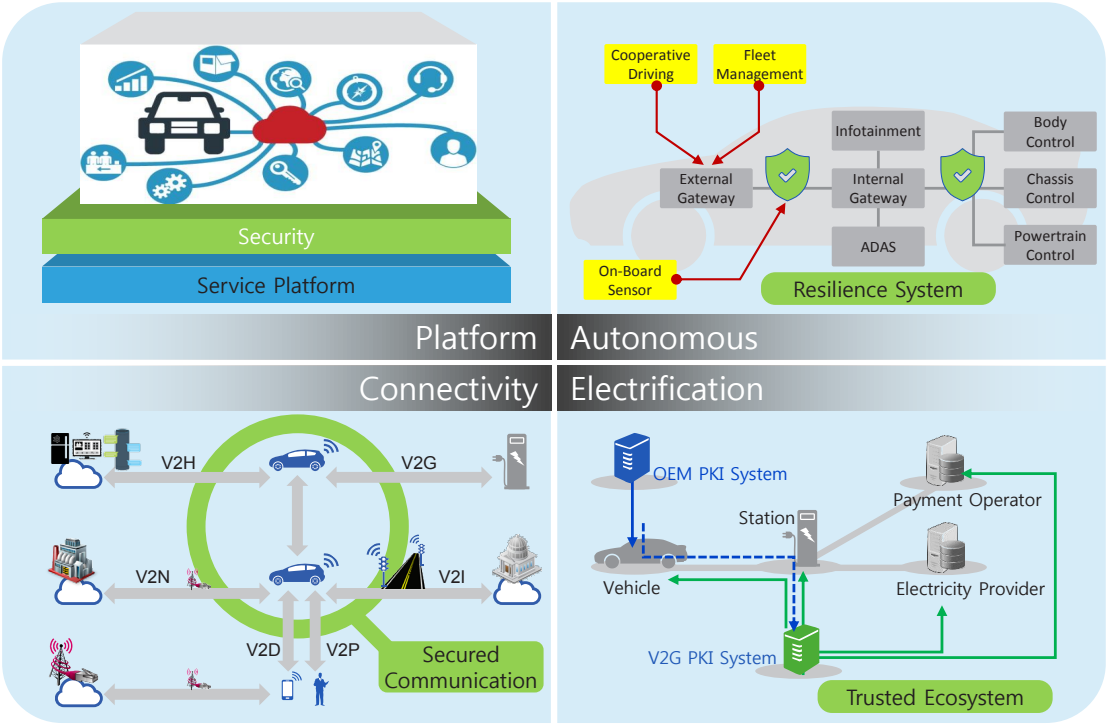
## Trend Keywords : Platform

ISO 20077, ISO 20078 – Road Vehicles – Extended vehicle (ExVe)



## Trend Keywords : Security

## "Secure First"



## "SPY CAR" (Security and Privacy in Your Car) Act (2015.07, US)

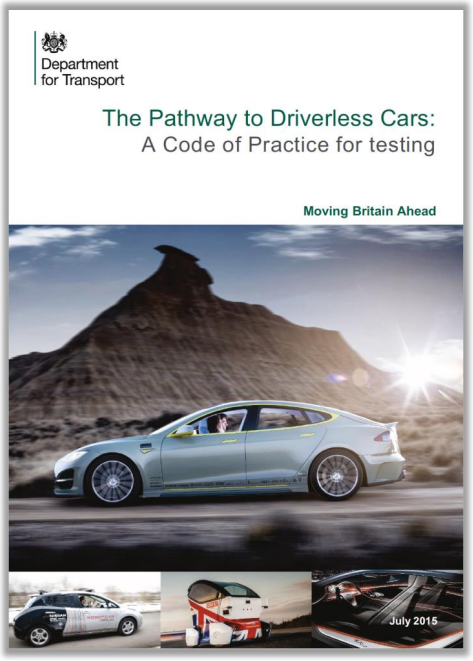
- I. Cybersecurity Standards
  - **Hacking protection**: all access points in the car should be equipped with reasonable measures to protect against hacking attacks, including isolation of critical software systems and evaluated using best security practices, such as penetration testing;
  - **Data security**: all collected information should be secured to prevent unwanted access—while stored on-board, in transit, and stored off-board; and
  - **Hacking mitigation**: the vehicle should be equipped with technology that can detect, report and stop hacking attempts in real-time.
- II: Privacy standards
  - **Transparency**: owners are made explicitly aware of collection, transmission, retention, and use of driving data;
  - **Consumer choice**: owners are able to opt out of data collection and retention without losing access to key navigation or other features (when technically feasible), except for in the case of electronic data recorders or other safety or regulatory systems; and
  - **Marketing prohibition**: personal driving information may not be used for advertising or marketing purposes without the owner clearly opting in.
- III: Cyber dashboard

NHTSA, in consultation with FTC, should establish a **"cyber dashboard"** that displays an evaluation of how well each automobile protects both the security and privacy of vehicle owners beyond those minimum standards. This information should be presented in a transparent, consumer-friendly form on the window sticker of all new vehicles.

http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system



## "The Pathway to Driverless Cars" (2015.07, UK)




https://www.gov.uk/government/publications/automated-vehicle-technologies-testing-code-of-practice

## "The Pathway to Driverless Cars" (2015.07, UK)

1. Introduction
2. Aim, scope and definitions
3. General requirements
   - Safety requirements, Insurance, Infrastructure and transport Authorities, Engagement
4. Test driver, operator and assistant requirements
   - Requirements for a test driver, License requirements, Test driver or operator training
   - Test driver hours, Test driver/operator behavior, Test assistants
5. Vehicle requirements
   A. General vehicle requirements
   B. Maturity of technologies under test
   C. Data recording
   D. Data protection
   E. Cyber security
   F. Process for transition between automated and manual modes
   G. Failure warning
   H. Software levels



## Data Recording

- 5.6 Automated vehicles under test should be fitted with a data recording device which is capable of capturing data from the sensor and control systems associated with the automated features as well as other information concerning the vehicle's movement.
- 5.7 As a minimum this device should record the following information (preferably at 10Hz or more):
  - Whether the vehicle is operating in manual or automated mode
  - Vehicle speed
  - Steering command and activation
  - Braking command and activation
  - Operation of the vehicle's lights and indicators
  - Use of the vehicle's audible warning system (horn)
  - Sensor data concerning the presence of other road users or objects in the vehicle's vicinity
  - Remote commands which may influence the vehicle's movement (if applicable)
- 5.8 This data should be able to be used to determine who or what was controlling the vehicle at the time of an incident. The data should be securely stored and should be provided to the relevant authorities upon request. It is expected that testing organizations will cooperate fully with the relevant authorities in the event of an investigation.
- 5.9 In addition, testers may wish to consider fitting vehicles under test with a video and audio recording system. However this should not be considered as an alternative to the data recording requirements specified in paragraph 5.7.

## Data Protection

- 5.10 Testing is likely to involve the processing of personal data. For example, if data is collected and analyzed about the behavior or location of individuals in the vehicle, such as test drivers, operators and assistants, and those individuals can be identified, this will amount to the processing of personal data under the Data Protection Act 1998. The project team must therefore ensure that the data protection legislation is complied with, including the requirements that the personal data is used fairly and lawfully, kept securely and for no longer than necessary.
- 5.11 Guidance for organizations on complying with the data protection laws can be found on the Information Commissioner's Office's website. We recommend that projects consider whether to undertake a privacy impact assessment as described in the Information Commissioner's Office's Code of Practice.
  - Information Commissioner's Office, Guide to data protection
    - https://ico.org.uk/for-organisations/guide-to-data-protection
  - Information Commissioner's Office, Conducting Privacy Impact Assessments – Code of Practice
    - https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- 5.12 Undertaking a privacy impact assessment is not a legal requirement, but is a useful tool to help a project comply with the data protection laws. As recognized in the Information Commissioner's Office's Code of Practice, the privacy impact assessment can be developed flexibly and proportionately, depending on how complex or straightforward the privacy issues are for a particular project.



## Cyber Security

- 5.13 As has already been stated in Chapter 4, a requirement for testing is that a test driver or operator oversees the movements of the vehicle under test and is capable of implementing a manual over-ride at any time.
- 5.14 Nevertheless, manufacturers providing vehicles, and other organizations supplying parts for testing will need to ensure that all prototype automated controllers and other vehicle systems have appropriate levels of security built into them to manage any risk of unauthorized access.
- 5.15 Testing organizations should consider adopting the security principles set out in *BSI PAS754 Software Trustworthiness - Governance and management - Specification* or an equivalent.
  - the overall principles for effective software trustworthiness, and includes technical, physical, cultural and behavioral measures alongside effective leadership and governance.
  - five aspects of software trustworthiness: *Safety, reliability, availability, resilience and security*
  - https://shop.bsigroup.com/ProductDetail/?pid=000000000030284608

## Declaration of Amsterdam (2016.04, EU)

https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam



## Declaration of Amsterdam (2016.04, EU) - Joint Agenda

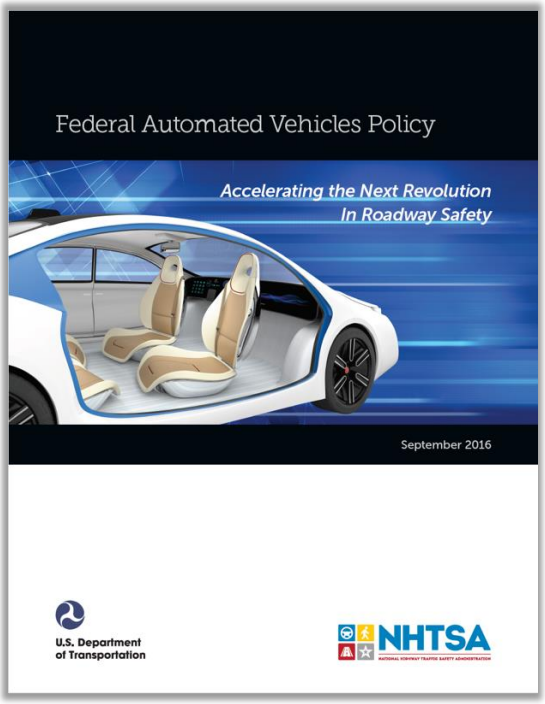
- a. Coherent international, European and national rules
  - The aim is to work towards the removal of barriers and to promote legal consistency. The legal framework should offer sufficient flexibility to accommodate innovation, facilitate the introduction of connected and automated vehicles on the market and enable their cross-border use.
- b. Use of data
  - Data generated through the use of connected and automated vehicles **can serve public and private value-added services**. Clarification is needed on the availability for public and private use and responsibilities of the parties involved.
- c. Ensure privacy and data protection
  - Respecting existing legislation on **privacy and data protection**, the conditions for the (re-) use and sharing of data generated by connected and automated vehicles need to be clarified.
- d. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication
  - In order to maximize benefits in road safety and environmental performance, it is essential to ensure that new services and systems are **compatible and interoperable at European level** and to coordinate investments towards reliable communication coverage, exploit the full potential of hybrid communications, where relevant, and improve the performance of location accuracy, benefiting in particular from the use of GALILEO and EGNOS.

## Declaration of Amsterdam (2016.04, EU) - Joint Agenda

- e. Security
  - In the light of the increase in cyber-threats and serious vulnerabilities, it is essential to ensure security and reliability of connected and automated vehicle communications and systems. **Common trust models and certification policies** should be developed to prevent risks and support cybersecurity, whilst ensuring safe and interoperable deployment.
- f. Public awareness and acceptance
  - It is important to manage societal expectations, to raise awareness and increase acceptance and appreciation of connected and automated vehicle technologies.
- g. Common definitions of connected and automated driving
  - Common definitions of connected and automated driving should be developed and updated, based on the Society of Automotive Engineering levels (SAE levels) as a starting point.
- h. International cooperation
  - It is important to develop and maintain close cooperation with other regions, particularly the US and Japan, to work towards a global framework and international standards for connected and automated vehicles.

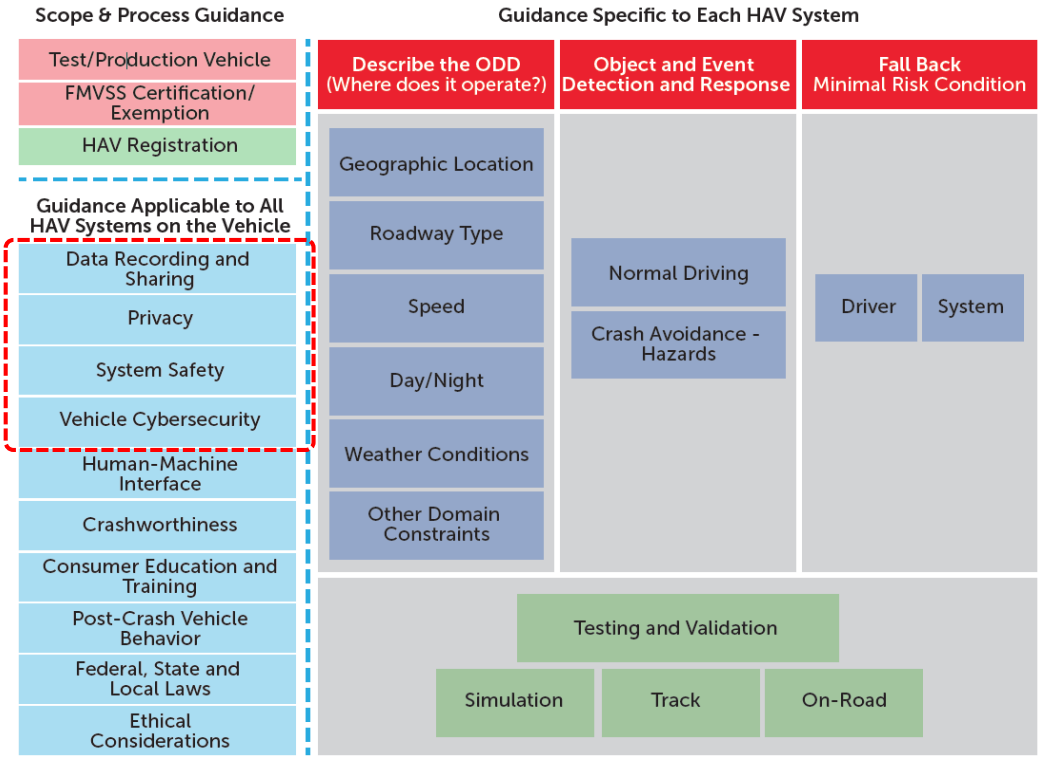


## "Federal Automated Vehicles Policy" (2016.09, US)



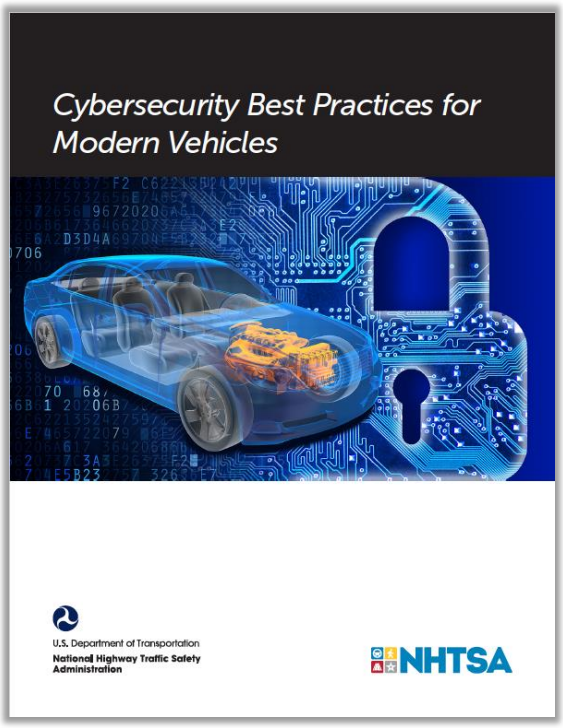

https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016/

## "Federal Automated Vehicles Policy (2016.09, US)






## Cybersecurity Best Practices (2016.10, US)



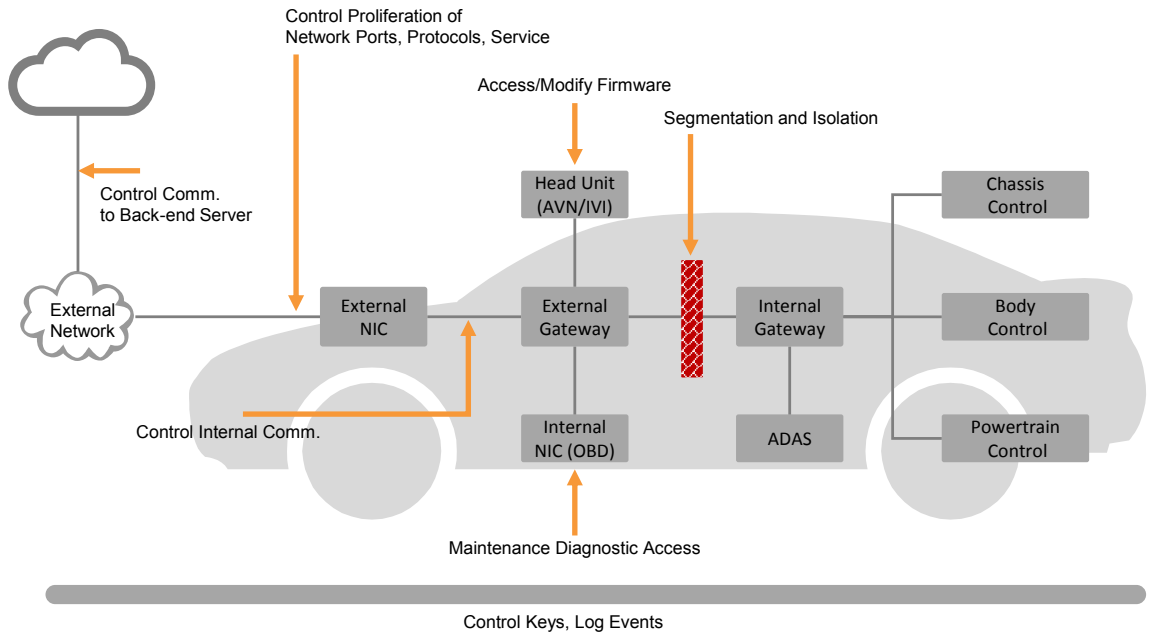

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

## Cybersecurity Best Practices (2016.10, US)

- Self-Auditing
  - Risk Assessment
  - Penetration Testing and Documentation
  - Self-Review
- Fundamental Vehicle Cybersecurity Protections
  - Limit Developer/Debugging Access in Production Devices
  - Control Keys
  - Control Vehicle Maintenance Diagnostic Access
  - Control Access to Firmware
  - Limit Ability to Modify Firmware
  - Control Proliferation of Network Ports, Protocols and Services
  - Use Segmentation and Isolation Techniques in Vehicle Architecture Design
  - Control Internal Vehicle Communications
  - Log Events
  - Control Communication to Back-End Servers
  - Control Wireless Interfaces



## Cybersecurity Best Practices (2016.10, US)

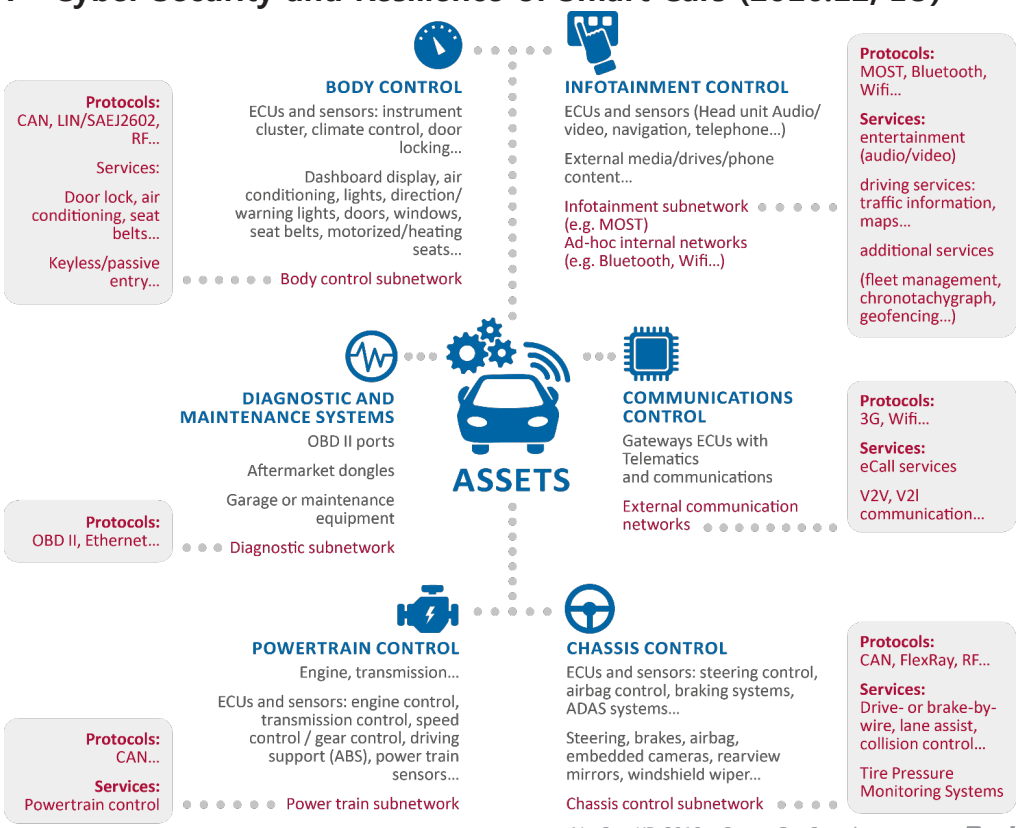


## ENISA – Cyber Security and Resilience of Smart Cars (2016.12, EU)

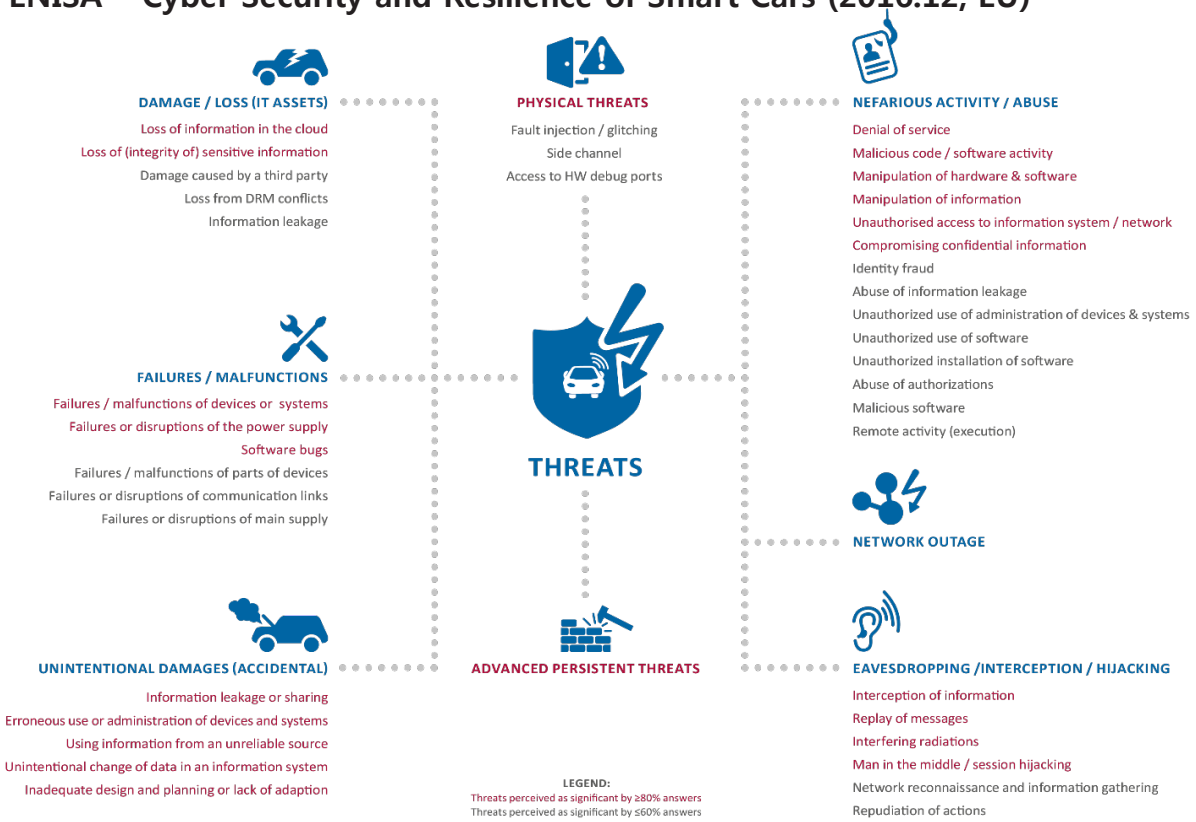
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/



## ENISA – Cyber Security and Resilience of Smart Cars (2016.12, EU)



## ENISA – Cyber Security and Resilience of Smart Cars (2016.12, EU)






## "SPY CAR" (Security and Privacy in Your Car) Act (2017.03, US)

- I. Cybersecurity Standards
  - Protection against Hacking : equipped with reasonable measures to protect against hacking attacks.
    - Isolation Measures : to separate critical software systems from noncritical software systems.
    - Evaluation : evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.
    - Adjustment : adjusted and updated based on the results of the evaluation
  - Security of Collected Information
    - All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access – (a) stored onboard, (b) transit to another location, and (c) offboard storage or use.
  - Detection, Reporting, and Responding to Hacking
    - Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.
- II. Cyber Dashboard
  - inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements.
- III. Privacy Standards for Motor Vehicles
  - Cont'd

https://www.congress.gov/bill/115th-congress/senate-bill/680

## "SPY CAR" (Security and Privacy in Your Car) Act (2017.03, US)

- III. Privacy Standards for Motor Vehicles
  - Transparency : Each motor vehicle shall provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle.
  - Consumer Control : the option of terminating the collection and retention of driving data.
  - Access to Navigation Tools : If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data, the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.
  - Exception : not apply to driving data stored as part of the electronic data recorder system or other safety systems on board the motor vehicle that are required for post incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.
  - Limitation on Use of Personal Driving Information
    - A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.
      - ✓ Consent requests shall be clear and conspicuous.
      - ✓ Consent requests shall be made in clear and plain language.
      - ✓ Consent requests may not be be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.

https://www.congress.gov/bill/115th-congress/senate-bill/680



## The Key Principles of Cyber Security (2017.09, UK)

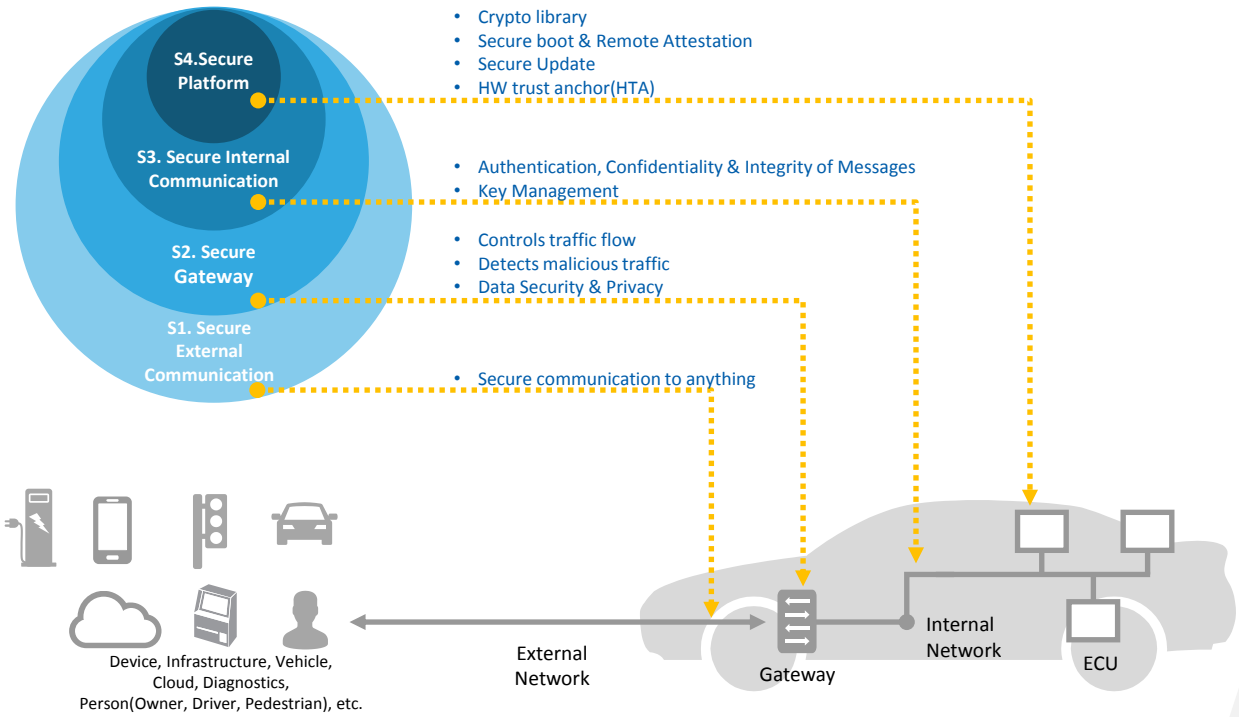
https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

## The Key Principles of Cyber Security (2017.09, UK)

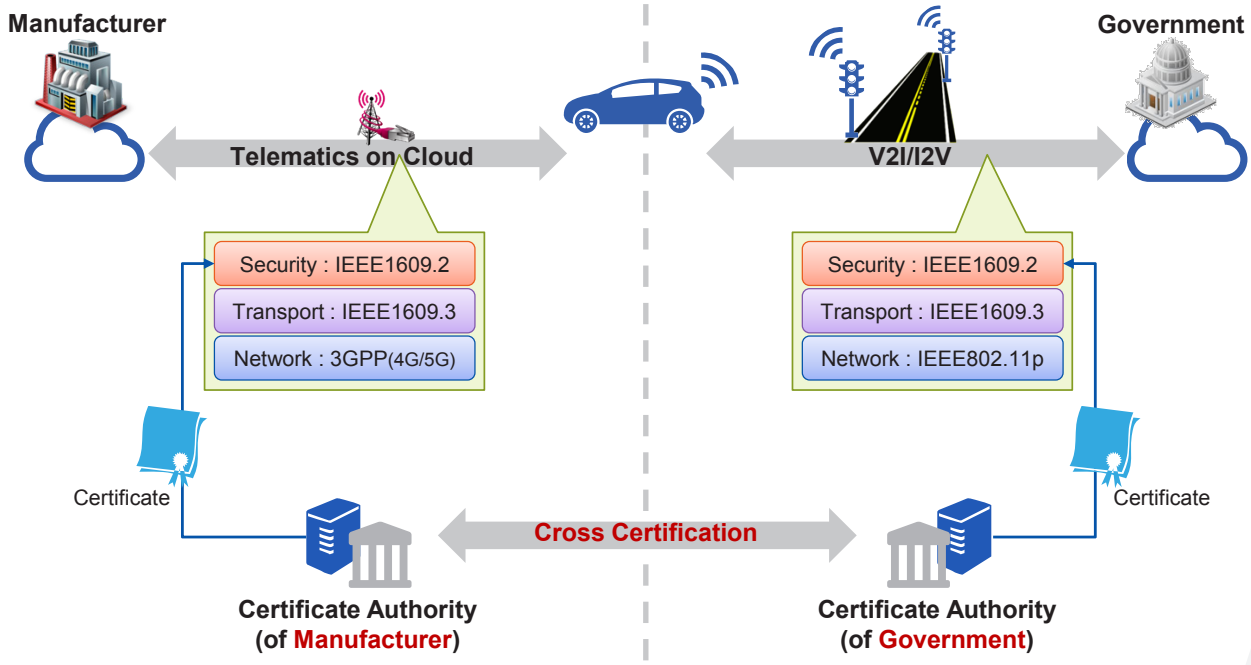
- Intelligent Transport System & Connected and Automated Vehicle – System Security
  - 1. Organizational security is owned, governed and promoted at board level.
    - 1.4 All new designs embrace Security by Design.
  - 2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.
  - 3. Organizations need product aftercare and incident response to ensure systems are secure over their lifetime.
- ITS/CAV System Design
  - 4. All organizations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.
    - Provide assurance… authenticity and origin of all supplies… safely and securely interact with external devices…
      manage external dependencies
  - 5. Systems are designed using a defense-in-depth approach.
    - Not rely on single points of failure… defense-in-depth & segmented… design controls to mediate transactions across trust boundaries… remote and back-end systems…
  - 6. The security of all software is managed throughout its lifetime.
    - Secure coding practices… ascertain the status of all SW… safely and securely update SW… open design practices…
  - 7. The storage and transmission of data is secure and can be controlled.
    - Confidentiality and integrity… personally identifiable data… "Users are able to delete sensitive data"
  - 8. The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail.
    - withstand receiving corrupt, invalid or malicious data or commands… resilient and fail-safe



## Cybersecurity Concept for Connected Car



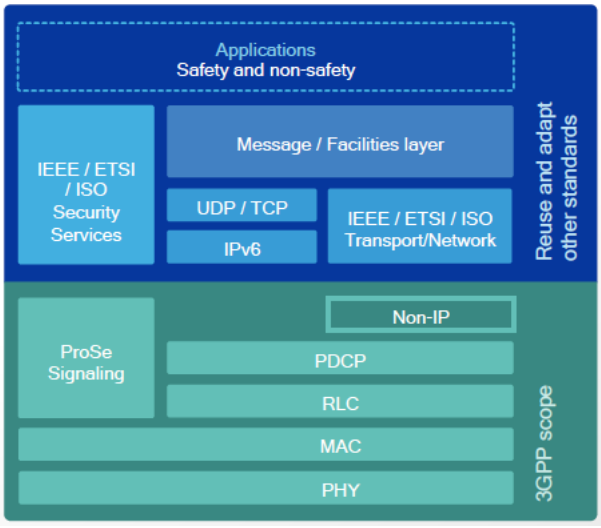
## S1. Secure External Communication






## IEEE 1609.x in C-V2X

### C-V2X reuses upper layers defined by automotive industry

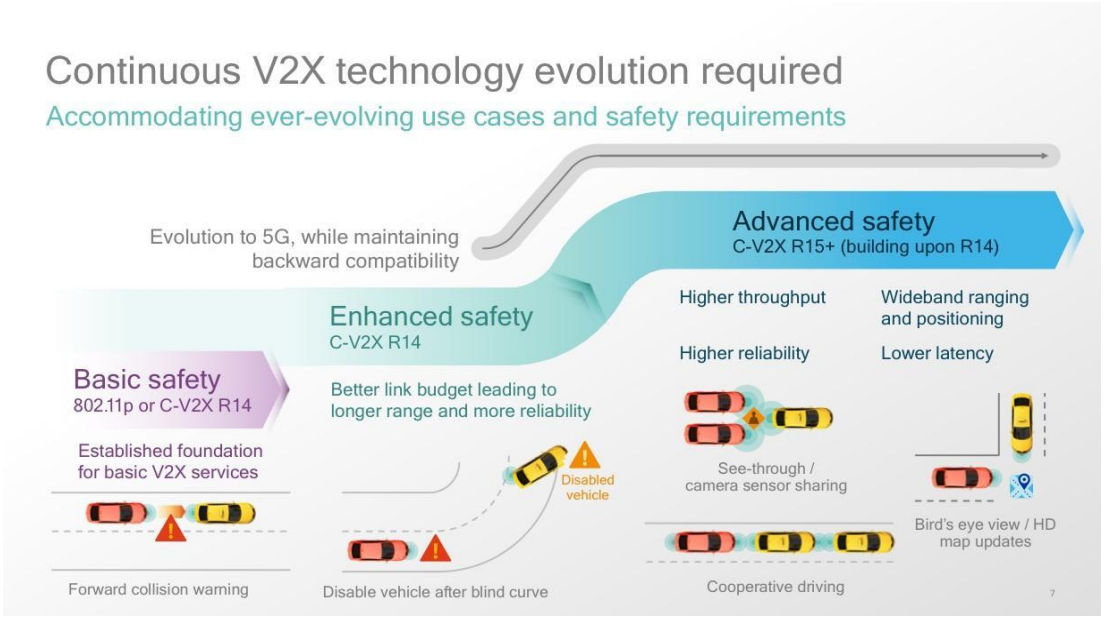



**Reuse established service and app layers**
- Already defined by automotive and standards communities, e.g. ETSI, SAE
- Developing abstraction layer to interface with 3GPP lower layers (in conjunction with 5GAA)

**Reuse existing security and transport layers**
- Defined by ISO, ETSI, and IEEE 1609 family

**Continuous enhancements to the radio/lower layers**
- Supports the ever-evolving V2X use cases

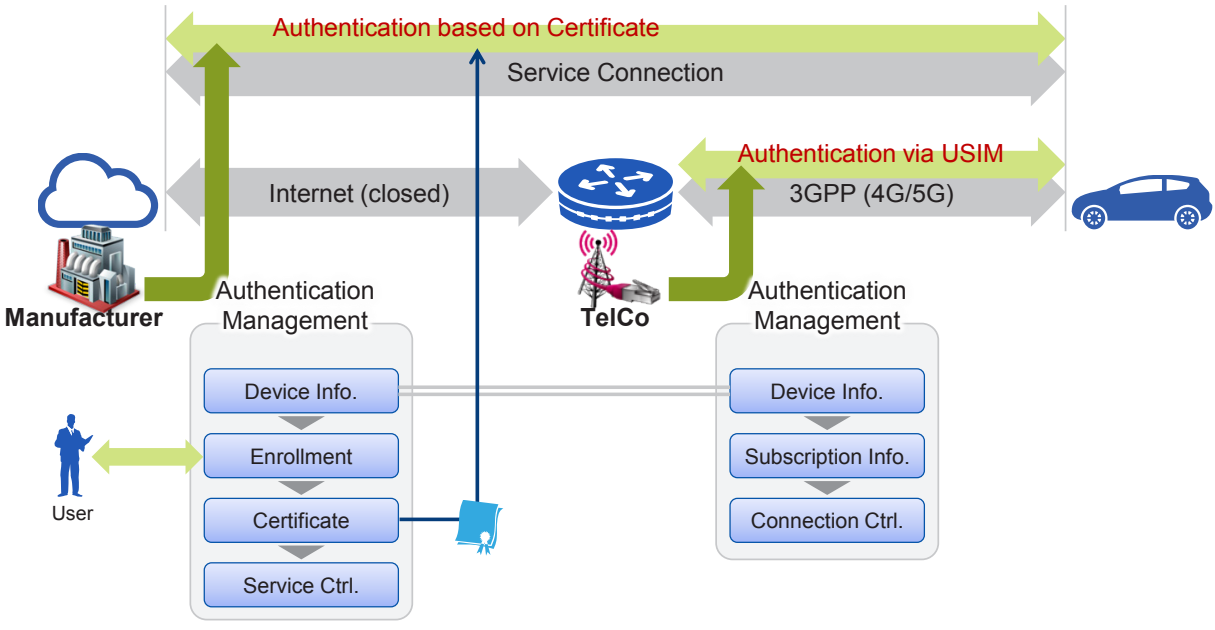
*출처 : Qualcom : The path to 5G : Cellular Vehicle-to-Everything(C-V2X)



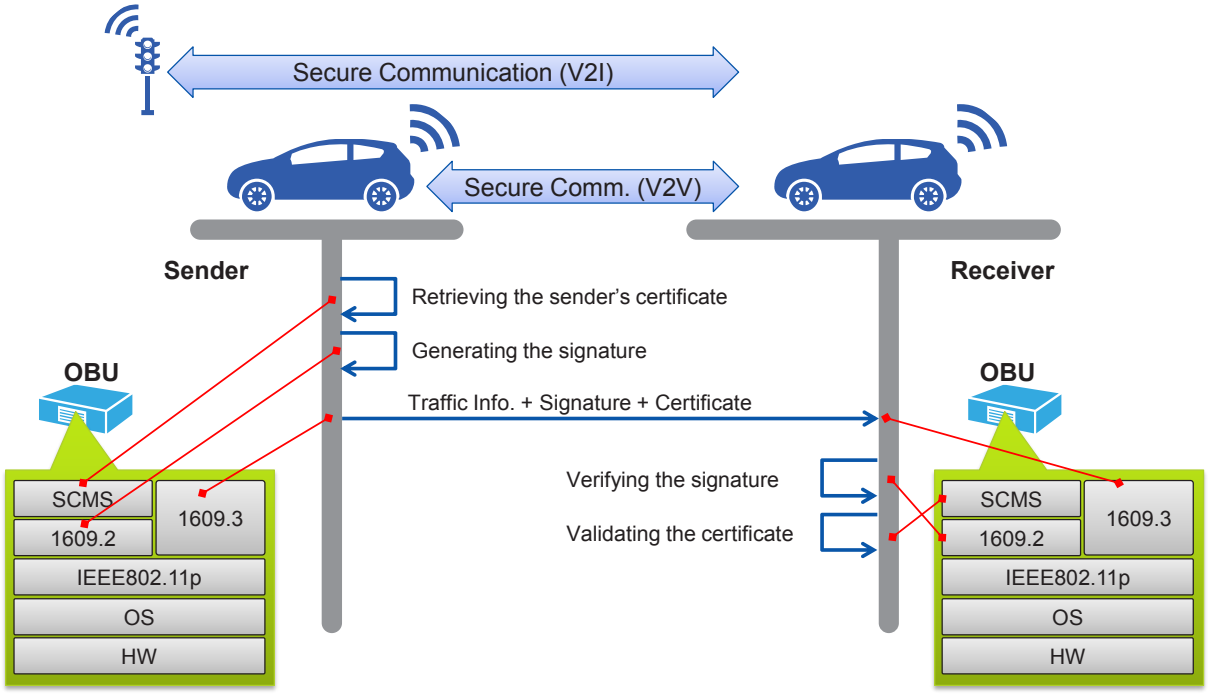

https://www.qualcomm.com/news/onq/2017/02/24/accelerating-c-v2x-toward-5g-autonomous-driving



## S1. Secure External Communication – TelCo & Manufacturer

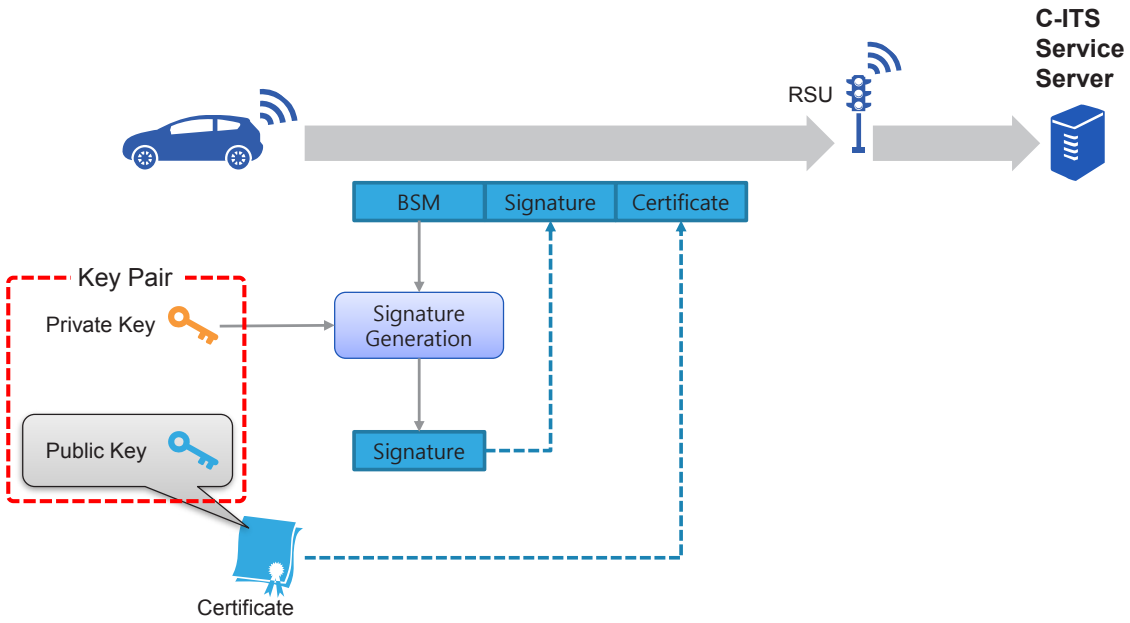


## C-ITS: Authenticated Communication

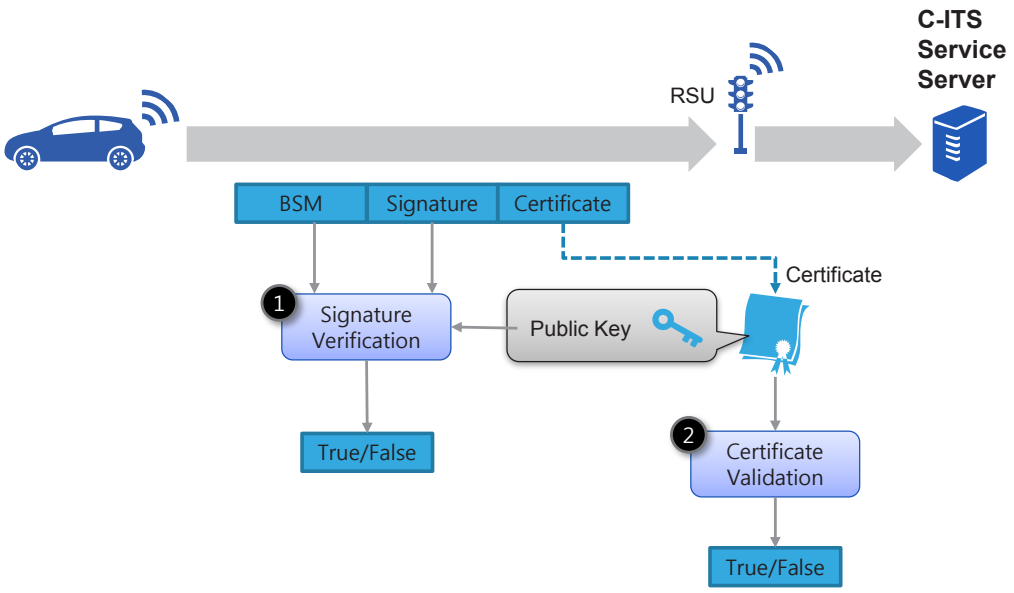





## C-ITS: Authenticated Communication (Sender)

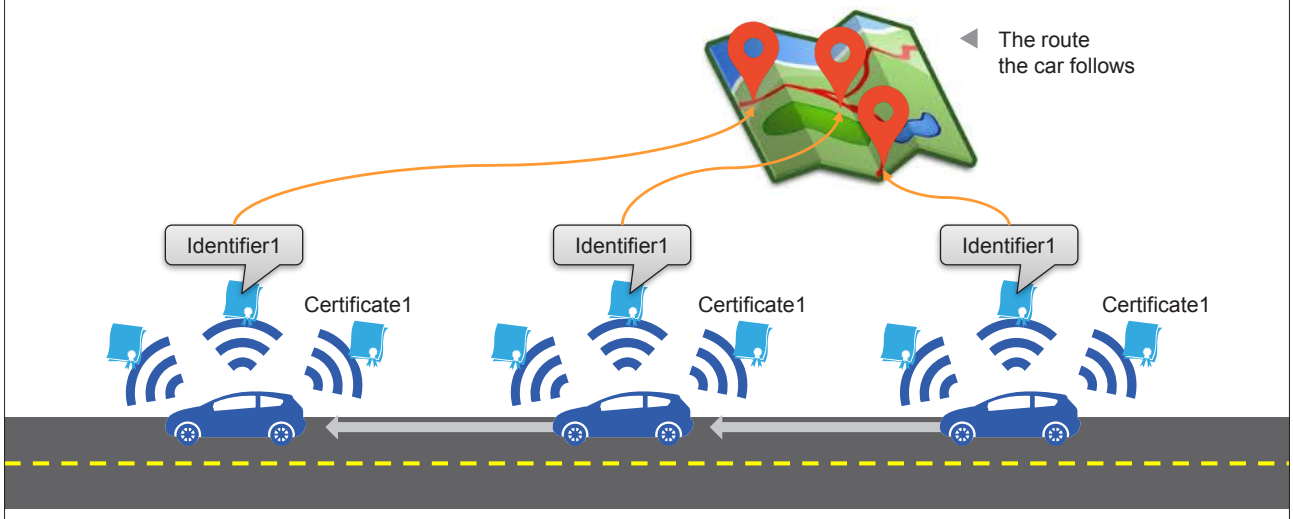


## C-ITS: Authenticated Communication (Receiver)

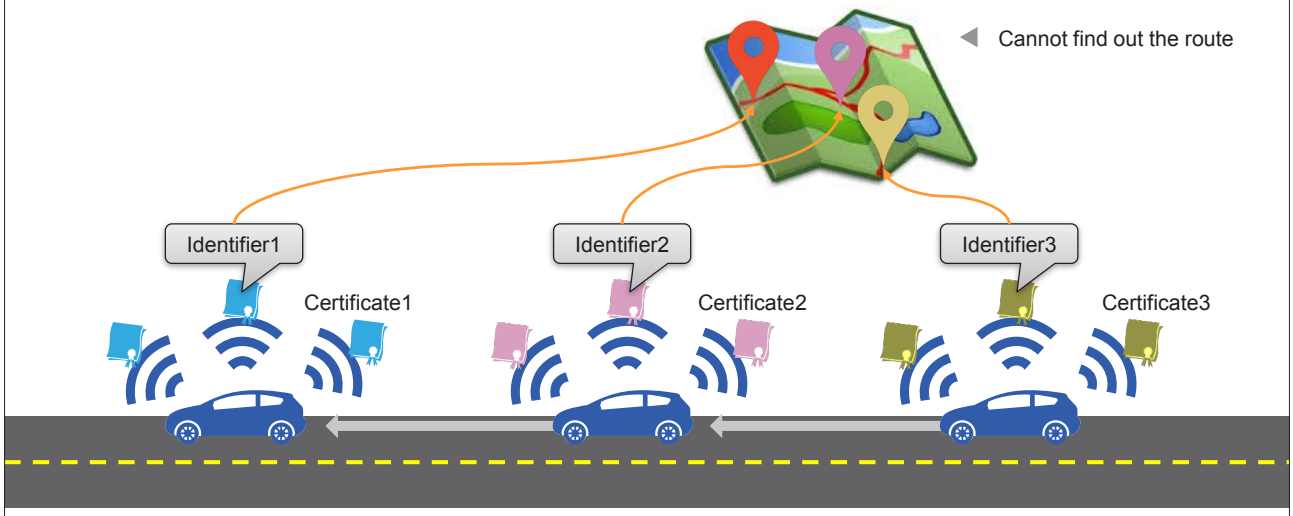





## Privacy Issue



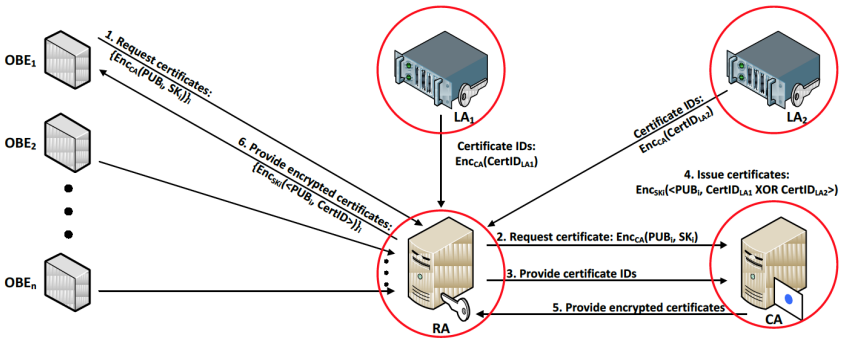
## Privacy Preserving





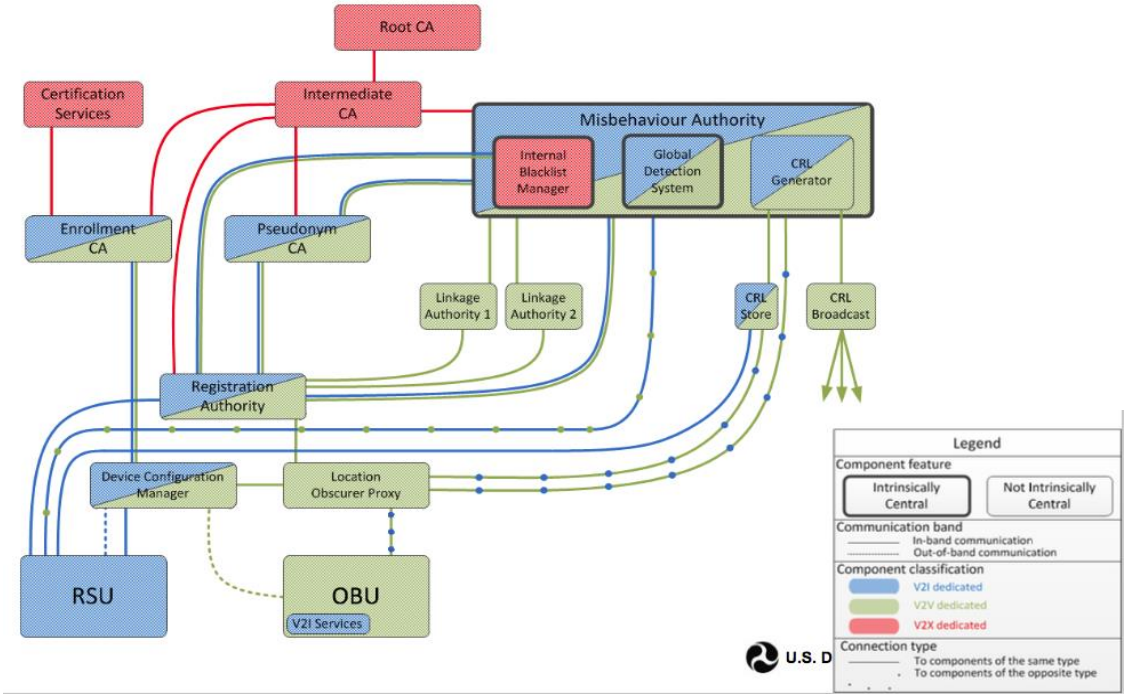

## CV-Pilot Phase 1 : SCMS Architecture

- SCMS Concept Design(2012)
  - Bootstrapping
  - Calculation Linkage Values
  - Request Certificates
  - Request Decryption Key
  - Report Misbehavior And Revocation
  - Request CRL




source : Security Credential Management System Design,USDOT,2012

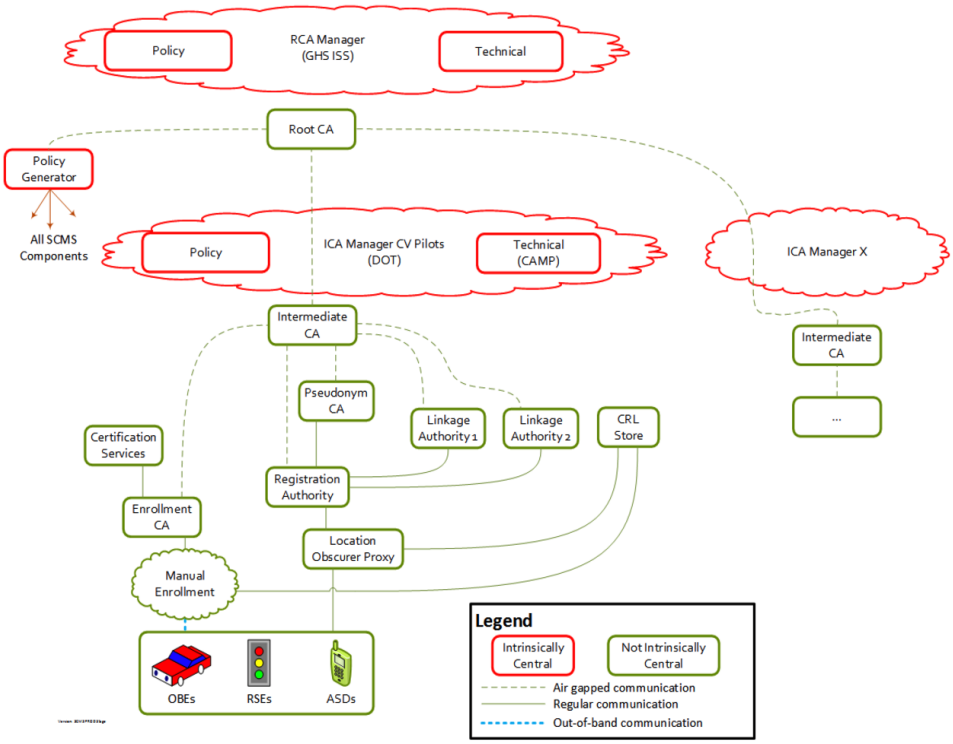
## SCMS Design (2016)




* NHTHA, "Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1," May 11,2016.



## SCMS Design (2017)



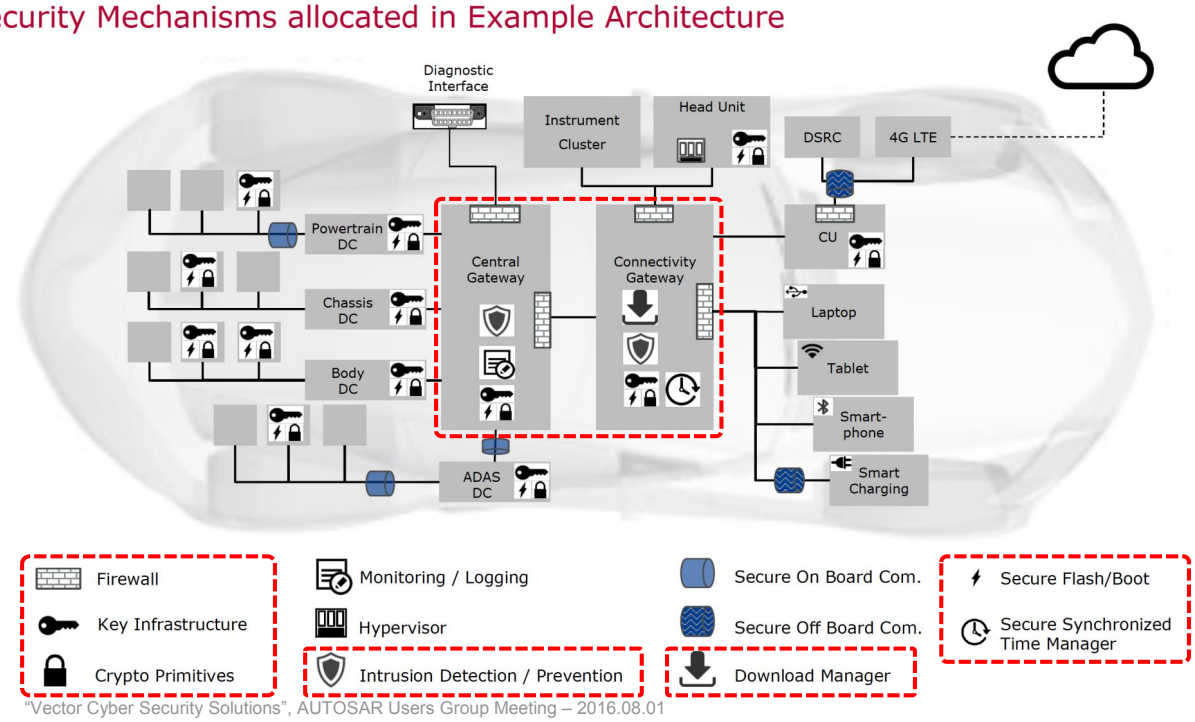

Source : *SCMS CV Pilots Documentation ,CAMPLLC,2017*

## S2. Secure Gateway

Security Mechanisms for Embedded Automotive Systems

VECTOR

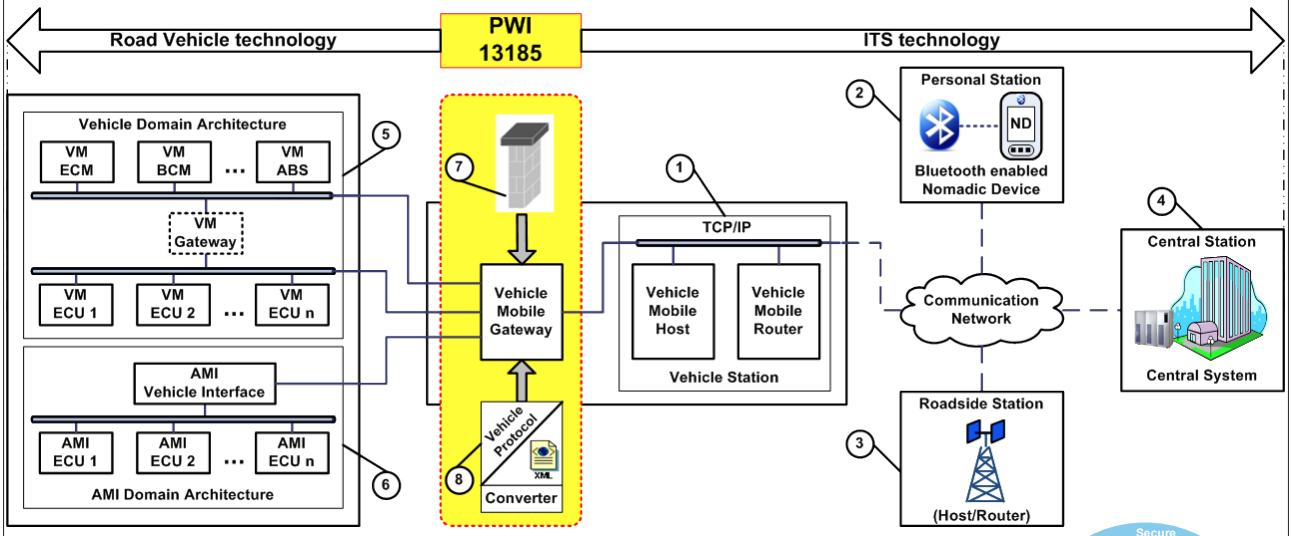
### Security Mechanisms allocated in Example Architecture



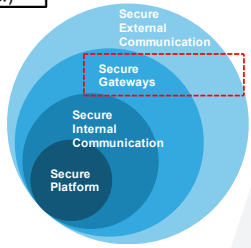

"Vector Cyber Security Solutions", AUTOSAR Users Group Meeting – 2016.08.01



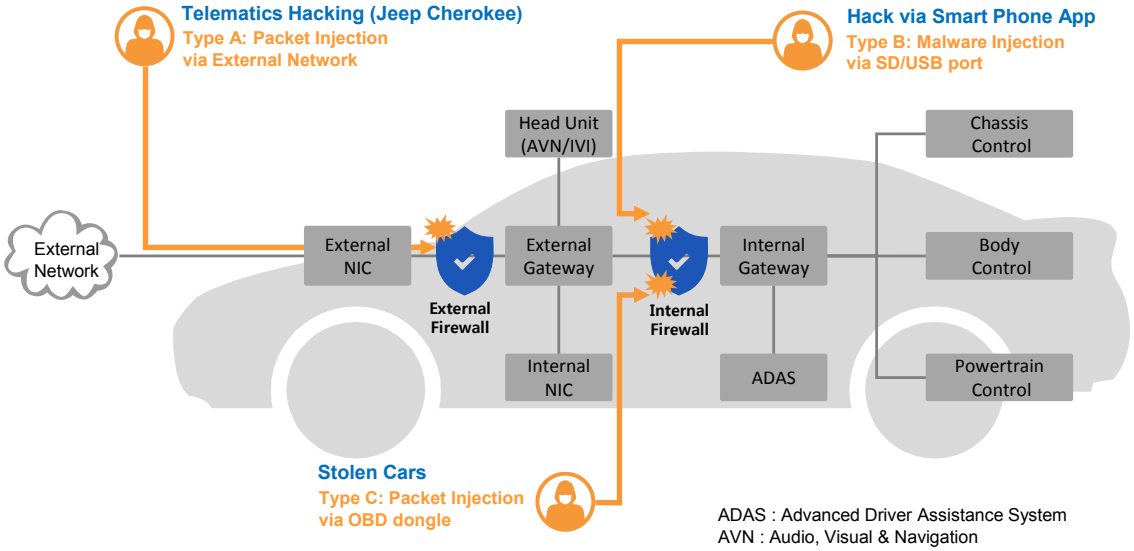
## ISO 13185




1 Vehicle Station: Vehicle Mobile Host and Vehicle Mobile Router
2 Personal Station
3 Roadside Station
4 Central Station
5 Vehicle Domain Architecture with optional VM Gateway
6 Automotive Multimedia Interface Domain Architecture
7 Firewall implemented in Vehicle Mobile Gateway
8 Vehicle Protocol converter to standardized XML based vehicle data transfer protocol



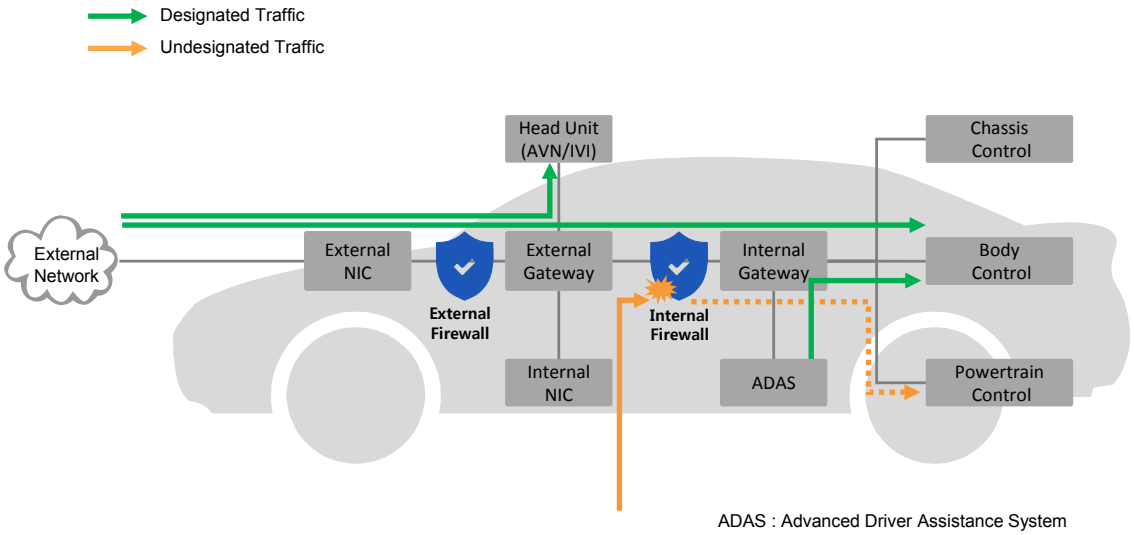
## S2. Secure Gateway – Detects malicious traffic




ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller


5 Public

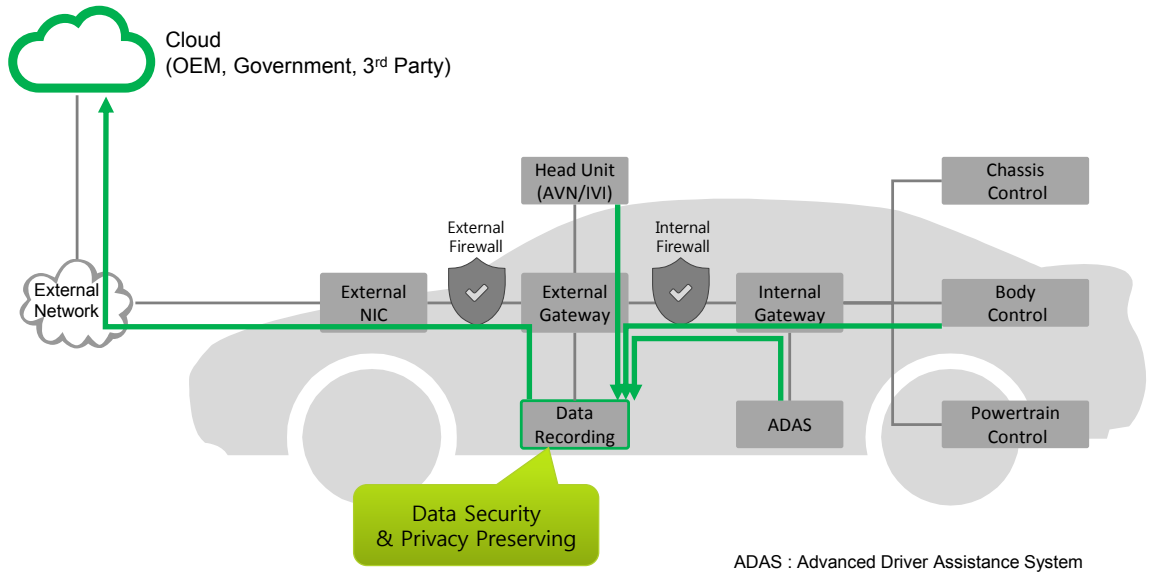
## S2. Secure Gateway – Controls traffic flow




ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller


5 Public

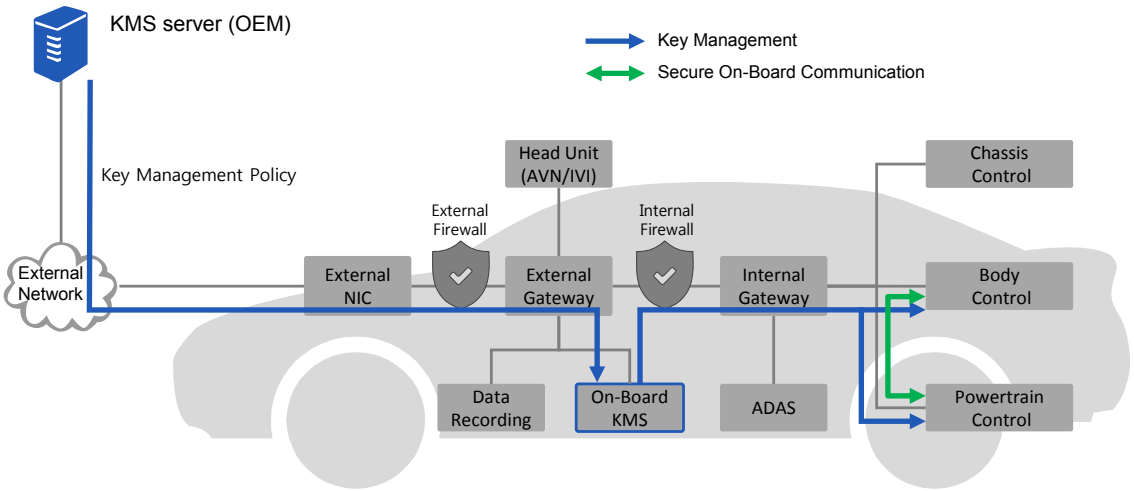
## S2. Secure Gateway – Data Security & Privacy Preserving




ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller

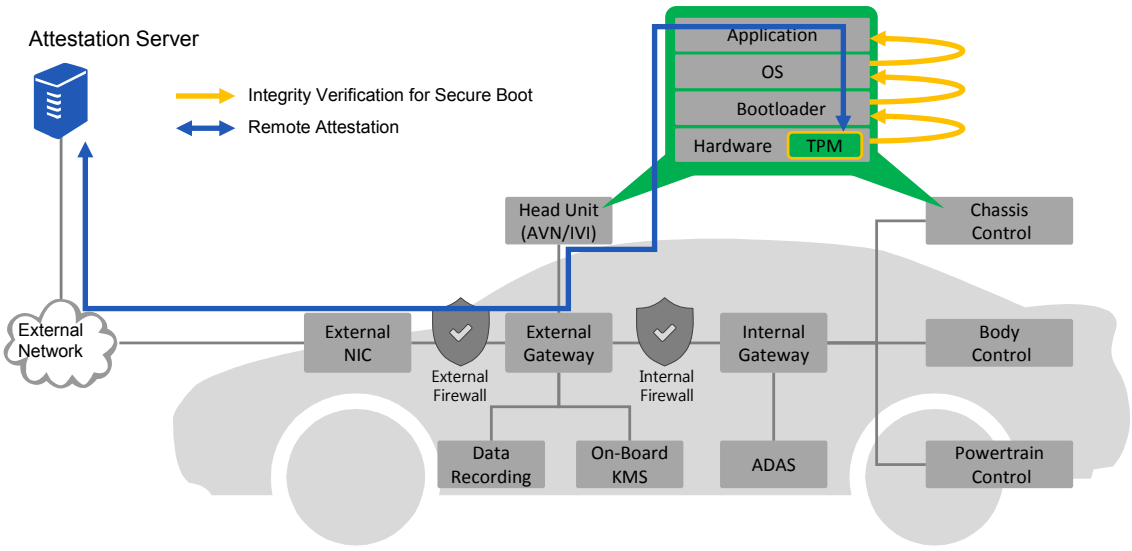


## S3. Secure Internal Communication




ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller
KMS : Key Management System

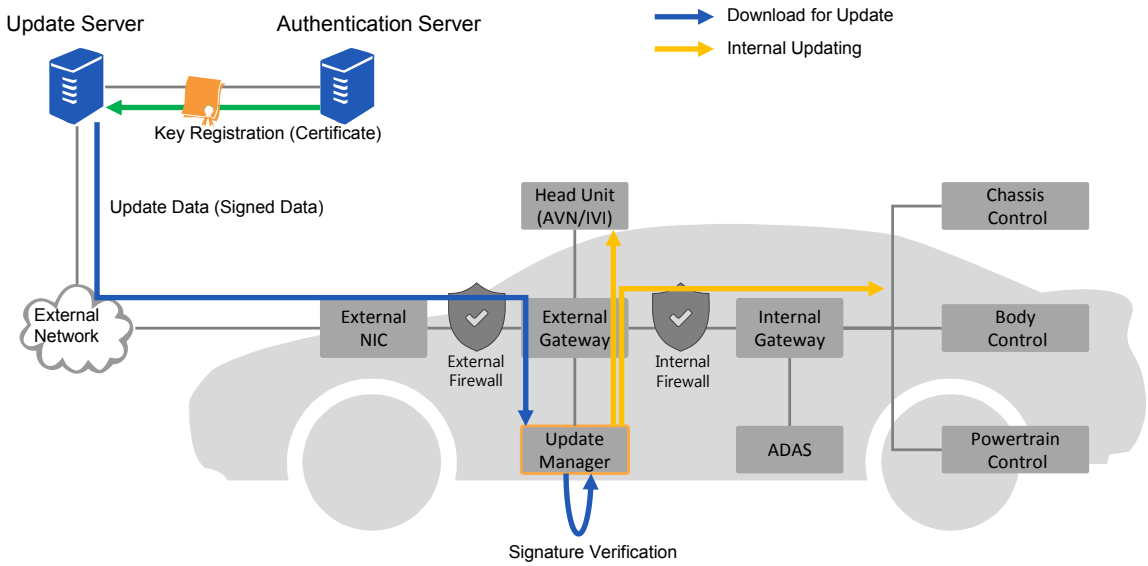
## S4. Secure Platform - Secure Boot & Remote Attestation




ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller
KMS : Key Management System
TPM : Trusted Platform Module

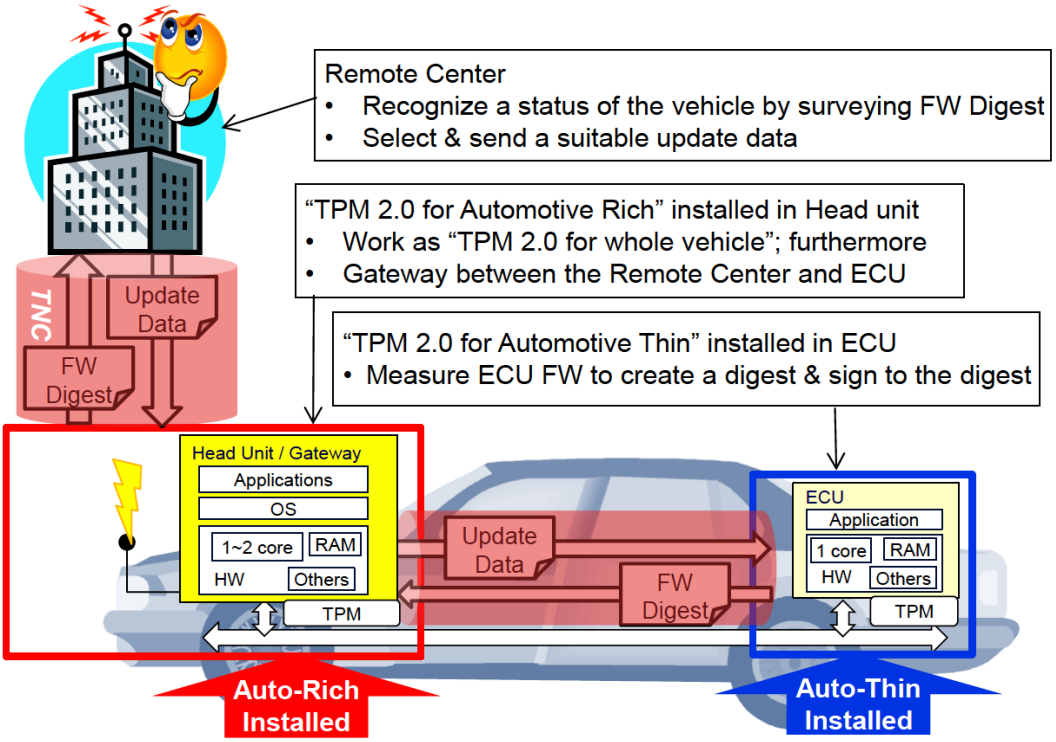


## S4. Secure Platform - Secure Update (OTA)



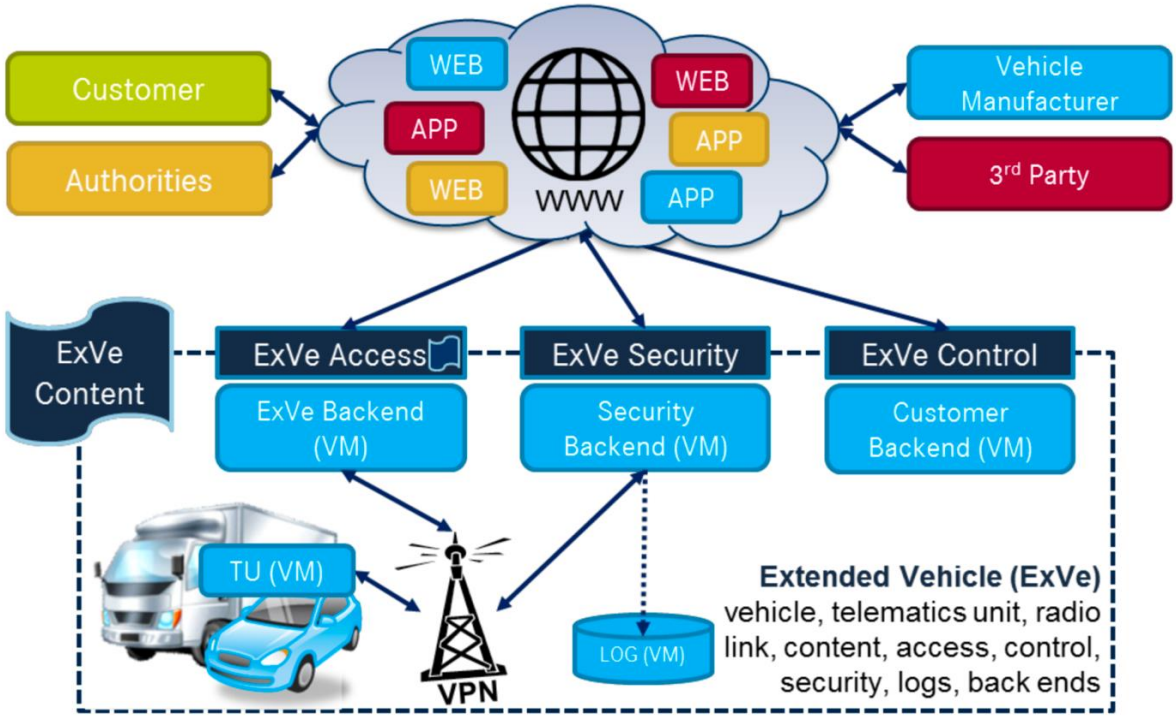

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller
KMS : Key Management System
TPM : Trusted Platform Module

## S4. Secure Platform - TCG TPM 2.0 Automotive-Thin Profile 1.0

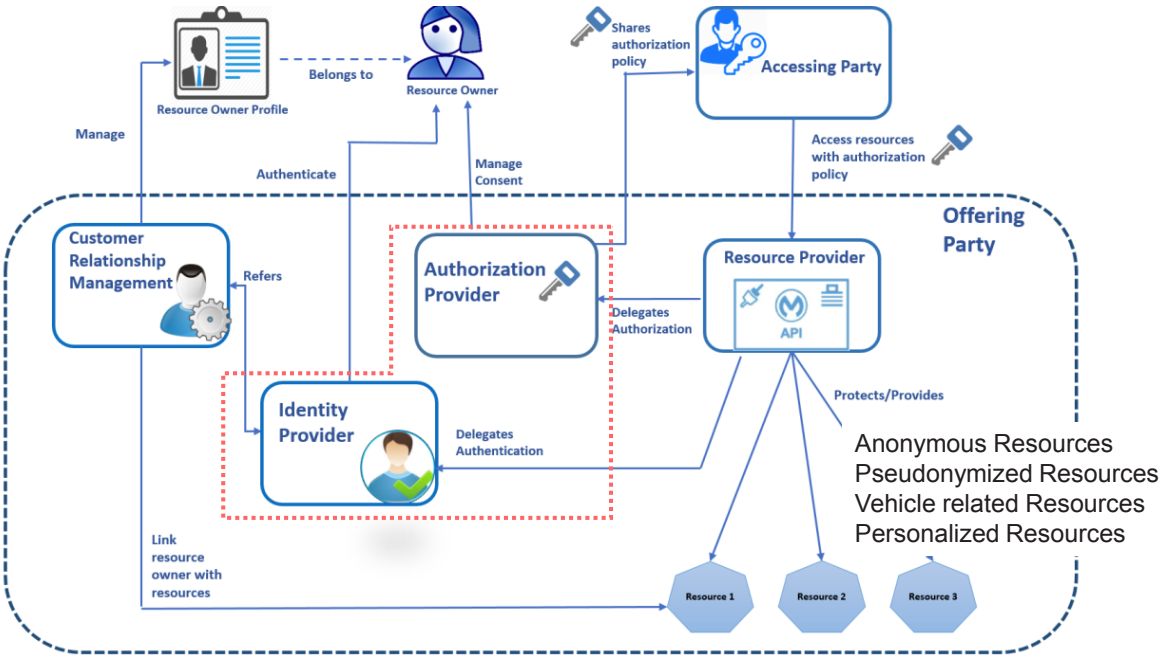





## Extended Vehicle (ISO 20077 & 20078)



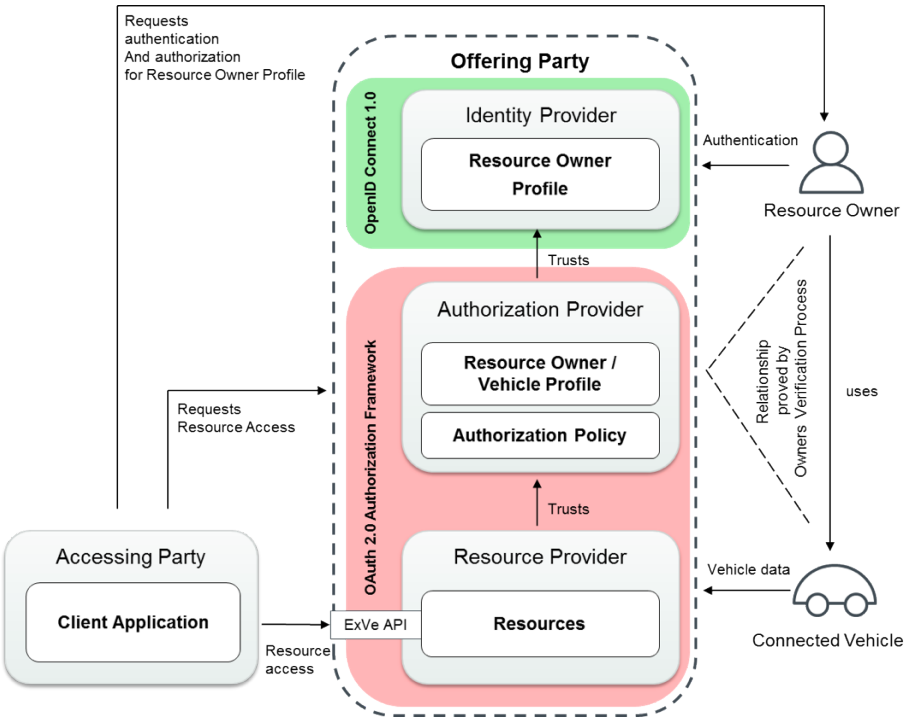
## ISO 20078-1 ExVe 'Web Services' – ExVe content (CD, 2017.06)



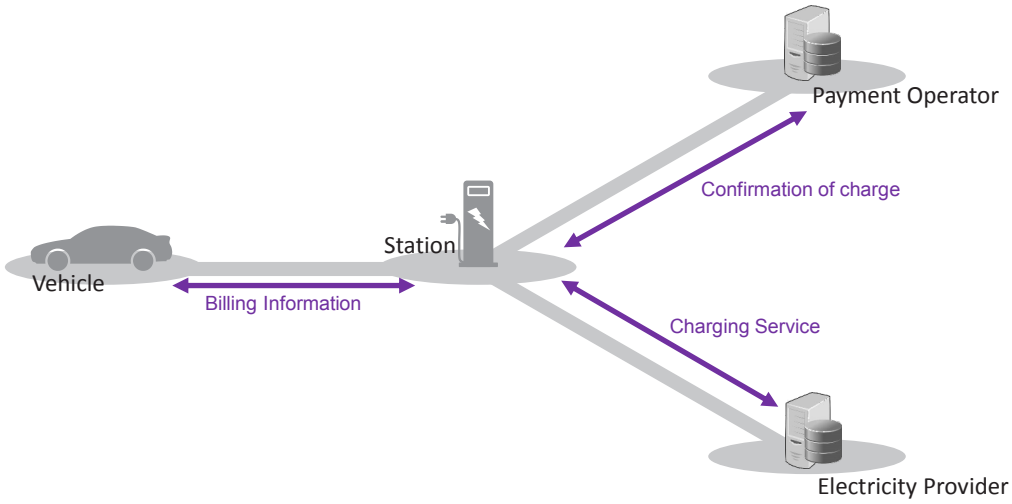

Authentication Infrastructure & Privilege Infrastructure



## ISO 20078-1 ExVe 'Web Services' – ExVe Security (CD, 2017.06)

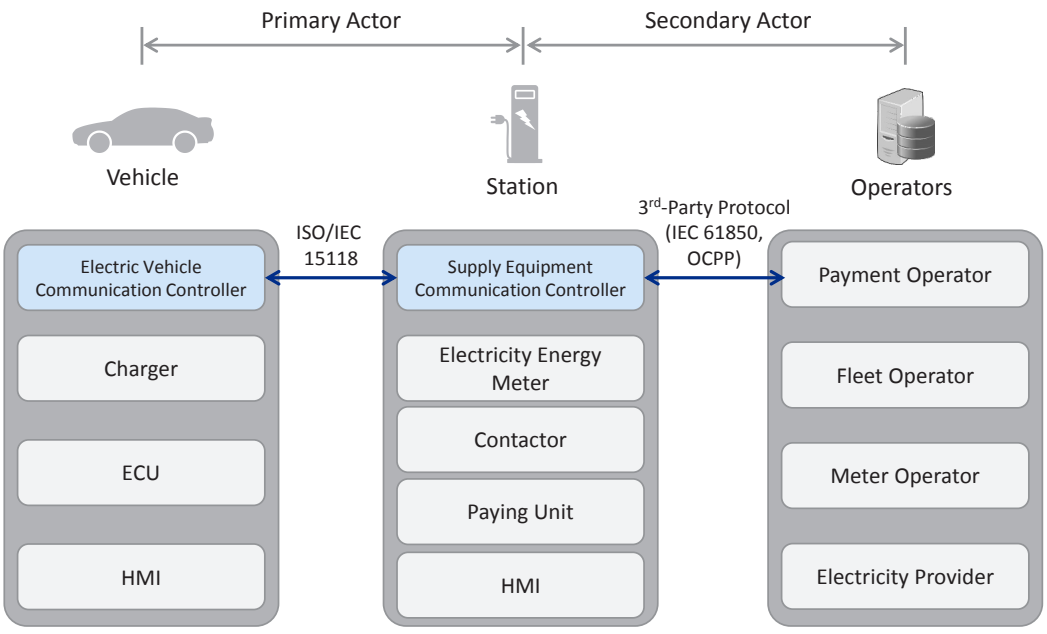


## Electric Vehicles

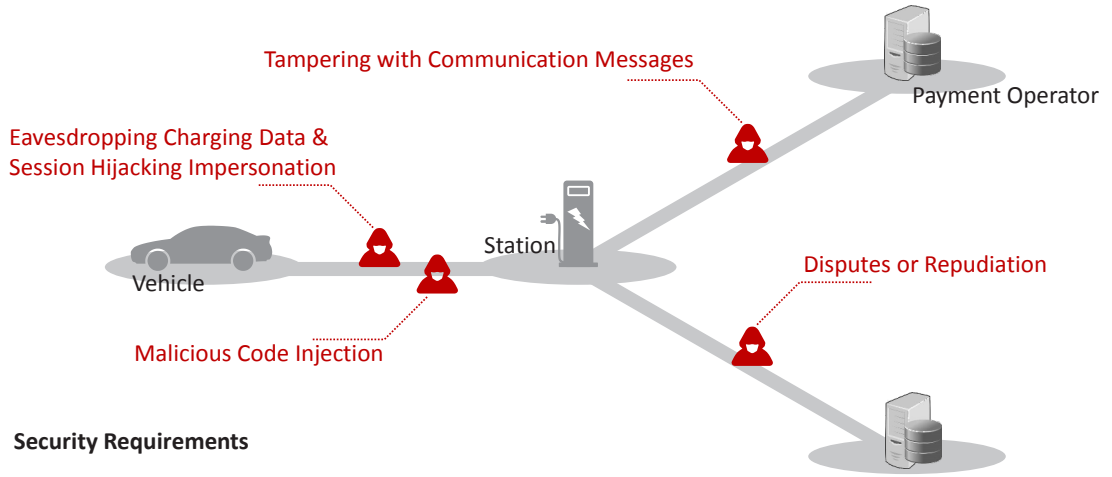





## EV Charging Infrastructure



## Security Threats in eVehicle



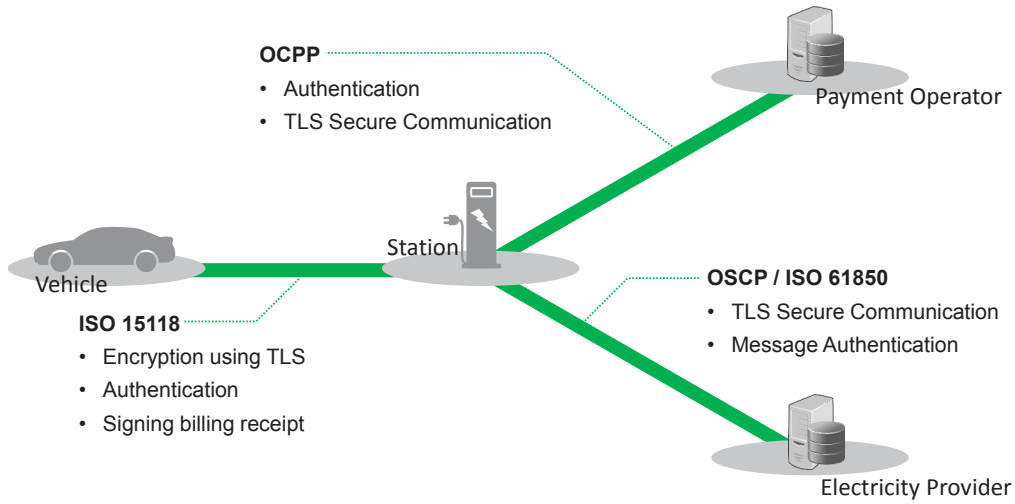

**Security Requirements**

- Secure Communication with mutual authentication
- Integrity and non-repudiation for billing
- Confidentiality for personal & business information
- Availability of electricity



## Secure Communication – eVehicle Protocols

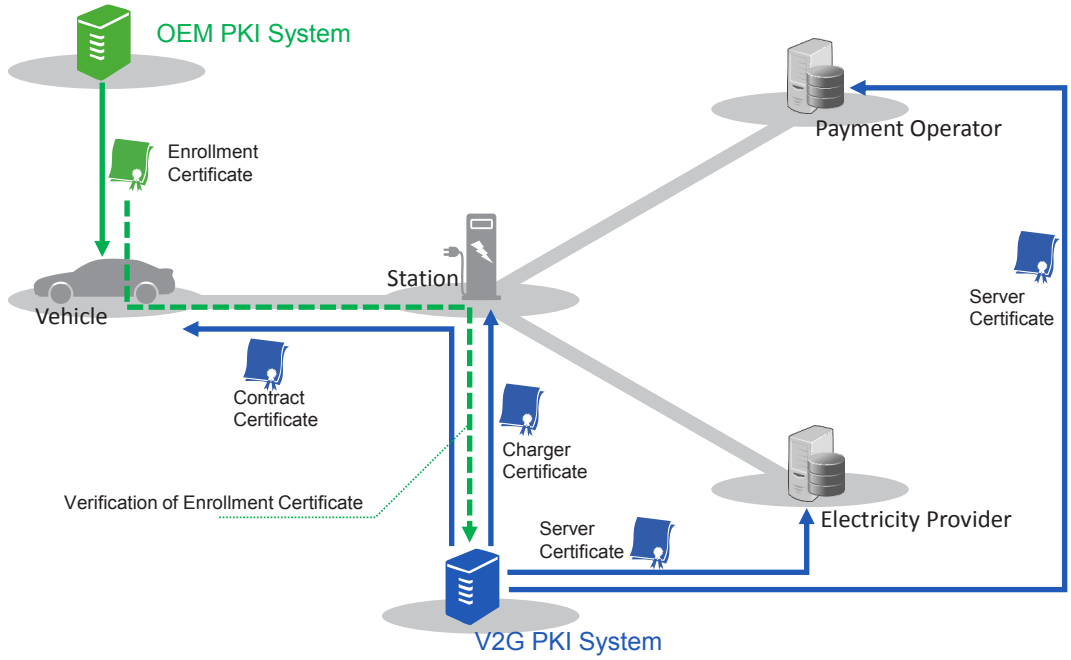
- OCA : Open Charge Alliance
- OCPP : Open Charge Point Protocol
- OSCP : Open Smart Charging Protocol




**OCA**

- OCPP standardizes the communication between the charge spot and the party that operates the charge, thereby allowing CSO back-ends and charge spots of different vendors to communicate.
- OSCP(Open Smart Charging Protocol) allows a DSO to vary the capacity available to charge stations in time, given the varying predicted capacity needed for other consumers in an area.

## Security Model for EV & EVS

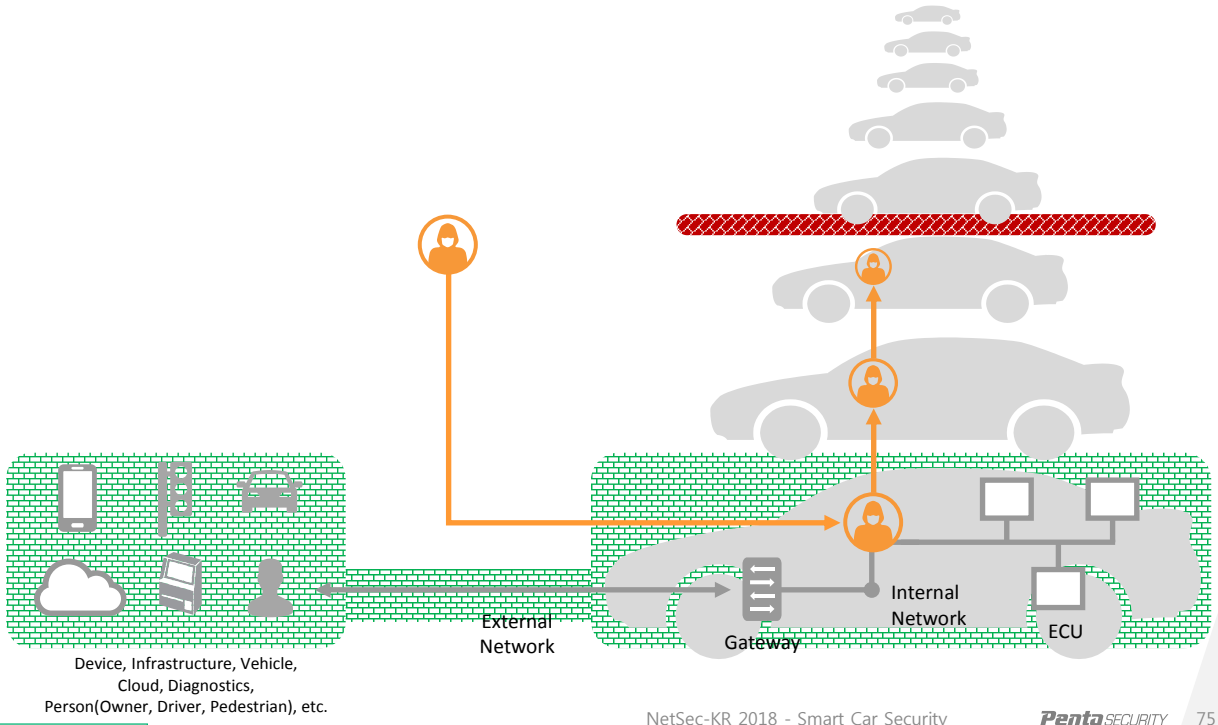





## Energy Architecture

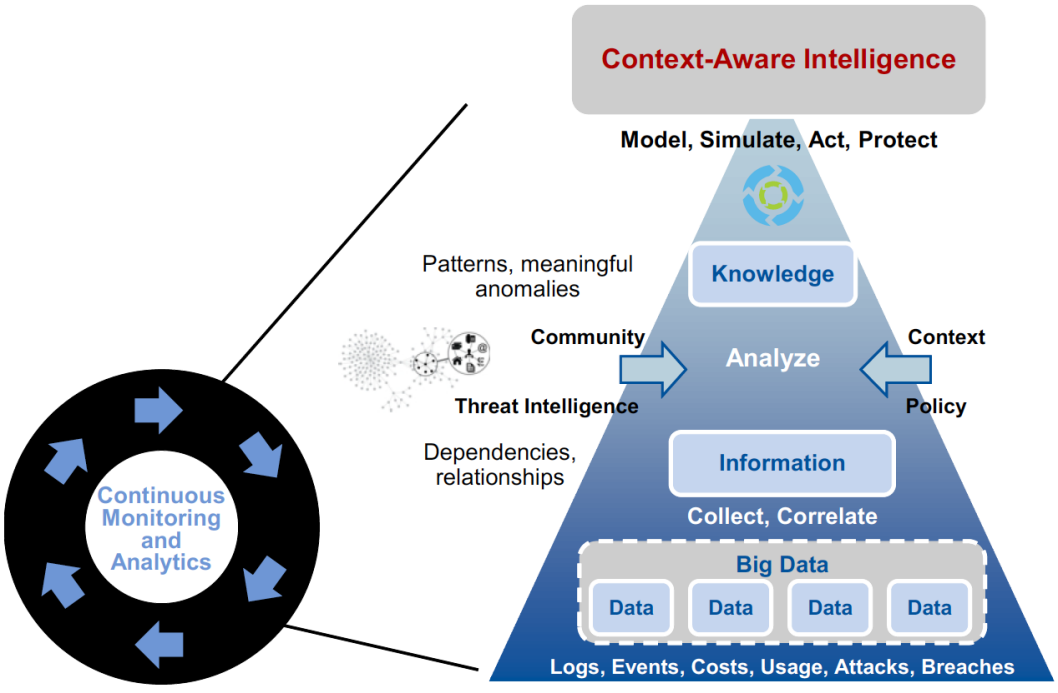
| Electricity Generation | Electric power Transmission | Electrical Substation | Electric power Distribution | Demand Equipment |
|---|---|---|---|---|
| IEC 61400 | | IEC 60870<br>IEC 61850<br>IEC 61970<br>IEC 62351 | | IEC 65056<br>IEC 63110 |

## Incident Response & Hacking Mitigation



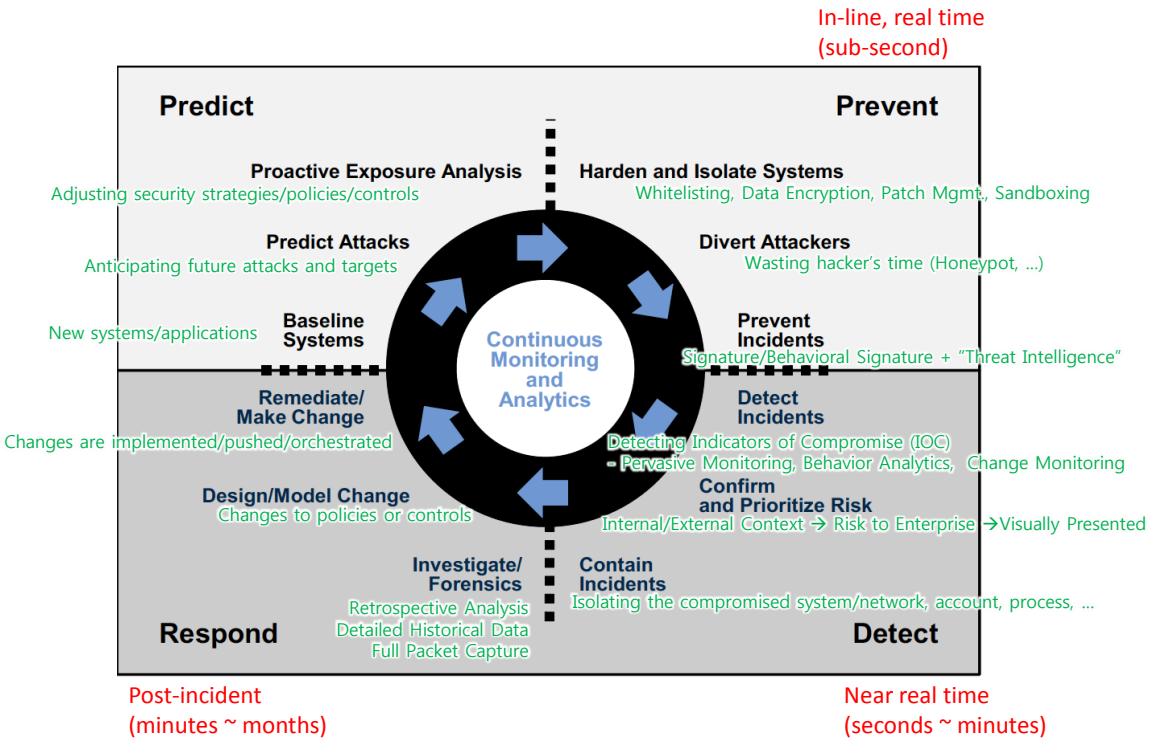



## Adaptive Security Architecture (Gartner)



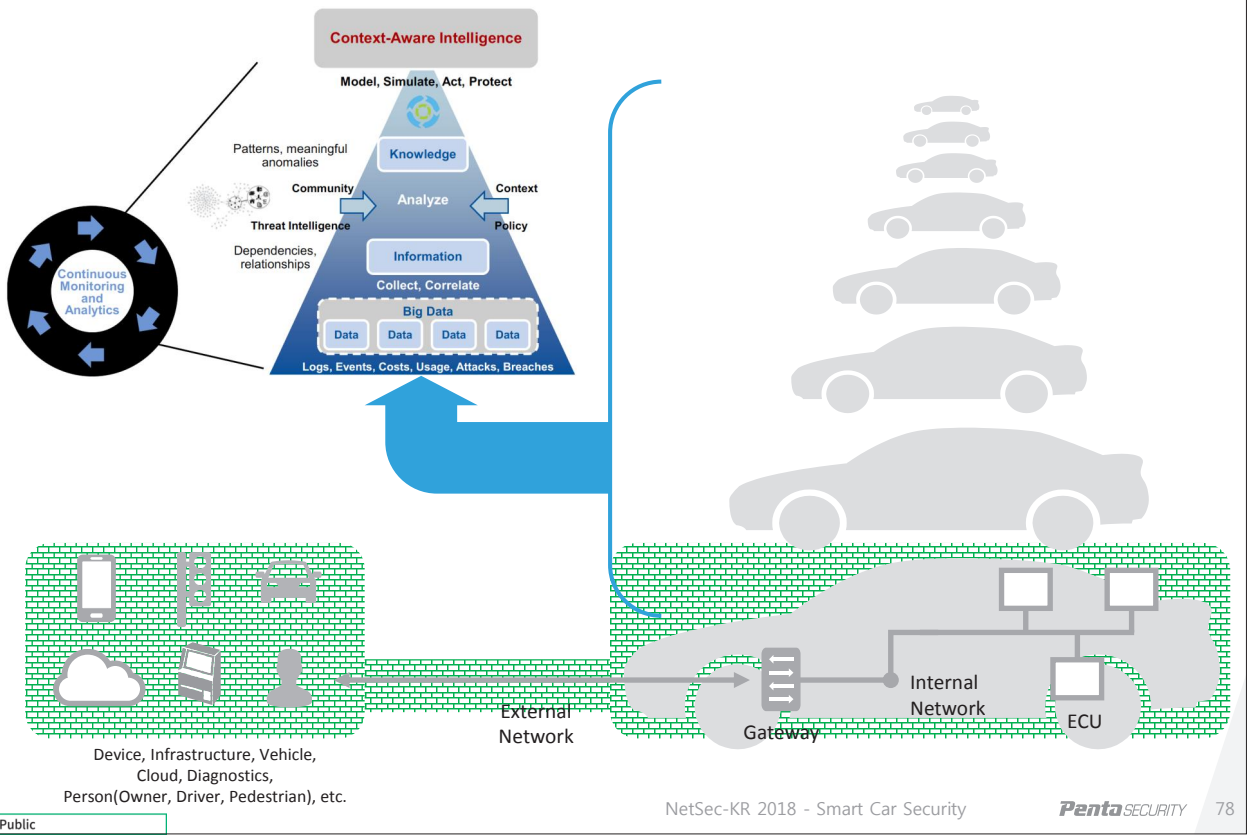

Source: Gartner (February 2014)

## Adaptive Security Architecture - Lifecycle

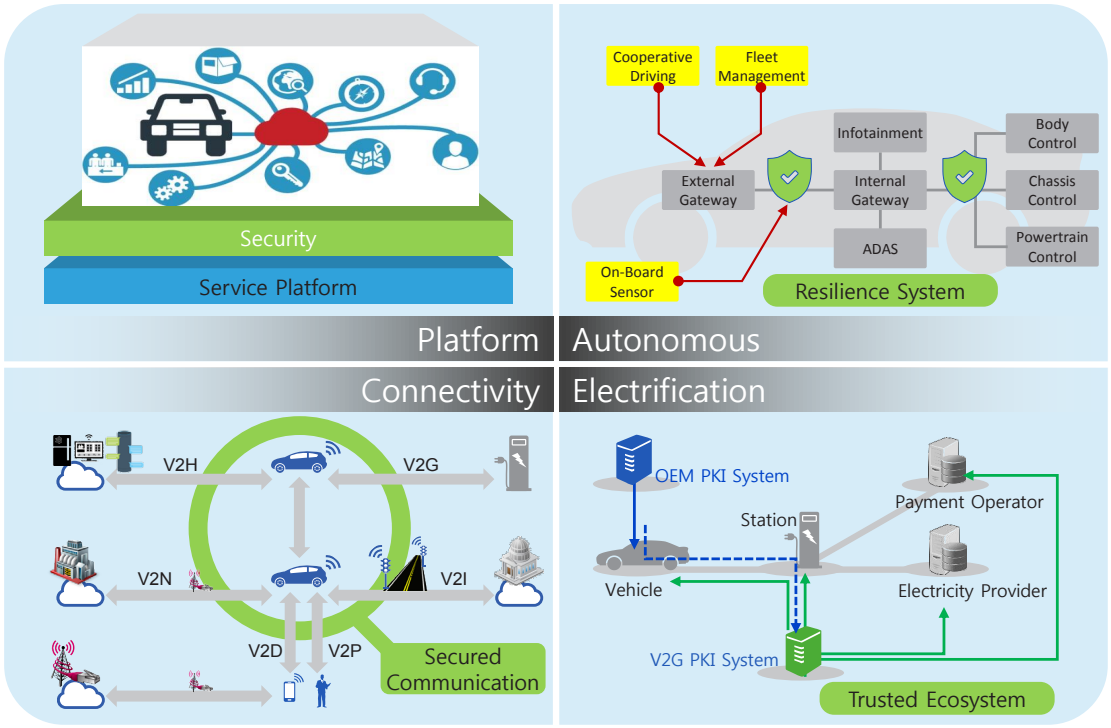





## Adaptive Security & Autonomous Car



## "Secure First"






20 year Anniversary

Asian Cyber Security Vendor of the Year

thank you

PentaSECURITY
KOREA Yeouido, Seoul www.pentasecurity.co.kr (HQ)
U.S.A. Houston, Texas www.pentasecurity.com
JAPAN Shinjuku-Ku, Tokyo www.pentasecurity.co.jp

The 24th Network Security Conference -Korea

# Semantic Transformation을 이용한 사용자의 패스워드 보안과 취약점분석

**우사이먼** 한국뉴욕주립대학교 교수

### 학력 및 경력사항

| | |
|---|---|
| 2003.08 | University of Washington (UW), Seattle, 전자공학과 학사 |
| 2005.06 | University of California, San Diego (UCSD) 컴퓨터 공학 석사 |
| 2012.12 | University of Southern California (USC) 컴퓨터 과학과 석사 |
| 2017.08 | University of Southern California (USC) 컴퓨터 과학과 박사 |
| 2017.08 ~ | 한국뉴욕주립대학교 컴퓨터과학과 |
| 2016.05 ~ 2016.08 | Verisign Research Lab, Reston, USA |
| 2005.09 ~ 2014.05 | NASA Jet Propulsion Laboratory (JPL), Pasadena, USA, 연구원 |

### 강연요약

사용자가 간단하고 기억하기 쉬운 패스워드를 만든다는 것은 이미 잘 알려진 사실이다. 특히 여러 개의 온라인 계정들을 만들 경우, 사용자에게 가중되는 부담은 더 크며, 사용자는 같은 패스워드를 여러 사이트에 반복적으로 사용함이 보였다. 이 같은 경우 Password Reuse Attack에 대하여 취약하며, 패스워드 정책을 일괄적으로 강요하는 것에서 벗어나, 근본적인 해결책 마련과 원인 분석이 시급하다. 특히, 사용자의 패스워드 생성습관과 Risk Perception 에 대한 이해와 분석이 선행되어야 한다.

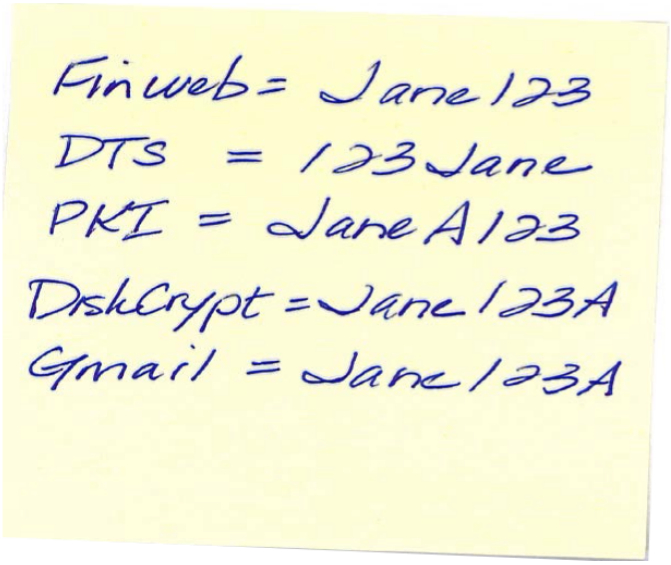
이 강연에서 궁극적으로 패스워드의 보안성을 높이기 위해서, 사용자에 대한 이해가 절실하며 다양한 계정에 실제로 사용되는 사용자의 패스워드를 비교, 분석한다. 특히, CloudSweeper 를 이용해 사용자의 실제 패스워드들에 semantic transformation을 적용하여 사용자의 privacy를 유지하면서 통계적 의미를 유추함으로써 qualitative 연구와 quantitative 연구를 동시에 수행할 수 있음을 보여준다. 이를 바탕으로 사용자의 의도와 습관, 공격과 보안에 대한 인식과 오해, 그리고 사용자가 실제 사용하는 패스워드들을 다양한 각도에서 분석, 비교한 뒤, 패스워드 보안의 근본적인 문제점을 해결하기 위해 몇 가지 대안들을 제시하려 한다.

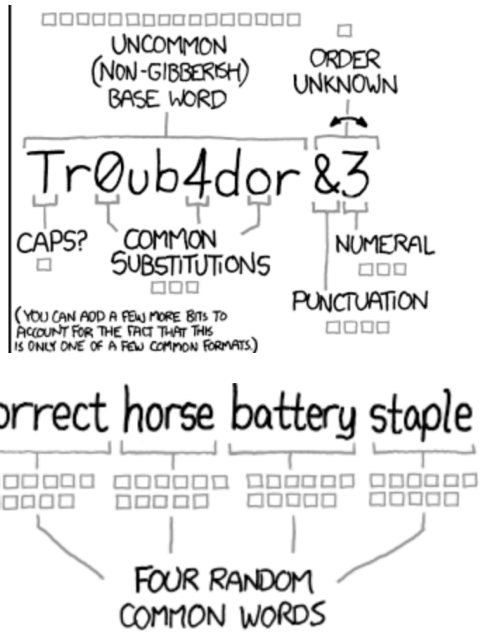
# Semantic Transformation을 이용한 사용자의 패스워드 보안과 취약점 분석

Simon S. Woo
Assistant Professor
CS. Dept. SUNY-Korea, Songdo
April12, 2018
At NetSec-KR 2018

SUNY Korea

# Challenges With Passwords



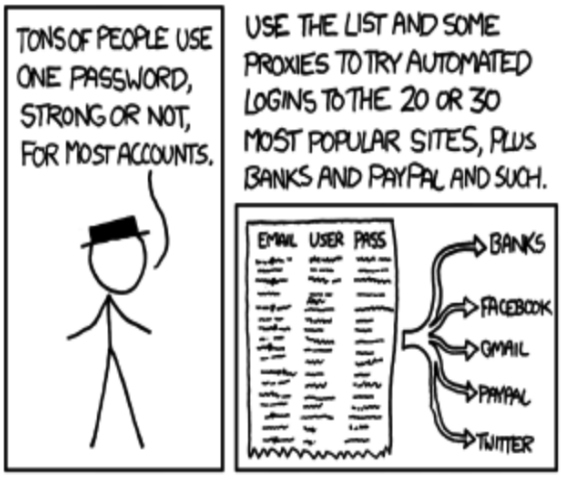




SUNY Korea

# Challenges With Passwords

**The DNC used incredibly weak passwords like 'obamain08'**

Users are advised to create a strong and unique password for each account but this is hard.




Many passwords have similar patterns which can result in password-reuse attacks.

SUNY Korea

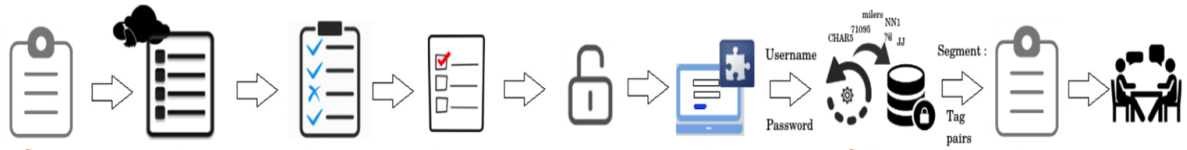
# Our Goal

- How prevalent are bad password habits?
- What influences password strength?
  - User's intent
  - Risk perception
  - Website importance
  - Website's password policy
- How well does users' password practices align with their intent?

**Joint work with**
**Ameya Hanamsagar* (Facebook), Chris Kanich (UI Chicago),**
**& Jelena Mirkovic (USC/ISI)**

SUNY Korea

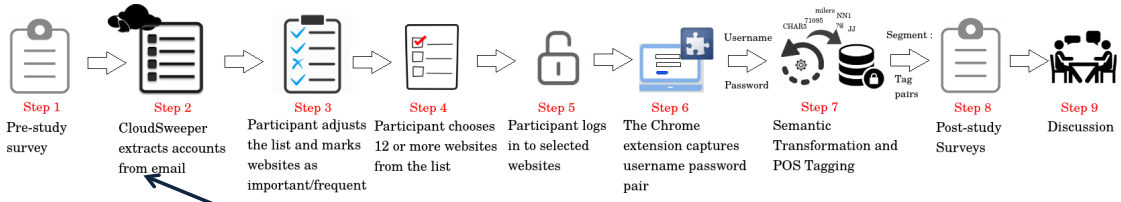
# Study Design




Step1. Statistics, Password Strategy, and Risk Perception surveys

SUNY Korea

# Study Design IRB approved

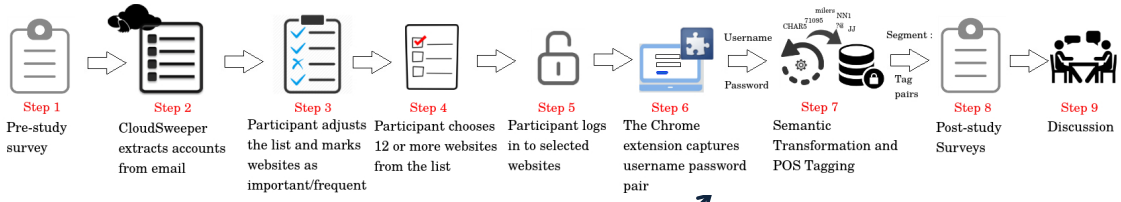



Step 2: **Cloudsweeper** tool scans a user's Gmail account to identify account creation and password reset E-mails and extract site URLs

| Pattern |
| --- |
| welcome to |
| reset password |
| thank you/thanks for registering/creating/signing |
| your .* account has been created |

SUNY Korea

# Study Design IRB approved



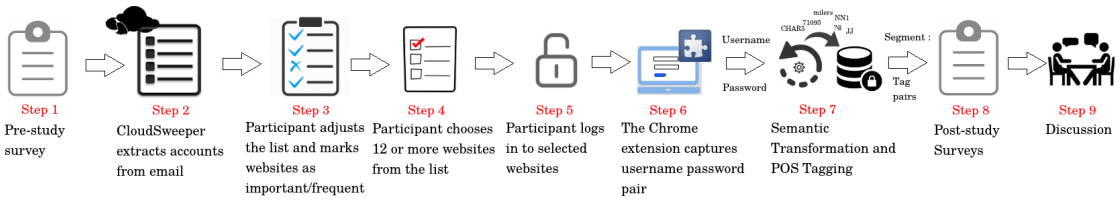

Step 6: A Chrome extension captures username and password for each
site and collects:

- Password length
- Password strength as measured by zxcvbn[zxcv]

[zxcv] https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation/

SUNY Korea

# Study Design IRB approved

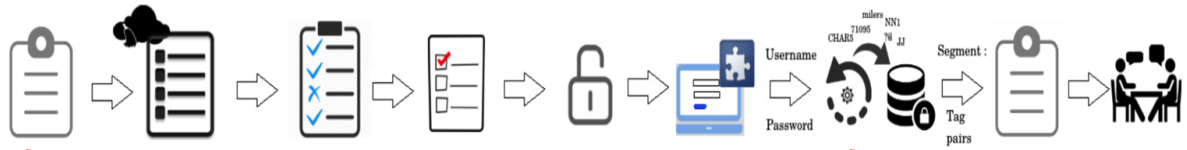



Step 7: We apply **semantic segmentation**[Vera2014] and **transformation** to username and password. We drop the originals and store the transformed values.

[Vera2014] R. Veras, C. Collins, and J. Thorpe. On the semantic patterns of passwords and their security impact. NDSS, 2014.

SUNY Korea

# Study Design




Step 1 Pre-study survey

Step 2 CloudSweeper extracts accounts from email

Step 3 Participant adjusts the list and marks websites as important/frequent

Step 4 Participant chooses 12 or more websites from the list

Step 5 Participant logs in to selected websites

Step 6 The Chrome extension captures username password pair

Step 7 Semantic Transformation and POS Tagging

Step 8 Post-study Surveys

Step 9 Discussion

john4723@

POS Tagging

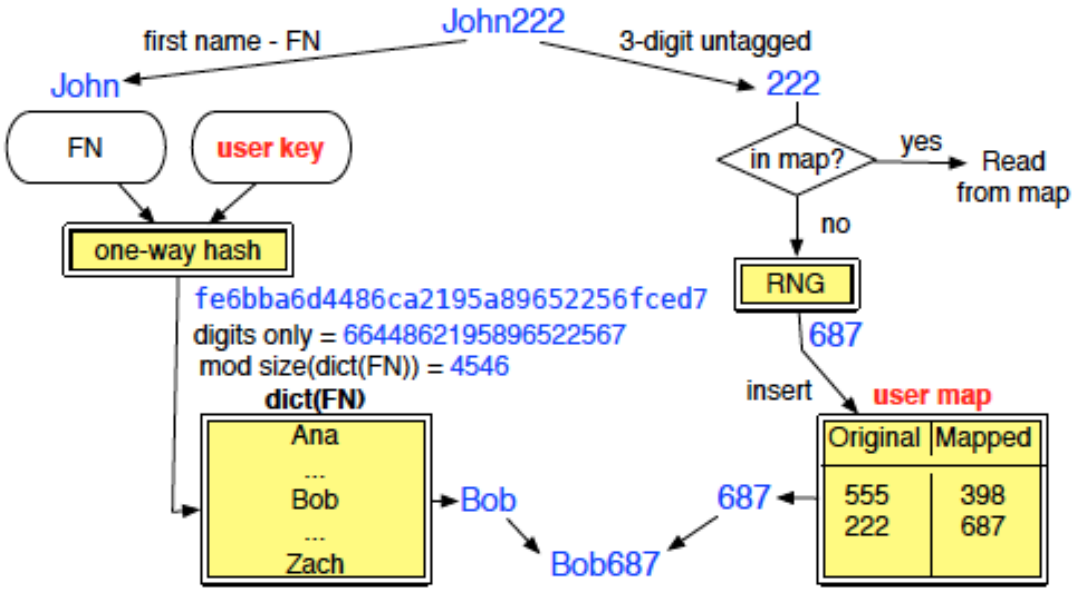
(proper-name)(4-digits)(1-special)

One-way hashing and dictionary lookup

richard2908$

We apply semantic transformation to username and password. We drop the originals and store the transformed values.

# Semantic Transformation



# Collected Data Stat.

## Account type by users

| Account | Frequent | Not frequent | Total |
|---|---|---|---|
| Important | 212 | 180 | 392 |
| Not important | 29 | 200 | 229 |
| Total | 241 | 380 | 621 |

## Successful Login(%)

| Account | Frequent | Not freq. | Total |
|---|---|---|---|
| Important | 86% | 71% | 79% |
| Not important | 76% | 57% | 59% |
| Total | 85% | 63% | 72% |

## Account classifications in 5 categories

| Financial | Email | Social | E-Commerce | Work/Study |
|---|---|---|---|---|
| paypal.com (29) | accounts.google.com (19) | facebook.com (54) | amazon.com (38) | dropbox.com (27)) |
| chase.com (15) | yahoo.com (14) | linkedin.com (43) | apple.com (22) | aws.amazon.com (15) ) |
| bankofamerica.com (13) | mail.google.com (11) | twitter.com (39) | groupon.com (14) | soundcloud.com (13) |
| moneybookers.com (12) | mail.aol.com (11) | skype.com (22) | ticketmaster.com (13) | coursera.org (13) ) |
| wellsfargo.com (12) | go.microsoft.com (10) | plus.google.com (22) | walmart.com (12) | sharelatex.com (13) |
| usbank.com (11) | live.com (10) | tumblr.com (17) | hanes.com (12) | wolframalpha.com (12) |
| capitalone.com (11) | www.copy.com (3) | login.skype.com (15) | newegg.com (12) | sas.com (11) |
| online.citibank.com (11) | login.live.com (3) | www.pinterest.com (15) | pacsun.com (11) | piazza.com (10) |

# Weak Passwords

- Study with 621 accounts
- Many passwords were long but weak:
  Median 11-12 chars but could be broken within 6 hours
- Causes of weak passwords?
  - Underestimate attacks (assume online)
  - Users know how to compose good passwords but make them too short
    - Sites that require shorter password get shorter, weaker password
    - Very few sites require more than 10 chars
  - Some users choose to create weak passwords because they are memor able (28%)

# Results - Password Reuse

Actual reuse is large and indiscriminate

| Type of reuse | Verbat. | Verbat. or similar |
|---|---|---|
| All accounts | 98% | 100% |
| Important/Non-imp | 84% | 90% |
| Important/Important | 98% | 100% |
| Non-imp/Non-imp | 64% | 72% |

Users are not aware of their reuse patterns and unintentionally reuse passwords

Simple Password Versioning

| | Type of change | Password pairs | Example |
|---|---|---|---|
| simple | Change/add numbers | 15 | qklt → qklt18 |
| | Change/add spec. chars | 4 | romine6719 → romine6719] |
| | Change/add alph. chars | 2 | jdofabergs36859 → cqkfabergs36859 |
| | Capitalize first/last char | 4 | coumadinjamkaran → Coumadinjamkaran |
| | Switch digit/spec. positions | 1 | vwuondfk.3 → vwuondfk3. |
| | Change/add one word | 12 | 2735770770 → benigno2735770770 |
| | Total | 38 | |
| cmplx | Combination of 2–3 techniques above | 20 | tranquillizersdenham → tranquillizersdenham9? |
| | Change/add two words and opt. num/spec. char | 3 | ddn1ddn → ddn1ddnauditionsboorstin372 |
| | Total | 23 | |

Users don't take advantage of password managers

SUNY Korea

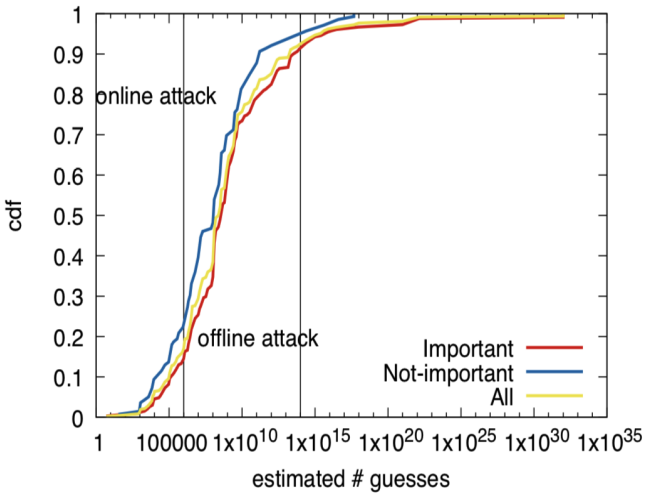
# Results - Password Strength and User Perceptions

Important sites have longer and stronger passwords

Risk-averse users do not have stronger passwords

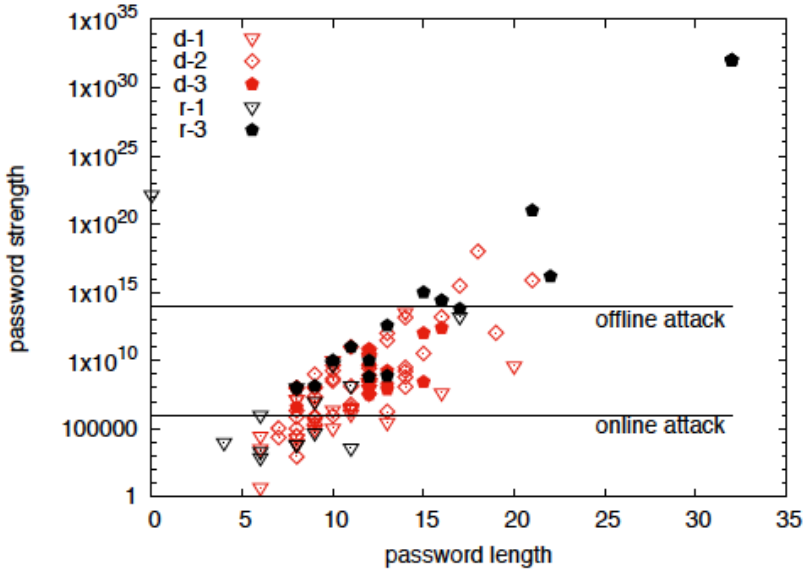
Users' understanding of password attacks is not proportional to strong passwords

Users' passwords are well-composed, but short




SUNY Korea

# Users' password creation strategy




Users understand password structure/class requirement but that is not enough to be strong

SUNY Korea

17

# Password Reuse

- All users reuse their passwords
  - 98% verbatim
  - 84% reuse an important password at a non-important site
- Reuse leads to password leakage
  - On authentication failure a user tries other existing passwords
- Main cause of reuse: memorability
  - 100% of participants

SUNY Korea

18

# Summary

- Help users in understanding their current choices
  - How many accounts they really have
  - How much reuse they practice
  - Help identify important accounts and choose strong but memorable passwords for those
  - Other accounts can have weak or one-time passwords
- Create new text-based authentication mechanisms that lower cognitive burden
- Use Password Manager
- Better way to help users create both memorable and strong passwords

SUNY Korea

19

# Final Remarks

## Password Managers

- Help users in understanding their current choices
- Suggest and automate better strategies

## Websites

- Improve password policies

SUNY Korea

# Thank you!
# Questions?

Assistant Professor Simon Woo
(http://rm-rf.onlne)

simon.woo@sunykorea.ac.kr

The 24th Network Security Conference -Korea

# 최근 랜섬웨어 동향 및 전망

**김병재** KISA 선임

### 학력 및 경력사항

동국대학교 대학원 정보보호학 석사
국군사이버사령부 근무 (2012 ~ 2016)
한국인터넷진흥원 근무 (2016 ~ 현재)

### 강연요약

랜섬웨어는 1989년 최초의 랜섬웨어 AIDS를 시작으로 유행하기 시작했으며, 국내의 경우 2015년 크립토락커(cryptolocker) 한글버전이 유포되면서 본격적으로 사회문제가 되었다.
작년 전세계를 강타한 워너크라이(wannacry) 랜섬웨어와 같이 새로운 기술과 결합되어 진화하고 있으며, 앞으로도 꾸준히 진화 할 것이다.
이 강의에서는 이슈된 랜섬웨어의 특징을 정리해보고, 어떤식으로 진화하였으며 앞으로의 전망에 대해 짚어보고자 한다.

# 최근 랜섬웨어 동향 및 전망

2018.04.12

사이버침해대응본부 침해사고분석단 분석2팀
김 병 재 선임연구원
kimbyeongjae@kisa.or.kr

KISA

KISA

## Contents

1. 랜섬웨어 동향
2. 랜섬웨어 종류 및 트렌드
3. 랜섬웨어 전망

# 1. 랜섬웨어 동향

## 1. 랜섬웨어 동향

### 1-1. 랜섬웨어란?

Ransom

+

SoftWare

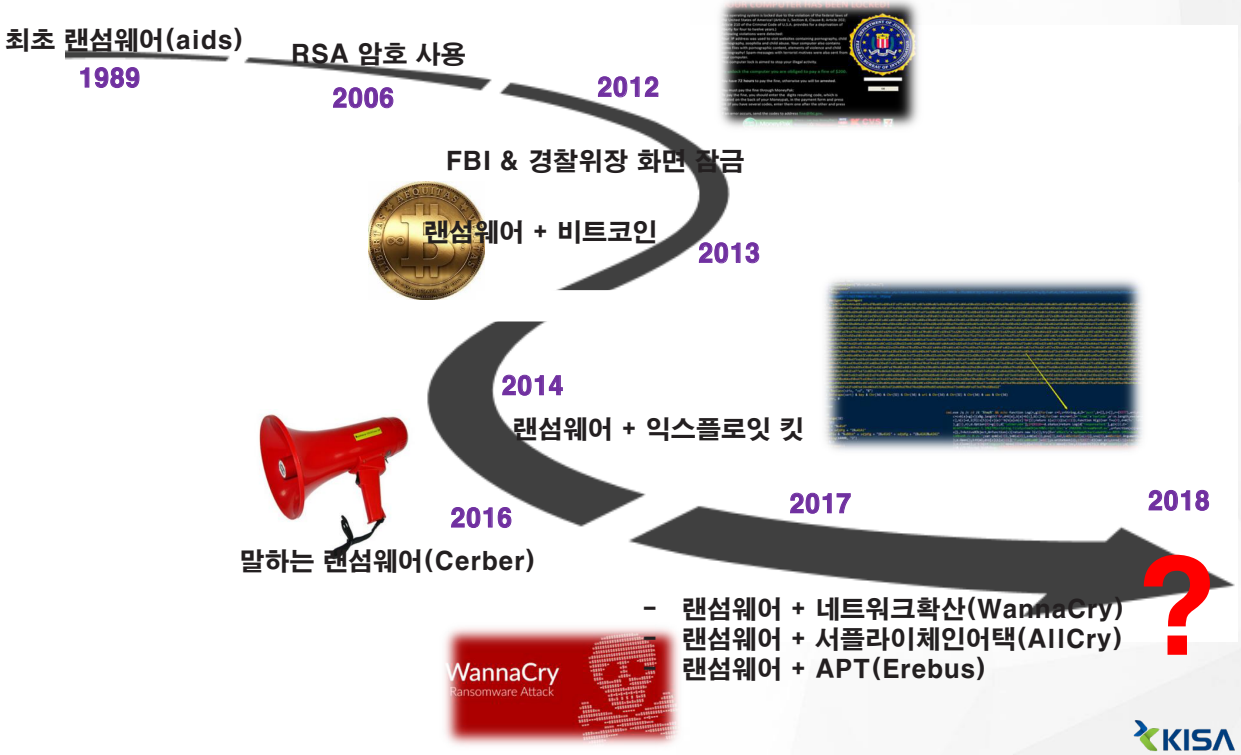
# 1. 랜섬웨어 동향

## 1-2. 랜섬웨어 분류

KISA

# 1. 랜섬웨어 동향

## 1-3. 랜섬웨어 역사

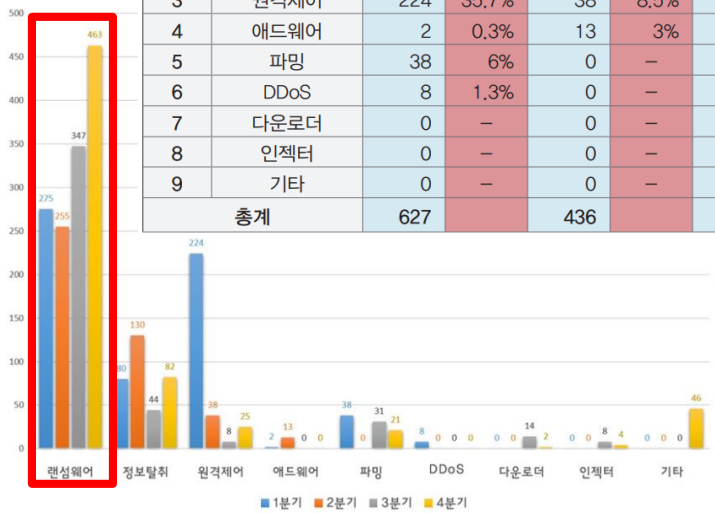



KISA

# 1. 랜섬웨어 동향

## 1-4. 통계(KISA)

| | 악성코드 종류 | 1분기 | | 2분기 | | 3분기 | | 4분기 | | 분기 증감률 (3분기대비 4분기) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 건수 | 비율 | 건수 | 비율 | 건수 | 비율 | 건수 | 비율 | |
| 1 | 랜섬웨어 | 275 | 44% | 255 | 58.5% | 347 | 77% | 463 | 72% | 33.4% ↑ |
| 2 | 정보탈취 | 80 | 12.7% | 130 | 30% | 44 | 10% | 82 | 13% | 86% ↑ |
| 3 | 원격제어 | 224 | 35.7% | 38 | 8.5% | 8 | 1.5% | 25 | 4% | 212.5% ↑ |
| 4 | 애드웨어 | 2 | 0.3% | 13 | 3% | 0 | – | 0 | – | – |
| 5 | 파밍 | 38 | 6% | 0 | – | 31 | 7% | 21 | 3% | 32% ↓ |
| 6 | DDoS | 8 | 1.3% | 0 | – | 0 | – | 0 | – | – |
| 7 | 다운로더 | 0 | – | 0 | – | 14 | 3% | 2 | 0.4% | 86% ↓ |
| 8 | 인젝터 | 0 | – | 0 | – | 8 | 1.5% | 4 | 0.6% | 50% ↓ |
| 9 | 기타 | 0 | – | 0 | – | 0 | – | 46 | 7% | – |
| 총계 | | 627 | | 436 | | 452 | | 643 | | |




※ 2017년 한국인터넷진흥원에서 진행한 과제에서 수집된 악성코드의 분석 자료를 바탕으로 작성되었으며, 타 기관의 통계자료와 상이할 수 있음

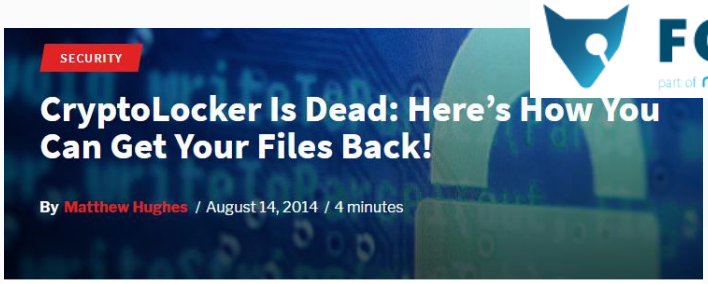
KISA

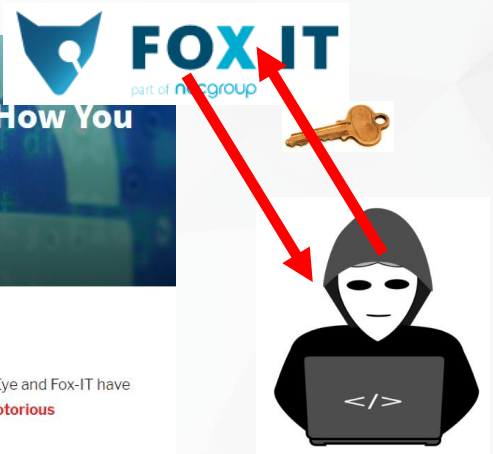
# 2. 랜섬웨어 종류 및 트렌드

# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 2014년 8월경 Crypt0L0cker V1 유포
- Fox-IT 보안업체가 복호화 키 탈취 및 복호화 툴 공개

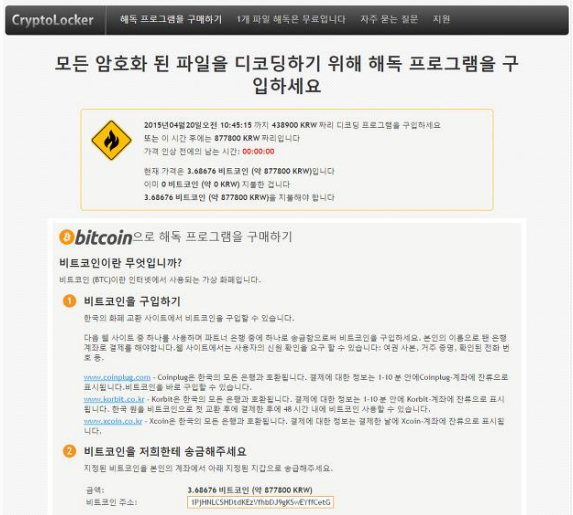


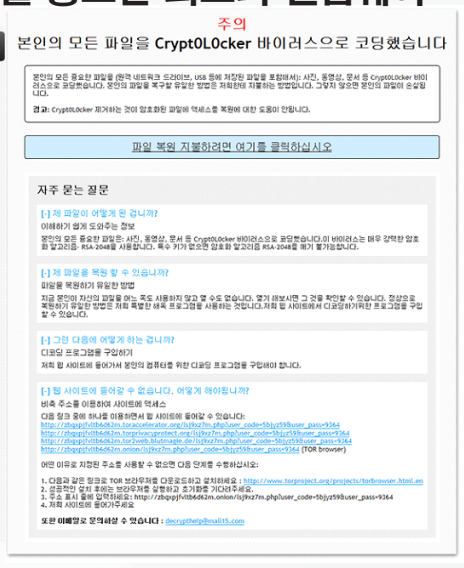




# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 2015년 4월경 국내에 최초로 유포된 랜섬웨어
- 한글 메시지를 이용하여 감염 사실 통보한 최초의 랜섬웨어

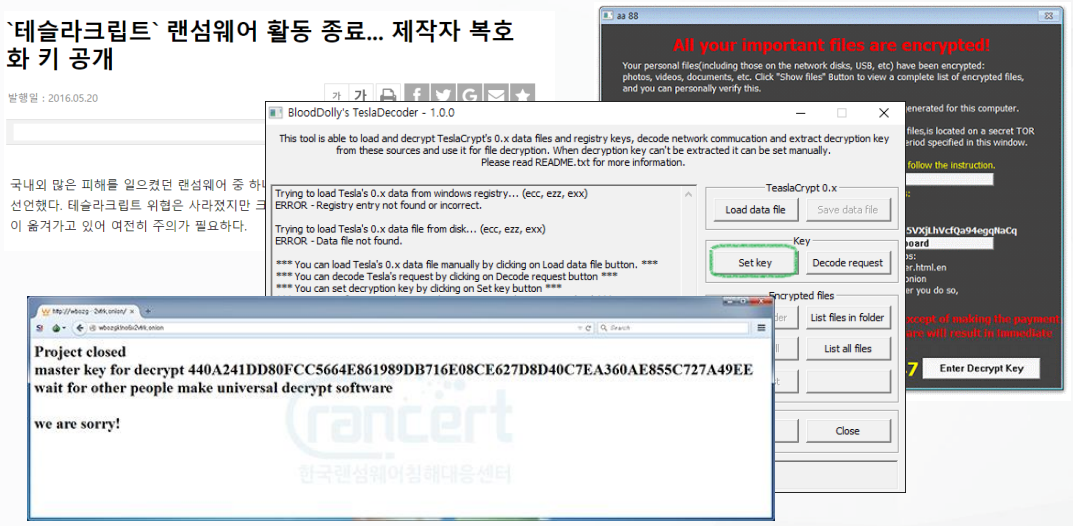


# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- ActiveX 및 스피어 피싱으로 유포
- 제작자가 복호화 키를 공개하여, 그 이후 활동 종료




rancert 한국랜섬웨어침해대응센터

KISA

# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 랜섬웨어 패치를 통해 지속적인 업데이트

**.CRYPT v1** : 카스퍼스키에서 복호화 도구 지원

↓ **취약점 패치**

**.CRYPT v2** : 안랩 복호화 도구 지원

↓ **취약점 패치**

**.CRYPT v3** : 복호화 불가 / 비트코인 지불시 복호화 불가

↓ **지불 방법 변경**

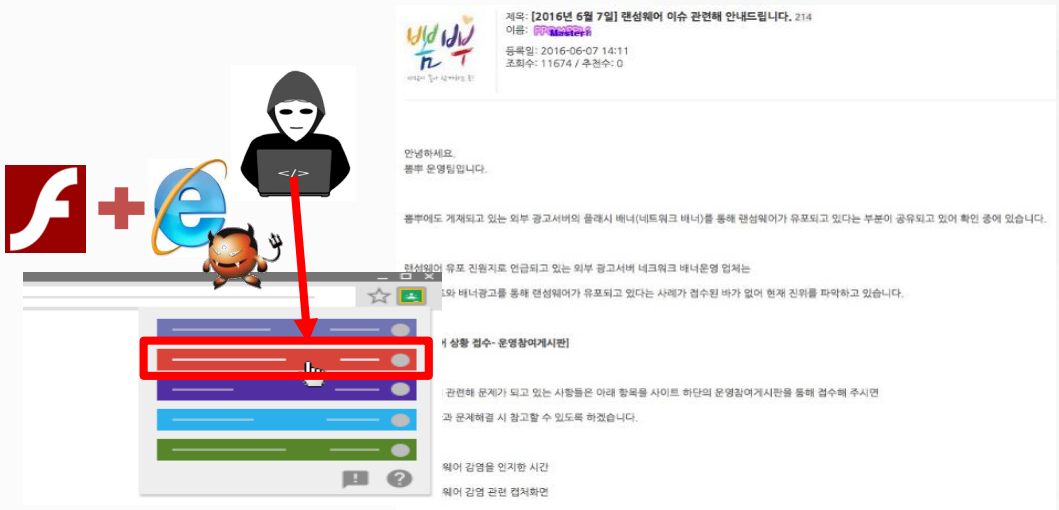
**.CRYPT v4** : 복호화 일부 가능 / 비트코인 지불시 복호화 가능

KISA

# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 국내 웹사이트에 멀버타이징 기법을 이용하여 유포

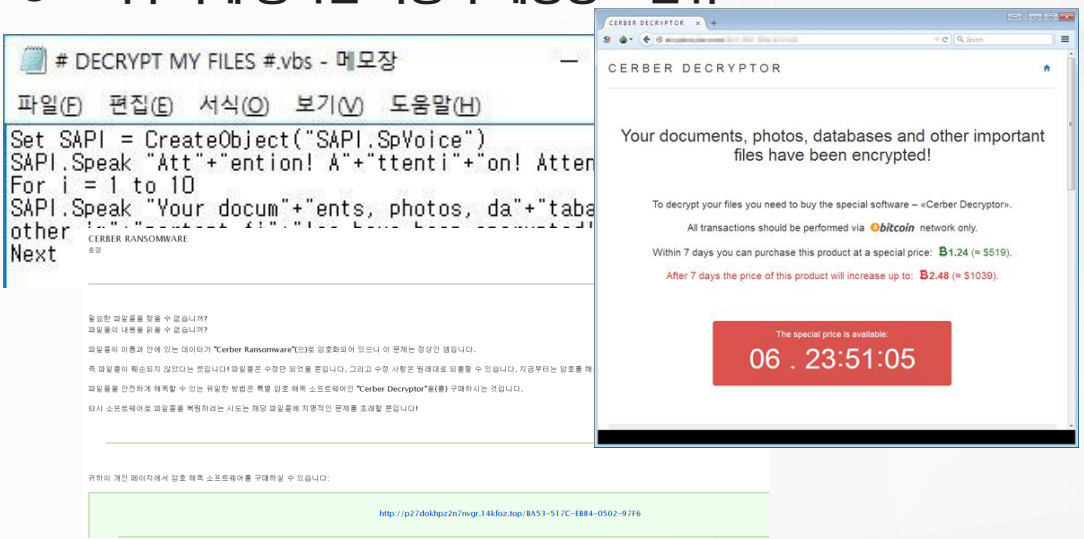





# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

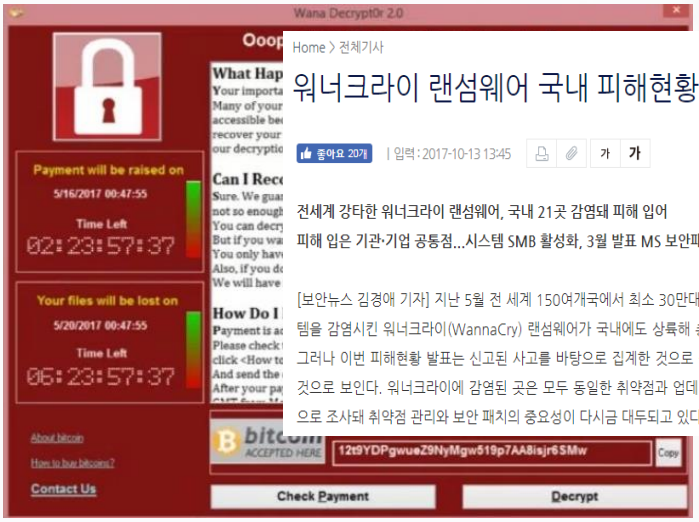
- 텍스트를 음성메세지로 변환하는 최초의 말하는 랜섬웨어
- 브라우저에 등록된 사용자 계정정보 탈취



# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → **Wannacry** → Erebus → AllCry → Hermes

- 2017년 2월 최초로 개발
- 4월 공개된 SMB 취약점을 추가하여 5월 변종 개발 및 유포




Home > 전체기사

## 워너크라이 랜섬웨어 국내 피해현황 집계해보니...21곳 감염 신고

좋아요 20개 | 입력 : 2017-10-13 13:45

전세계 강타한 워너크라이 랜섬웨어, 국내 21곳 감염돼 피해 입어

피해 입은 기관·기업 공통점...시스템 SMB 활성화, 3월 발표 MS 보안패치 미적용

[보안뉴스 김경애 기자] 지난 5월 전 세계 150여개국에서 최소 30만대 이상이 컴퓨터 시스템을 감염시킨 워너크라이(WannaCry) 랜섬웨어가 국내에도 상륙해 총 21곳이 감염됐다. 그러나 이번 피해현황 발표는 신고된 사고를 바탕으로 집계한 것으로 실제 피해는 더 컸을 것으로 보인다. 워너크라이에 감염된 곳은 모두 동일한 취약점과 업데이트를 하지 않은 것으로 조사돼 취약점 관리와 보안 패치의 중요성이 다시금 대두되고 있다.

가장 많이 본 기사 [주간]

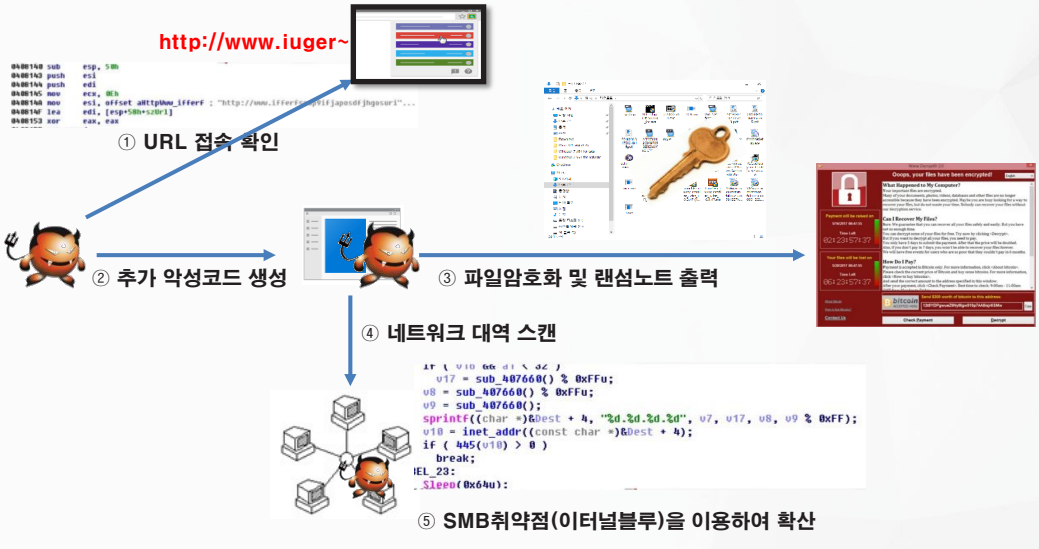
1 행정전자서명, 시도교육청의 무분별한 발급
2 한국정보보호산업협회, '정보보호인정협회'
3 코드게이트 2018, 한국 '앙진모띠' 팀 우...
4 해킹 몰라도 해킹 범죄 일으키게 해주는 새로
5 한국인 노리는 안드로이드 및 윈도우용 멀웨
6 북한 관련자들 노린 '레드 아이즈'의 사이버
7 [주말판] GDPR이 만들 부정적 현상들을 걱
8 봄바람 휘날리며~ 늘어나는 보안인력 채용
9 애플, 보안 취약점 대거 발견! 최신 버전 업
10 봄 나들이 갈 때 교통안전도 챙기세요
11 악마의 컴백? 돌아온 사탄 랜섬웨어 감염 주



# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → **Wannacry** → Erebus → AllCry → Hermes

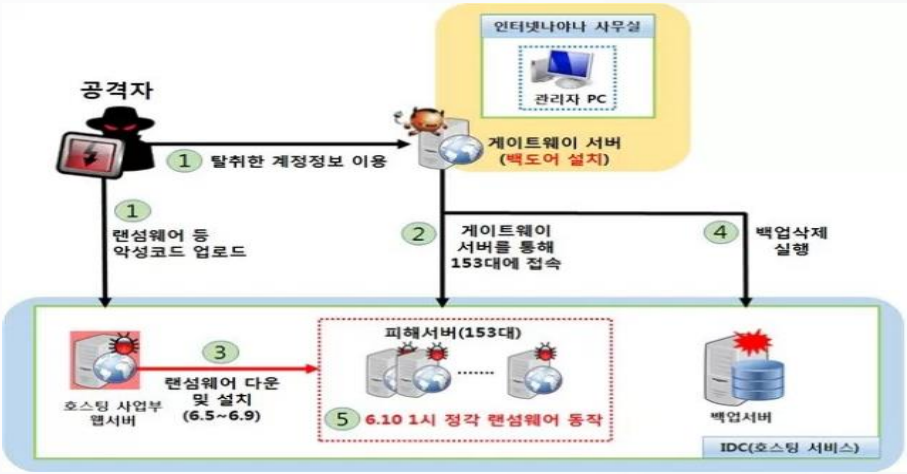
- 4월 공개된 SMB 취약점을 추가하여 5월 변종 개발 및 유포
- URL 접속여부 체크를 위한 킬스위치 존재(샌드박스 우회)



# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 최초에 윈도우용이 나왔으나, 리눅스 서버용 유포
- 국내 최초 기업타겟형 APT 랜섬웨어

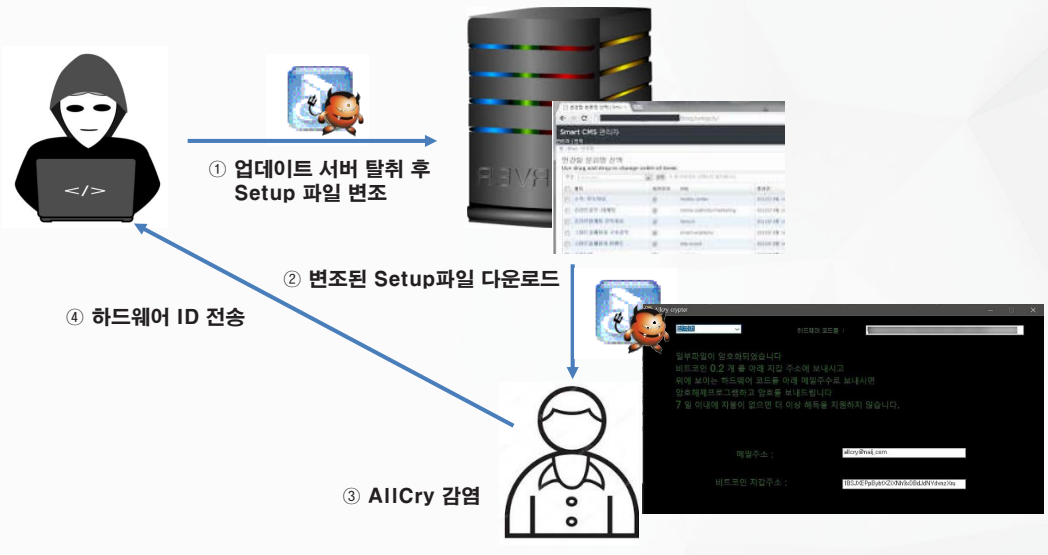





# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

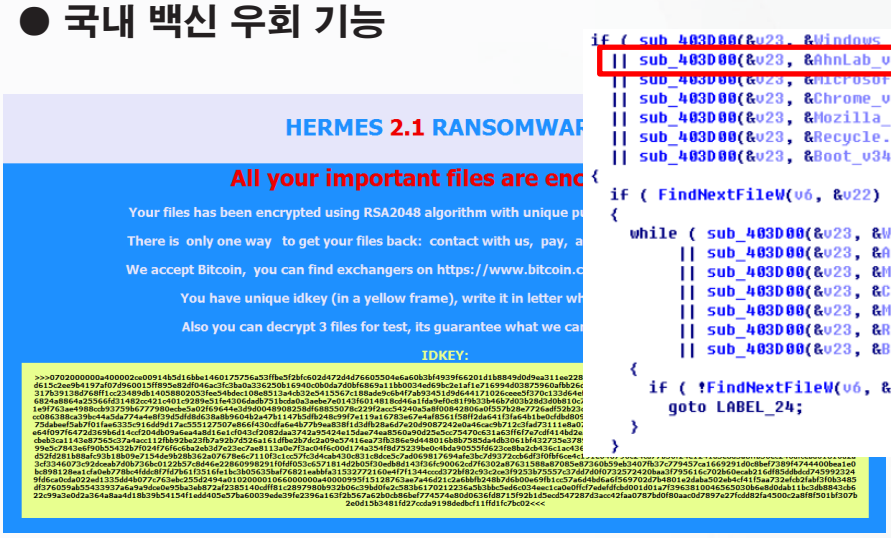
- 추석연휴 Supply Chain Attack 기법을 이용하여 유포



# 2. 랜섬웨어 종류 및 트렌드

Crypt0L0cker → TeslaCrypt → CryptXXX → Cerber → Wannacry → Erebus → AllCry → Hermes

- 최신 플래쉬 취약점(CVE-2018-4878)을 활용하여 유포
- 국내 백신 우회 기능




```
if ( sub_403D00(&v23, &Windows_v40)
  || sub_403D00(&v23, &AhnLab_v42)
  || sub_403D00(&v23, &Microsoft_v38)
  || sub_403D00(&v23, &Chrome_v47)
  || sub_403D00(&v23, &Mozilla_v28)
  || sub_403D00(&v23, &Recycle.Bin_v24)
  || sub_403D00(&v23, &Boot_v34) )
{
  if ( FindNextFileW(v6, &v22) )
  {
    while ( sub_403D00(&v23, &Windows_v40)
         || sub_403D00(&v23, &AhnLab_v42)
         || sub_403D00(&v23, &Microsoft_v38)
         || sub_403D00(&v23, &Chrome_v47)
         || sub_403D00(&v23, &Mozilla_v28)
         || sub_403D00(&v23, &Recycle.Bin_v24)
         || sub_403D00(&v23, &Boot_v34) )
    {
      if ( !FindNextFileW(v6, &v22) )
        goto LABEL_24;
    }
  }
```

KISA

# 3. 랜섬웨어 전망

# 3. 랜섬웨어 전망

● 산업용 시스템 마비를 통한 금전 요구

● 자동차 등 IoT 장비의 감염을 통한 사회적 혼란

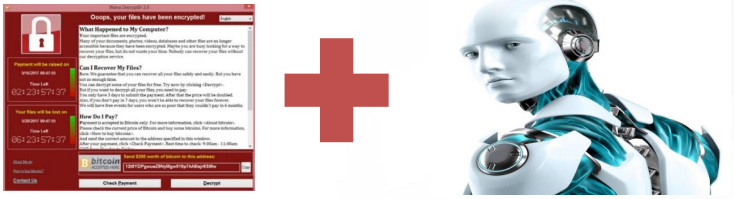
《자료:프리스케일

KISA

# 3. 랜섬웨어 전망

● 의료업계(개인정보, 의료데이터 등) 타겟 랜섬웨어

● AI 기술을 이용한 지능형 랜섬웨어



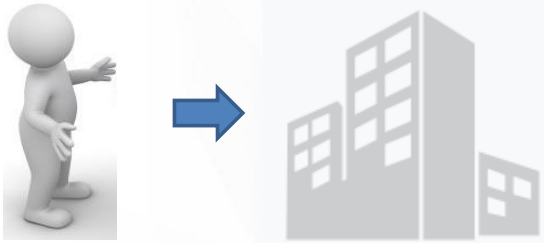
● 랜섬웨어와 암호화폐 채굴형 악성코드의 결합

KISA

# 3. 랜섬웨어 전망

● 타겟의 확장

- 개인에서 기업으로
- 데스크탑에서 서버로



● Supply Chain Attack 증가

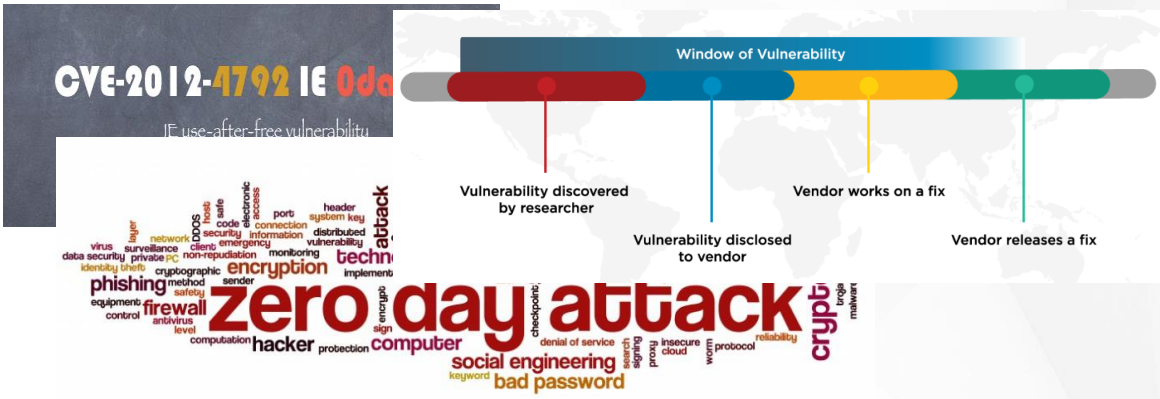
- NETSARANG Xshell Setup File( '17.8)
- Avast ccleaner Setup File( '17.9)
- Web Hard Setup File( '17.9)

한국 겨냥 '올크라이' 랜섬웨어 소강상태 "긴장 늦춰선 안 돼"
디지털데일리 | 2017.10.03. | 네이버뉴스
이스트시큐리티 시큐리티대응센터(ESRC)에 따르면 지난달 26일부터 올크라이(AllCry) 랜섬웨어가 국내에 전파됐다. 한국의 특정 웹하드 **설치** 프로그램, 잠재적으로 불필요한 프로그램(PUP) 등을 변조해 사용자 몰래...

KISA

# 3. 랜섬웨어 전망

● Not 0-day, 1-day vulnerability is enough




● 결국..금전

- 정보 유출 등 해킹 후 랜섬웨어 or 채굴형 악성코드 감염

KISA

Internet On, Security In!
감사합니다
사이버침해대응본부 침해사고분석단 분석2팀
김 병 재 선임연구원
kimbyeongjae@kisa.or.kr, kimbyeongjae@krcert.or.kr

The 24th Network Security Conference -Korea

# 브라우저 보안의 진화

**박세준** 티오리 대표

### 학력 및 경력사항

Carnegie Mellon University (2011, 2012)
– Computer Science 학사 및 석사
CMU 해킹동아리 PPP 설립
– DEFCON 최다 우승 (4회)
– 코드게이트 최다 우승 (4회)
– 시큐인사이드 최다 우승 (3회)
– 이외 40여 이상 대회 우승
Kaprica Security 공동창업자 (2011 ~ 2016)
Theori 및 티오리한국 대표 (2016 ~ 현재)

### 강연요약

웹브라우저는 가장 많은 사용자를 보유한 가장 복잡한 프로그램 중 하나다. 이에 따라, 각종 범죄 그룹 및 정부간 사이버 공격에 필수적으로 사용되는 APT 공격 벡터 중 하나가 됐다.
이번 강연에서는 다양한 브라우저들의 보안성이 지난 몇 년간 어떻게 진화해왔는지 살펴보고, 이러한 진화가 익스플로잇 기법 및 보호기법 우회 기술의 변화에 어떤 영향을 미쳤는지 등을 설명한다. 더 나아가, 공격자 입장에서 분명히 난이도가 올라갔음에도 불구하고 최신 버전들 조차도 여전히 공격에서 자유롭지 못하다는 점을 시사한다.

강연자의 요청으로
발표자료를 공개해 드리지 못한 점
양해 부탁드립니다.

The 24th Network Security Conference -Korea

# 비트코인 시스템의 이해

**김형식** 성균관대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1995 ~ 1999 | 성균관대 정보보학과 학사 |
| 1999 ~ 2001 | 카이스트 전산학과 석사 |
| 2008 ~ 2011 | 케임브리지 대학교 전산학과 박사 |
| 2004 ~ 2008 | 삼성전자 책임 연구원 |
| 2012 ~ 2013 | 브리티쉬 콜럼비아 대학 박사 후 연구원 |
| 2013 ~ 현재 | 성균관대학교 조교수 |

### 강연요약

A blockchain a digitized, decentralized, public ledger of all cryto–related transactions to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. The technology might be used for many different purposes from financial applications to supply chains to identity management. Blockchain is so appealing to users because they are decentralized and programmable for smart contracts. In this talk, I will present how blockchains work, how to use them, and how to develop software that works with them through the Bitcoin system.

Sungkyunkwan University

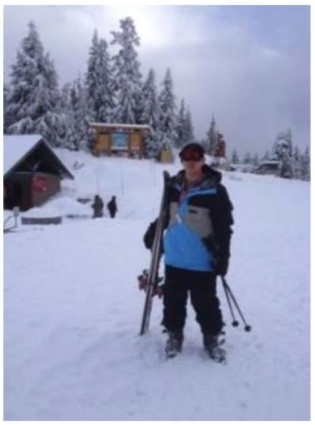
# 비트코인 시스템의 이해

**Hyoungshick Kim**
Department of Software
College of Software
Sungkyunkwan University

# Hyoungshick Kim (김형식)

**Assistant Professor** in Department of Software, Sungkyunkwan University

- Education
  - ✓ Ph.D. in Computer Science, University of Cambridge
- Experiences
  - ✓ Professor, Sungkyunkwan University, Korea (2013 – present)
  - ✓ Postdoctoral Fellow, University of British Columbia, Canada (2012-2013)
  - ✓ Senior Engineer, Samsung Electronics (2004-2008)
- Research interests:
  - ✓ Security engineering
  - ✓ Usable security
  - ✓ Security vulnerability analysis
- Homepage: http://seclab.skku.edu/

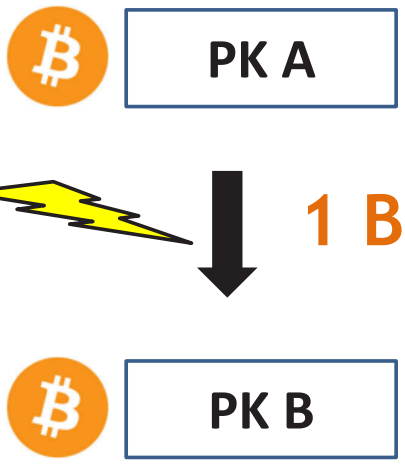


- Lab members:
- Academic staff: 2
- PhD students: 5
- MS students: 12

# Bitcoin

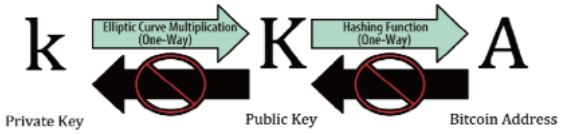
- A distributed, decentralized digital currency system
- Invented by Satoshi Nakamoto 2008
- Private money based on
  - cryptography
  - a distributed transaction log (public ledger)
    - history shows how many bitcoins each user has

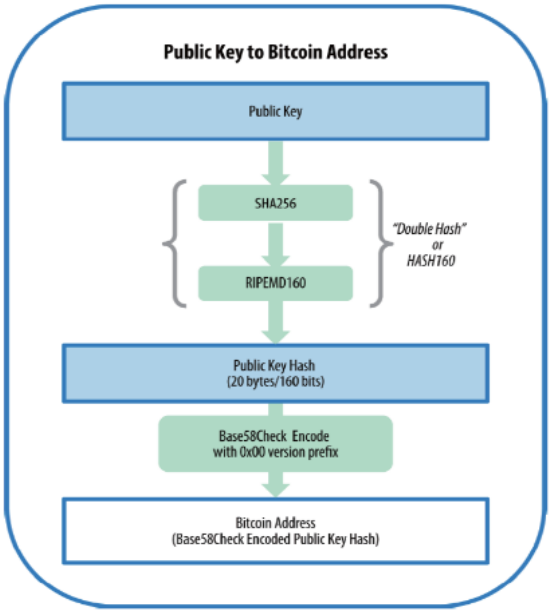
# In a public ledger




PK A: 1 BTC PK B: 2 BTC

# Bitcoin key and address



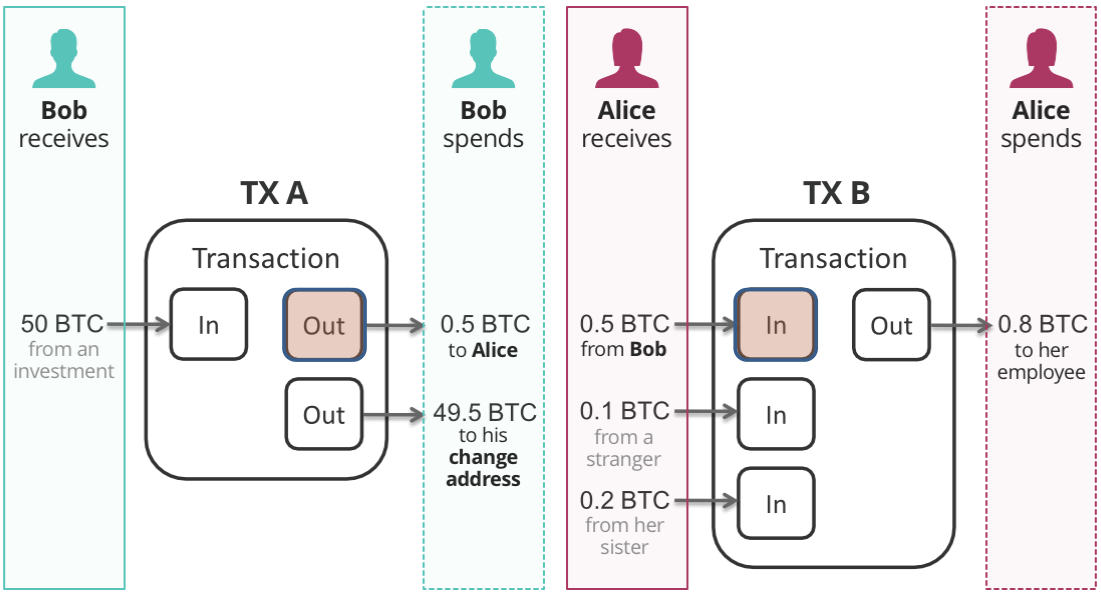




Double hash can be effective against "length-extension" attack

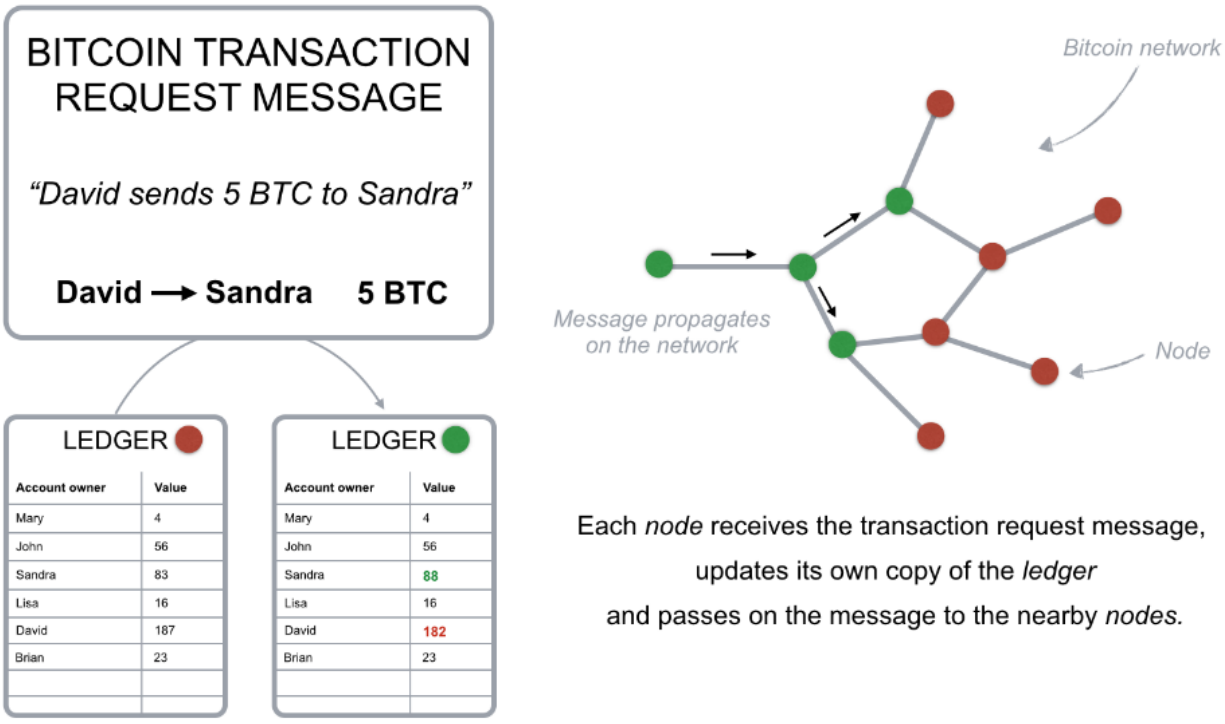
Base58 is Base64 without the 0 (number zero), O (capital o), l (lower L), I (capital i), + and /.

# Transactions in Bitcoin

A transaction is of the form "Send 0.5 Bitcoins from Bob to Alice"



# Ledger is synchronized

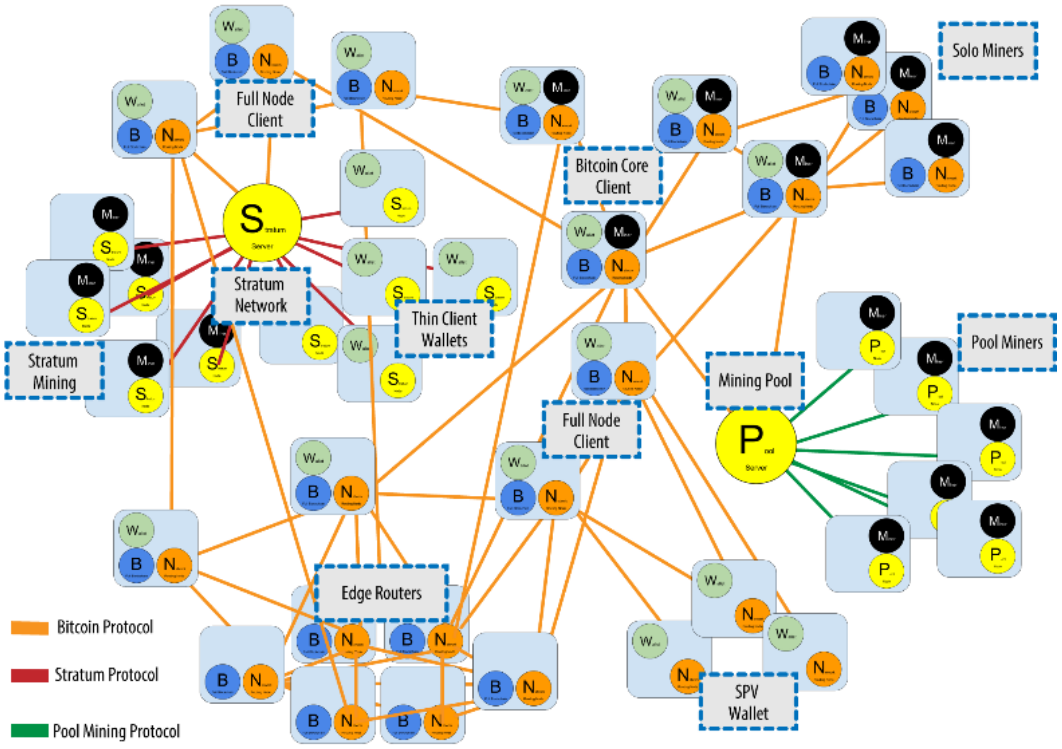



Each *node* receives the transaction request message,
updates its own copy of the *ledger*
and passes on the message to the nearby *nodes*.

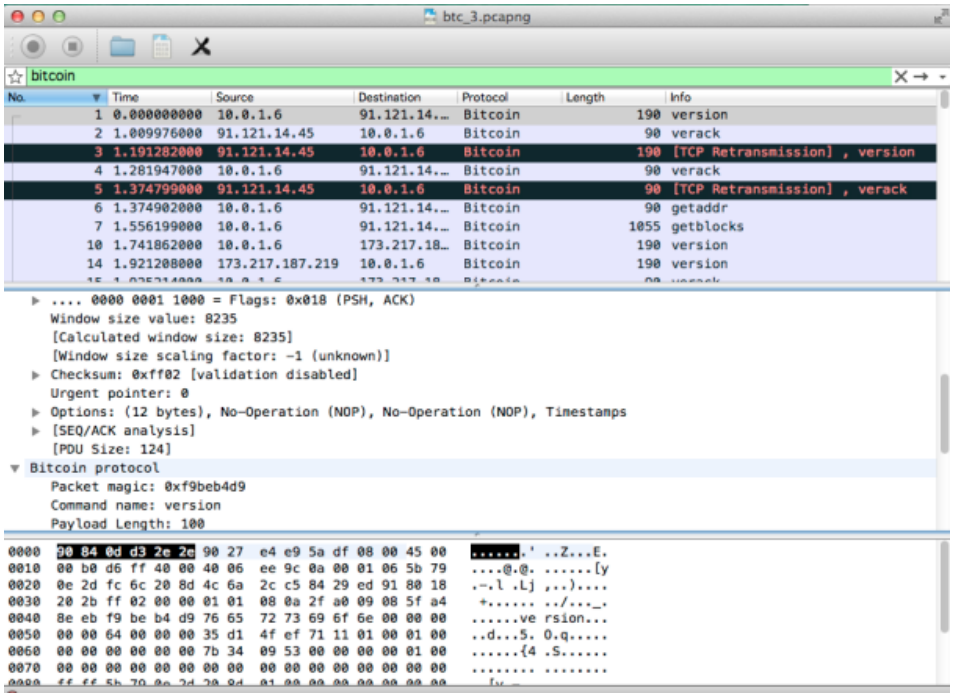
# Transaction agreement

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a proof-of-work for its block (The one to finish early will probably win).
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
6. Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

# Bitcoin P2P network




# Bitcoin message in Wireshark



# Bitcoin node

- A bitcoin node is a collection of functions:
  - routing, the blockchain database, mining, and wallet services.

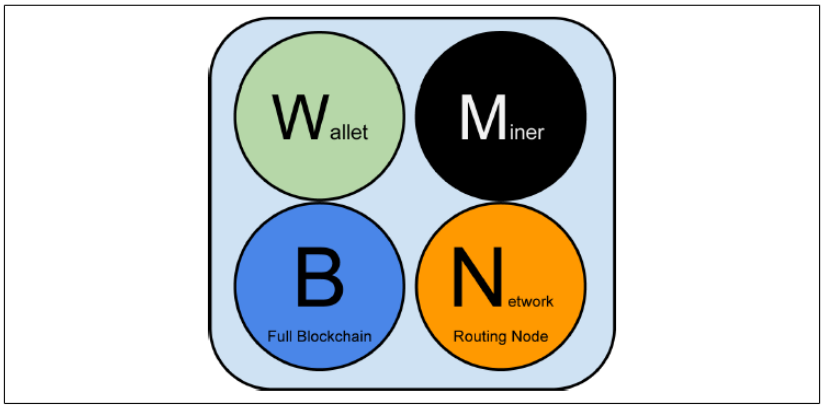
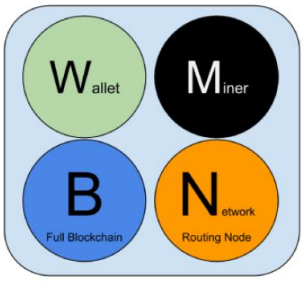
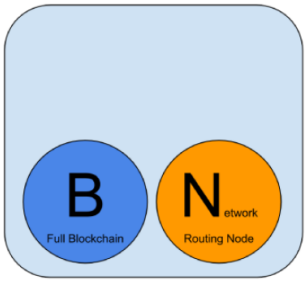



*Figure 8-1. A bitcoin network node with all four functions: wallet, miner, full blockchain database, and network routing*

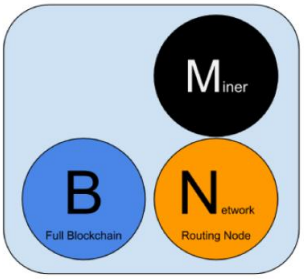
# Node types and roles



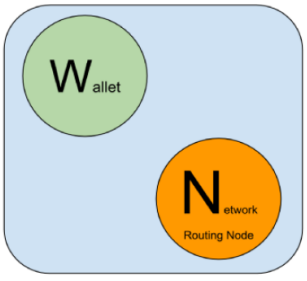

**Reference Client**




**Full Block Chain Node**




**Solo Miner**




**Lightweight (SPV) wallet**

# Network discovery

- How does a new node find peers?

1. "**DNS seeds**" which are DNS servers that provide a list of IP addresses of Bitcoin nodes
   - The Bitcoin Core client contains the names of five different DNS seeds
   - **-dnsseed** (by default)
2. Known IP address of at least one Bitcoin node
   - After the initial seed node is used to form introductions, the client will disconnect from it and use the newly discovered peers.
   - **-seednode**

# Handshake

- To connect to a known peer, nodes establish a TCP connection (usually to port 8333)
- The node will start a "handshake" by transmitting a version message
- The node receiving a version message will examine the reported nVersion and, if compatible, it will acknowledge the version message by sending a verack

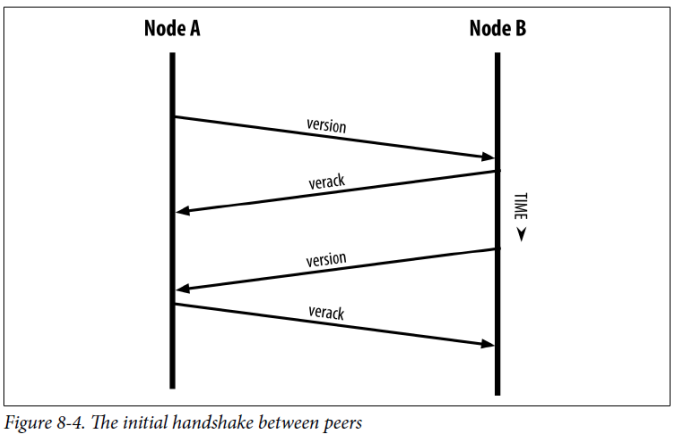



*Figure 8-4. The initial handshake between peers*

# Updating peers

- Once one or more connections are established, the new node will send an addr message containing its own IP address to its neighbors
- The new node can send getaddr message to the neighbors, asking them to return a list of IP addresses of other peers

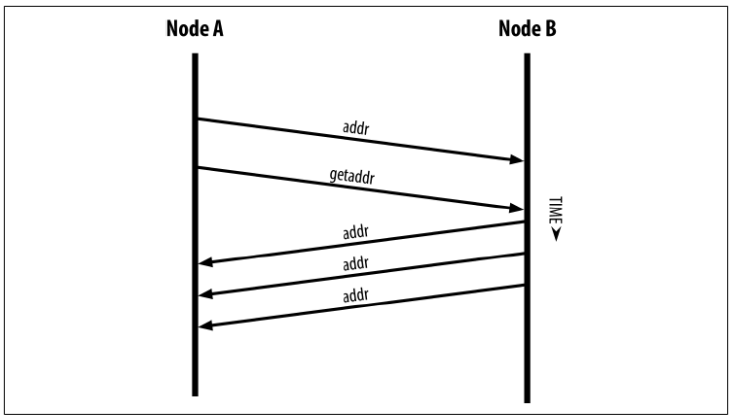


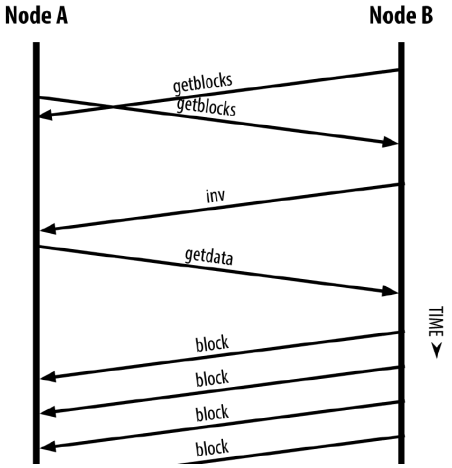

*Figure 8-5. Address propagation and discovery*

# Full nodes

- Full blockchain nodes maintain a **complete and up-to-date copy of the bitcoin blockchain** with all the transactions
- A full blockchain node can independently verify any transaction without reliance on any other node or source of information
- Full blockchain node relies on the network to receive updates about new blocks of transactions, which are incorporated into its local copy of the blockchain

# Synchronizing the blockchain

- Nodes exchange a ***getblocks*** message that contains the hash of the top block on their local blockchain
- The node that has the longer blockchain shares the first 500 blocks with other nodes (***inv*** containing hashes of blocks)




# SPV nodes

- For space- and power-constrained devices, a simplified payment verification (SPV) method is used to allow them to operate **without storing the full blockchain**
- SPV nodes download only the block headers and do not download the transactions included in the block
  - 1,000 times smaller than full blockchain

# Synchronizing the headers

- To get the block headers, SPV nodes use a ***getheaders*** message instead of *getblocks*
  - The responding peer will send up to 2,000 block headers using a single ***headers*** message

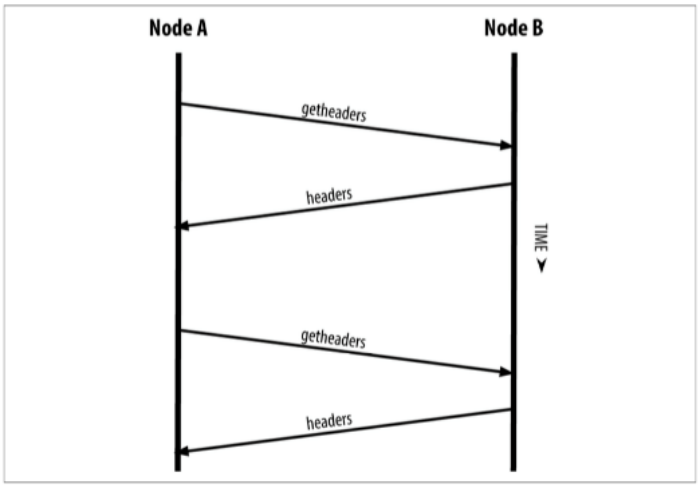



*Figure 8-7. SPV node synchronizing the block headers*

19

# Operations of SPV nodes

- SPV nodes need to retrieve specific transactions using ***getdata*** message in order to selectively verify them

- SPV node's requests for specific data can inadvertently reveal the likability between its network address and wallet address
  - For example, a third party monitoring a network could keep track of all the transactions requested by a wallet and use those to associate bitcoin addresses with network address.

# Use of Bloom filters

- Bloom Filters
  - A probabilistic data structure that is used to test membership of an element.
  - SPV nodes ask their peers **for transactions matching a specific pattern using Bloom filters**, without revealing precisely which addresses they are interested in.

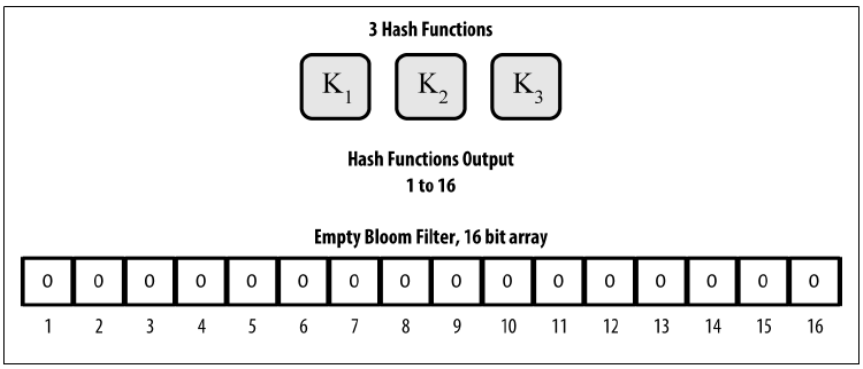



*Figure 8-8. An example of a simplistic bloom filter, with a 16-bit field and three hash functions*

# How Bloom filters work (1)

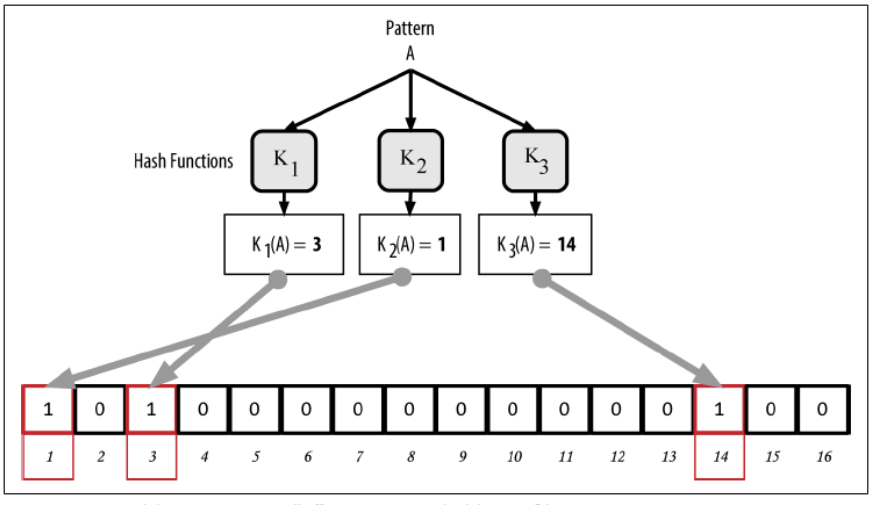



*Figure 8-9. Adding a pattern "A" to our simple bloom filter*

# How Bloom filters work (2)

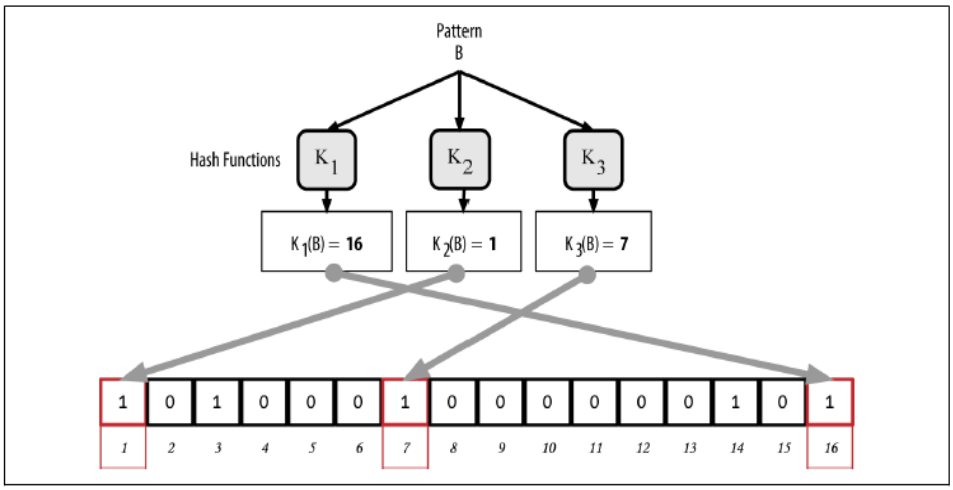



*Figure 8-10. Adding a second pattern "B" to our simple bloom filter*

# How Bloom filters work (3)

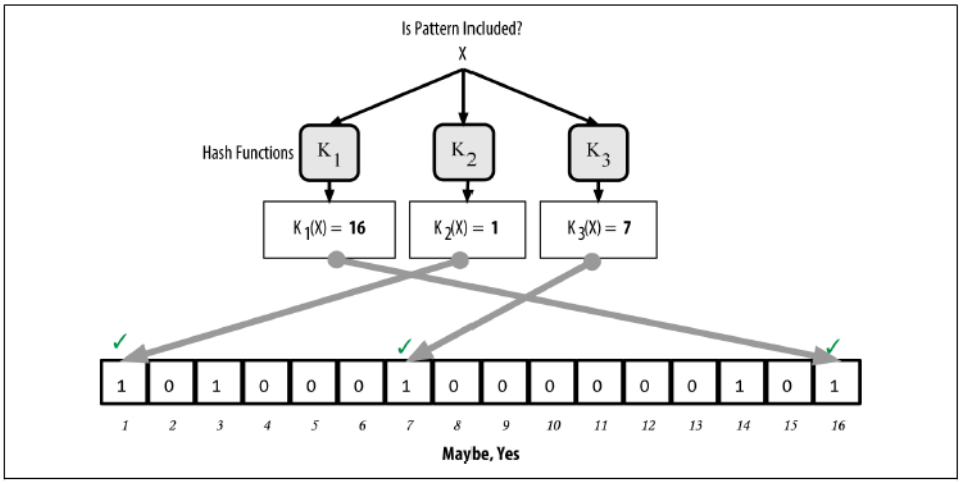


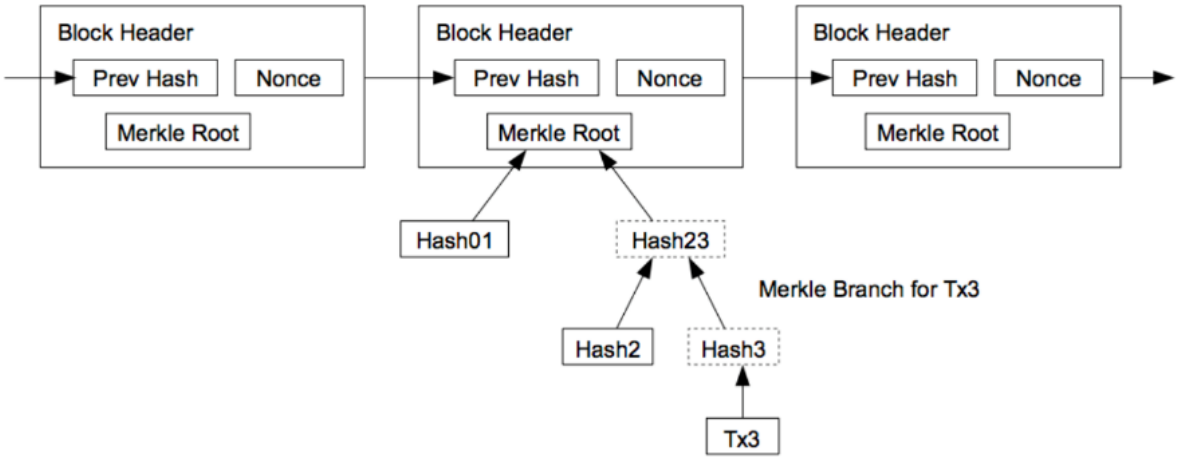

*Figure 8-11. Testing the existence of pattern "X" in the bloom filter. The result is a probabilistic positive match, meaning "Maybe."*

# How to use Bloom filters

- A SPV node adds TXID, Script hash, and PubKey hash (from any UTXO controlled by its wallet) to the bloom filter
- The SPV node sends the bloom filter to a full node using the message filterload
- If the filter has been loaded, then full nodes will send a modified form of blocks, called a Merkle block that contains only block headers for blocks matching the filter and a Merkle path for each matching transaction

# Merkle block and path

- SPV node can check whether the transaction (Tx3) is included in the block.
- Only need Hash01 and Hash2 to verify; not the entire Tx's.



# Encrypted connections

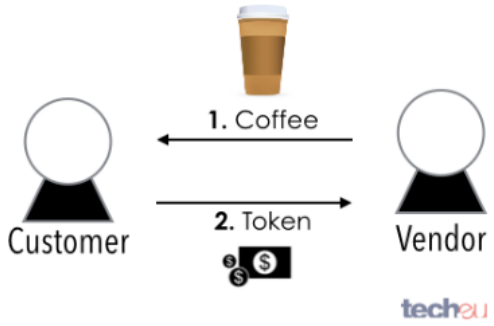
- The original implementation of bitcoin communicates entirely in the clear. It raises a privacy concern for SPV nodes.
- Two solutions that provide encryption of the communications:
  - Tor (The Onion Routing network) transport: since Core v0.12
  - P2P authentication and encryption (BIP-150 and BIP-151)
    - BIP-150 uses ECDSA (Each node's public key must be pre-shared over a different channel)
    - BIP-151 uses ECDH to generate symmetric encryption keys

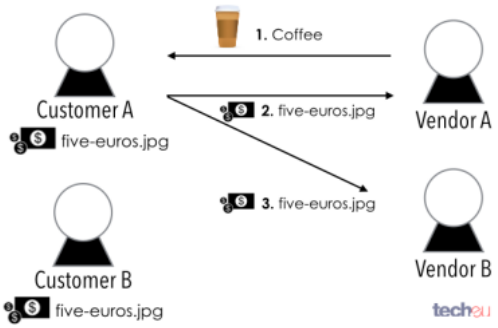
BIP: Bitcoin Improvement Proposal is a design document for introducing features or information to Bitcoin.

# Transaction pool

- Almost every node on the Bitcoin network maintains a temporary list of unconfirmed transactions called the memory pool, mempool, or *transaction pool*
- Nodes use this pool to keep track of transactions that are known to the network but are not yet included in the blockchain.
- For example, a wallet node will use the transaction pool to track incoming payments to the user's wallet that have been received on the network but are not yet confirmed.

# Double spending issue

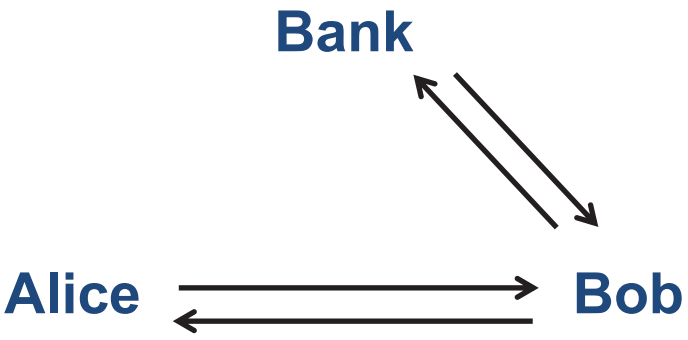



Digital objects can be copied many times.

**How can we prevent this?**

# How traditional e-cash handled problem

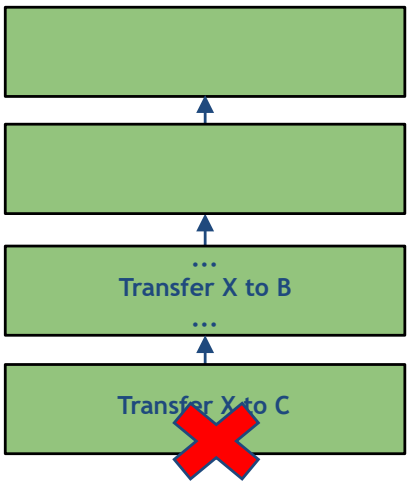



- When Alice pays Bob with a coin, Bob validates that coin hasn't been spend with trusted third party

Bank maintains a linearizable log of transactions

# Can we solve it in decentralized environment?

Maintain a global public append-only log!
The only way is to be aware of all transactions.




*The blockchain -a public ledger of all transactions.*

(In Bitcoin, the log is extended in increments of blocks, each of which may contain thousands of transactions.)

# Consensus of the block state is needed

- The system must agree on some “canonical order” of transactions
- Who will be responsible for managing blocks?
- Think of this mechanism as being like some kind of “voting”

# Election based on "work"

- Rather than "count" IP addresses, bitcoin "counts" the amount of CPU time / electricity that is expended
- Economic defense against sybil attacks

> **"The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."**
> **- Satoshi Nakamoto**

- Proof-of-work: Cryptographic "proof" that certain amount of CPU work was performed

# *Hashcash* – Proof of Work

To demonstrate work on $x$, find $y$ such that

$$H(x, y) < z,$$

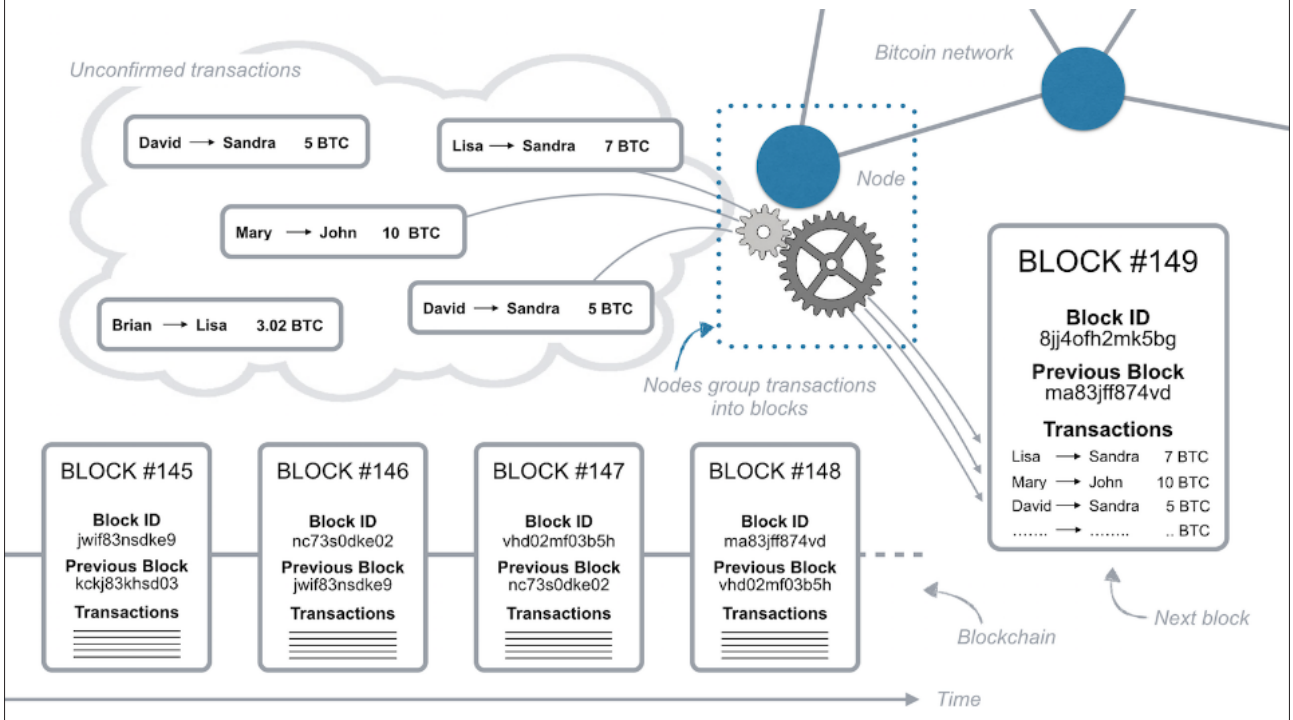
for some pre-determined bound $z$.

The core idea is that before accepting a transaction, the sender must first demonstrate a "cost" via a computationally "hard" problem that can simultaneously be easily verified.

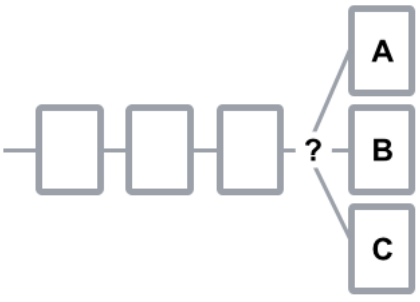
Application: spam email prevention

"Hashcash," Adam Back, 1997 (http://www.hashcash.org/papers/announce.txt).

# Bitcoin network overview

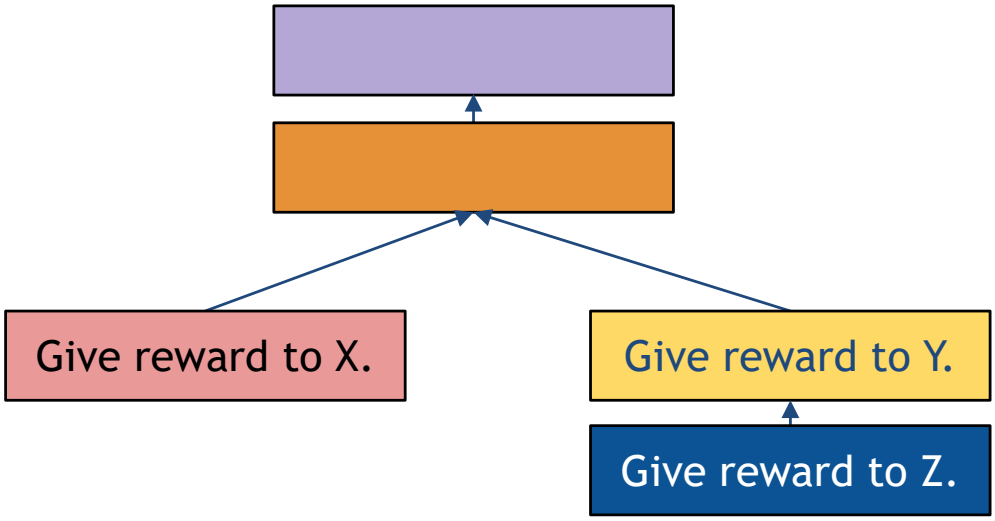



# Problem remains: forking

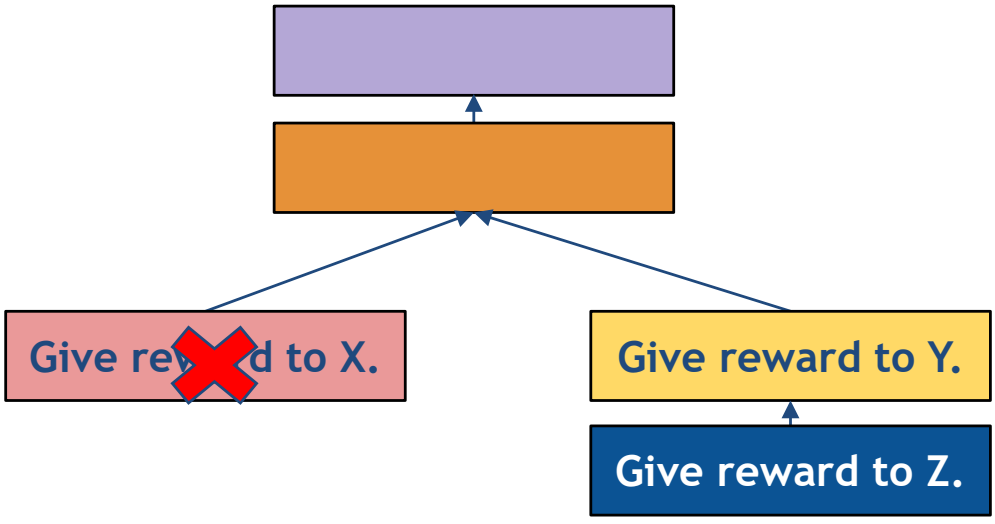



Sometimes multiple nodes solve the mathematical problem at the same time.

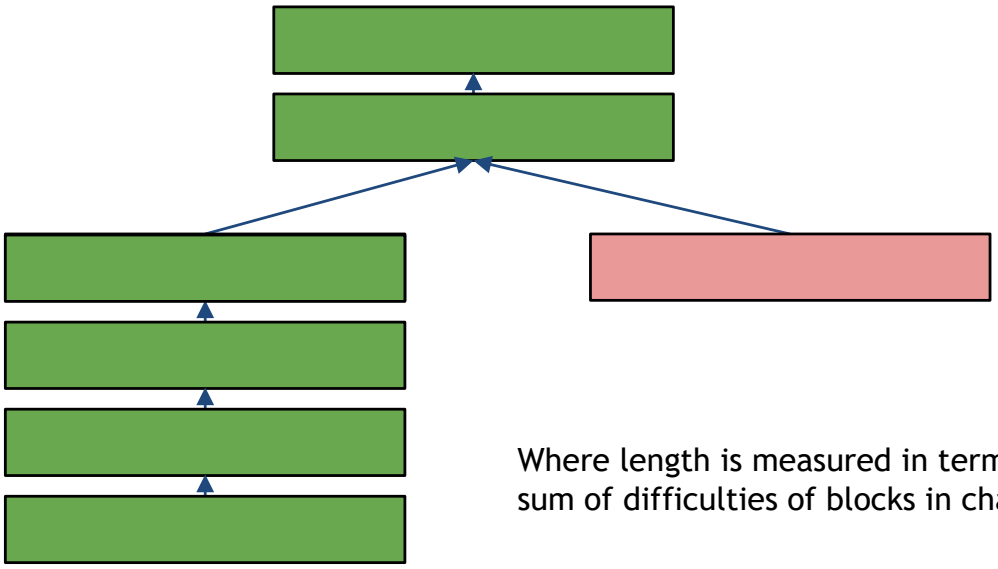
A *fork* can occur when two miners publish blocks simultaneously. Such blocks are almost always in conflict.




Effort spent on a fork that eventually loses is wasted.



More generally, longest chain wins.

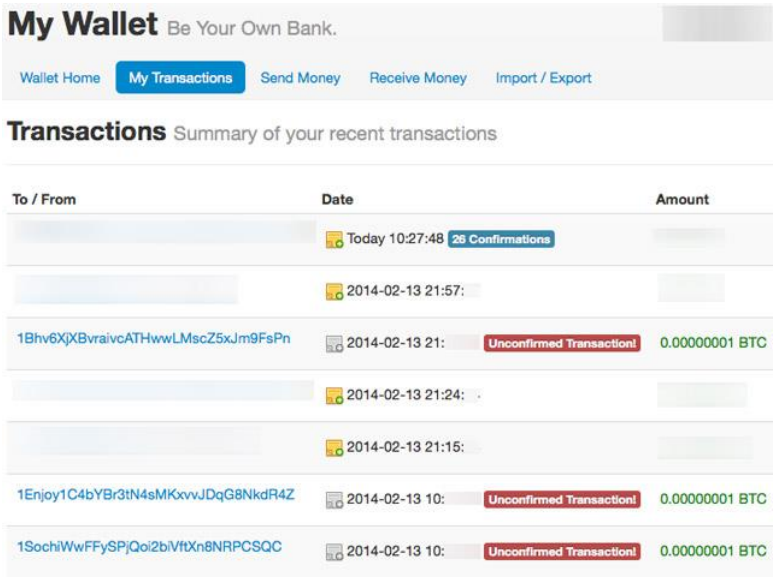


Where length is measured in terms of sum of difficulties of blocks in chain.

# Transaction confirmations

- A transaction is said to have received *k* confirmations if it has been published in a block that has been added to the blockchain, and *k-1* more blocks have also been added.
- A transactions is typically considered “confirmed” once it has 6 confirmations (the success rate of double spending is less than 0.1% against the attacker with the hashrate of 10%).
- Newly minted Bitcoins (i.e., in COINBASE transaction) are typically considered confirmed once they have received 100 confirmations.

# Transaction confirmation (in real-world)




# Practical limitation

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).

# A real Bitcoin transaction

metadata

input(s)

output(s)


```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "in":[
   {
    "prev_out":{
     "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
     "n":0
    },
     "scriptSig":"30440....3f3a4ce81"
   },
   {
    "prev_out":{
     "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
     "n":0
    },
    "scriptSig":"304602210....3f3a4ce81"
   }
  ],
  "out":[
   {
    "value":"10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```


Transaction ID

signature and public key of sender

signature and public key of sender

script for verifying transaction

https://blockchain.info/tx/b657e22827039461a9493ede7bdf55b01579254c1630b0bfc9185ec564fc05ab?format=json

# Questions?

# 프라이빗/컨소시움 블록체인 vs 퍼블릭 블록체인

**양대헌** 인하대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1994.02 | KAIST 전산학과 학사 |
| 1996.02 | 연세대학교 전산학 공학석사 |
| 2000.08 | 연세대학교 전산학 공학박사 |
| 2000.09 ~ 2003.02 | ETRI 선임연구원 |
| 2003.03 ~ | 인하대학교 컴퓨터정보공학부 |

### 강연요약

비트코인의 등장과 더불어 가상화폐와 블록체인에 대한 관심이 뜨겁다. 최근 들어 변동폭이 매우 높기는하지만 비트코인의 가격이 치솟으며 가상화폐에 대한 관심이 블록체인에 대한 관심을 증폭시키고 있다. 정부에서도 가상화폐에 대한 시각과 블록체인에 대한 시각을 달리하며, 많은 R&D 지원자금을 블록체인쪽에 투입하고 있다. 특히 프라이빗/콘소시움 블록체인에 대한 관심은 금융권을 시작으로 촉발되어 현재는 많은 상업적인 프로젝트가 진행 중이다. 프라이빗/콘소시움 블록체인은 처리속도 및 폐쇄성으로 인해 금융 인프라를 바꿀 수 있는 기술로 현재 각광받고 있다.

이 강연에서는 가상화폐가 필요 없는 프라이빗/콘소시움 블록체인이 사실은 가상화폐를 위한 퍼블릭 블록체인의 개념과는 전혀 다르다는 점을 설명하고, 이 두가지 블록체인에서 사용되는 기술적인 배경의 차이, 그리고 이들이 제공할 수 있는 보안서비스의 차이 등을 설명하고자 한다. 또한, 이를 통해 현재 진행되고 있는 블록체인 프로젝트들의 의미를 짚어보고자 한다.

Netsec-KR 2018

# Private/Consortium Block Chain vs. Public Block Chain

2018.4.12.
인하대학교 양대헌
nyang@inha.ac.kr

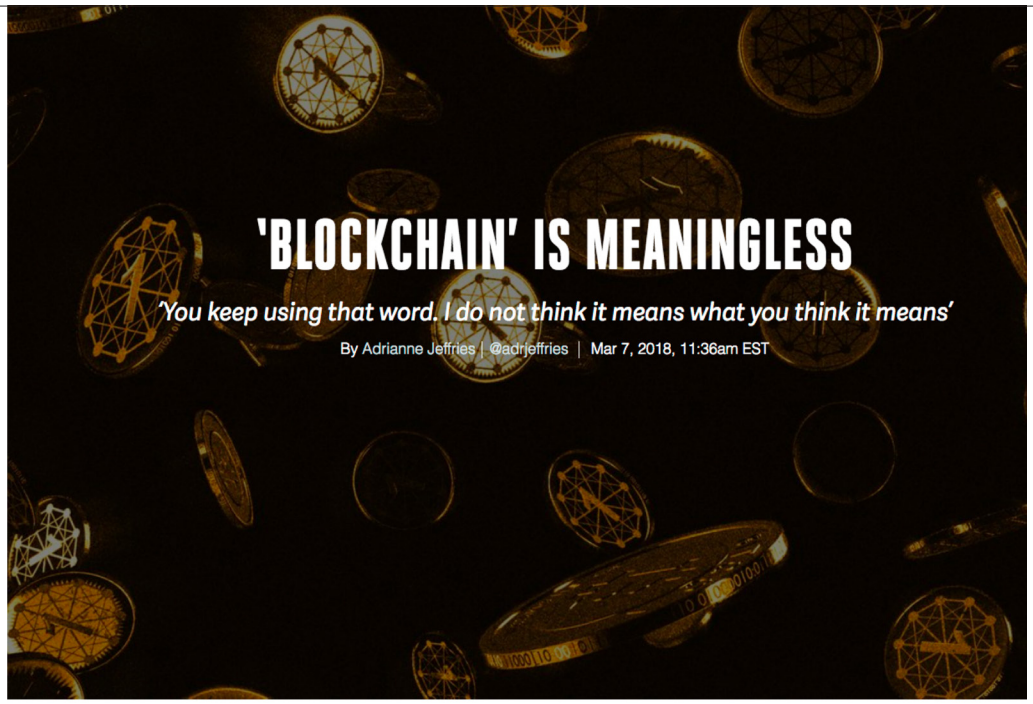



Illustration by Alex Castro / The Verge

Arvind Narayanan, an assistant computer science professor at Princeton who co-teaches a popular blockchain class on Coursera wrote that

"'Private blockchain' is just a confusing name for a shared database"

"The key innovation behind Bitcoin's blockchain was the so-called proof-of-work consensus mechanism, which was intended to replace the need for a central authority with rules and incentives"

https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning

## Continued…

**Quotes from "Private blockchain is just a confusing name for a shared database", Arvind Narayanan**

- It is true that adding signatures and hash pointers makes a shared database a bit more secure. However, it's qualitatively different from the level of security, irreversibility, and censorship-resistance you get with the *public* blockchain.

https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

## Continued…

**Quotes from "Private blockchain is just a confusing name for a shared database", Arvind Narayanan**

- Mindshare that has gotten Wall Street to converge on it, driven by the fear of missing out.

https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

## Continued…

**Quotes from "Private blockchain is just a confusing name for a shared database", Arvind Narayanan**

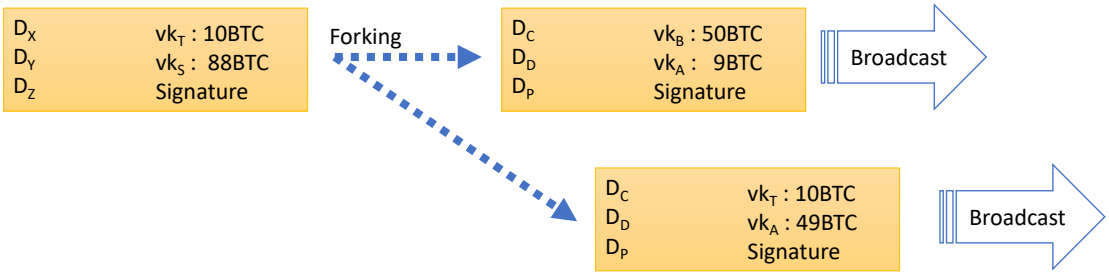
- To build these private blockchains, banks start with the Bitcoin Core code and rip out all the parts they don't need. It's a bit like hammering in a thumb tack, but if a hammer is readily available and no one's told you that thumb tacks can be pushed in by hand, there's nothing particularly wrong with it.

https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

In view of anonymous voting by PoW.

# Public Block Chain

# Double Spending?




At some point after spending her BTCs, Alice spends her BTC again!
→ Double spending! One for Bob and the other for Tom.

What can be done?

## Double Spending: Mint model

- A common solution is to introduce **a trusted central authority, or mint**
  - Checks every transaction for double spending.
  - Single Point of Failure
- Need to know that **the previous owners did not sign any earlier transactions**.
- The mint is an authority to be aware of all transactions and decide which arrived first by its **authentic ledger**.

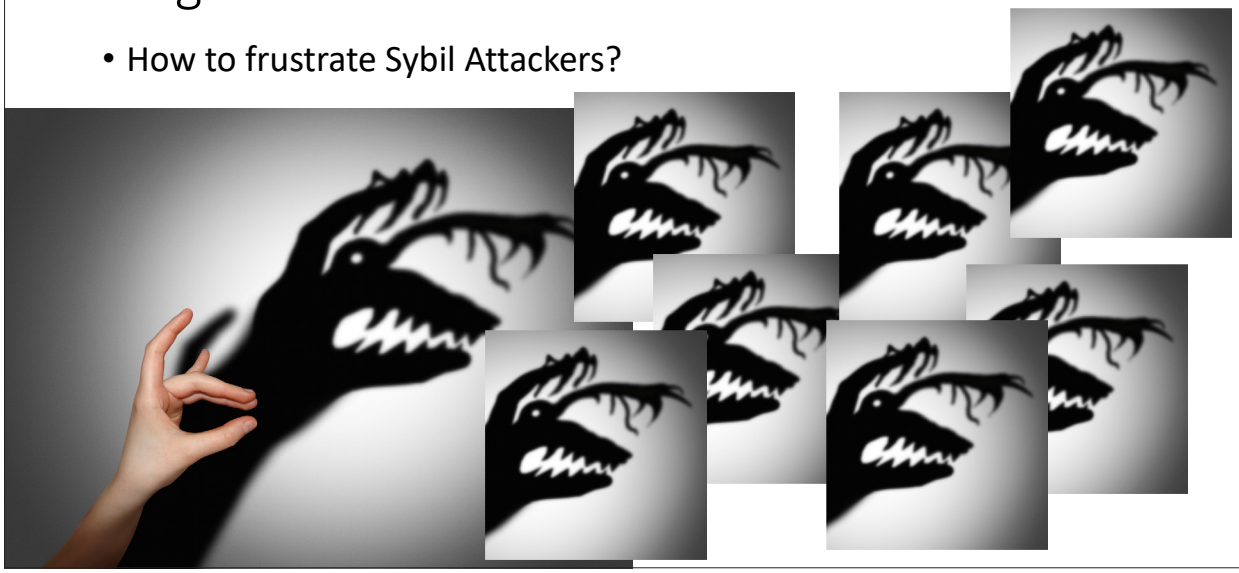
## Double Spending: Blockchain Model

- To accomplish this **without a trusted party, transactions must be publicly announced**, and we need a system for **participants to agree on a single history of the order** in which they were received.
- The **payee needs proof** that at the time of each transaction, the majority of nodes agreed it was the first received.

- **Majority Voting for the Online Ledger!!!**
- But how to define majority?

## Majority Vote: Agree on the single online ledger.

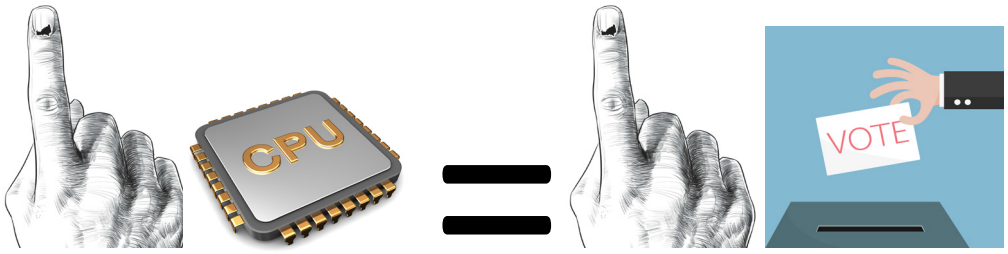
- How to frustrate Sybil Attackers?



## Frustrating Sybil Attackers.

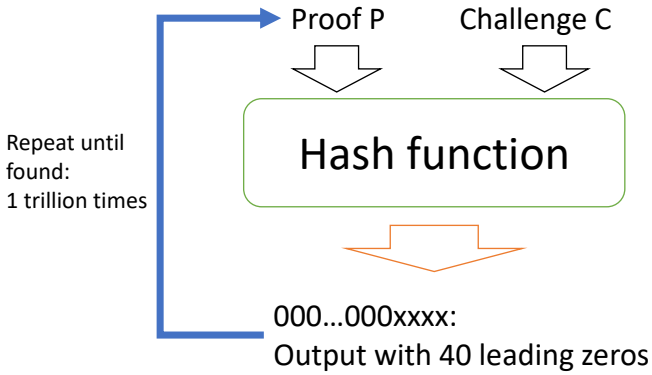
OR

?

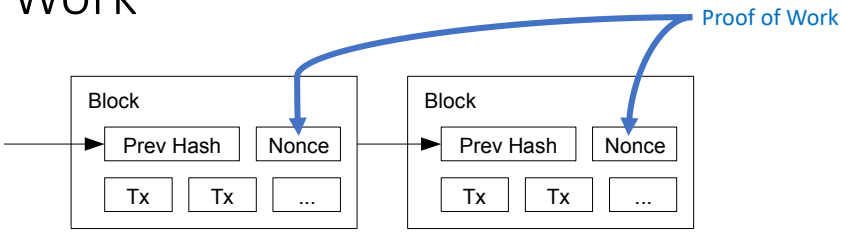


# Proof of Work

- Hard challenge but easy to verify
- Puzzle
- SPAM
- DoS
- BitCoin



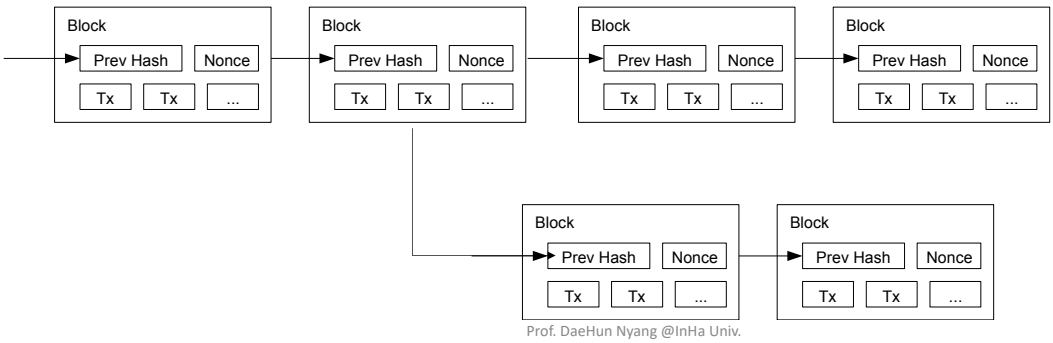

# Proof of Work




- As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.
- One-IP-address-one-vote? Proof-of-work is essentially one-(CPU?)entity-one-vote.
- To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour.

# Double Spending = Chain Forking

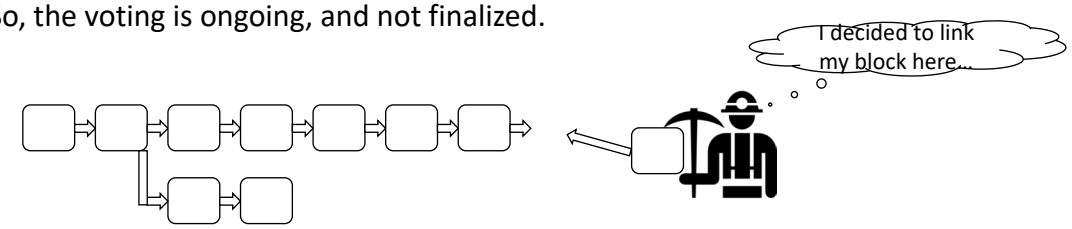
- Chain forking happens: Break a tie by sticking with the longest chain.
- “The longest” means the highest aggregate difficulty.




Prof. DaeHun Nyang @InHa Univ.

# PoW for Voting by Anonymous/Unlinkable Nodes

- By choosing the longest chain means that miners vote for the chain.
- Double voting is disadvantageous.
- Cryptographically, PoW is a kind of relaxed version of bit commitment that cannot be withdrawn.
- We can retract but, it takes quite amount of computation, and thus, the accumulated hash computation guarantees the ”immutability” of the ledger.
- So, the voting is ongoing, and not finalized.



In view of ID-voting by PBFT.

# Private/Consortium Block Chain

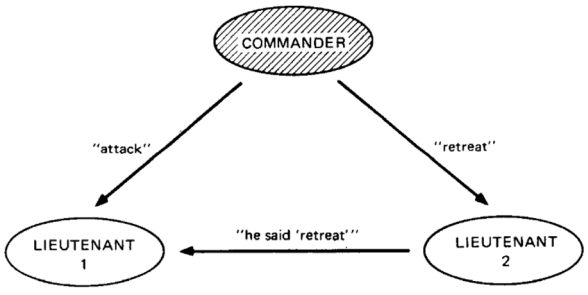



Fig. 2. The commander a traitor.

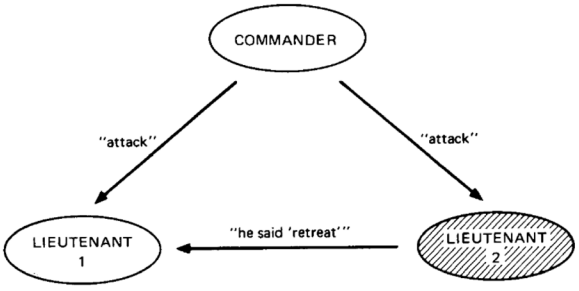



Fig. 1. Lieutenant 2 a traitor.

## Byzantine Generals Problem

Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem" (PDF). ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.

| | PoW consensus | BFT consensus |
|---|---|---|
| Node identity management | **open, entirely decentralized** | permissioned, nodes need to know IDs of all other nodes |
| Consensus finality | no | **yes** |
| Scalability (no. of nodes) | **excellent (thousands of nodes)** | limited, not well explored (tested only up to $n \leq 20$ nodes) |
| Scalability (no. of clients) | **excellent (thousands of clients)** | **excellent (thousands of clients)** |
| Performance (throughput) | limited (due to possible of chain forks) | **excellent (tens of thousands tx/sec)** |
| Performance (latency) | high latency (due to multi-block confirmations) | **excellent (matches network latency)** |
| Power consumption | very poor (PoW wastes energy) | **good** |
| Tolerated power of an adversary | $\leq 25\%$ computing power | $\leq 33\%$ voting power |
| Network synchrony assumptions | physical clock timestamps (e.g., for block validity) | **none for consensus safety** (synchrony needed for liveness) |
| Correctness proofs | no | **yes** |

The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, Marko Vukolic at IBM Research - Zurich

## Public vs. Private (PoW vs. PBFT)

- permissionless participation is made possible by PoW, as PoW inherently addresses the Sybil attack, infamous in anonymous networks.
- In contrast, the BFT approach to consensus typically requires every node to know the entire set of its peer nodes participating in consensus.
  → $O(N^2)$

# Public vs. Private (PoW vs. PBFT)

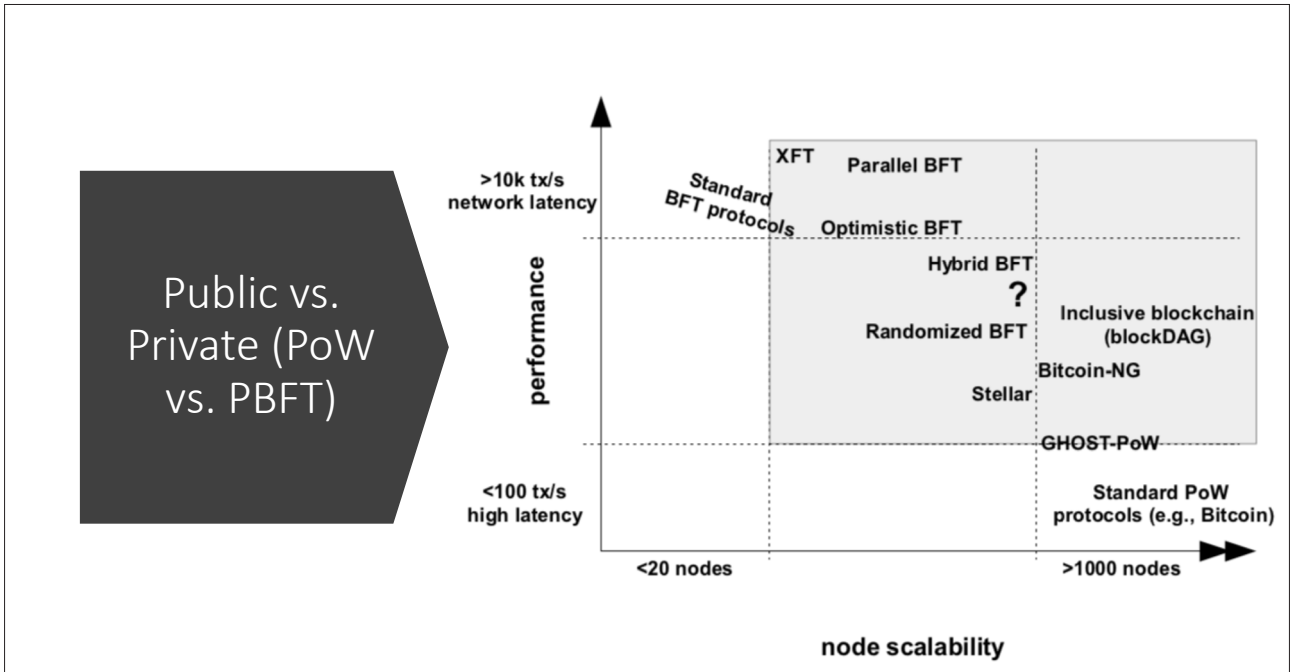
- PoW and BFT consider different adversaries.
- In PoW blockchains, what matters is the total computational (hashing) power controlled by the adversary. Initially, Bitcoin was thought to be invulnerable so long as the adversary controls less than 50% of hashing power. Years later, it was shown that Bitcoin mining is actually vulnerable even if only 25% of the computing power is controlled by an adversary*.
- In contrast, BFT voting schemes are known to tolerate at most n/3 corrupted nodes.

* Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security - 18th International Conference, FC 2014*, pages 436–454, 2014.

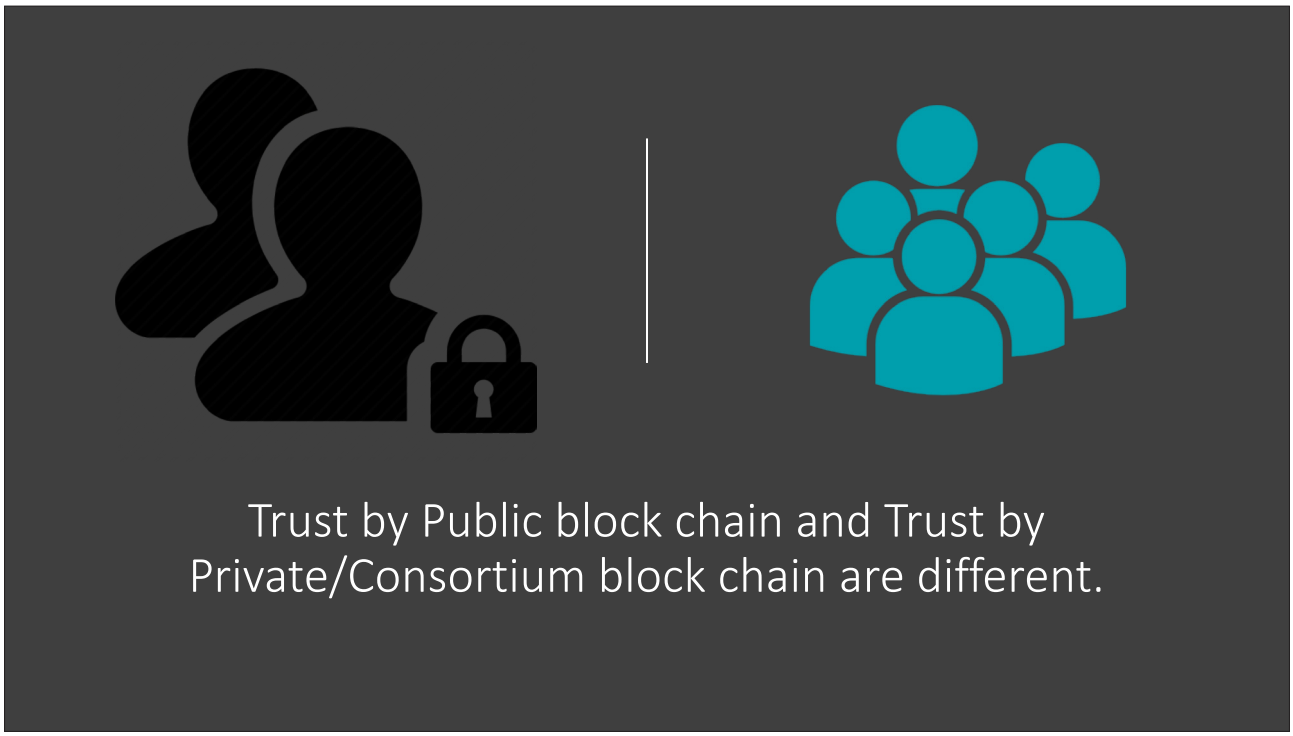
# Public vs. Private (PoW vs. PBFT)

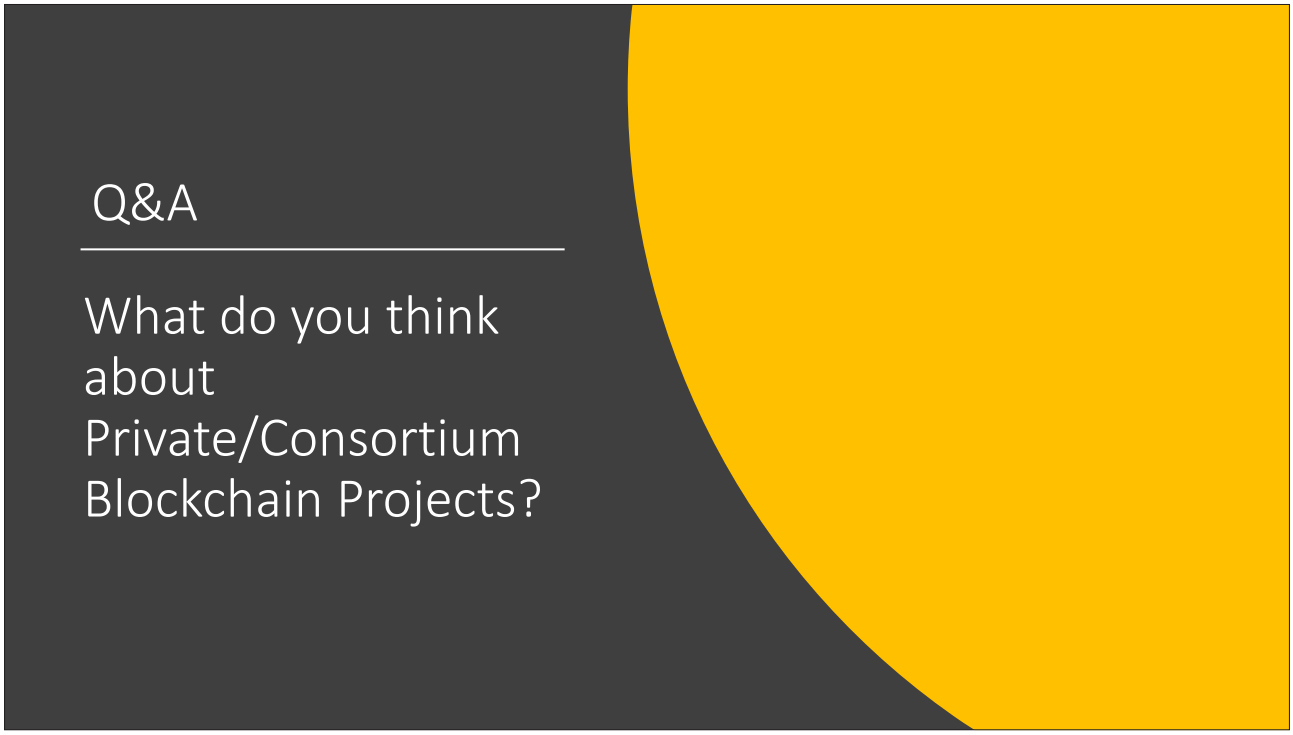
- Public block chain focuses on how to allow peers to vote anonymously in a large scale.

- Private block chain's focus is not on voting owing to digital signature. (eg HyperLedger)
- Its focus lies rather on how to synchronize efficiently the shared database among replicas under the existence of faulty nodes in a small scale (< 20).

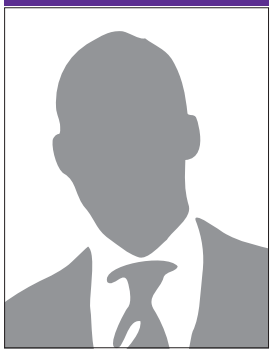



The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, Marko Vukolic at IBM Research - Zurich




Q&A
What do you think about Private/Consortium Blockchain Projects?

The 24th Network Security Conference -Korea



# 블록체인 프라이버시 보호 기술 동향

**조남수** ETRI 선임

### 학력 및 경력사항

| | |
|---|---|
| 1995.03 ~ 1999.08 | 한국과학기술대학교 수학과 학사 |
| 2001.03 ~ 2007.08 | 서울대학교 대학원 암호학 박사 |
| 2007.10 ~ 현재 | ETRI 정보보호연구본부 선임연구원 |

### 강연요약

블록체인 기반 암호 화폐의 성공으로 인해 다양한 분야로 블록체인 기술 적용이 가속화되고 있으나, 분산 원장 개념을 통한 데이터 무결성 제공이라는 근본적인 기술적 특성으로 인해 블록체인 활용 환경의 데이터 및 사용자 프라이버시 유출 문제가 지속적으로 제기되고 있다. 이에 암호화 및 영지식 증명 등의 기술 적용을 통한 프라이버시 보호 기술이 제시되고 있으나 정형화된 데이터에 대한 제한적인 프라이버시 보호 기능을 제공하고 있는 실정으로, 블록체인 활용 환경의 데이터 및 사용자 프라이버시 보호 기술에 대한 한계점 및 향후 발전 방향에 대해서 살펴본다.

# Block Chain 프라이버시 보호 기술

정보보호연구본부
조남수

2018. 4. 12.

ETRI
Electronics and Telecommunications Research Institute

ETRI

목차

- Bitcoin Privacy
- Zero-Knowledge Proof
- Transaction Encryption
- Smart Contract Encryption
- 결론

# 개요

ETRI

- **BitCoin**
  - 기존 암호화폐의 난제인 효율적인 double spending 방지 문제를 모든 거래 정보 공개 검증을 통해 해결
  - Coin 발행부터 모든 송금 정보의 공개 → 프라이버시 유출
- **Privacy**
  - 익명화
    - 거래에 사용되는 공개키가 익명 ID 역할 수행
    - 임의 공개키 생성이 가능하여 일정 수준의 익명화를 제공하지만 linkage 공격 등에 대한 이론적 고려가 없음
  - CoinJoin, CoinShuffle : 다수의 비트코인을 묶어서 재분배를 통한 익명성 제공
  - Transaction Encryption : Zerocash 등
    - Zero-knowledge proof 기반의 암호화된 transaction 검증 기법 제공
  - Smart Contract Encryption : Hawk 등
    - Zero-knowledge proof 기반 encrypted coin 확장 기법



# Bitcoin Transactions

ETRI

Block #516690

Tx bf496f39d908246ad52bda13e6562ee1af3daa2dcf48e16b2808e168f2dc041a

| Input | | Output | |
|---|---|---|---|
| 1Kc5kUk4f1xDbAGHRAppeyLNcFSFywFBAm | 0.01070596 BTC | 1CjtZWaocf7HKguSeUoNHxocmjW5yz2f2g | 4.63341656 BTC |
| 14tbHPadekfDUAESiP32x8HVkJTK7YWChR | 0.00815000 BTC | 157iuGcUSPPWKxXC9mCFLrZ6W9fATYf1xf | 0.00606618 BTC |
| 18pSmi1PyCrpPpeDeuGmxpCErCijp7PxhZ | 1.11731966 BTC | | |
| 15KehY4bRRuBK78Uh7wCBnUgonAgu8J2V9 | 3.43789269 BTC | | |
| 1NJCbfSq8tRUEtntihY8JktHpCTizUEG23 | 0.07154943 BTC | | |
| Input : 4.645618 BTC | | Output : 4.645618 BTC | fee : 0.006135 BTC |

⋮

출처 : blockexploer.com

# Bitcoin Transactions

ETRI

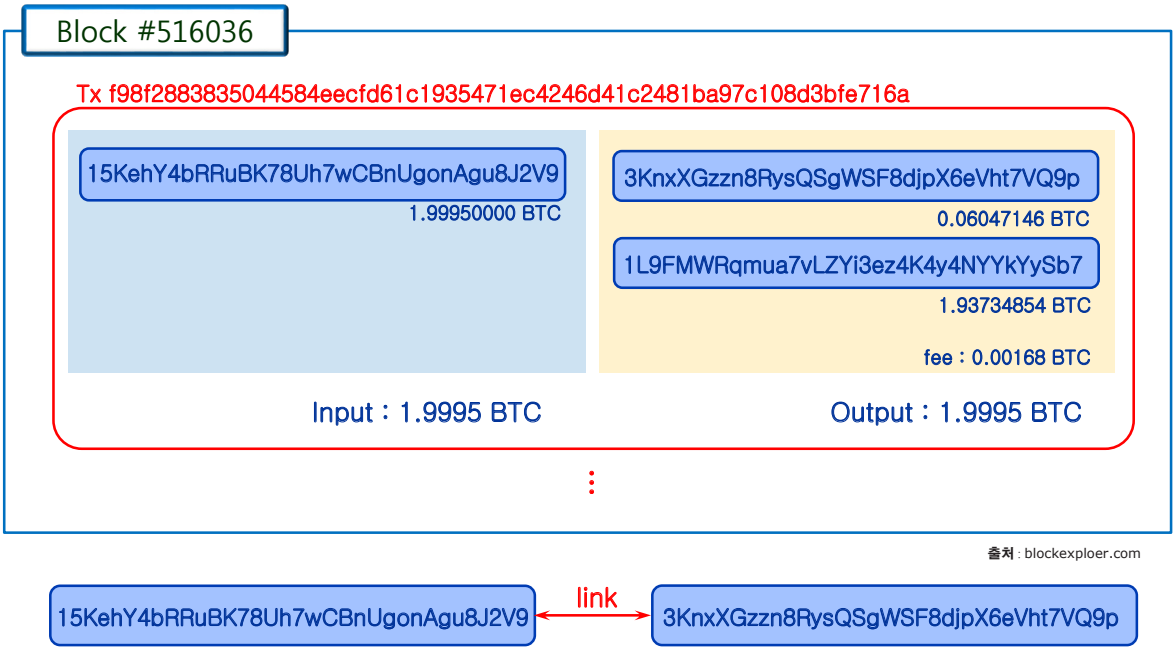
| Address | Total Input | Total Output | Balance | Number of Tx's |
|---|---|---|---|---|
| 1Kc5kUk4f1xDbAGHRAppeyLNcFSFywFBAm | 0.01070596 | 0.01070596 | 0 | 2 |
| 14tbHPadekfDUAESiP32x8HVkJTK7YWChR | 1.03073534 | 1.03073534 | 0 | 94 |
| 18pSmi1PyCrpPpeDeuGmxpCErCijp7PxhZ | 1.1173966 | 1.11731966 | 0 | 2 |
| 15KehY4bRRuBK78Uh7wCBnUgonAgu8J2V9 | 50.25237069 | 43.01428402 | 7.23808667 | 101 |
| 1NJCbfSq8tRUEtntihY8JktHpCTizUEG23 | 2.21904548 | 2.09492221 | 0.12412327 | 13 |

출처 : blockexploer.com



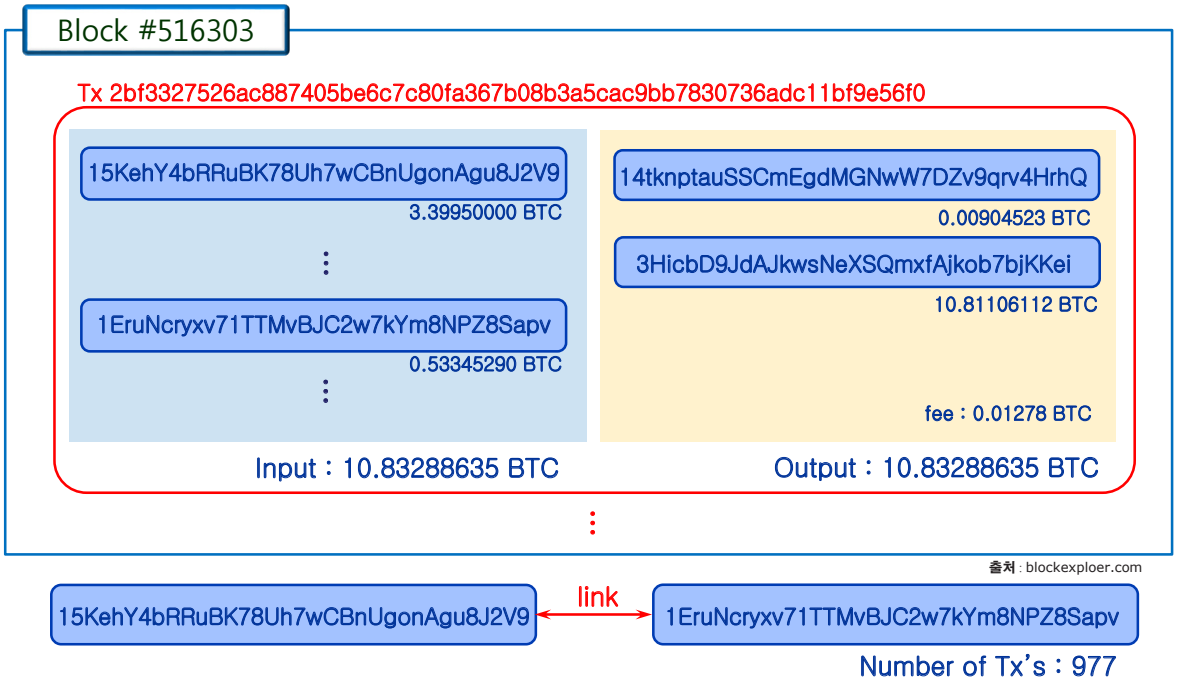
# Bitcoin Transactions

ETRI




출처 : blockexploer.com

# Bitcoin Transactions






# Zero-Knowledge Proof 개요

❖ **Intro**
- 1982년 Goldwasser, Micali, Rackoff 가 최초 아이디어 제안
- 1985년 Goldwasser, Micali, Wigderson이 모든 NP-set에 대해서 구성 가능함을 증명

❖ 기본 구조
- Two party protocol
  - Prover : 증명을 생성하는 사람
  - Verifier : Prover의 증명에 대한 검증을 수행하는 사람
  - Language : 증명할 statement의 집합
- 목표
  - Prover가 주어진 statement가 True임을 Verifier에게 증명
  - (or) NP-statement의 경우, witness $w$가 존재함을 증명

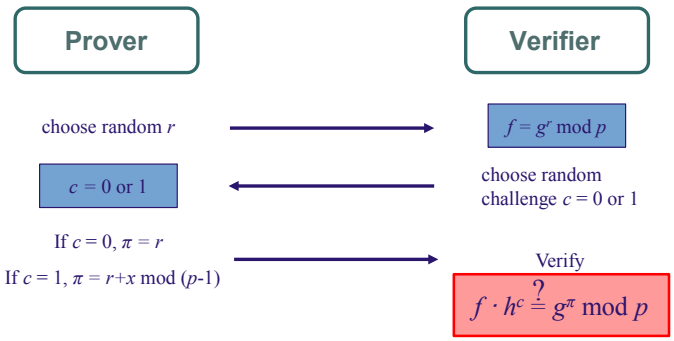
# Zero-Knowledge Proof 개요

- **Completeness**
  - Statement가 True인 경우, 1의 확률로 증명을 통과할 proof가 존재
- **Soundness**
  - Statement가 False인 경우, 증명을 통과할 확률은 negligible
- **Zero-knowledge**
  - Verifier에게 $w$에 어떠한 정보도 제공하지 않고, 주어진 statement에 대한 $w$가 존재함을 증명
- **Proof of Knowledge**
  - $w$의 존재성에 추가로 Prover가 $w$의 실제 값을 알고 있음을 증명



# Zero-Knowledge Proof 개요

- **Ex) Discrete Log Problem**
  - Prover's goal : 주어진 $p, h, g$에 대해서 $h = g^x \bmod p$를 만족하는 $x$에 대한 지식 증명



# Zerocash – Sketch

ETRI

## Goal

- 중앙 신뢰 기관없이 분산 환경에서 완전 익명화된 coin의 생산, 전달, 소비를 위한 기법
- 기존 block chain 기반 화폐(basecoin)의 구성을 동일하게 사용하며 일부 transaction을 추가하는 형태로 구성

## Constructions

- Step 1 : User anonymity
- Step 2 : Coin list compressing
- Step 3 : Direct anonymous payment
- Step 4 : Transfer coins
- Step 5 : Public Outputs
- Step 6 : Non-Malleability



# Zerocash – Construction

ETRI

## Step 1 : User Anonymity

- Goal : 사용자 익명성 제공

- 모든 coin은 동일 value(ex. 1BTC)를 가지는 것으로 가정
- 사용자($u$)는 serial number $sn$과 trapdoor $r$,을 임의로 선택, coin commitment $cm = \mathrm{COMM}(r; sn)$을 계산
- Coin : $c = (r, sn, cm)$, $TX_{mint} = cm$
- 정해진 value를 public coin에서 지불하고 $TX_{mint}$ 를 공개원장에 추가하는 것으로 coin 발생
- CMList : 생성된 모든 coin commitment의 리스트
- $u$가 $TX_{spend}$를 통해 coin 사용
  - $TX_{spend} = (sn, \pi)$
  - $\pi$ : zk-SNARK for the statement : "I know $r$ such that $\mathrm{COMM}(r; sn)$ appears in the list of CMList"
- 과거 사용 기록이 없는 serial number $sn$에 대해서 proof 수행 후 coin 사용
- User anonymity ← zk-SNARK property

# Zerocash – Construction

ETRI

## Step 2 : Compressing CMList

- Step1의 zero-knowledge는 전체 CMList를 input으로 처리하기 때문에 비효율적
- Merkle-tree 기반 CMList 구성
  - Collision-resistant hash 함수를 이용한 구성
  - 사전에 충분히 큰 tree를 구성하고, leaf node에 새로운 coin commitment를 추가하는 append-only Merkle-tree
- zk-SNARK의 statement를 다음과 같이 수정
  - "I know $r$ such that $\mathrm{COMM}(r; sn)$ appears in the list of CMList"
    → "I know r such that $\mathrm{COMM}(r; sn)$ appears as a leaf in a Merkle tree whose root is $rt$"



# Zerocash – Construction

ETRI

## Step 3 : Direct anonymous payments

- Step1의 문제점 해결
  - $u$가 생성한 coin $c$를 새로운 사용자 $u'$에 그대로 전달하는 경우, $c$의 사용 정보는 $u$에 노출
  - $u'$에 coin $c$를 전달한 이후에도 $u$는 coin $c$의 정보를 모두 알고 있으므로 coin 사용 가능
  - 고정된 coin value로 지불 수단으로 사용에 한계
- Coin 지불 방식 변화
  - 모든 사용자는 public-private key pair$(a_{pk}, a_{sk})$를 구성하고
  - 모든 coin은 특정 $a_{pk}$에 종속되어, coin spending 과정에 $a_{sk}$의 정보를 요구
- Coin commitment 변화
  - $sn$에 대한 commitment를 $(a_{pk}, v, \rho)$에 대한 two phase commitment로 변화
  - $\mathrm{COMM}(r; sn) \rightarrow k = \mathrm{COMM}(r; a_{pk}, \rho),\ cm = \mathrm{COMM}(s; v, k)$
  - Where $\rho$ is a seed for $sn = \mathrm{PRF}(a_{sk}, \rho)$, $v$ is coin value, $s$ random
  - $c = (a_{pk}, v, \rho, r, s, cm),\ \mathrm{TX}_{\mathrm{mint}} = (v, k, s, cm)$
- Note
  - 모든 참여자가 value에 대한 commitment 검사 가능
  - 사용자의 identity 정보인 $a_{pk}$는 확인 불가

# Zerocash – Construction

ETRI

## ❖ Step 3 : cont.

- Pour operation : coin spending
  - Two input $(c_1, c_2)$ → two output $(c'_1, c'_2)$ 가정
  - $u$는 주어진 두 공개키 $a'_{pk,1}, a'_{pk,2}$에 대해서 새로운 coin $c'_1, c'_2$를 생성
    (Note : coin 생성에는 공개키 $a_{pk}$만을 사용하고 $a_{sk}$는 포함하지 않음)
- Zero-knowledge proof
  - 다음 coin 들에 대한 proof $\pi_{\text{pour}}$ 생성

    $c_1 = (a_{pk,1}, v_1, \rho_1, r_1, s_1, cm_1)$, $\quad c_2 = (a_{pk,2}, v_2, \rho_2, r_2, s_2, cm_2)$

    $c'_1 = (a'_{pk,1}, v'_1, \rho'_1, r'_1, s'_1, cm'_1)$, $\quad c'_2 = (a'_{pk,2}, v'_2, \rho'_2, r'_2, s'_2, cm'_2)$

  - Statement : root가 $rt$인 Merkle-tree에 포함된 serial number가 $sn_1, sn_2$인 coin과 새로운 coin commitments $cm'_1, cm'_2$에 대해서
  - I know coins $c_1, c_2, c'_1, c'_2$ and secret key $a_{sk,1}, a_{sk,2}$ and those satisfy followings :
  - Coins are well-formed : $k_1 = \text{COMM}(r_1; a_{pk,1}, \rho_1)$, $cm_1 = \text{COMM}(s_1; v_1, k_1)$ … ,
  - Secret key : $a_{pk,1} = \text{PRF}(a_{sk,1};0)$, $a_{pk,2} = \text{PRF}(a_{sk,2};0)$,
  - Serial number : $sn_1 = \text{PRF}(a_{pk,1}; \rho_1)$, $sn_2 = \text{PRF}(a_{pk,2}; \rho_2)$,
  - $\text{cm}_1$ and $\text{cm}_2$ are leaves of the Merkle-tree with root $rt$,
  - and $v'_1 + v'_2 = v_1 + v_2$
- $\text{TX}_{\text{pour}} = (rt, sn_1, sn_2, cm'_1, cm'_2, \pi_{\text{pour}})$



# Zerocash – Construction

ETRI

## ❖ Step 4 : Transfer coin

- Goal : coin을 전달받은 사용자 $u'$이 coin을 사용하기 위한 비밀 정보 전송을 위한 secure channel 생성
- Key–pair 수정
  - $(a_{pk}, a_{sk})$ → $((a_{pk}, PK_{enc}), (a_{sk}, SK_{enc}))$로 구성
- 사용자 $u$는 $u'$에 필요한 정보를 암호화하여 전달
  - $\text{Enc}(PK_{enc}; v'_1, \rho'_1, r'_1, s'_1)$를 $\text{TX}_{\text{pour}}$에 추가

# Zerocash – Construction

ETRI

## ❖ Step 5 : Public Outputs

- Goal : Private coin을 public coin으로 전환
- Statement 수정
  - $v'_1 + v'_2 + v_{pub} = v_1 + v_2$
  - $v_{pub}$ 의 값을 공개하고, 동일 value의 public coin을 생성
  - Coin 생성 transaction을 $TX_{pour}$ 의 추가 정보인 info에 포함



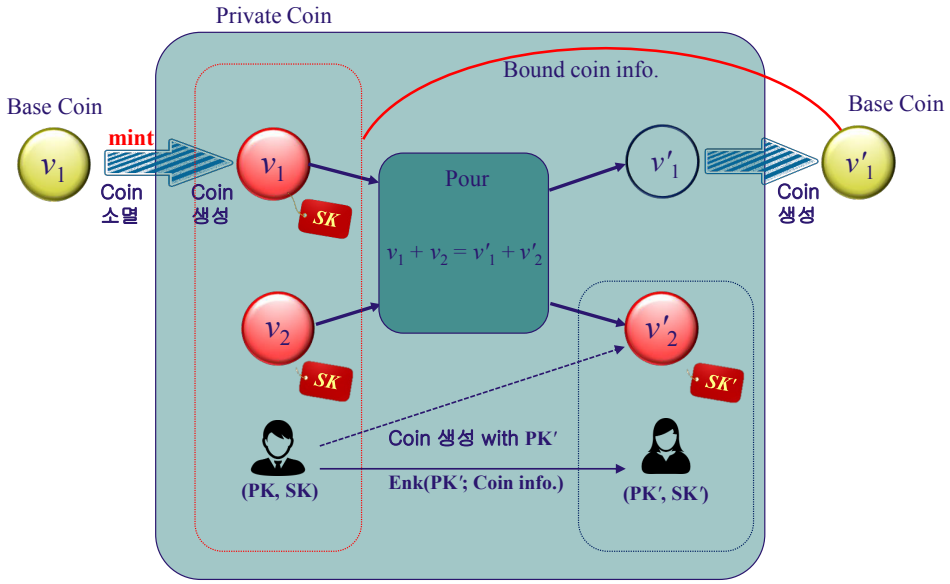
# Zerocash – Construction

ETRI

## ❖ Step 6 : non-malleability

- Step5에서 public output인 info를 수정하는 공격을 방지
- Note : public output은 basecoin이므로 추가적인 정보 제공을 통한 인증이 어려움
- Public output 되는 coin의 value 값에 대한 서명 제공
  - 서명을 검증하는 public key를 $TX_{pour}$의 input coin의 정보와 결합하여, 다른 $TX_{pour}$ 에서 생성된 info를 그대로 사용하는 것을 방지
  - One-time signature key pair $(PK_{sig}, SK_{sig})$ 생성
  - $h_1 = \mathrm{PRF}(a_{sk,1}; h_{sig}),\ h_2 = \mathrm{PRF}(a_{sk,2}; h_{sig}), h_{sig} = \mathrm{PRF}(PK_{sig})$
  - $h_1,\ h_2$에 대한 zero-knowledge proof 추가
  - Public output의 value에 대해서 $SK_{sig}$로 생성된 서명과 검증을 위한 공개키 $PK_{sig}$를 $TX_{pour}$에 추가

# Zerocash – Summary






# Zerocash – Security

- **Algorithm-independent**
  - 특정 zero-knowledge proof algorithm에 의존하지 않고 독립적임
  - 효율적인 zero-knowledge proof algorithm을 이용한 성능 향상 가능

- 모든 안전성은 기반하고 있는 **zero-knowledge proof** 시스템의 안전성에 의존

# BC Data Encryption

ETRI

- **Coin Transaction Encryption**
  - 코인 거래 transaction의 경우, 중복 사용 방지를 위한 안전장치로 transaction 사이의 연관 관계 증명이 요구됨
    - input coin value = output coin value
    - There is no double spending coins in the input list
    - 모든 참여자가 다른 사용자의 거래 내역 감시 필요
  - Smart contract를 위한 transaction의 경우에도 안전장치 필요

- **일반 데이터 transaction의 경우**
  - 거래 당사자 이외의 다른 참여자는 실제 transaction의 내용과 무관
  - 마이너는 데이터가 암호화된 경우에도 실제 transaction의 내용을 검증할 이유가 없음
  - 데이터의 무결성 및 부인방지는 거래 당사자의 문제



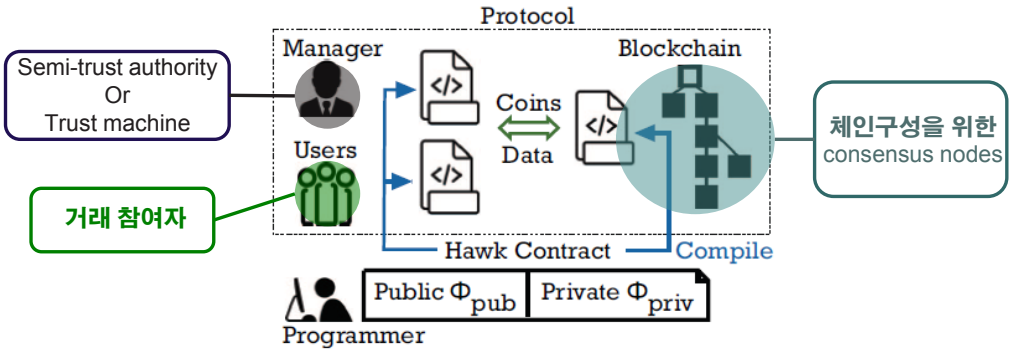
# Smart Contract Encryption

ETRI

- **HAWK : The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts**
  - 2016 IEEE SNP
  - A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou

- **Contribution**
  - BC의 transaction privacy → Zerocash 등
  - Zero-knowledge proof 기반의 Zerocash를 기본으로 smart contract privacy 보호 기능 추가
  - Formal security model for decentralized smart contracts

# Hawk – Structure




**실행 주체에 따라** Smart Contract**를 세 종류로 나누어 구성**

**출처** : "HAWK : The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", IEEE SNP 2016



# Hawk – Example

- **Sealed, second-price Auction**
  - 비공개 입찰을 통한 경매
  - 각 참여자는 자신의 입찰가를 비공개로 입찰하고 가장 높은 입찰가를 제시한 참여자가 낙찰
  - 최종 낙찰자는 두 번째로 높은 입찰가를 지불
  - 기존 smart contract
    - 모든 참여자의 입찰 정보가 공개
    - 뒤에 참여하는 사람이 유리
  - Hawk
    - 모든 참여자는 manager에 비밀 금액을 송금
    - 입찰이 종료되면 각 참여자는 자신의 입찰 금액을 manager에 전달 or 복호화
    - Manager는 낙찰자 결정
    - Manager의 낙찰자 정보를 바탕으로 blockchain에서 금액 분배

# Hawk – Construction

- **Init**
  - Manager는 각 contract에 대한 frozen coin list 및 private data list 생성
- **Freeze**
  - Zerocash 형태의 private coin 필요
  - Coin의 소유 증명만을 수행
  - Coin의 지불에 필요한 Sn을 공개하여, 특정 coin을 지불 정지
  - Blockchain 합의와는 별도의 list를 통한 관리



# Hawk – Construction

- **Compute**
  - Contract의 참여자는 manager에게 자신의 private 정보 제공
  - 해당 frozen coin의 value 정보 공개
- **Finalize**
  - Manager는 모든 private input 을 바탕으로 contract 의 private part에 대한 output 계산
  - 모든 Frozen coin이 지닌 value 합이 contract output의 value합과 동일한지 확인
  - Private part의 output을 public part로 제공

# Hawk – Construction

- **Run Public Contract**
  - Manager의 output에 따른 public part 수행
  - Blockchain에 포함
- **Redistribute public deposits**
  - 일부 참여자가 contract 실행 도중 중단
  - 일부 참여자가 잘못된 input data 제공
  - 이런 경우, contract 중단 및 잘못된 행동을 한 참여자의 deposit을 몰수
  - Contract 실행 도중 manager가 output 계산을 중단한 경우, frozen coin list 삭제를 통한 deposit refund



# Hawk – Security

- **Privacy**
  - 모든 private 정보를 manager에 제공하는 limited privacy
    - Auction의 경우, 낙찰자의 낙찰가만을 공개하는 cryptographic protocol 존재
- **Security**
  - Semi-trust authority 존재
    - 특정 신뢰 기관 및 참여자에 의존하는 문제 발생
    - 일부 응용 환경에서는 manager의 공모에 의한 공격 가능
    - Trust-machine으로 대체하는 방안 제시
  - Chain consensus node는 manager의 output을 신뢰해야 하는 문제 발생
    - Manager가 악의적인 행동을 하는 것은 불가능하다고 설명하고 있으나, consensus node가 manager의 계산 결과를 신뢰하기 위해서는 manager의 계산 과정이 모두 공개되어야 함

## Q & A

ETRI

*Thank You*

The 24th Network Security Conference -Korea

# SPAI (Secure and Private AI)

**윤성로** 서울대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2006 | 미국 스탠퍼드대학교 공학박사 (EE) |
| 2002 | 미국 스탠퍼드대학교 공학석사 (EE) |
| 1996 | 서울대학교 공학사 (EE) |
| 2016 ~ 2017 | 미국 스탠퍼드대학교 방문교수 |
| 2007 ~ 2012 | 고려대학교 전기전자공학부 조교수 |
| 2006 ~ 2007 | 미국 인텔 선임연구원 |
| 2006 | 미국 스탠퍼드대학교 박사후연구원 |

### 강연요약

최근 딥러닝은 인공지능 적용 영역의 다양한 분야에서 뛰어난 성능을 보여주고 있다. 그러나 디바이스나 네트워크 해킹을 통해 인공지능 모델의 각종 매개변수들이 유출될 경우, 막대한 양의 데이터와 컴퓨팅 자원을 들여 학습한 모델을 그대로 공격자에게 노출시키게 된다. 따라서 작성된 학습 모델의 지적 소유권을 증명하기 위한 수단이 필요하고, 또한 모델을 공격하려는 여러 가지 시도에 대한 방어와 보안 유지 기법에 대한 연구가 필수적이다. 한편으로 인공지능 기술 발달은 개인별 데이터를 활용하는 개인화 서비스를 가능하게 하였다. 개인화 서비스를 위해서는 대규모 개인별 데이터의 수집이 필수적이다. 그러나 의료, 금융 등의 민감한 개인 정보를 수집하려면 여러 가지 법적 제한이 작용하며, 원본데이터의 사용을 크게 어렵게 만든다. 따라서 수집된 데이터들을 외부에 유출되지 않게 하거나, 혹은 유출되더라도 익명화, 부호화 등의 보안기법을 통해 제 3자가 이용할 수 없도록 하는 기술이 필요하다. 서울대학교 SPAI (Secure and Private AI) 연구센터에서는 인공지능 모델에 대한 지적 소유권 증명 및 공격 방어와 보안 유지와 관련된 기법을 연구하는 Secure AI 기술과 민감한 사적 정보 및 기밀 정보를 공유하지 않는 프라이빗 학습 모델 설계를 목표로 하는 Private AI 기술을 연구한다.

# 시큐어-프라이빗 인공지능

윤성로

서울대학교 전기정보공학부

2018. 04. 12

http://ailab.snu.ac.kr

## 목차

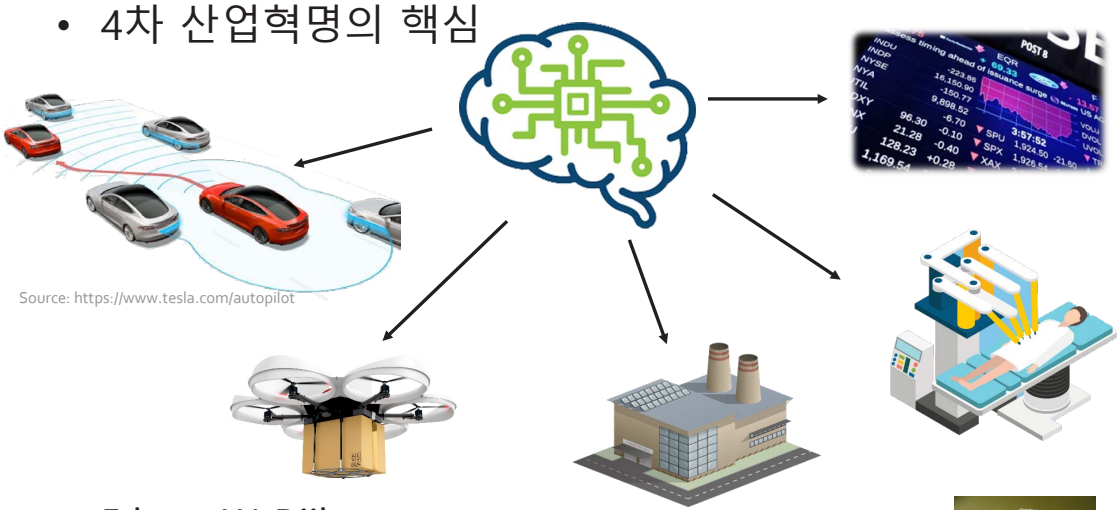
1. 연구 배경
   1) 인공지능 보안 연구의 필요성
   2) 시큐어 AI와 프라이빗 AI
2. 시큐어 AI
   1) 보안 위협 시나리오
   2) 관련 연구 동향
3. 프라이빗 AI
   1) 데이터 프라이버시를 고려한 AI
   2) Collaborative learning
   3) Differential privacy
4. 마무리

## 목차

1. 연구 배경
   1) 인공지능 보안 연구의 필요성
   2) 시큐어 AI와 프라이빗 AI
2. 시큐어 AI
   1) 보안 위협 시나리오
   2) 관련 연구 동향
3. 프라이빗 AI
   1) 데이터 프라이버시를 고려한 AI
   2) Collaborative learning
   3) Differential privacy
4. 마무리

## [연구 배경] 인공지능 시대의 개막

- 4차 산업혁명의 핵심



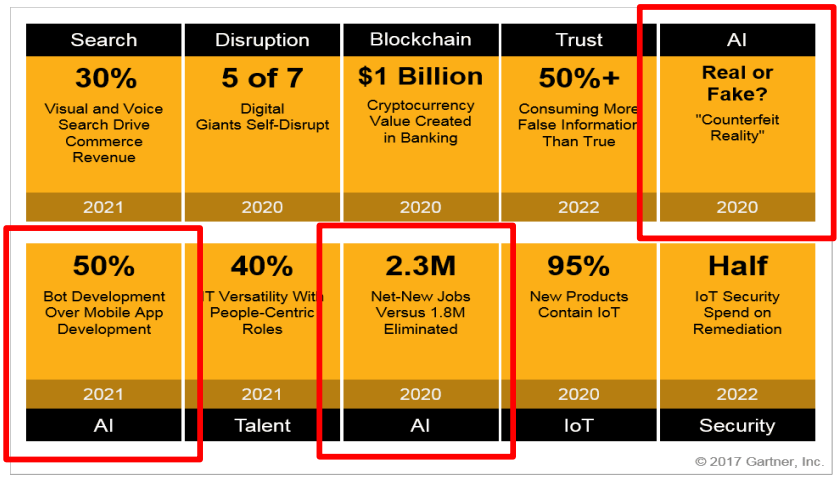
Source: https://www.tesla.com/autopilot

- Edsger W. Dijkstra
  - "The question of whether a computer can think is no more interesting than the question of whether a submarine can swim." (1995)

## [연구 배경] 인공지능의 비약적인 발전

- 빅데이터와 학습 알고리즘

- Gartner 선정 올해 전략적 예측 10가지 중 3가지가 AI 관련




## [연구 배경] 기존 인공지능의 보안 위험성

- 각종 분야에서 사용되는 AI 모델에 대한 보호 기술이 빈약
- 악의적인 인공지능 시스템 오동작 및 공격
  - Ex) MS Tay의 모델 오염

  - Ex) Stop sign 모델 오염

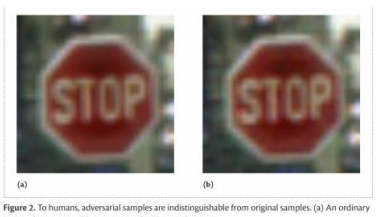
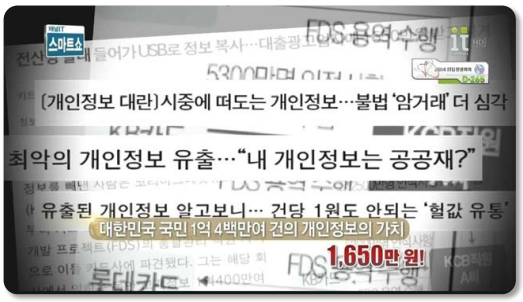


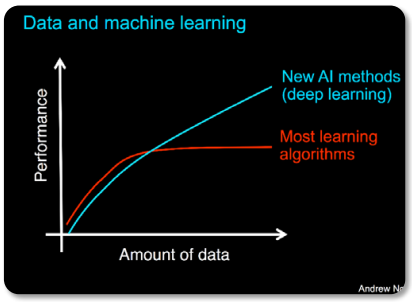

Figure 2. To humans, adversarial samples are indistinguishable from original samples. (a) An ordinary image of a stop sign. (b) An image crafted by an adversary.

McDaniel, Patrick, Nicolas Papernot, and Z. Berkay Celik. "Machine learning in adversarial settings." *IEEE Security & Privacy* 14.3 (2016): 68-72.

## [연구 배경] 데이터 프라이버시와 AI

- 민감한 프라이버시 정보나 기밀 데이터 유출에 대한 위험
  - 그러나 AI 모델 학습을 위해서는 방대한 양의 학습 데이터가 필요
  - 예측 서비스 사용시 프라이버시 데이터가 필요



Medical

Genomic

Financial

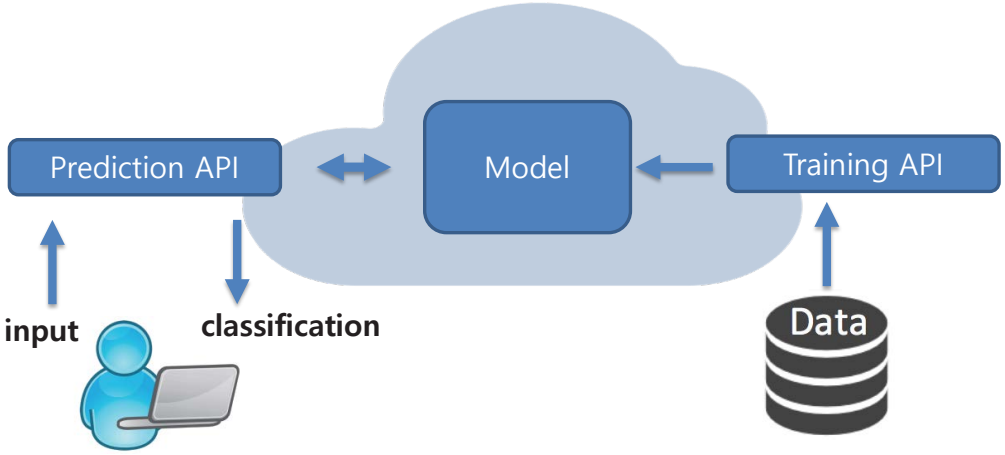
## [연구 배경] Machine Learning as a Service

MetaMind

amazon web services

Google Cloud Platform

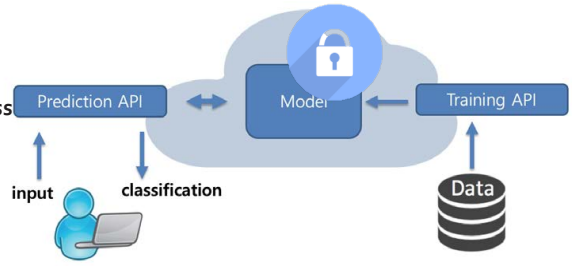
Microsoft Azure



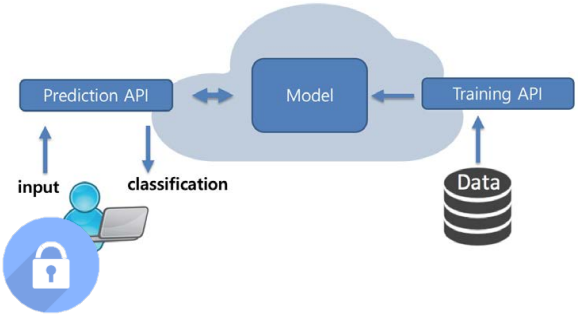

Tramèr, Florian, et al. "Stealing Machine Learning Models via Prediction APIs." *USENIX Security Symposium*. 2016.

## [연구 배경] 시큐어-프라이빗 인공지능

- **Secure AI**
  - **목적:** AI 모델 보안
  - **공격 유형**
    - Aims to find blind spots to exploit ML weakness
    - Attacks at test time
    - Subverts the learning process
    - Degrades the performance of the system




- **Private AI**
  - **목적:** AI에 적용되는 데이터의 보안
  - **공격 유형**
    - Compromises private data

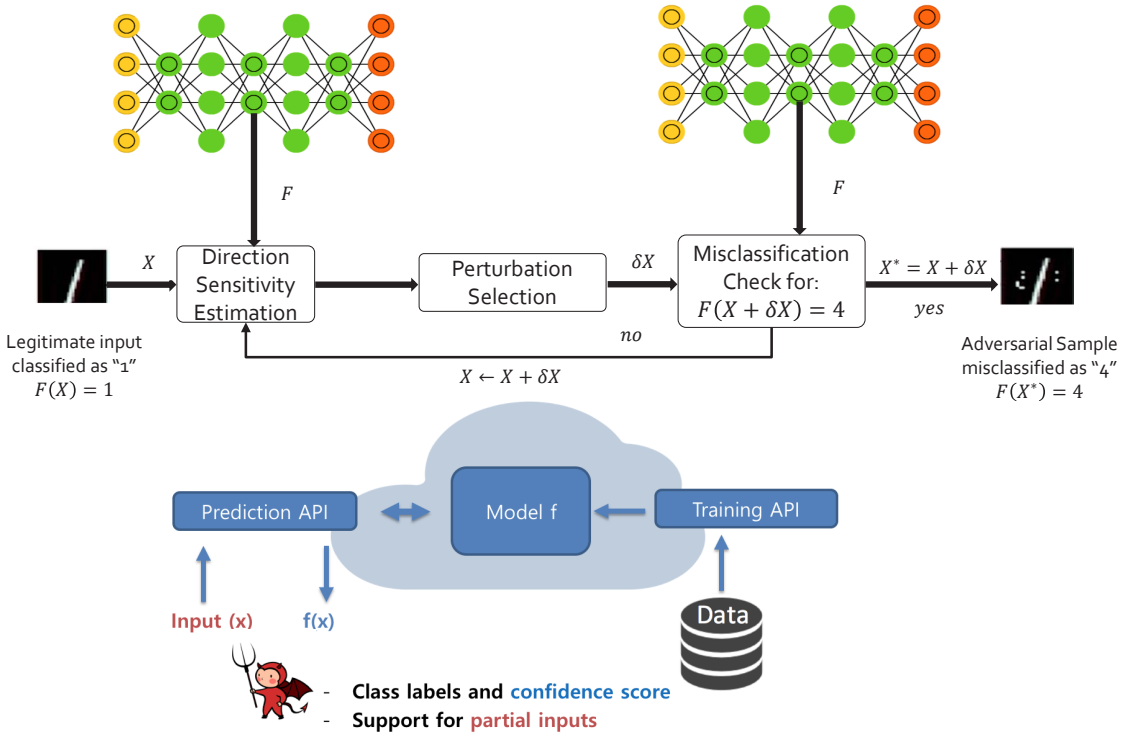



Muñoz-González, Luis, et al. "Towards poisoning of deep learning algorithms with back-gradient optimization." *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*. ACM, 2017.

## 목차

1. 연구 배경
   1. 인공지능 보안 연구의 필요성
   2. 시큐어 AI와 프라이빗 AI
2. **시큐어 AI**
   1. **보안 위협 시나리오**
   2. **관련 연구 동향**
3. 프라이빗 AI
   1. 데이터 프라이버시를 고려한 AI
   2. Collaborative learning
   3. Differential privacy
4. 마무리

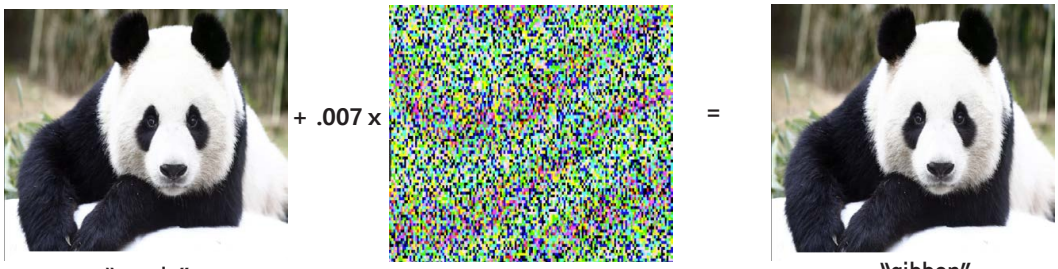
## [시큐어 AI] 시나리오




Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." *arXiv preprint arXiv:1412.6572* (2014).

## [시큐어 AI] 공격

- **Adversarial examples**
  - Aims to find blind spots to exploit ML weakness
  - Attacks at test time
  - Subverts the learning process
  - Degrades the performance of the system




"panda"
57.7% confidence

"gibbon"
99.3% confidence

[GSS15] Goodfellow et al. Explaining and Harnessing Adversarial Examples

## [시큐어 AI] 공격

- **Adversarial examples**
  - Aims to find blind spots to exploit ML weakness
  - Attacks at test time
  - Subverts the learning process
  - Degrades the performance of the system

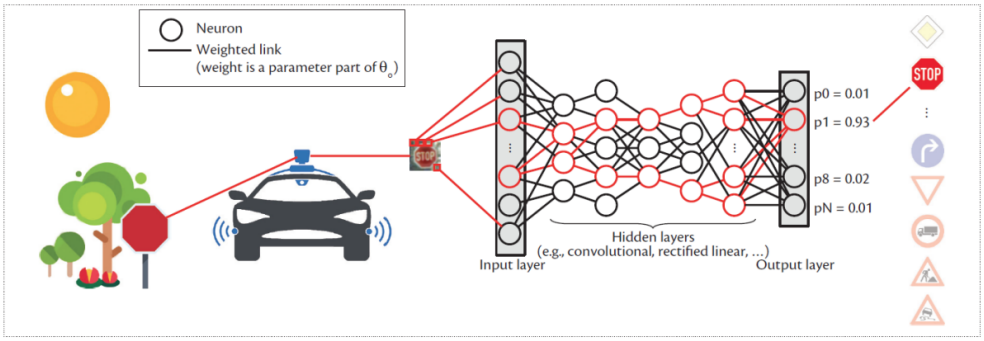
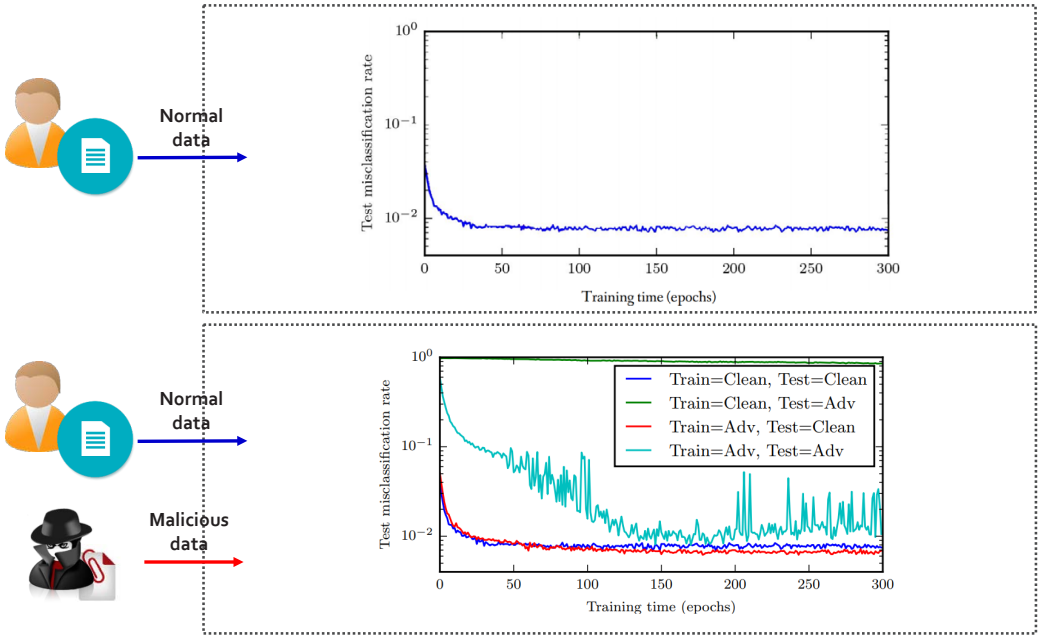



**Figure 1.** An autonomous vehicle uses a camera to identify and recognize roadside signs. Once a sign has been identified, its image is fed to a neural network for classification in one of the predefined sign classes. Here, the neural network identifies the sign as a stop sign.

McDaniel, Patrick, Nicolas Papernot, and Z. Berkay Celik. "Machine learning in adversarial settings." *IEEE Security & Privacy* 14.3 (2016): 68-72.

## [시큐어 AI] 방어

- **Adversarial training**




Papernot, Nicolas, Patrick McDaniel, and Ian Goodfellow. "Transferability in machine learning: from phenomena to black-box attacks using adversarial samples." *arXiv preprint arXiv:1605.07277* (2016).

## [시큐어 AI] 방어

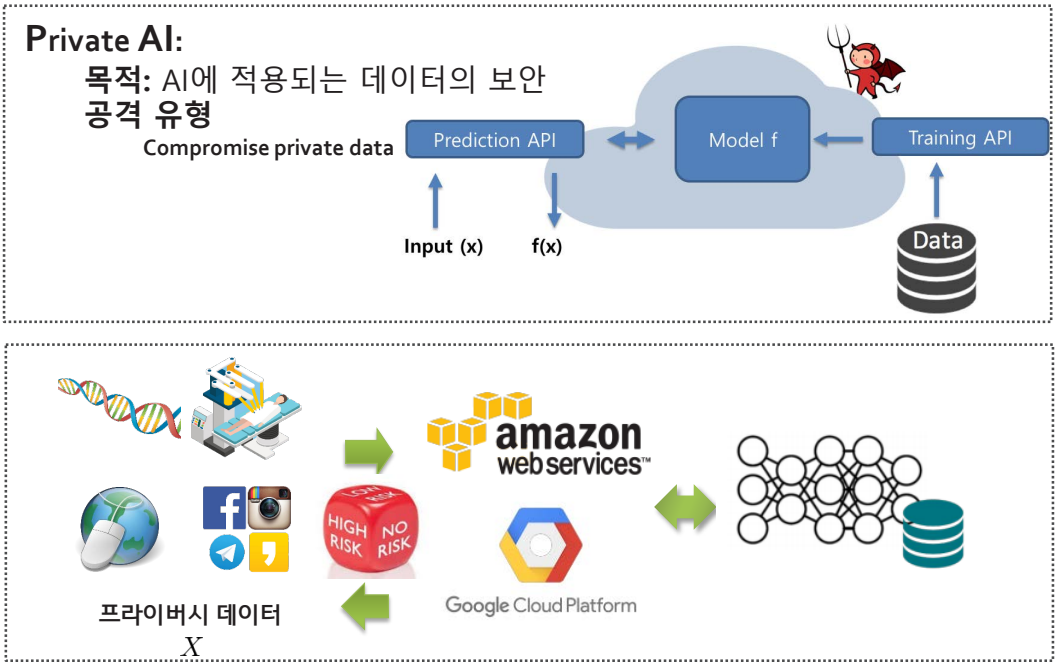
- **Adversarial training limitations**
  - Works well here because same attack used by adversary and classifier
  - Harder to generalize model that is robust to adaptive attacks
  - Classifier needs to be aware of all attacker strategies

Papernot, Nicolas, Patrick McDaniel, and Ian Goodfellow. "Transferability in machine learning: from phenomena to black-box attacks using adversarial samples." *arXiv preprint arXiv:1605.07277* (2016).

## 목차

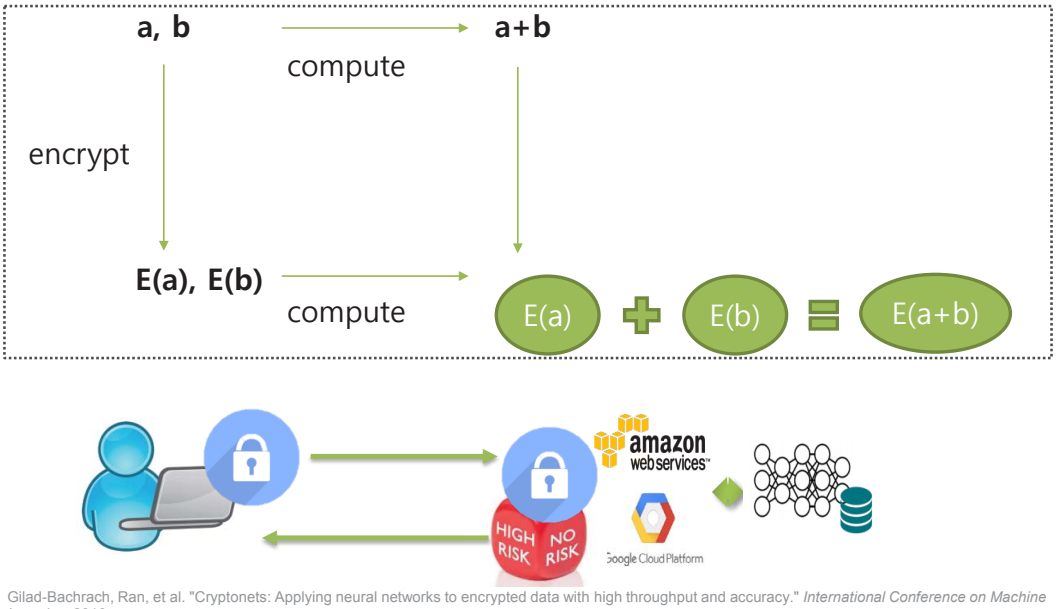
1. 연구 배경
    1. 인공지능 보안 연구의 필요성
    2. 시큐어 AI와 프라이빗 AI
2. 시큐어 AI
    1. 보안 위협 시나리오
    2. 관련 연구 동향
3. **프라이빗 AI**
    1. **데이터 프라이버시를 고려한 AI**
    2. **Collaborative learning**
    3. **Differential privacy**
4. 마무리

## [프라이빗 AI] 데이터 프라이버시와 위협 시나리오




## [프라이빗 AI] 해결책?

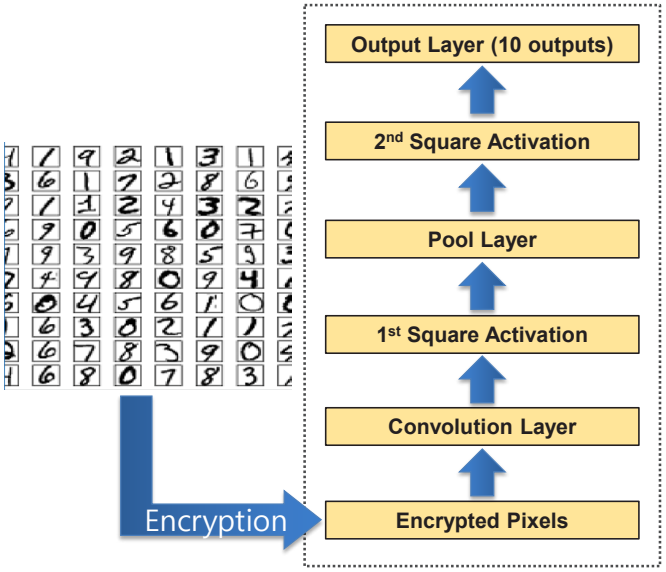
- **Inference over encrypted data**
  - Homomorphic encryption




Gilad-Bachrach, Ran, et al. "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy." *International Conference on Machine Learning*. 2016.

## [프라이빗 AI] 사례 1

- CryptoNets

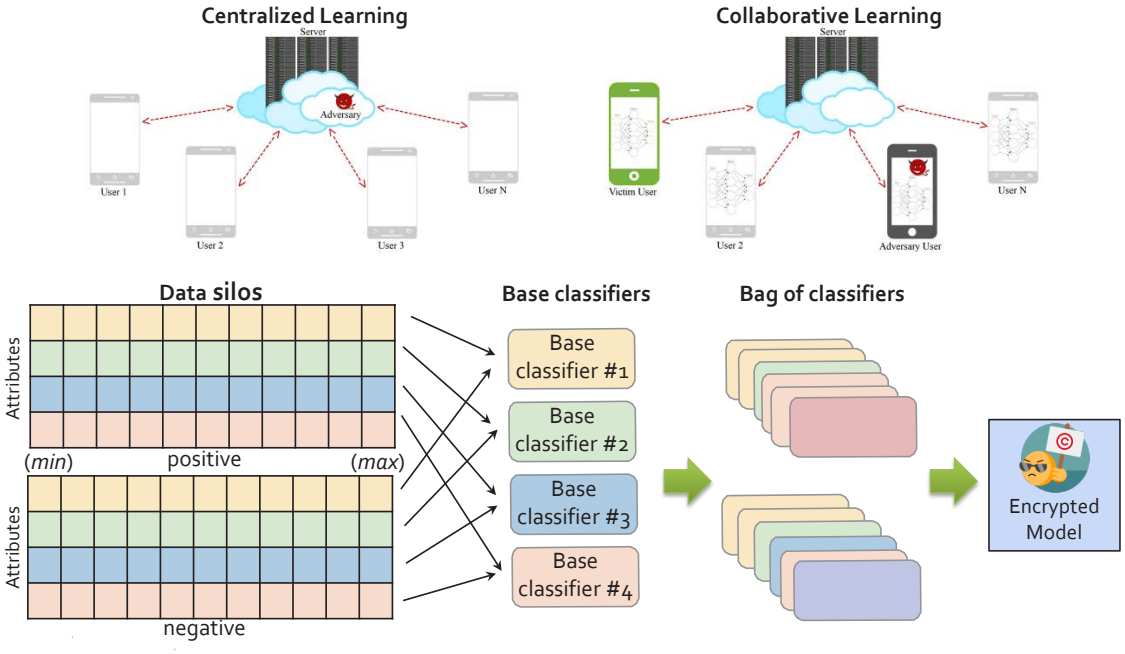



| Encryption Method/Trick | Accuracy | Latency (seconds) |
|---|---|---|
| Square Activation Network | 97.3 % | 1,360 |
| Plain Multiplication | 97.3 % | 24 |
| Chinese Remainder Theorem | 97.6 % | 60 |
| Convolution Network | 99.0 % | 3,976 |
| Skipping Relinearization | 99.0 % | 590 |
| Pre-Computing Linear Layers | 99.0 % | 538 |
| Splitting Plaintext Ring | 99.0 % | 538 |
| Improved Parameters | 99.0 % | 250 |

Gilad-Bachrach, Ran, et al. "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy." *International Conference on Machine Learning*. 2016.

## [프라이빗 AI] 사례 2

- Collaborative 딥러닝을 위한 모델 병합 방법론

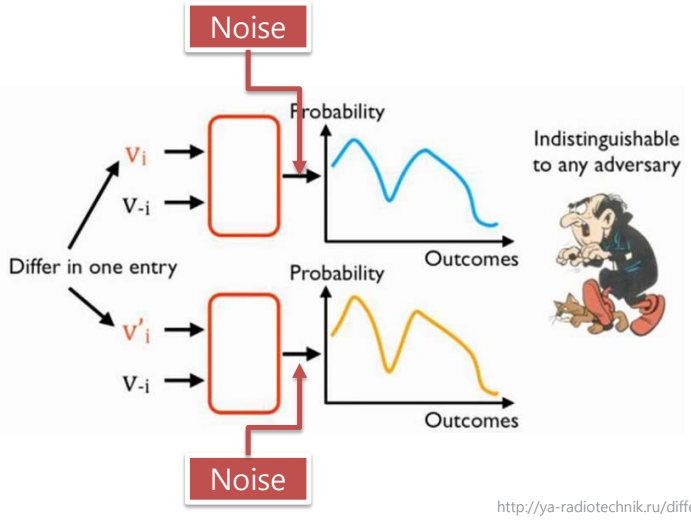



Kim, Jinkyu, et al. "Collaborative analytics for data silos." *Data Engineering (ICDE), 2016 IEEE 32nd International Conference on*. IEEE, 2016.

## [프라이빗 AI] Differential Privacy

- **Differential Privacy 기반 데이터 보안**
  - A randomized algorithm $\mathcal{A}$ is $(\epsilon, \delta)$-differentially private for all datasets $D_1$ and $D_2$ differing at most one element

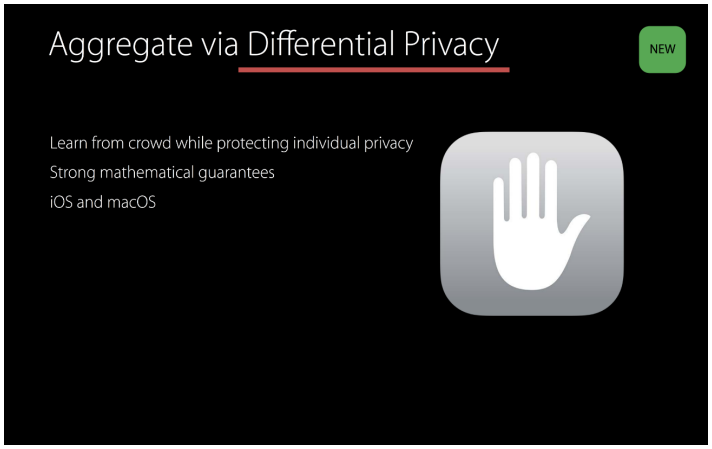
$$\Pr[\mathcal{A}(\mathcal{D}_1) \in \mathcal{O}] \leq e^{\epsilon} \times \Pr[\mathcal{A}(\mathcal{D}_2) \in \mathcal{O}] + \delta$$




http://ya-radiotechnik.ru/differential-privacy

## [프라이빗 AI] 사례 3

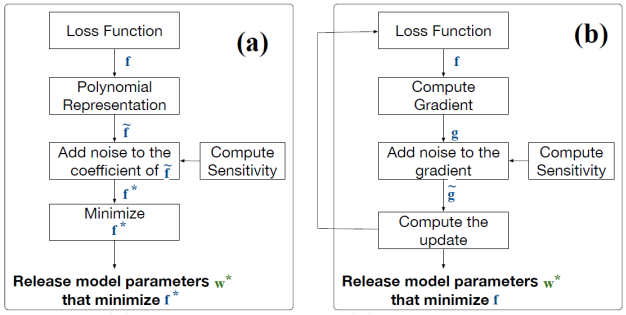
- **Apple uses differential privacy**
  - Differential Privacy in iOS 10 and macOS Sierra




http://www.idownloadblog.com/2016/06/25/differential-privacy-overview/

## [프라이빗 AI] 사례 4

- **Differential privacy on deep neural networks**
  - **Functional mechanism**
    - Add noise on objective function level
  - **Non-functional mechanism**
    - Add noise on gradient level




Functional mechanism　　Non-functional mechanism

Manco, Giuseppe, and Giuseppe Pirrò. "Differential Privacy and Neural Networks: A Preliminary Analysis." *International Workshop on Personal Analytics and Privacy*. Springer, Cham, 2017.

## 목차

1. 연구 배경
   1. 인공지능 보안 연구의 필요성
   2. 시큐어 AI와 프라이빗 AI
2. 시큐어 AI
   1. 보안 위협 시나리오
   2. 관련 연구 동향
3. 프라이빗 AI
   1. 데이터 프라이버시를 고려한. AI
   2. Collaborative learning
   3. Differential privacy
4. 마무리

## [마무리] A Diverse Set of Applications!

National Research Foundation of Korea

감사합니다.

For more information: sryoon@snu.ac.kr

The 24th Network Security Conference -Korea

# 딥러닝을 이용한 악성코드 분석 연구

**윤명근** 국민대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1996 | 연세대학교 이학사 (컴퓨터과학) |
| 2002 | 연세대학교 공학사 (컴퓨터공학) |
| 2006 | 미국 University of Florida 공학박사 (컴퓨터공학) |
| 1998 ~ 2010 | 금융결제원 전자금융연구소 연구원 |
| 2010 ~ 현재 | 국민대학교 소프트웨어융합대학 부교수 |

### 강연요약

정보보호 분야에서 인공지능 기술을 이용한 악성코드의 분류 문제는 꾸준히 연구되어왔다. 최근에는 악성코드의 숫자가 급증하면서 빅데이터를 형성하게 되었고, 딥러닝 기술의 보급으로 인하여 연구 기법에도 변화가 필요하게 되었다. 본 강연에서는 수백만 개 이상의 최신 악성코드 빅데이터를 사용해서 딥러닝 모델을 학습시키고 악성코드 분류기를 개발한 최근 연구 사례를 소개한다. 딥러닝 학습 과정에서 고려되어야할 다양한 이슈들에 대해서 소개하고, 데이터 학습량과 딥러닝 모델의 정확도 사이의 상관관계에 대해서 살펴본다. 향후 악성코드 분석 연구에서 딥러닝 기술이 가지게 될 의미와 한계점, 그리고 새로운 연구 주제들에 대해서 소개한다.

# 딥러닝을 이용한 악성코드 분석 연구

국민대학교 소프트웨어융합대학
윤명근

KMU KOOKMIN UNIVERSITY

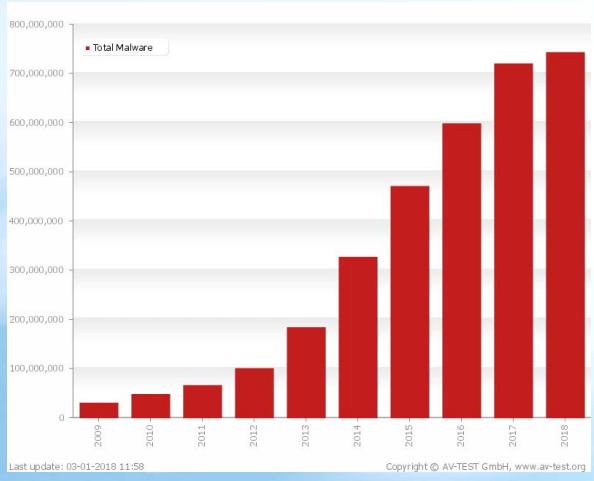
NetSec-KR'18

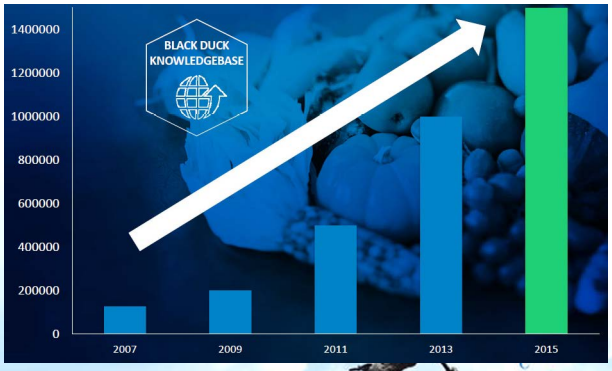
## 목차

- 연구 배경
- 딥러닝 모델
- 악성코드 빅데이터
- 향후 연구 방향

# 연구 배경

- 악성코드 증가
  - 오픈소스 발전 영향



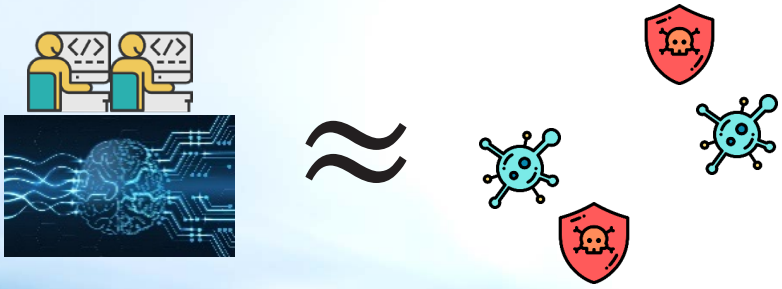



# 연구 배경

- 악성코드 증가
  - 악성코드 물량이 보안전문가 분석 능력 압도

# 연구 배경

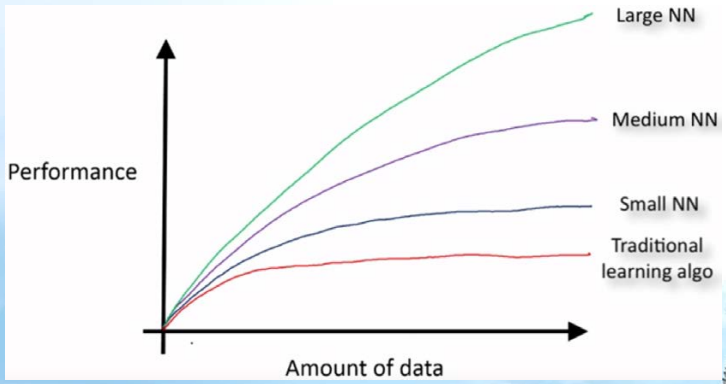
- 머신러닝 자동분석
  - 변종 코드 탐지



# 연구 배경

- 머신러닝
  - 지도학습 vs 비지도학습
  - 분류(classification) vs 구분(clustering)

- 전통적 기법(SVM, DT, RF) vs 딥러닝(deep learning)

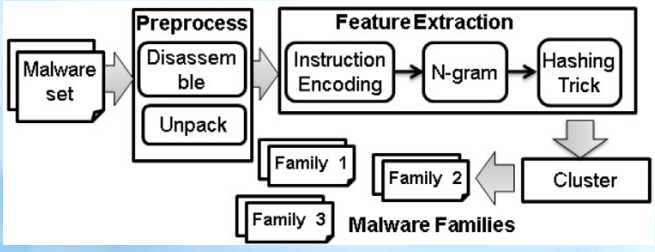


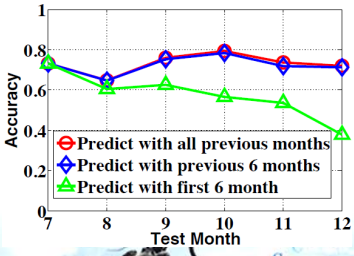

A. NG, "How Scale is Enabling Deep Learning",https://www.youtube.com/watch?v=LcfLo7YP8O4, 2016.2.

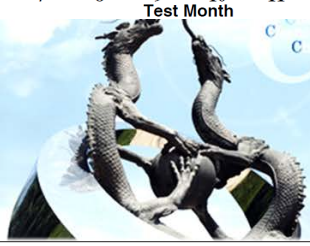
# 연구 배경

## ▪ 관련 연구 사례

- [1] MutantX-S: Scalable Malware Clustering Based on Static Features, USENIX ATC'13
- Unpacking, feature vector, hashing kernel, clustering
- Opcode sequence > mnemonic sequence
- 약 130,000 malware samples
- 6개월 학습, 6개월 테스트



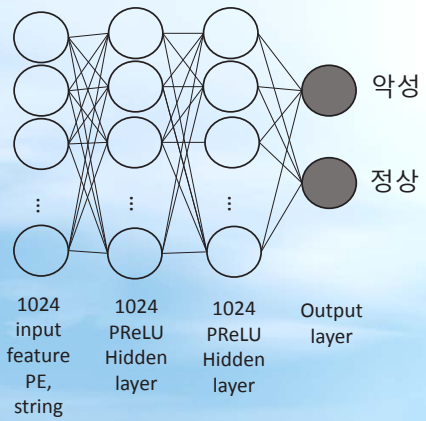





# 연구 배경

## ▪ 관련 연구 사례

- [2] Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features, IEEE Malware'15
- Deep-learning, ANN, byte/entropy histogram, PE Import features
- 약 400,000 malware samples
- 4-fold cross-validation



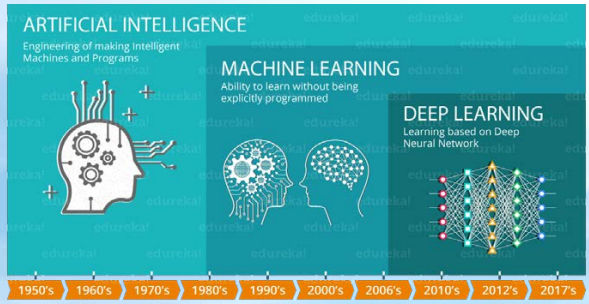

| 1. Feature extraction | | | |
|---|---|---|---|
| Contextual byte features | PE import features | String 2d histogram features | PE metadata features |

| 2. Deep neural network |
|---|
| Input layer, 1024 input features |
| Hidden layer, 1024 PReLU units |
| Hidden layer, 1024 PReLU units |
| Output layer, 1 sigmoid unit |

| 3. Score calibration model |
|---|
| Non-parametric score distribution estimation |
| Bayesian estimation of P(malware) |

# 딥러닝 모델

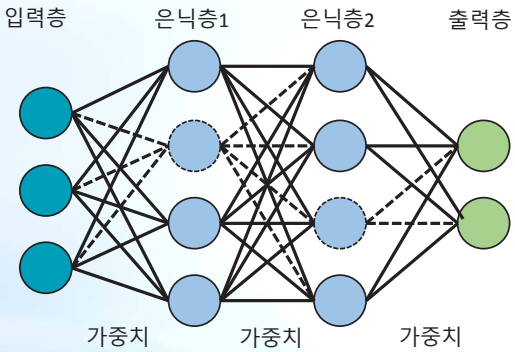
- 연구 동기
  - 다양한 딥러닝 모델 적용
    - 입력 데이터: Opcode n-gram vs 원본 파일
    - 신경망 모델: ANN vs CNN (Convolutional Neural Network)
    - 분류 형태: 이진 분류 vs 다중 클래스 분류
  - 빅데이터 학습
    - 3,000,000개 이상 악성코드 파일
    - 유료사이트 구매 + 자체 수집
    - VirusTotal 라벨 사용




https://www.edureka.co/blog/what-is-deep-learning

# 딥러닝 모델

- 연구 동기
  - 딥러닝 요소 기술

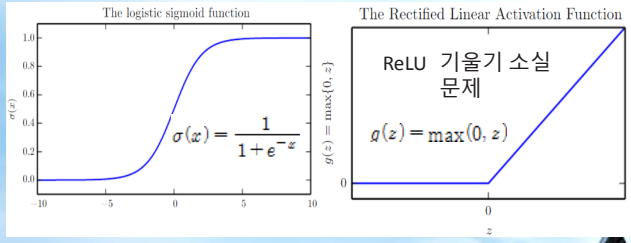


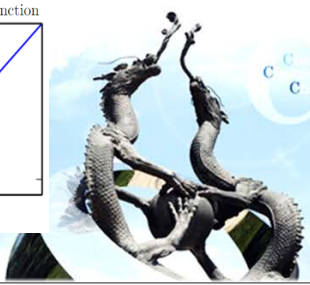

소프트맥스 함수

$$y_k = \frac{\exp(a_k)}{\sum_{i=1}^{n} \exp(a_i)}$$

dropout

과적합문제 (overfitting)

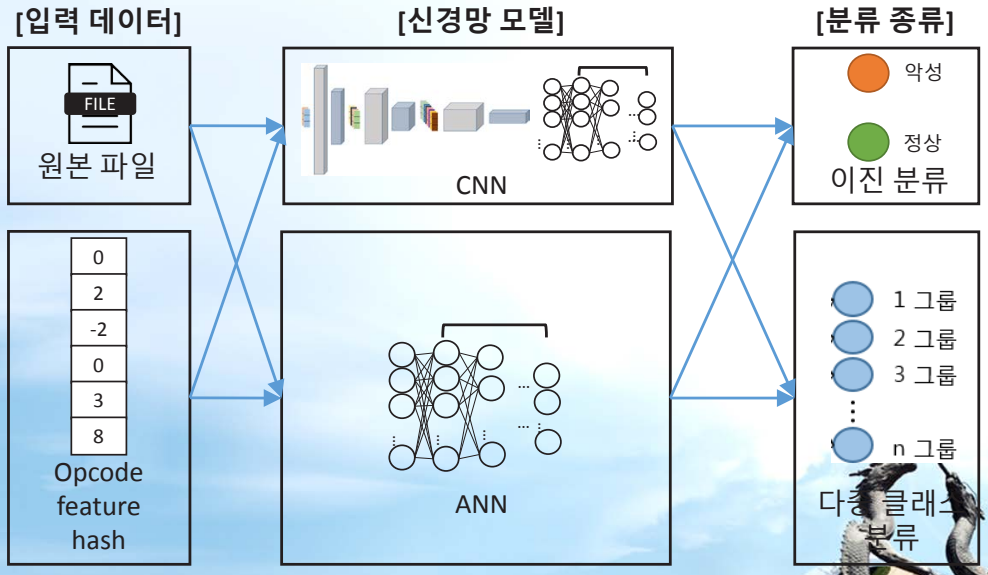


# 딥러닝 모델

- 딥러닝 모델
  - 8개 모델 구현 및 검증

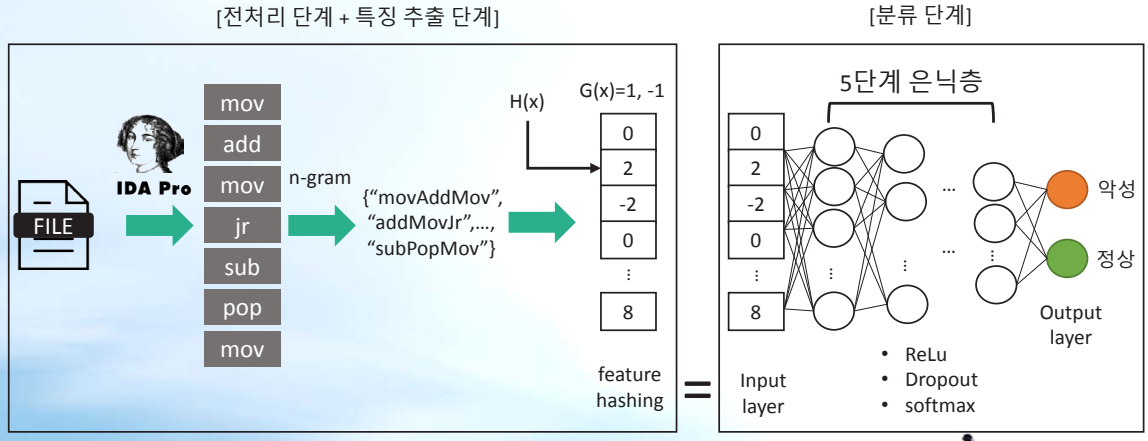
TensorFlow






# 딥러닝 모델

- 딥러닝 모델
  - opcode, ANN, 이진 분류

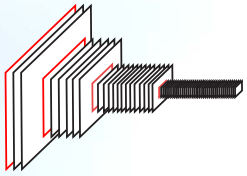


# 딥러닝 모델

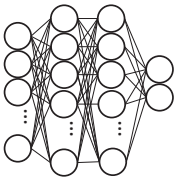
## ▪ 딥러닝 모델

- **CNN**

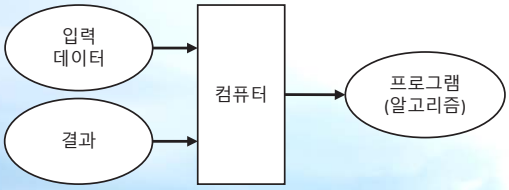
이미지



합성곱 계층
풀링 계층



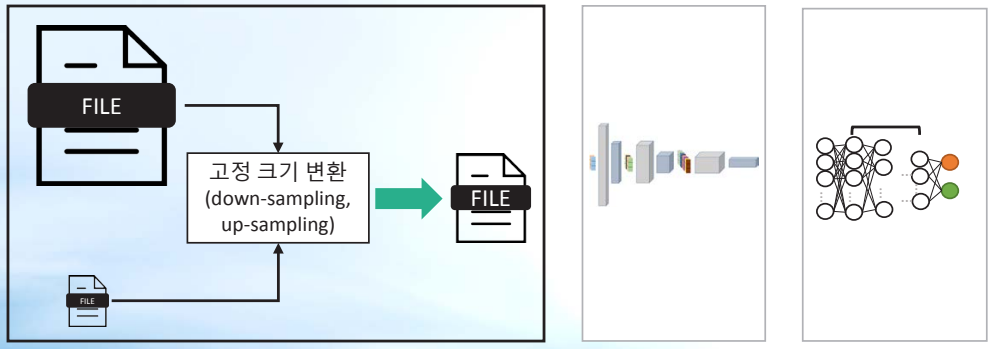
심층 신경망



# 딥러닝 모델

## ▪ 딥러닝 모델

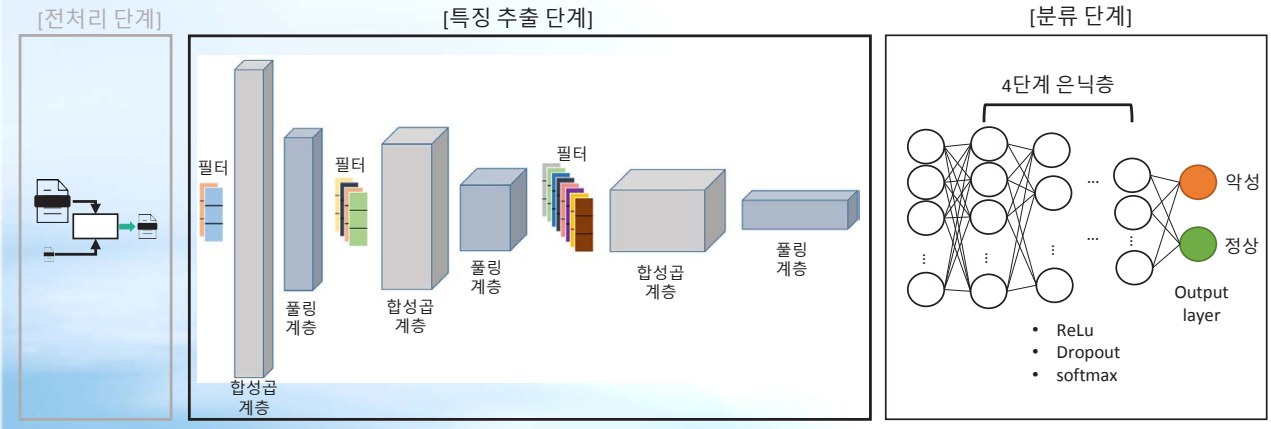
- **원본 파일, CNN, 이진 분류**



# 딥러닝 모델

## ▪ 딥러닝 모델

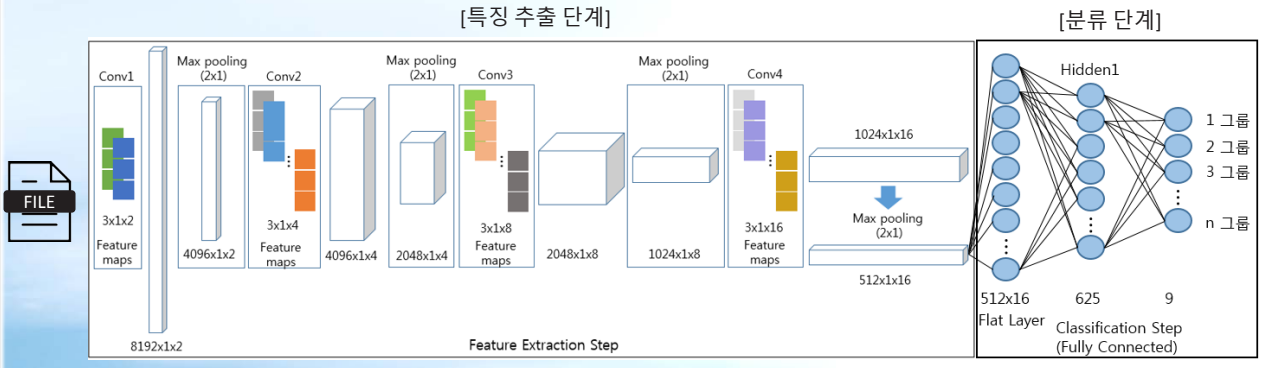
- 원본 파일, CNN, 이진 분류



# 딥러닝 모델

## ▪ 딥러닝 모델

- 원본 파일, CNN, 다중 클래스 분류



# 악성코드 빅데이터

## ▪ 실험 검증 (데이터셋 1)

Microsoft Malware Classification Challenge (BIG 2015)

Classify malware into families based on file content and characteristics

$16,000 · 377 teams · 2 years ago

https://www.kaggle.com/c/malware-classification

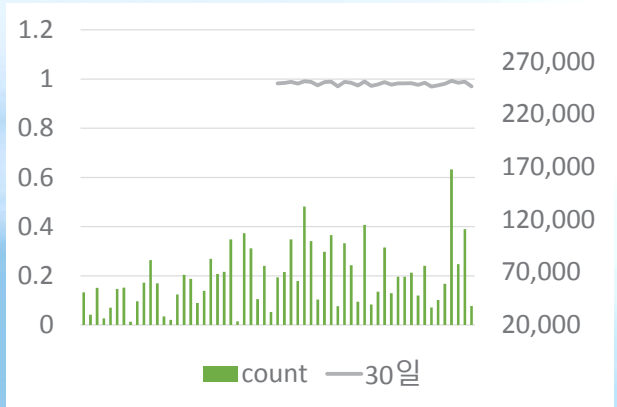
| 학습 데이터 | 테스트 데이터 |
|---|---|
| 10,868 개 (9 그룹) | 10,873 개 |

- PE 헤더가 제거된 Hexadecimal 표현 파일
- IDA Pro 분석 정보
- 악성코드 가정 후 그룹 분류 문제
- 정확도 99.7% (Winner Solution: 99.87%)
- 실험 환경
  - Windows10 (64bits), Intel i7-6850k, 128GM DDR4, GPU X 2(TiTan Xp), TensorFlow 1.3.0, Python 3.5.4

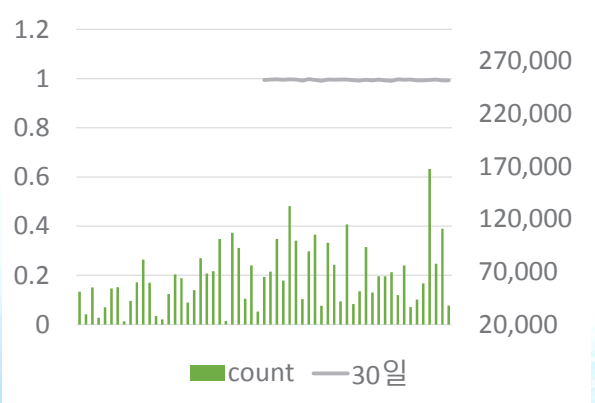
# 악성코드 빅데이터

## ▪ 실험 검증 (데이터셋 2)

- 윈도우 PE 포맷 파일
- 정상 파일 (자체 수집): 44,010개
- 악성 파일 (유료 구매): 3,814,840개 (2017.08.02~9.30, 60일)
  - 처음 30일 학습, 나중 30일 테스트




precision




recall

# 악성코드 빅데이터

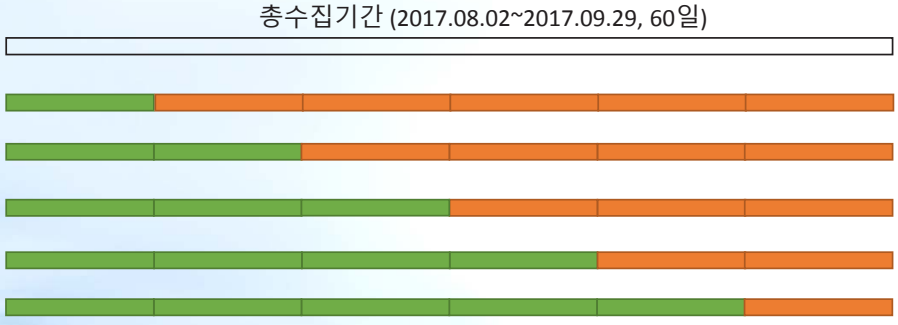
## ▪ 실험 검증

| 분류 형태 | 신경망 모델 | 입력 데이터 | 정확도(%) |
|---|---|---|---|
| 이진 | CNN | opcode | 99.55 |
| | | 파일 원본 | 85.82 |
| | ANN | opcode | ***99.76*** |
| | | 파일 원본 | 94.92 |
| 다중 클래스 (29개 그룹) | CNN | opcode | 83.7 |
| | | 파일 원본 | 83.4 |
| | ANN | opcode | 88.4 |

# 악성코드 빅데이터

## ▪ 실험 검증

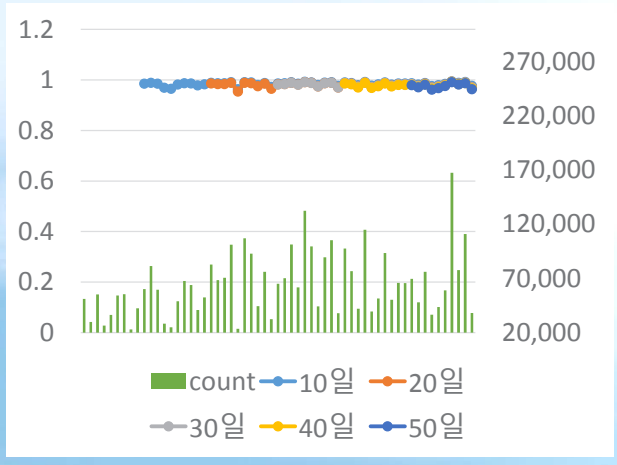
- **학습 기간 변동 실험**



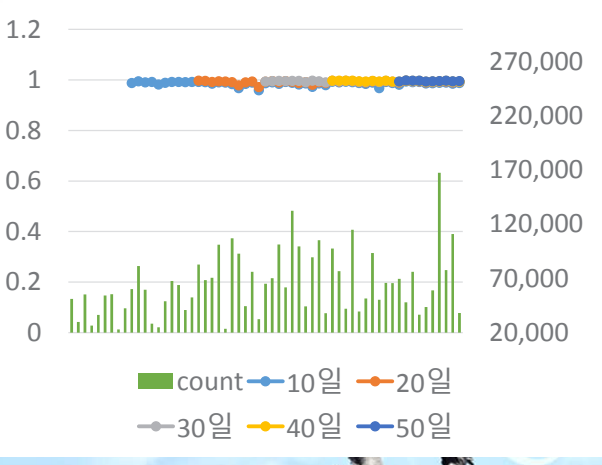

- 학습기간 : 10일
- 테스트기간:

# 악성코드 빅데이터

- 실험 검증
  - 정확도 ∝ 데이터 수집 기간 or 데이터 분량 ?




precision

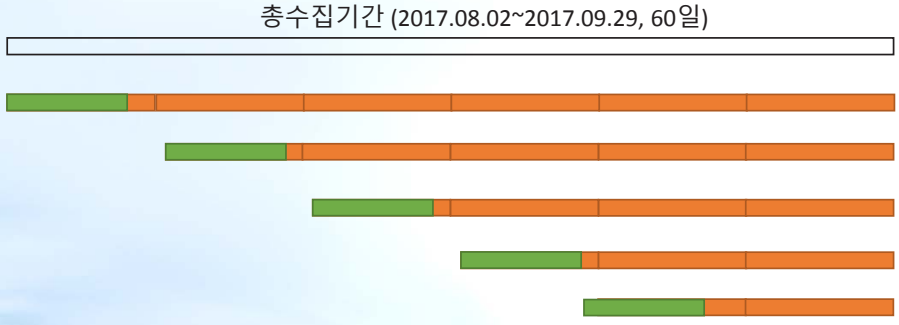



recall



# 악성코드 빅데이터

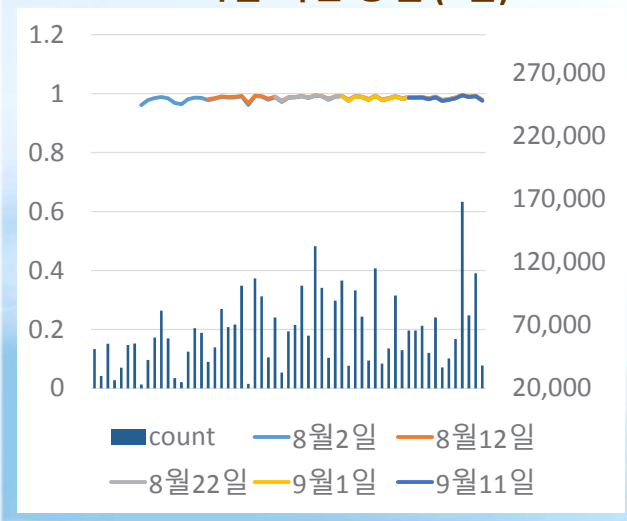
- 실험 검증
  - 학습 시점 변동 실험



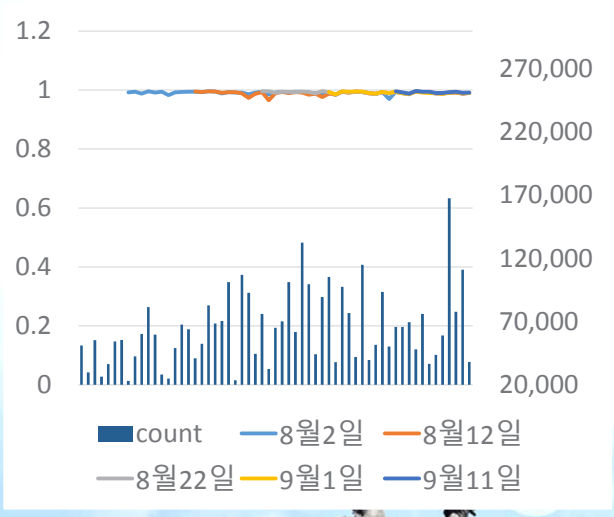

- 학습기간 : 8일
- 테스트기간:

# 악성코드 빅데이터

- 실험 검증
  - 학습 시점 변동 실험
  - 학습 기간 동일 (8일)




precision

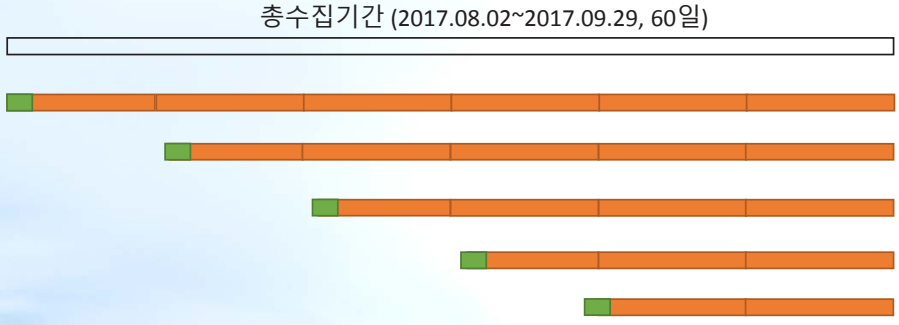



recall



# 악성코드 빅데이터

- 실험 검증
  - 학습 시점 변동 실험 (학습 기간 1일 고정)

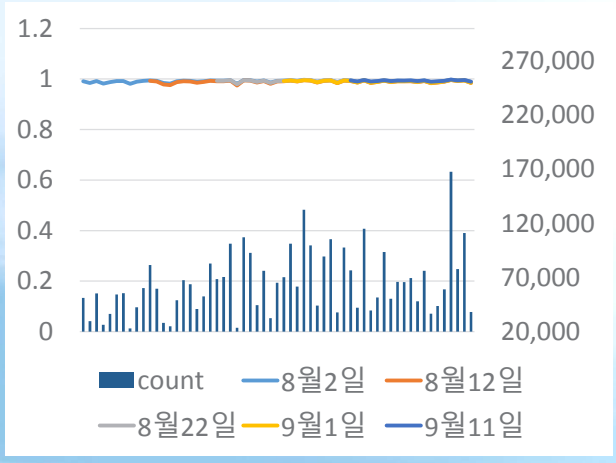



- 학습기간 : 1일
- 테스트기간:

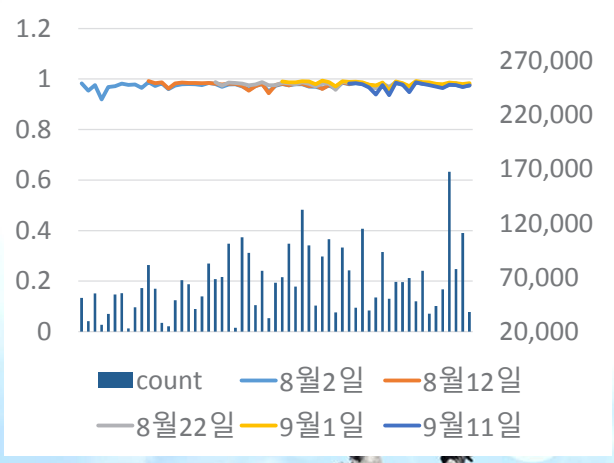
# 악성코드 빅데이터

## ▪ 실험 검증

### • 학습 시점 변동 실험 (학습 기간 1일 고정)




precision



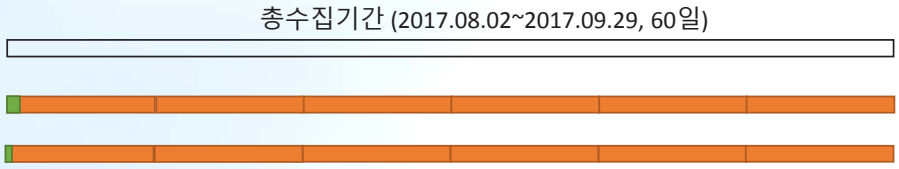

recall



# 악성코드 빅데이터

## ▪ 실험 검증

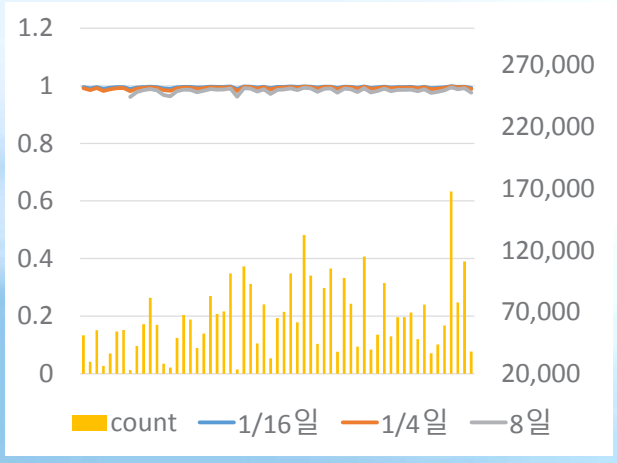
### • 학습 시점 변동 실험 (학습 기간 1일 미만)



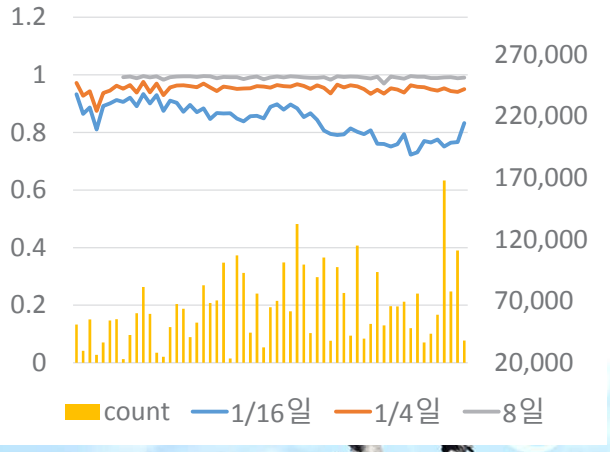

- 학습기간 : 학습 기간 1/4일 (=6시간) 학습 기간 1/16일 (=1.5시간)
- 테스트기간:

# 악성코드 빅데이터

- 실험 검증
  - 학습 시점 변동 실험
    - 학습 기간 1/4일 (=6시간)
    - 학습 기간 1/16일 (=1.5시간)




precision

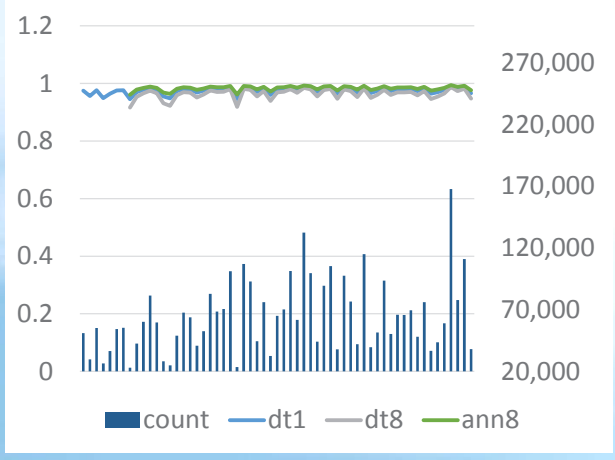



recall

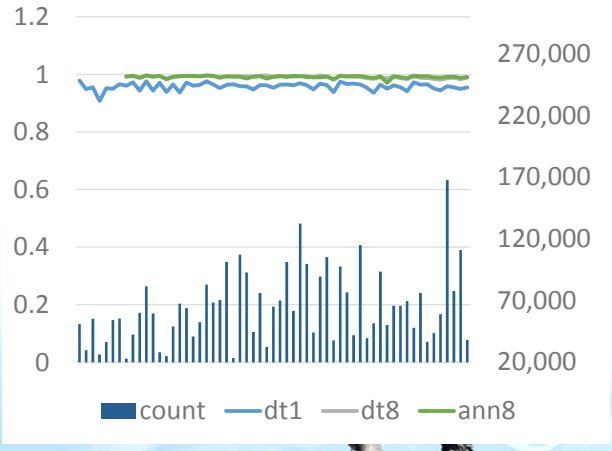


# 악성코드 빅데이터

- 실험 검증
  - 전통적 머신 러닝 vs 딥러닝
    - decision tree vs ANN




precision




recall

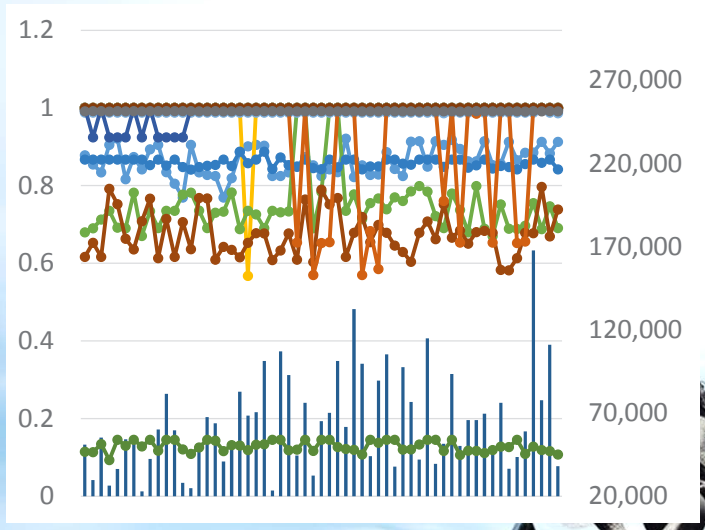
# 악성코드 빅데이터

- 실험 검증
  - 유사 파일 반복 등장 검증 (32개 샘플)

| | |
|---|---|
| 0 | 0 |
| 2 | 1 |
| 4 | 3 |
| 1 | 1 |

feature hashing

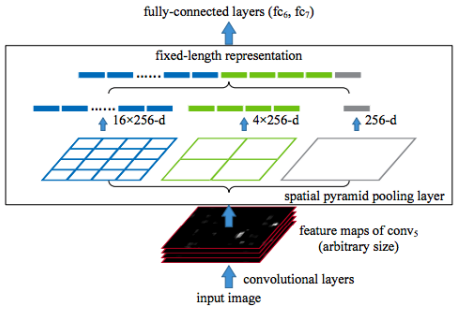
$$cos(\theta) = \frac{A \cdot B}{|A||B|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} (A_i)^2} \times \sqrt{\sum_{i=1}^{n} (B_i)^2}}$$



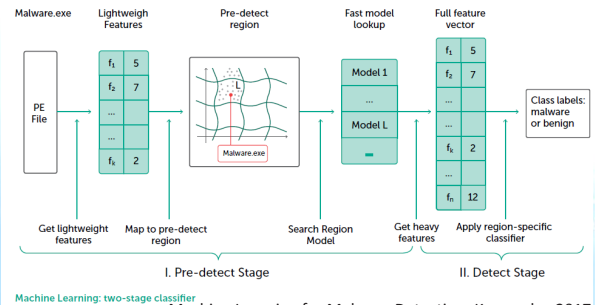



# 향후 연구 방향

- 딥러닝 모델 고도화
  - CNN 가변 크기 데이터 입력
  - 다양한 모델 실험
- 악성코드 분석 실전 활용
  - 위협 인텔리전스, Indicator of attacks
  - 설명 가능 분석 모델
- 빅데이터 처리
  - Locality-sensitive hash
  - Storage, cloud computing
- 정적 분석 한계 극복
  - 난독화
  - 동적 분석




Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition, K. He et al, ECCV14.




Machine Learning for Malware Detection, Kaspersky, 2017

# Q & A

- mkyoon@kookmin.ac.kr

The 24th Network Security Conference -Korea

# 딥러닝 기반 이상징후 탐지시스템 실적용 사례

**유경식** 인피니그루 대표

### 학력 및 경력사항

| | |
|---|---|
| 2014.11 ~ 현재 | (주)인피니그루, 대표이사 |
| 2011.12 ~ 2013.04 | 알티베이스, 해외사업본부장 |
| 2001.06 ~ 2011.01 | 다쏘시스템 한국지사, 3DVIA Brand Leader |
| 1999 ~ 2001.05 | 단암데이타 시스템 |

### 강연요약

기존의 거의 대부분의 보안관련 이상징후탐지 시스템은 룰기반 시스템 으로 적용되어 있습니다. 기존 룰기반의 이상징후탐지 시스템의 문제는 룰의 생성에서 부터 사람의 가설로 룰을 만들고 상당부분 이분법적인 분석으로 룰을 만들어서 시스템에 적용을 하기 때문에 약간의 변경만을 가해진 새로운 사기패턴,이상징후패턴에 항상 취약할수 밖에 없습니다. 사고후에는 같은 사고를 두번다시 당하지 않기 위한 분석에 돌입하고 이를 룰에 반영하는 다분히 기계적이고 반복적인 관리 문제점을 안고 있습니다.

인피니그루는 이런 문제를 해결하고자 딥러닝기반의 이상징후 탐지 시스템을 개발하고 시장에서의 검증을 마쳤습니다. 인피니그루는 기존 룰방식보다 훨씬 정교하고 정탐률이 높은 딥러닝방식의 시스템을 제공하고 또한 기존 룰방식에서의 장점 또한 병행하는 하이브리드(AI+Rule)방식의 이상징후탐지 시스템을 시장에 공급하고 있습니다.인공지능의 장단점, 룰방식의 장단점을 서로 보강하는 이상적인 이상징후탐지시스템을 실적용사례 위주로 소개 합니다

YGruADS Suite YGruSLS Platform

# NetSec-KR

# 딥러닝기반 이상징후 탐지 실적용 사례

2018. 04. 12
KyoungSik YOO | CEO | InfiniGru
010-9033-8913 | ks@infinigru.com

(주)인피니그루

Copyright©2018 INFINIGRU Corp. All right reserved

(주)인피니그루

(주)인피니그루

인피니그루는 인공지능 기술을 기반으로 이상징후탐지 및 데이터 분석(큐레이션) 서비스를 제공합니다. 특히, 국내 기업 중 이상징후탐지 영역에서 최초로 딥러닝 기술을 검증 받았으며 현재 최대 성공적 적용사례를 보유한 회사 입니다.

| 회사명 | (주)인피니그루 |
|---|---|
| 설립일 | 2014년 10월 31일 |
| 대표이사 | 유경식 |
| 자본금 | 1억2천5백만원 |
| 주소 | 서울시 서초구 서초대로78길 22 홍우제2빌딩 513호 |
| 사업분야 | 컴퓨터관련 서비스사업, 패키지소프트웨어 개발 공급 |
| 독자보유기술 | 딥러닝기반 이상징후탐지 기술<br>머신러닝기반 데이터 큐레이션 기술 |
| 솔루션 내용 | 하이브리드[AI+Rule]기반 이상징후탐지 솔루션<br>머신러닝기반 데이터 분류 및 큐레이션 솔루션 |
| 제품 | GruADS Suite, GruSLS Platform, GruCurator |

연구소 | 벤처기업 | 특허등록 | K-Global 300

투자자 현황

GMB 지엠비인베스트먼트 | SCI 평가정보(주) | 신한카드

| 년 | 월 | 비즈니스 내용 |
|---|---|---|
| **2018** | **3** | **베트남 ACB은행 FDS 우선협상대상업체 선정** |
| | **2** | **SBI저축은행 대출사기 모형개발 계약** |
| 2017 | 12 | **K-Global 300 업체 선정, 서울시 창업허브 선정** |
| | **07** | **투자유치(Seed 단계) – SCI평가정보, GMB인베스트먼트, 신한카드 투자계약** |
| | **07** | **SBI저축은행 – GruDEEP Hybrid 계약** |
| | **06** | **한국스마트카드 – GruCurator 계약** |
| | 03 | **KB국민카드 – GruDEEP 계약** |
| | 01 | 신한퓨쳐스랩 핀테크육성업체 선정 |
| 2016 | 11 | 현대카드 핀베타 육성업체 선정 |
| | 10 | **중소기업청 창업성장기술 개발사업 계약** |
| | | **한국스마트카드 –GruDEEP Hybrid 계약** |
| | | 딥러닝기반 마케팅분석 특허 출원 中 |
| | 07 | **신한은행 – GruDEEP 계약** |
| | 05 | **SK증권 – GruFDS 구축, GruCurator 계약** |
| | 03 | 비정상행위 탐색방법 및 탐색프로그램 특허출원 |
| 2015 | 11 | 벤처기업 인증 |
| | **05** | **유안타증권 – GruFDS 계약** |
| | 04 | 기업부설연구소 설립 |
| 2014 | **10** | **㈜인피니그루 설립** |

## 이상징후 탐지

2

## 이상징후 탐지

(주)인피니그루

자금세탁방지 시스템

내부통제 시스템

이상징후 탐지 시스템

개인정보 유출 방지 시스템

상시감사 시스템

문서보안관리 시스템

위협/패치/자산관리 시스템

네트웍 침입탐지 시스템

통합 관제 시스템

장애예측 시스템

기타 보안 솔루션

3

Everything is Rules based system

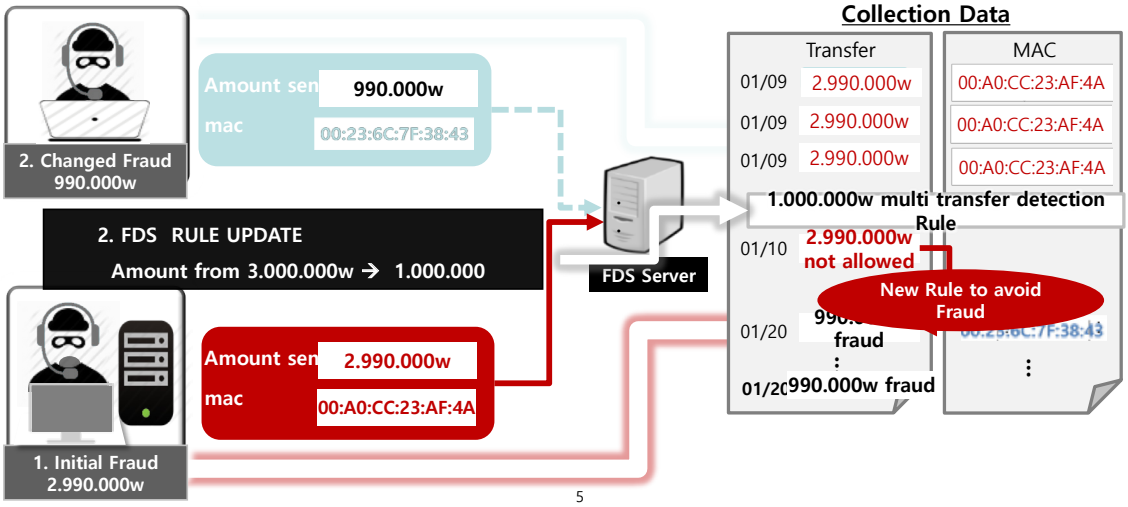
4

## 룰방식의 한계점

(주)인피니그루

| 년도 | 금감원 정책 | 사기 행위 |
|---|---|---|
| 2014 | 300만원 이체시 → 30분 지연 이체 | 299만원 이하 이체 |
| 2015 | 100만원 이체시 → 30분 지연 이체 | 99만원 이하 이체 |

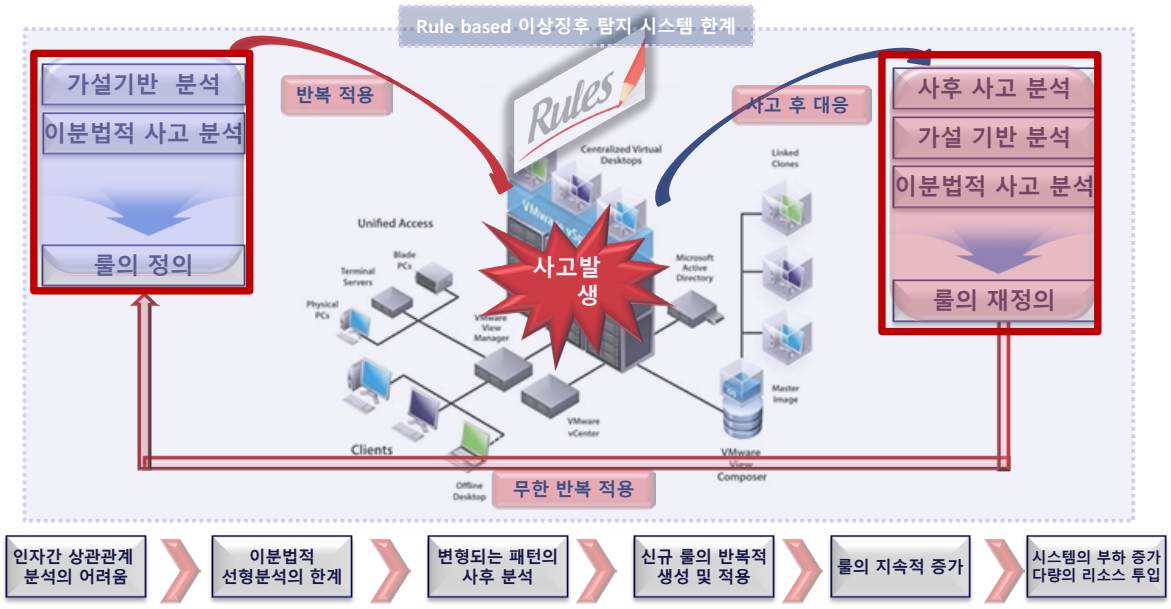
룰은 정책과 사기꾼 행위에 따라 항상 변경 되어야 한다.




5

## 현시장의 문제점

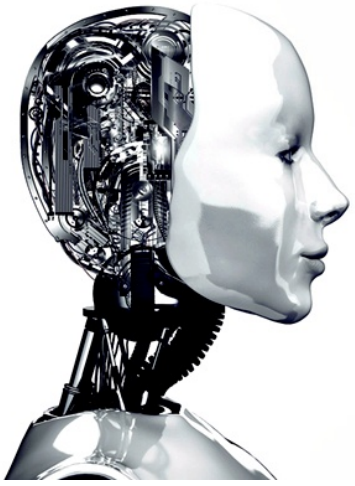
(주)인피니그루






## What is the SOLUTION !!

(주)인피니그루



"Artificial Intelligence"

"Deep Learning"

## 기술 적용 현황

(주)인피니그루

8

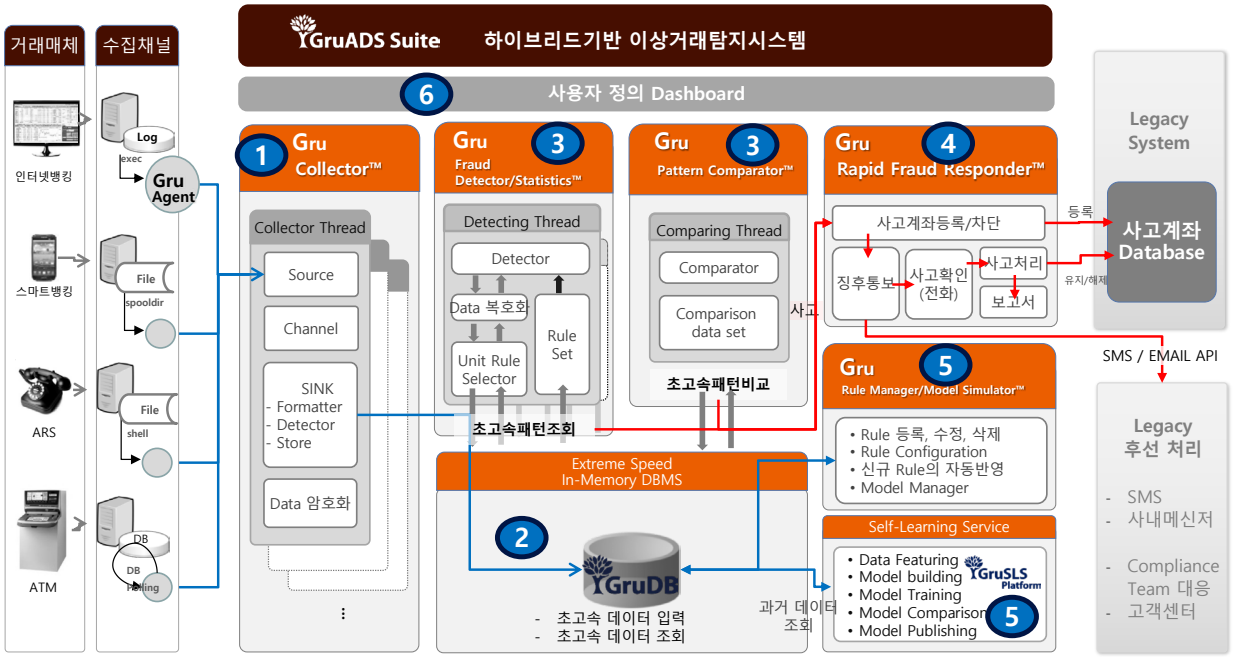
## 핵심 필요 기능

(주)인피니그루

9

## 시스템 구조도

(주)인피니그루






## FDS 3대 성공 요소

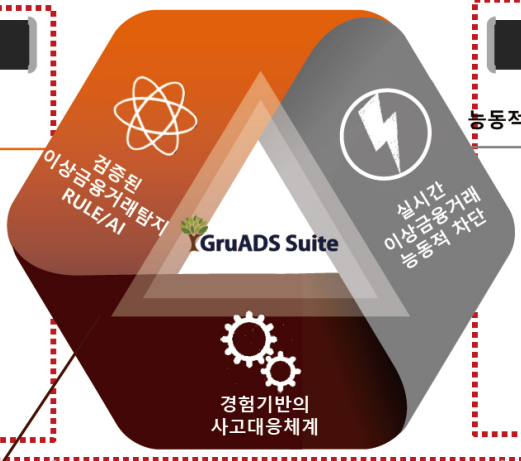
(주)인피니그루

성공적인 이상거래탐지시스템의 구축과 지속적인 운영을 위해서는 최소적으로 충족할 3대 요소가 있습니다.

### 1. 검증된 RULE 매카니즘 / 인공지능

**고객사 현장에서 검증된 룰 매카니즘 및 모형 재학습 플랫폼**

- 성공적으로 운영되는 RULE 매카니즘 제공으로 즉시 운영가능
- 시스템 정지 없이 즉각적 룰 적용
- 인공지능을 활용한 정오탐률의 최대 최소화 지원
- 딥러닝 모형 개발의 자동 재학습 플랫폼 지원




### 2. 사전 탐지/차단 아키텍처

**이상금융거래를 능동적 대응인 선탐지/선차단 아키텍처로 설계**

- 모든 이상금융거래를 선탐지 / 선차단하는 초고속 In-Memory Architecture 로 설계
- 초고속 데이터 비교/분석 인프라로 금융사고의 피해를 획기적으로 최소화
- 실시간 인공지능 병행 탐지

### 3. 현장경험이 반영된 사고대응체계

**기존 업무에 영향을 최소화하여 반영된 대응체계 제공으로 누구도 쉽게 대응 가능**

- 실 금융사고를 대응한 경험을 기반으로 만든 금융사고 대응체계를 제공
- 금융사고를 경험해보지 못한 업무 담당자도 체계적으로 금융사고에 대응 가능

## 하이브리드 이상징후 탐지 – RULE

(주)인피니그루

이상금융거래탐지 인자 피라미드



## 하이브리드 이상징후 탐지 – 딥러닝 사례

(주)인피니그루

1. A 증권
2. B 은행
3. C 카드
4. D 카드

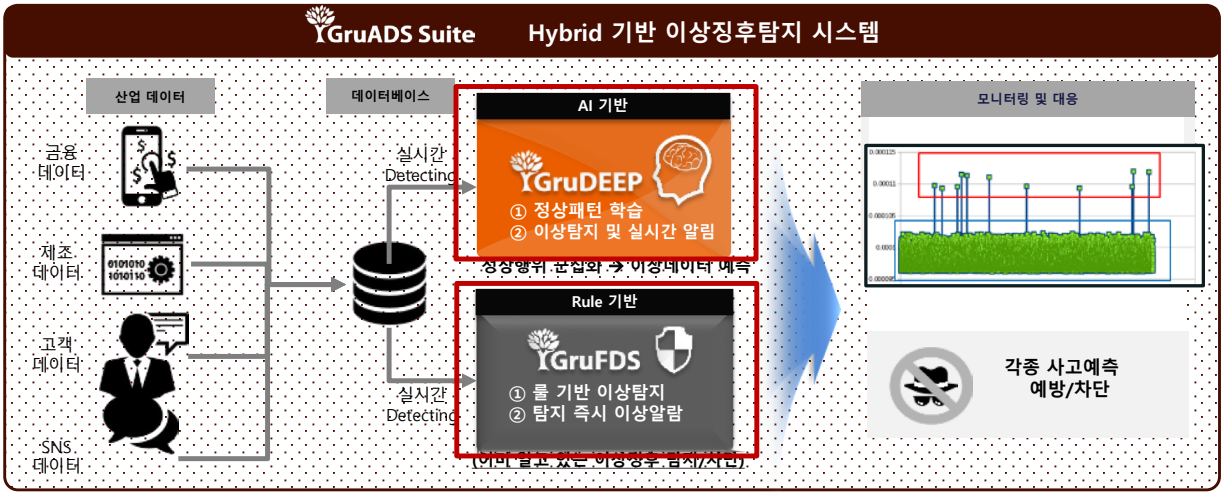
당일 발표

## 인공지능기반 – 분석/하이브리드 개념 분석

(주)인피니그루

미탐과 오탐을 최소화 하기 위해 데이터 분석은 룰(Rule) 기반 시스템과 인공지능(AI) 기반 시스템을 병행하는 하이브리드 방식이 가장 이상적입니다.

| 이상징후 시스템 유형 | 장점 | 단점 |
|---|---|---|
| 룰 기반 이상징후 탐지 시스템 | 이상징후의 사유해석이 가능함, 즉시대응 | 탐지율이 낮음, 사전대응 불가, 사후대응 |
| 인공지능 기반 이상징후 탐지 시스템 | 월등한 탐지율, 이분법적 아닌 종합적 탐지 | 사유해석이 어려움, 학습시간 필요 |
| 하이브리드(Rule+AI)기반 이상징후 탐지 시스템 | 룰의 장단점과 인공지능의 장점을 융합한 이상적인 이상징후 탐지시스템 | |



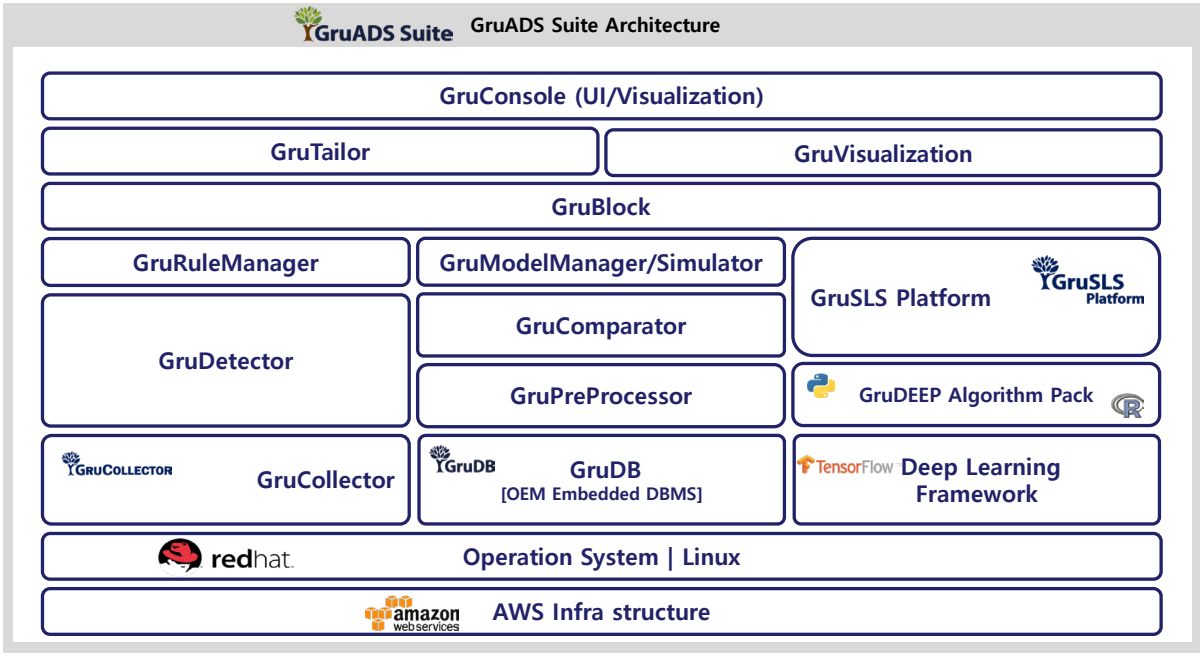



## 모형개발 프로세스

(주)인피니그루

## FDS Architecture

(주)인피니그루




16

GruADS Suite GruSLS Platform

NetSec-KR

# 감사합니다

GruADS

(주)인피니그루

Copyright©2018 INFINIGRU Corp. All right reserved

The 24th Network Security Conference -Korea

# 생체신호를 이용한 차세대 인증기술

**김재성** KISA 연구위원

### 학력 및 경력사항

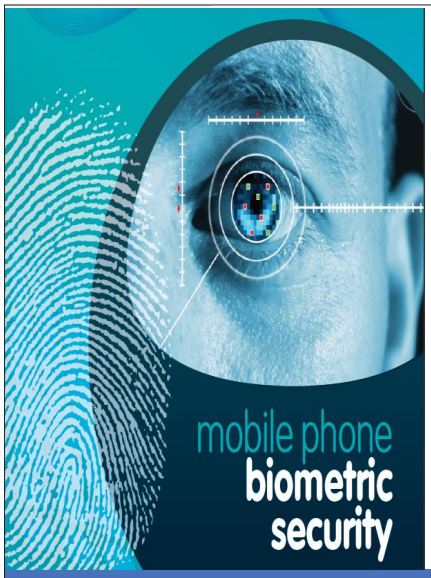
| | |
|---|---|
| 1982.02 | 경성고등학교 졸업 (경성 12기) |
| 1986.02 | 인하대학교 전산학 학사 |
| 1989.02 | 인하대학교 전산학 석사 |
| 2005.08 | 인하대학교 정보통신공학(바이오인식) 박사 |
| 1989 | LG정보통신 중앙연구소 TDX10 교환기SW (연구원) |
| 2005 | 한국전자통신연구원 국가전파감시망 (선임연구원) |
| 2006 ~ 현재 | 한국인터넷진흥원 바이오인식 (연구위원) |

※ 생체신호를 이용한 텔레바이오인식기술 국제공동연구 과제책임자

### 강연요약

최근에 들어, 공인인증서 의무화 폐지에 따라, 스마트폰상의 모바일 지급결제서비스, 인터넷전문은행 등 핀테크 분야에서 비대면 인증 수단으로 각광을 받고있는 바이오인식기술이 전세계적으로 주목받고 있다. 이와 함께 독일 해커그룹을 통하여 스마트폰에 탑재된 지문 · 얼굴 · 홍채 · 정맥인식기술에 대한 위변조 해킹위협 또한 증가되고 있는 추세이다. 이에 따라 영국 · 캐나다 등 주요 선진국에서는 은행권을 중심으로 위변조에 강하고 편리한 심전도 · 심박수 등 생체신호를 이용한 차세대 바이오인식기술 개발과 시범서비스가 추진중에 있다.

2014년도부터 KISA에서는 심전도 · 심박수를 이용한 텔레바이오인식기술에 대하여 TTA PG505를 통한 국내표준화 및 ITU-T SG17를 통한 국제표준화를 추진중에 있으며, 2016년도부터 스페인, 미국 등 주요선진국과 지문 · 심전도 · 심박수 등 다중 생체신호 인증플랫폼 개발을 위한 국제공동연구를 수행중에 있다. 지문 · 얼굴 · 홍채 · 정맥 등 기존의 바이오인식기술이 살아있는 사랑의 외부에 노출되어있는 신체적 특징을 이용함에 따라 위변조에 취약한 반면에, 생체신호 인증기술은 사람의 내부 신체에서 발생되는 전기적 · 화학적 · 행동적인 특징을 이용함에 따라 차세대 인증기술로 각광받을 전망이다. 본 강연에서는 바이오인식기술의 위변조 위협과 함께 새롭게 출현되는 생체신호를 이용한 차세대 인증기술의 특징과 이에 대한 기술개발 및 국내외 표준화 추진현황을 고찰하고자 한다.




NetSec-KR 2018

# 생체신호를 이용한 차세대 인증기술

2018. 04. 12.(목)

공학박사 김 재 성 연구위원 (kimjs@kisa.or.kr)
보안기술확산팀, TTA PG505 & ABC(아시아 ) 의장

KISA 한국인터넷진흥원

## 발표순서

I 바이오인식분야 변천사

II 바이오인식분야 보안이슈

III 바이오인식분야 KISA 대응현황

IV 다중 생체신호 인증플랫폼 개발

V 텔레바이오인식기술 표준개발

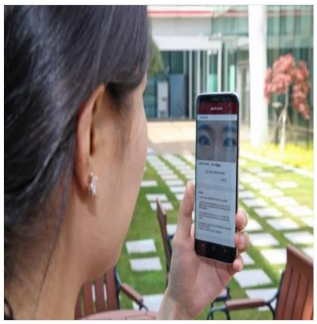
## I 바이오인식분야 변천사 – Definition

**공인인증서 폐지, Why?**

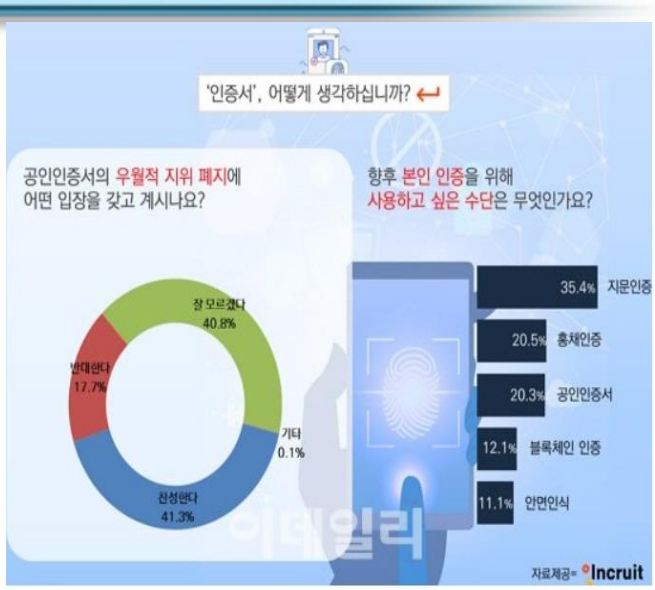
- 공인인증서에 대한 보관, 편의성(전자거래 등), 양도가능성
- 공인인증서에 대한 비밀번호 보안취약성 등

공인인증서 20년만에 폐지...간편한 생체·모바일 인증 시대 도래

박태근 기자 입력 2018-03-29 16:01 수정 2018-03-30 15:55



홍채 및 지문 인식 공인인증 서비스(SK㈜C&C금융그룹 제공)

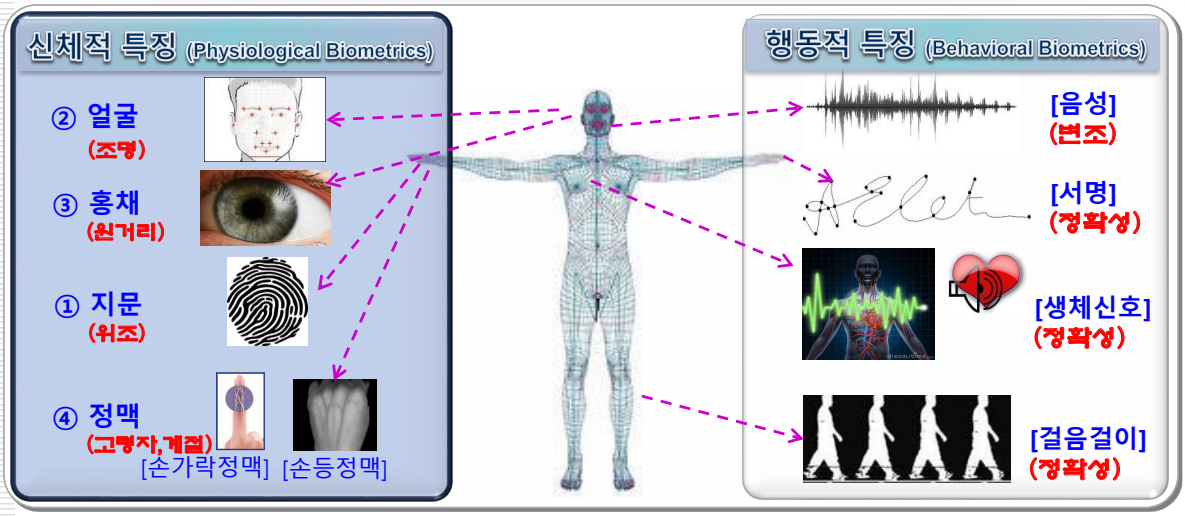





## I 바이오인식분야 변천사 – Definition

**바이오인식이란?**

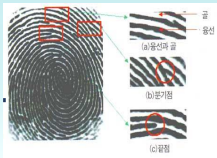
**사람의 신체적(얼굴/홍채/지문/정맥 등), 행동적(음성/서명/생체신호/걸음걸이 등) 특징을 자동화된 IT 기술로 추출·저장해, 다양한 IT 기기로 개인의 신원을 확인하는 수단**



## I 바이오인식분야 변천사 – Modality

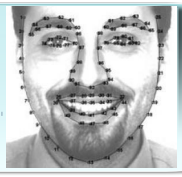
**① 지 문**

- 가장 오래 사용된(100년 이상) 생체인식 종류
- 임신 24주째에 생성되어, 평생 불변
- 지문 취득 불가(무지문, 다한증), 접촉식



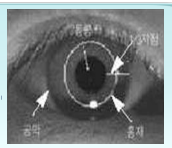
**② 얼 굴**

- 얼굴 외곽, 눈/눈썹/코모양, 눈/코/턱 간격 등 측정
- 비접촉 방식으로 사용자의 거부감이 적음
- 환경(안경,가발,조명 등) 영향이 많고, 인식 시간이 오래 걸림



**③ 홍 채**

- 홍채 모양, 색깔, 망막 모세혈관의 형태소 등 인식
- 생후 18개월에 모양이 완성된 후, 평생 불변
- 사용자 거부감이 높으며, 제품의 크기가 큼



**④ 정 맥**

- 손등 또는 손가락의 혈관 형태를 측정
- 적외선 카메라를 이용, 혈관을 투시 후, 잔영을 인식
- 하드웨어 구성이 복잡해, 제품 가격이 고가임

## I 바이오인식분야 변천사 – Industry

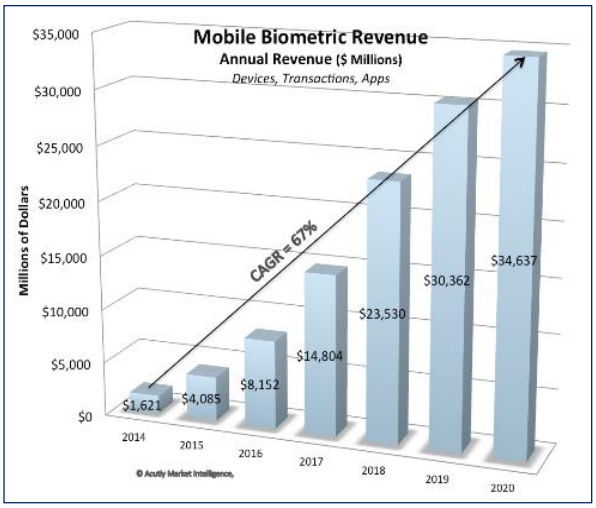
<2015년도 KISA 정보보호산업실태조사>

| 세부항목 | 2014년 | 2015년 (E) | 2016년 (E) | 2017년 (E) | 2018년 (E) | 2019년 (E) | 2020년 (E) | CAGR (13-'18) |
|---|---|---|---|---|---|---|---|---|
| 얼굴인식시스템 | 53,299 | 57,299 | 65,433 | 71,199 | 77,151 | 83,372 | 89,919 | 9.11 |
| 지문인식시스템 | 106,765 | 112,564 | 123,252 | 131,111 | 139,645 | 148,866 | 158,796 | 6.84 |
| 홍채인식시스템 | 2,529 | 2,687 | 2,170 | 1,885 | 1,656 | 1,464 | 1,298 | -10.52 |
| 정맥인식시스템 | 5,783 | 6,293 | 6,975 | 7,494 | 8,045 | 8,629 | 9,251 | 8.14 |
| 기타(음성인식등) | 6.151 | 7,276 | 8,630 | 9,339 | 10,079 | 10,858 | 11,681 | 11.28 |
| **소계** | **174,527** | **186,119** | **206,469** | **221,028** | **236,576** | **253,188** | **270,046** | **7.61** |

## I 바이오인식분야 변천사 – Markets

# 2020년에 346억 달러(약 38.2조원) 시장 전망

- AMI는 2020년 까지
  - ✓ 스마프톤, 태블릿PC, 웨어러블 등 모든(100%) 스마트기기에 바이오인식 기술 적용
  - ✓ 시장 규모는 연평균 67%씩 성장해 346억 달러에 이를 것으로 전망
- 2017년부터 결제거래, 사용자 인증수단으로 활용 되며 시장 규모가 증가함

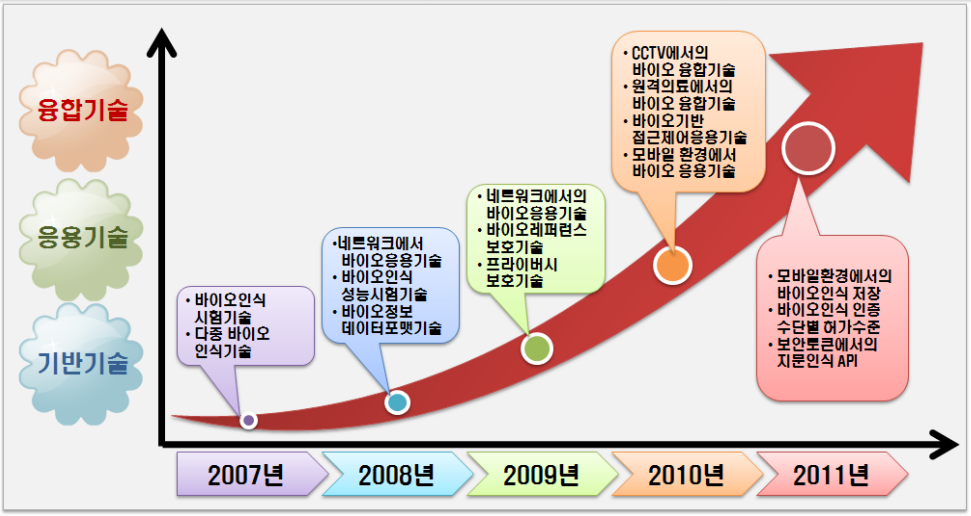





## I 바이오인식분야 변천사 – Trends

**Worldwide** (미국 01년 911 테러, 02.12 ISO/IEC SC37 발족, 06년 전자여권 도입, 12년 애플社 아이폰),

***대면 ☞ 비대면서비스로*** 전환됨에 따라 ***위변조에 강인한 New 융합인증기술이 요구됨***




**Korea** (01년 KBA 협의회발족, 06년 KISA 시험센터발족, 08년 전자여권 발급/US-VISIT 무비자, 13년 삼성전자 갤럭시S)

## I 바이오인식분야 변천사 – Trends

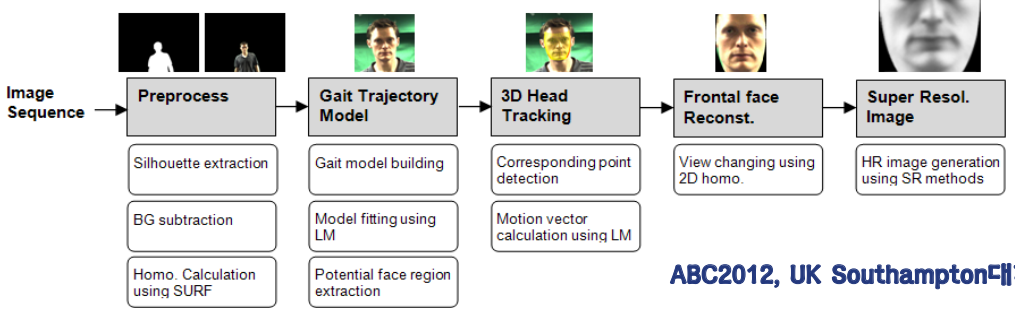
Body

Face

ABC2011, China Beijing 중산대학

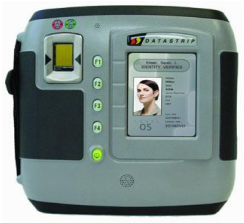
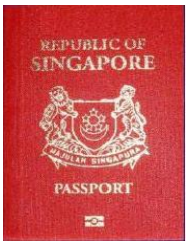


## I 바이오인식분야 변천사 – Trends




ABC2012, UK Southampton대학

## I 바이오인식분야 변천사 – Trends

Handheld Scanners

Desktop Scanners

ABC2011, Singapore 창이공항



## I 바이오인식분야 변천사 – Trends

# 온라인 ⇒ 모바일 기반 오프라인으로 성장

▌바이오인식 기술 : 물리적 통제 수단 → 모바일, 금융 등 사용 환경 다변화

### 모바일 분야 바이오인식 활용 증가

- 지문인식, 홍채인식, 얼굴인식(예정) 탑재 스마트폰 제품 증가
  - (최초) 베가 LTE-A : 지문인식
  - 아이폰 5~(터치ID) : 지문인식
  - (최초) 갤럭시 노트 7 : 홍채인식

⇒ 아이폰 8 얼굴인식(예정), 초음파식 지문인식기 다양한 제품 출시 예정

### 바이오인식을 이용한 모바일금융 증가

| 은행명 | 인증수단 |
|---|---|
| 신한은행 | 지문, 홍채 |
| KB국민은행 | 지문 |
| KEB하나은행 | 지문, 홍채 |
| 우리은행 | 지문, 홍채 |
| NH농협은행 | 지문 |
| 씨티은행 | 지문 |

※ 홍채인증은 삼성 갤럭시 노트 7의 판매중단으로 서비스 지연

## I 바이오인식분야 변천사 – ATM Machines

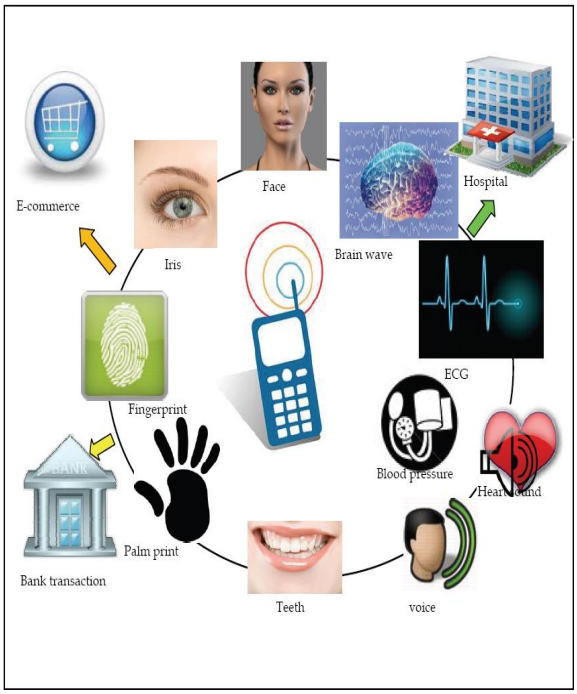
| 활용국가 | 적용내용 | Bio인증 |
|---|---|---|
| 영국<br>(홍채) | O Barclays 은행 (신원도용 피해방지용), ' 15년~<br>- 인터넷뱅킹 이체거래시 *지정맥*으로 본인확인서비스 시범운영중 | 지정맥<br>(손가락) |
| 일본<br>(정맥) | O 도쿄 미쓰비시 UFJ, 미쓰이 스미토모 등 주요은행권<br>- ATM 거래시 *손바닥/손가락 정맥*으로 금융사고 예방서비스 실시중<br>O 오가키 교리츠 등 일부은행권<br>- 무매체 거래를 위해 정맥정보를 은행서버에 저장/관리중<br>☞ '04년 도입후, '08년 ATM 범죄발생율이 1/3 수준으로 격감 | 손바닥<br>/손가락 정맥 |
| 기타<br>주요국가<br>(지문) | O 브라질, Banco do Brazil(*지문*), Bradesco S.A 은행(*정맥*)<br>- 연금운영비 절감을 위한 본인확인절차 적용중<br>- 바이오정보를 IC카드에 저장하여 ATM 거래에 활용하고 있음<br>O 인도, State Bank of India(*지문*) : ATM거래시 적용중<br>O 호주/뉴질랜드, 텔레뱅킹에 *음성*인식 활용중<br>O 미국, 중소형 금융기관에서 *지문*인식 활용중<br>O 한국, **대포통장근절을 위한 *바이오인식제품 도입확산(2016)*** | 지문,홍채,<br>정맥,음성<br>인식기술 |

2014.12, 금융위 대포통장 근절을 위한 공청회



## I 바이오인식분야 변천사 – Mobile Biometrics

### Concept of mobile Biometrics




### Products for mobile Biometrics

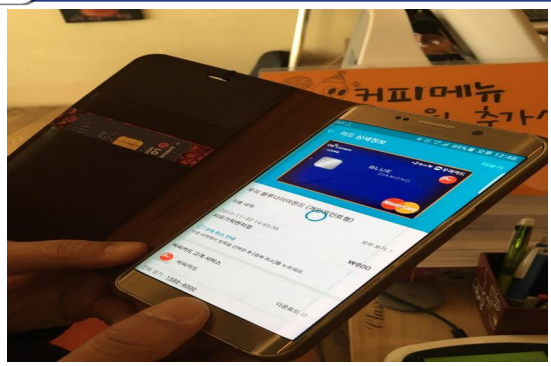
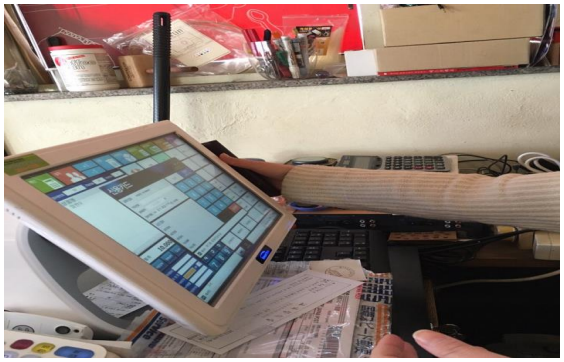
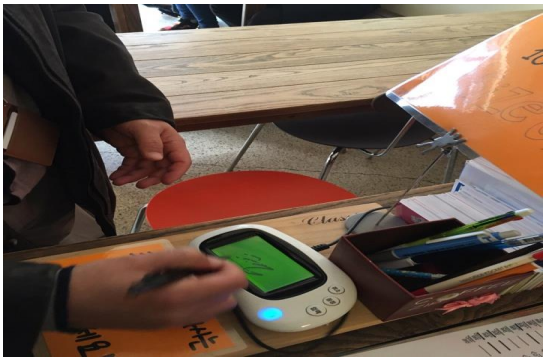
GOODE INTELLIGENCE
Mobile Phone Biometric Security 2011-2015

Table 14: Company Summary

| Company | Country | Biometric modality | Interviewee Name |
|---|---|---|---|
| Anakam, an Equifax Company | USA | Voice | Brent Williams – Chief Technology Officer |
| Animetrics Inc | USA | Face | Joel Breen – Vice President |
| Authentec | USA | Fingerprint | Brent Dietz, Director, Corporate Communications |
| Authentify | USA | Voice | John Zurawski, Vice President Sales and Marketing |
| Bio-Key | USA | Fingerprint | No Interview |
| Blue Planet Apps, Inc | USA | Iris, Face, Voice | Jason Braverman – Chief Executive Officer |
| 3M Cogent | USA | Face, Fingerprint, Palm, Iris | No Interview |
| Daon (IdentityX) | USA | Face, Palm, Voice | No Interview |
| L1 | USA | Face, Finger, Palm, Iris | No Interview |
| Mobbeel | Spain | Iris, Signature | No Interview |
| M2SYS | USA | Fingerprint, Finger vein, Palm vein, Iris | John Trader – Communications Specialist |
| Nuance Communications | USA | Voice | No Interview included for this section. Chuck Buffum interviewed for other sections. |
| Persay | Israel | Voice | No Interview |
| PhoneFactor | USA | Voice | Steve Dispensa – CTO |
| Precise Biometrics | Sweden | Fingerprint | No Interview |
| SecuriMobile | USA | Voice | No Interview |
| Transaction Security Inc | USA | Signature/Sign | Rod Beatson – President and CEO |
| Voice Commerce Group | UK | Voice | Nick Ogden – Chairman and CEO |
| VoiceVault | UK/USA | Voice | Nik Stanbridge, Director of Product Marketing |

Source: Copyright © Goode Intelligence 2011

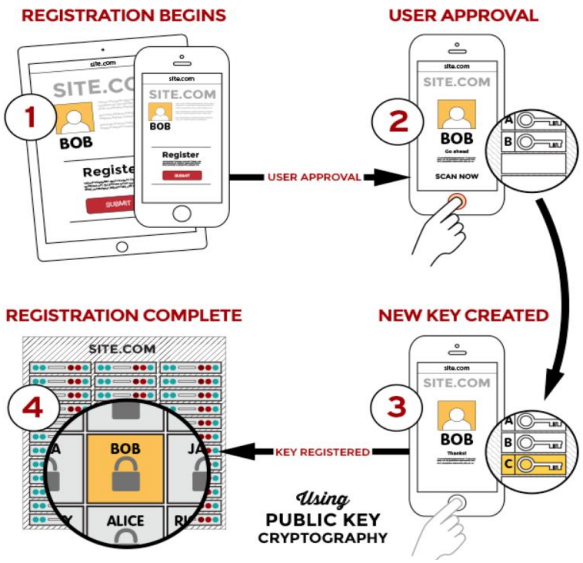
## I 바이오인식기술 변천사 및 국외동향 – e-Payment(삼성페이)

## I 바이오인식분야 변전사 – FIDO defacto STD

**FIDO Alliance**

HUAWEI, Alibaba Group, SAMSUNG, PayPal, LG Electronics, VISA, QUALCOMM, lenovo, Microsoft, MasterCard, RSA, Google



## I 바이오인식분야 변천사 – Medical Biometrics : biosignals

### ▶ MEDICAL(COGNITIVE WITHIN BEHAVIORAL BIOMETRICS) BIOMETRICS = 2 IN 1

- Doing 'medical biometrics' will waste processing source and time
  - Biometrics authentication processing
  - Medical biometrics processing
- Better way to do authentication and health monitoring at the same time is using bio-signals
  - Same features are used for both purposes
  - Suitable for daily/weekly application e.g. physical access to office

Authentication — ECG, EEG, ABR, EMG, Heart Sound

Continuous Health Monitoring — Heart, Brain, Muscle, Nerve, Ear

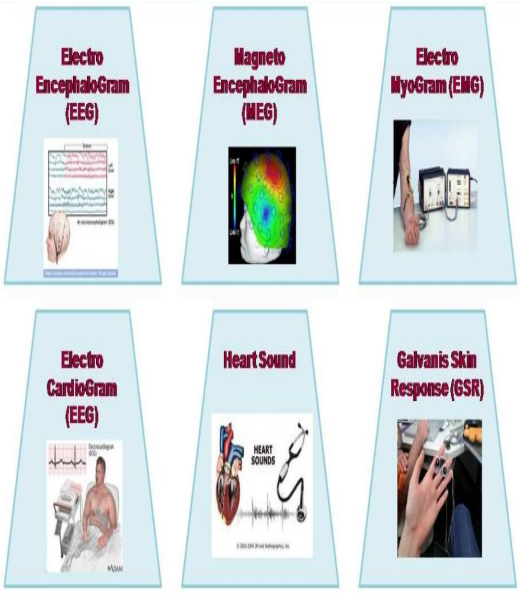
Alert if there is health problem



## I 바이오인식분야 변천사 – Medical Biometrics : biosignals

### ABC2011, Malaysia 공과대학

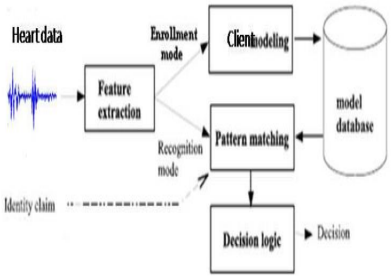
### TYPES OF BIO-SIGNAL

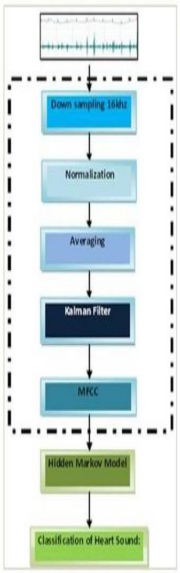



Others e.g. Electrooculography (EOG) – measurement of the resting potential of the retina.

## I 바이오인식분야 변천사 – Medical Biometrics : biosignals

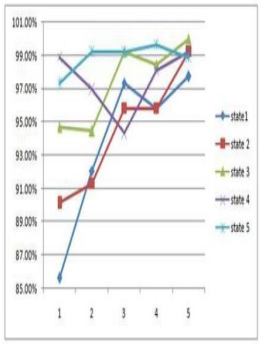
### ▶ HEART SOUND AS MEDICAL BIOMETRICS




- Welch-Allyn meditron electronic stethoscope
- Location : V1 (aortic)
- 5 normal vs. 5 abnormal
- Change number of HMM states and mixtures

| state/mix | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 85.61% | 90.15% | 94.70% | 98.86% | 97.35% |
| 2 | 92.05% | 91.29% | 94.45% | 96.97% | 99.24% |
| 4 | 97.35% | 95.83% | 99.24% | 94.32% | 99.24% |
| 8 | 95.83% | 95.83% | 98.48% | 98.11% | 99.62% |
| 16 | 97.73% | 99.24% | 100% | 99.24% | 98.86% |
| Average | 93.71% | 94.47% | 97.37% | 97.50% | 98.86% |



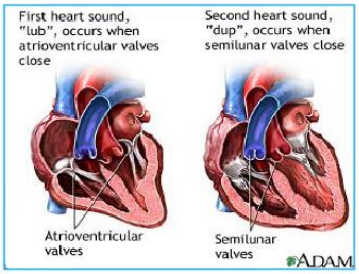

- Best combination : 3 state 16 mixtures

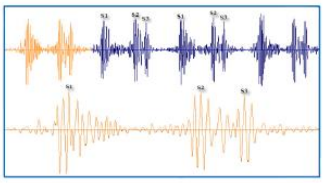
- We are only concentrate on medical application with our database
- Now we are moving into *biomedical biometrics*, so we just got preliminary results
- 20 clients vs more than 20 impostors

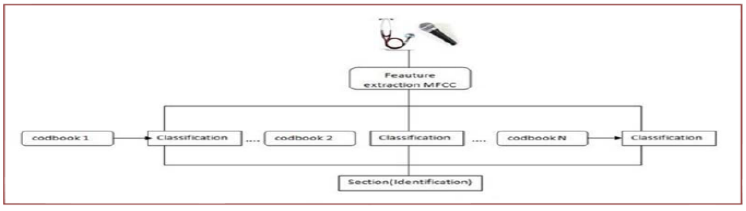


## I 바이오인식분야 변천사 – Medical Biometrics : biosignals

### ▶ HEART AND SPEECH SOUNDS AS MEDICAL BIOMETRICS






**Identification**

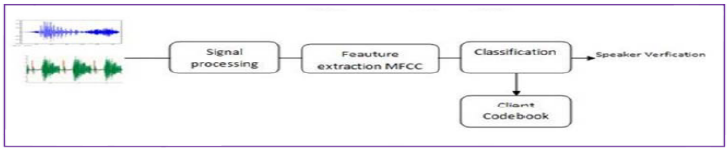
Are you really one of us?

1 : N authentication

**Verification**

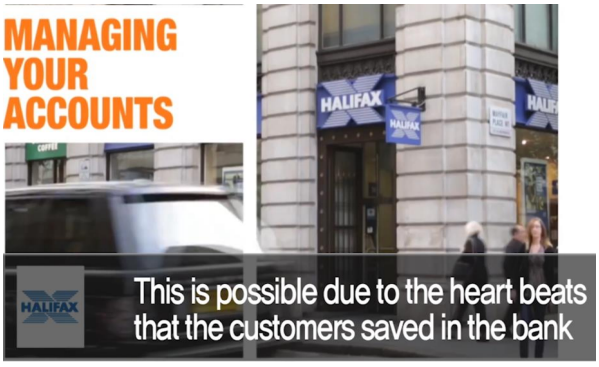
Seriously, you are him/her?

1 : 1 authentication

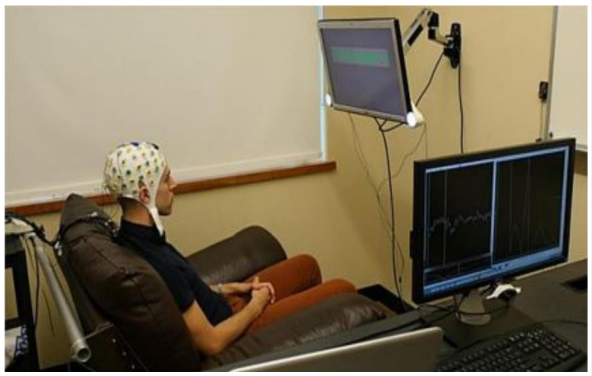


## I 바이오인식분야 변천사 – Telebiometrics using bio-signals

***Bank customers verification service using ECG (Halifax Bank of UK, Royal Bank of Canada)***




***Developing personal authentication technology using EEG(Univ. of Washington, USA)***

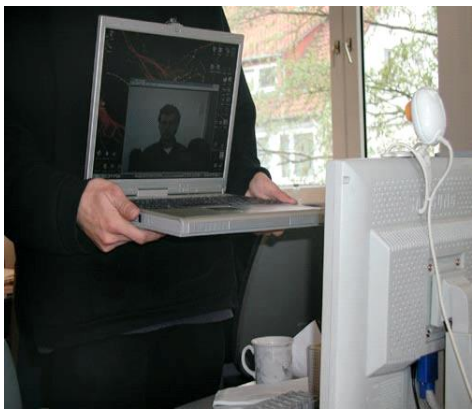


**위변조에 강인한 차세대 바이오인식기술로 뇌파(EEG), 심전도(ECG), 심박수(PPG) 등 생체신호를 이용한 텔레바이오인식기술 각광을 받고 있음**



## // 바이오인식분야 보안이슈 – Fake Biometrics

**"바이오정보(얼굴) 위조사례"**

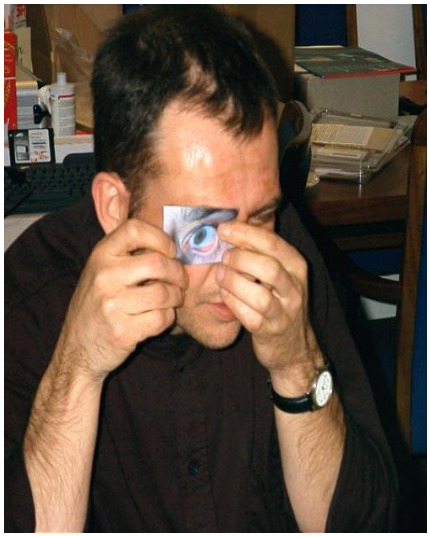


모니터 상의 얼굴 사진을
이용한 등록을 시도하는 예

얼굴을 통한 안면 인식 잠금 장치를
사진만으로 우회 할 수 있음을 시연

## 바이오인식분야 보안이슈 – Fake Biometrics

**"바이오정보(홍채) 위조사례"**



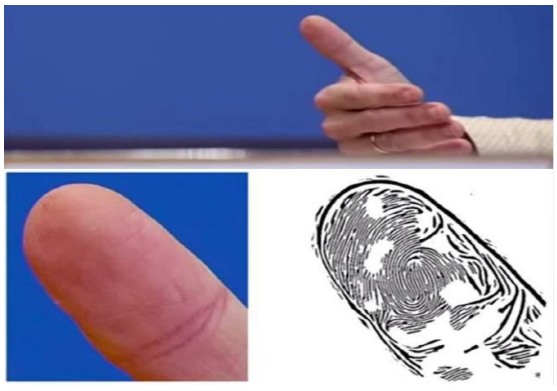
홍채 사진을 이용한
등록 시도

독일의 해커집단 '카오스 컴퓨터 클럽', 일명 CCC는 삼성전자 레이저프린터로 눈동자 사진을 뽑고 콘택트렌즈로 간단히 홍채 인식 보안을 뚫었습니다. 그 모습은 유튜브 동영상으로 올라왔습니다. 영상의 길이는 1분 17초로 딱 그 시간에 보안을 뚫었죠.



## 바이오인식분야 보안이슈 – Fake Biometrics

**"바이오정보(지문) 위조사례"**



독일 CCC는 독일국방장관을 3M 거리에서 촬영,
위조지문을 제작(2014년 CCC 컨퍼런스)

## 바이오인식분야 보안이슈 – Fake Biometrics

**"증가하는 위조 지문의 위협"**

● 위조 지문 제작 방법의 대중화

- 종이/실리콘 위조 지문 제작 방법을 Youtube에 공개
- Google, Youtube에 종이/실리콘/고무찰흙 위조 지문 제작 방법 수십 건 검색
- 일반인도 도장 제작 업체(고무), 의수 제작 업체(실리콘), 인쇄 업체(수지 제판) 통해 고품질 위조 지문을 별다른 제약 없이 제작 가능

● 위조 지문 공격 실제 사례

- http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000743616
- http://blog.naver.com/tbroadgg?Redirect=Log&logNo=117854858
- http://www.bbc.co.uk/news/world-latin-america-21756709

## 바이오인식분야 보안이슈 – Fake Biometrics

# 위조 바이오인식에 의한 공격 사례

▌독일 해킹그룹인 CCC는 스마트폰 지문인식기 해킹(2014)

← 동영상

## 바이오인식분야 보안이슈 – ITU-T X.1086 국제표준(2008.9)

### Biometric System & Attack Points (ITU-T SG17 Q9.Telebiometrcs, X.1086 by KISA)

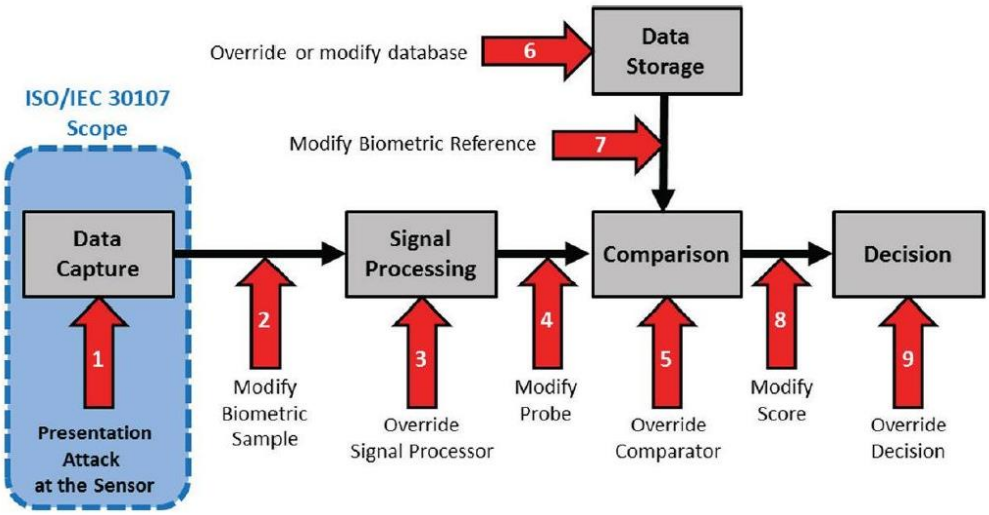



Figure 1 — Examples of points of attack in a biometric system (inspired by[1])



## 바이오인식분야 보안이슈 – ISO/IEC 30107 국제표준(2015.12)

### PAD, Biometrics presentation attack detection (ISO/IEC SC37 30107-1,-2,-3)

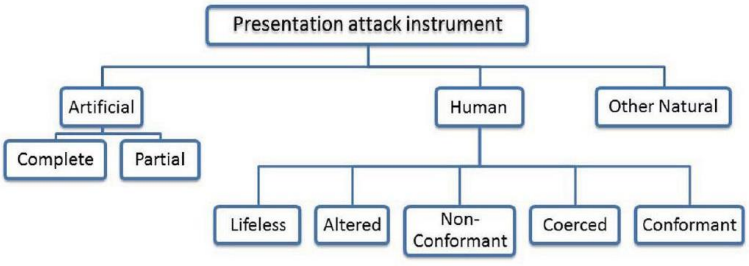



Figure 2 — Types of Presentation Attacks

Table 1 — Examples of Artificial and Human Presentation Attack Instruments

| | | |
|---|---|---|
| **Artificial** | *Complete* | gummy finger, video of face |
| | *Partial* | glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up |
| **Human** | *Lifeless* | cadaver part, severed finger/hand |
| | *Altered* | mutilation, surgical switching of fingerprints between hands and/or toes |
| | *Non-Conformant* | facial expression/extreme, tip or side of finger |
| | *Coerced*[<?>] | unconscious, under duress |
| | *Conformant* | zero effort impostor attempt |

## 바이오인식분야 보안이슈 – ISO/IEC 30107 국제표준(2015.12)

### PAD-part1, General Biometric Framework

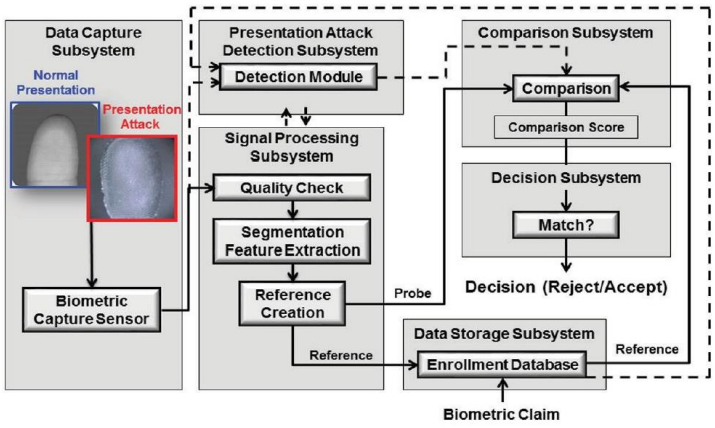



Figure 3 — A general biometric framework with presentation attack detection (other configurations are possible)

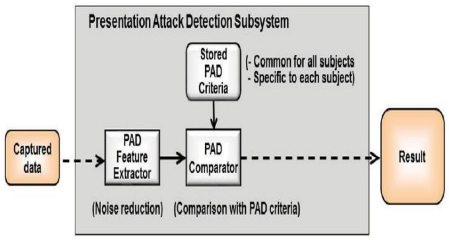



Figure 4 – Components in a general presentation attack detection subsystem



## 바이오인식분야 보안이슈 – ISO/IEC 30107 국제표준(2017.7)

### PAD-part2, Data Formats (CD2, developing)

**[Scope]**

센서에서 발생하는 공격에 대해 PAD 사용과 PAD 결과 제시를 위한 데이터 형식 정의

(PAD output & PAD input)

XML schema와 binary format 포괄 정의

### PAD-part3, Testing and Reporting (CD1, developing)

**[Scope]**

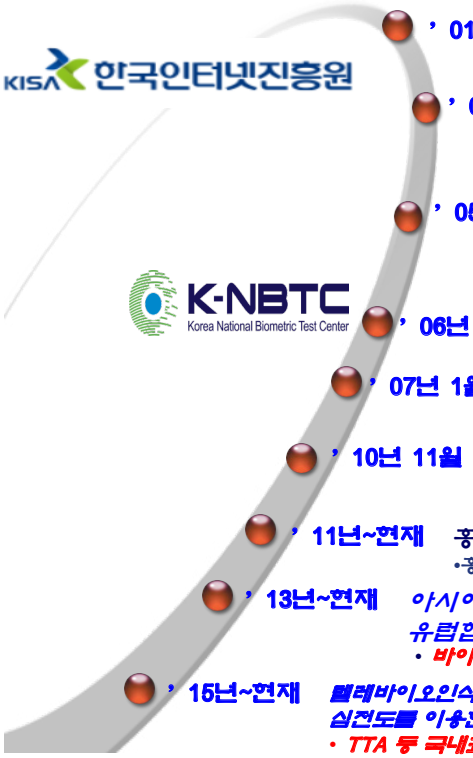
PAD 테스트 방법 정의

평가 결과와 보고서 출력 정의

Presentation attacks 분류

| Artefact species | Description | Illustration |
|---|---|---|
| Silicon finger artefact | Matte or glossy | |
| Laser print finger artefact | Ordinary 2D print out | |
| Gelatin finger artefact | Half-transparent gelatin with glycerin | |

## /// 바이오인식분야 KISA 대응현황 – 추진연혁



KISA 한국인터넷진흥원

- ' 01년 1월 — *정통부지원 한국바이오인식협의회(KBA) 발족*
- ' 02~04년 — 지문, 얼굴인식 DB 구축, R&D 과제수행
  - •지문(3,600명, 57만장)
  - •얼굴(2,020명, 82,680장)
- ' 05년 4월 — 정와대, 바이오인식 종합 인프라 구축계획(안)
  『바이오인식정보시험센터』 구축보고
  *생체정보보호 가이드라인 개발보급(2015.12, 정통부)*
- K-NBTC Korea National Biometric Test Center
- ' 06년 6월 — ***바이오인식정보시험센터(K-NBTC) 개소***
- ' 07년 1월 — ISO/IEC 바이오인식 호환규격 적합성 시험표준 완료
  *생체정보보호 가이드라인 개정(2007.12, 정통부)*
- ' 10년 11월 — 표준적합성 시험분야
  국제공인시험기관 인정(KOLAS) 획득
- ' 11년~현재 — 홍채, 정맥인식 DB 구축
  •홍채(20,400장), 정맥(61,200장)
- ' 13년~현재 — *아시아바이오인식협의회(ABC) 의장(KISA 김재성),*
  *유럽협의회(EAB)와 MoU 체결*
  • *바이오인식 정보보호 기술적/관리적 지침 (TTAK.KO-12.0034/R2, 2013.12)*
- ' 15년~현재 — ***블레바이오인식기술 표준개발과제 추진중*** *(2015.3~2018.2, 6.72억원),*
  ***심전도를 이용한 블레바이오인식 국제공동연구 추진중*** *(2016.6~2018.12, 14억원)*
  • *TTA 등 국내표준, ISO/IEC, SC37 ITU-T SG17 등 국제표준 개발 및 산업표준화 추진중*



## /// 바이오인식분야 KISA 대응현황 – PAD 시험(2007년)

### ■ KISA 위조지문 BMT 시험기준 (행자부 무인민원발급기, 2007.7월)

- 위조지문 종류 : 종이, 필름, 실리콘, 젤라틴, 고무
- 위조지문 BMT 시험방법
  - 제작된 위조지문을 지문인식 센서를 통해 이미지화
  - 실제지문(10명, 4대 발급기별 3회 스캔/발급 확인시험)
  - 4종 위조지문(흑백종이, OHP 필름, 실리콘, 젤라틴 제작) 각센서당 3회 모조지문 감별 확인
  - 피시험자(지문제공자, 연령 20~40대 남녀 총12명), 참관자(언론기자, 행자부 지자체 담당자)
- 검증 시나리오

| 시나리오 (Scenario) | 등록(Enrollment) | 인증(Authentication) |
|---|---|---|
| 실제 – 위조 | 실제 지문 | 위조 지문 |
| 위조 - 실제 | 위조 지문 | 실제 지문 |
| 위조 - 위조 | 위조 지문 | 위조 지문 |

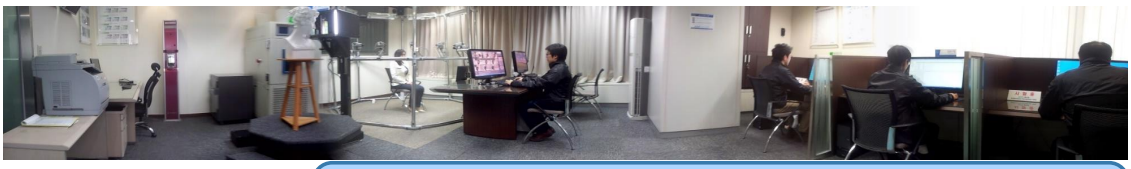
●위조지문 비공개 BMT 시험결과

- 실제지문의 경우, C社 지문인식기 성능저하(인증시도 7회) 확인
- 종이모조지문(A社 스캔오류), OHP필름(4개社 탐지), 실리콘(4개社 탐지), 젤라틴(3개社 실패)
- 2008년이후 1,564대 무인민원발급기에 위조지문 판별가능한 지문인식기로 전면 대체됨

## /// 바이오인식기술 관련 KISA 대응현황 – 시험인증서비스(2006년.6월)

고정형 바이오인식 성능 시험, 인증을 위해
KISA는 지문, 얼굴, 홍채, 정맥인식 성능시험용 DB를 구축해, 사용

〈KISA내 위치한 바이오인식정보시험센터 모습〉



〈KISA 연도별 바이오인식시스템 시험/인증 건수〉

| 구분 | '06 | '07 | '08 | '09 | '10 | '11 | '12 | '13 | '14 | '15 | '16 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 시험 | 3 | 4 | 5 | 4 | 5 | 4 | 9 | 12 | 13 | 13 | 31 |
| 인증 | 3 | 4 | 5 | 4 | 5 | 3 | 1 | 12 | 7 | 7 | 29 |
| 합계 | 6 | 8 | 10 | 8 | 10 | 7 | 10 | 24 | 20 | 20 | **60** |



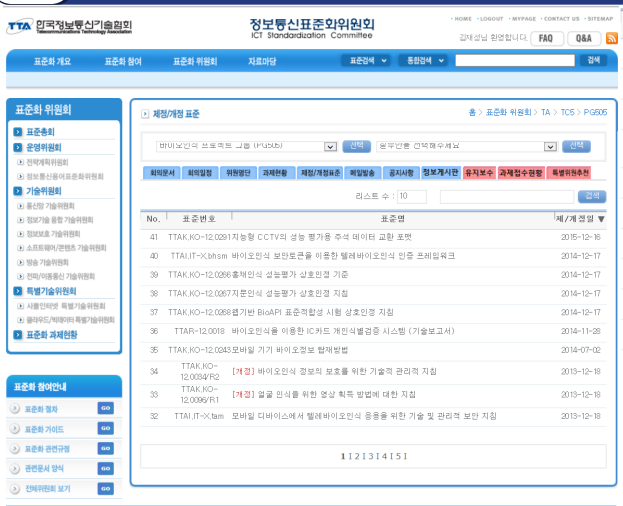
## /// 바이오인식분야 KISA 대응현황 – 국내외 표준화 선도기관

### ❖ KISA 바이오인식 국내외 표준화 선도

- **국내 표준화 활동** (TTA PG505 의장, KS 국가표준 심의위원)
  - ➢ *바이오인식 산학연 전문가그룹인 표준연구회를 운영, 산업표준 개발 및 보급(2015.5.~현재)*
  - ➢ *TTA PG505를 통해 단체표준, KS 국가표준 등 국내표준화 추진중*
  - ➢ *바이오정보 보호기술, 시험기술, 생체신호 인증기술 등 표준보급을 통해 국내산업 활성화*
    - ✓ *산업체, 정부 공공기관 등에 바이오인식제품에 대한 호환성, 안전신뢰성 보장에 기여*

- **국제표준화 활동** (ABC 아시아협의체 의장, ISO/IEC SC37, ITU-T SG17 국제표준 에디터)
  - ➢ *KISA 보유기술을 ISO/IEC, ITU-T, CJK 한중일 정보보호협의체 등에 국제표준을 개발하여 글로벌 표준기술 선도를 통해 관련산업 활성화 및 신규 시장창출에 기여*
    - ✓ *바이오인식기술 관련 미국, 유럽, 아시아 등 주요선진국과 국제공동연구 및 국제협력 채널제공*
  - ➢ *ISO/IEC SC37(시험기술), ITU-T SG17(텔레바이오인식 응용기술) 등을 통해 국제표준화 추진중*

## /// 바이오인식분야 KISA 대응현황 – 국내표준화 활동현황




| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 41 | TTAK.KO-12.0291 | 지능형 CCTV의 성능 평가용 주석 데이터 교환 포맷 | 2015-12-16 |
| 40 | TTAI.IT-X.bhsm | 바이오인식 보안토큰을 이용한 웰레바이오인식 인증 프레임워크 | 2014-12-17 |
| 39 | TTAK.KO-12.0266 | 홍채인식 성능평가 상호인정 기준 | 2014-12-17 |
| 38 | TTAK.KO-12.0267 | 지문인식 성능평가 상호인정 지침 | 2014-12-17 |
| 37 | TTAK.KO-12.0268 | 웹기반 BioAPI 표준적합성 시험 상호인정 지침 | 2014-12-17 |
| 36 | TTAR-12.0018 | 바이오인식을 이용한 IC카드 개인식별검증 시스템 (기술보고서) | 2014-11-28 |
| 35 | TTAK.KO-12.0343 | 모바일 기기 바이오정보 탑재방법 | 2014-07-02 |
| 34 | TTAK.KO-12.0034/R2 TTAK.KO-12.0096/R1 | [개정] 바이오인식 정보의 보호를 위한 기술적 관리적 지침 | 2013-12-18 |
| 33 | | [개정] 얼굴 인식을 위한 영상 획득 방법에 대한 지침 | 2013-12-18 |
| 32 | TTAI.IT-X.bam | 모바일 디바이스에서 웰레바이오인식 응용을 위한 기술 및 관리적 보안 지침 | 2013-12-18 |

| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 31 | TTAK.IT-X. 1092 | [개정] 바이오인식 기반 원격 의료 통합 프레임워크 | 2013-12-18 |
| 30 | TTAK.KO-12.0215 | 원거리 얼굴인식을 위한 영상 품질 객체 검출 및 인식 성능평가 지침 | 2012-12-21 |
| 29 | TTAK.KO-12.0216 | 영상감시 시스템에서의 개인 영상 정보보호 지침 | 2012-12-21 |
| 28 | TTAK.KO-12.0207 | 네트워크 영상 감시 시스템에서 증거 영상 수집을 위한 지침 | 2012-12-21 |
| 27 | TTAR-12.0012 | 원거리 얼굴인식을 위한 영상 품질 요구 사항(기술보고서) | 2012-12-13 |
| 26 | TTAR-12.0013 | 원거리 사람 검출 및 인식을 위한 테스트 데이터베이스 요구 사항(기술보고서) | 2012-12-13 |
| 25 | TTAK.KO-12.0187 | 지문 라이브스캐너 품질평가 기준 | 2011-12-21 |
| 24 | TTAK.KO-12.0186 | 바이오인식 정보 보호를 위한 워터마킹 기법 | 2011-12-21 |
| 23 | TTAK.KO-12.0117/R2 | [개정] 영상 보안 시스템들 간의 상호 연동을 위한 인터페이스 | 2011-12-21 |
| 22 | TTAR-12.0009 | 지문 데이터베이스의 난이도 특성화 및 측정 (기술보고서) | 2011-12-02 |

| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 21 | TTAK.KO-12.0165 | 바이오 보안 토큰용 API | 2011-06-29 |
| 20 | TTAK.KO-12.0160 | 바이오 인식 정보 및 개인 식별 정보 데이터베이스의 분리 운영 방법 | 2010-12-23 |
| 19 | TTAK.KO-12.0159 | 얼굴 영역 검출을 이용한 CCTV 영상 정보 프라이버시 보호를 위한 보안 요구 사항 | 2010-12-23 |
| 18 | TTAK.KO-12.0048/R1 | [개정] 바이오인식 용어 | 2010-12-23 |
| 17 | TTAK.KO-12.0158 | 얼굴 인식 시스템 시나리오 기반 성능 시험 방법 | 2010-12-23 |
| 16 | TTAR-12.0005 | 영상 감시 시스템에서의 객체 추적 및 이동궤적 분석 (기술보고서) | 2010-11-24 |
| 15 | TTAR-12.0006 | 위조지문 탐지 기술 (기술 보고서) | 2010-11-24 |
| 14 | TTAK.KO-12.0127 | 현금자동입출금기에서의 사용자 영상 저장 방법 | 2009-12-22 |
| 13 | TTAE.IT-X.1084 | 통신상에서의 바이오기반 시스템 인증 메커니즘 | 2009-12-22 |
| 12 | TTAK.KO-12.0126 | 개인 식별정보 및 바이오 인식 정보 보호를 위한 저장 및 전송 포맷 | 2009-12-22 |

| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 11 | TTAK.KO-12.0125 | 지문인식 알고리즘 성능 시험 지침 | 2009-12-22 |
| 10 | TTAK.KO-12.0124 | 얼굴 영상 획득 시스템의 보안 요구 사항 | 2009-12-22 |
| 9 | TTAR-12.0004 | 지문인식 시스템의 안전성 확보를 위한 지문입력기의 취약점 분석 | 2009-11-24 |
| 8 | TTAK.KO-12.0097 | 스마트카드 기반의 지경맥 인증 방법론 | 2008-12-19 |
| 7 | TTAK.IT-X.1088 | 바이오 인식 정보에 기반한 전자서명 키생성 프레임워크 | 2008-12-19 |
| 6 | TTAK.KO-12.0098 | One-Time 템플릿 기반의 바이오 인증 프레임워크 | 2008-12-19 |
| 5 | TTAK.KO-12.0095 | 얼굴 인식 알고리즘 성능 시험 방법 | 2008-12-19 |
| 4 | TTAS.KO-12.0050 | 네트워크 환경에서의 다중 바이오정보 보호 가이드라인 | 2007-06-22 |
| 3 | TTAS.KO-12.0047 | 온라인 인증 시스템을 위한 지문 센서 인터페이스 | 2006-12-27 |
| 2 | TTAS.KO-12.0046 | 지문 영상 품질 분류 방법 | 2006-12-27 |

| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 1 | TTAS.OT-10.0001 | BioAPI 표준적합성 시험방법 및 절차(K-CTS) | 2004-12-23 |



## /// 바이오인식분야 KISA 대응현황 – 국제표준화 활동현황

*(ISO/IEC JTC1)*

- 2002.12월 부터, SC37(Biometrics)의 WG2(인터페이스), WG5(시험평가) 분과에서 바이오인식 원천기술에 대한 표준화 활동중
- 2005.12월 부터, SC27(Security) WG5 분과에서 바이오정보 보호기술 표준화

o KISA ISO/IEC 국제표준 개발현황(2013년 ~ 현재)

| 순번 | 표준명 (표준번호/과제번호) | 주요내용 (현재단계) | 제개정일 (완료예정일) | 경제적/기술적 파급효과 |
|---|---|---|---|---|
| 1 | Conformance testing for BioAPI – Part 1: Methods and procedures ( ISO/IEC 24709-1Rev1 ) | 생체인식 호환규격(BioAPI) 적합성 시험기술 개정 (JTC1 SC37 IS 단계) | 2017.1월 개정완료 | 전세계 전자여권 등 바이오인식제품의 호환성·신뢰성 보장 |
| 2 | Object oriented BioAPI – Part 1: Architecture – Amendment 1: Additional specifications and conformance statements ( ISO/IEC 30106-1AMD1 ) | 객체지향형 BioAPI 적합성 시험방법 (JTC1 SC37 CD 단계) | 2018.8월 제정 | 전세계 모바일 바이오인식제품의 호환성·신뢰성 보장 |
| 4 | Object oriented BioAPI – Part 4: C++ implementation ( ISO/IEC 30106-4 ) | 객체지향형 BioAPI 호환규격 (JTC1 SC37 WD1 단계) | 2019.1월 제정 | 전세계 모바일 바이오인식제품의 호환성·신뢰성 보장 |
| 5 | Telebiometric authentication framework using biometric hardware security module ( ISO/IEC 17922 I X.1085 ) | 바이오인식기반의 하드웨어 보안토큰 인증기술 (JTC1 SC27 IS 단계) | 2017.3월 제정 | 바이오인식을 이용한 공인인증서(PKI) 소유자 신원확인으로 인증시장 창출 |

## /// 바이오인식분야 KISA 대응현황 – 국제표준화 활동현황

*(ITU-T SG17)*

▸ 2005년 4월 부터, ITU-T SG17 Q9(*Telebiometrics*) 분과에서 텔레바이오인식 응용기술에 대한 표준화 활동중

o KISA ITU 국제표준 개발현황(2013년 ~ 현재)

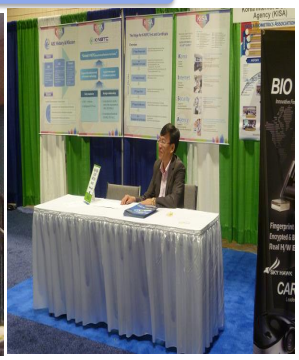
| 순번 | 표준명 (표준번호/과제번호) | 주요내용 | 제개정일 (완료예정일) | 경제적/기술적 파급효과 |
|---|---|---|---|---|
| 1 | *Integrated framework for telebiometric data protection in e-health and worldwide telemedicine ( X.1092 )* | 원격의료분야에서 텔레바이오정보 보안대책 | *2013.9월 제정완료* | 원격의료서비스에서 생체인식기술을 이용한 의료진(의사, 간호사, 보험관계자)에 대한 신원확인서비스 |
| 2 | *Telebiometric authentication framework using biometric hardware security module ( ISO/IEC 17922 I X.1085 )* | 바이오인식기반의 하드웨어 보안토큰 인증기술 | *2016.10월 제정* | 생체인식을 이용한 공인인증서(PKI) 소유자 신원확인으로 인증시장 창출 |
| 3 | *Technical and operational countermeasure for telebiometric applications using mobile devices ( X.1087 )* | 모바일기기에서의 텔레바이오정보에 대한 기술적·관리적 보안대책 | *2016.10월 제정* | 스마트폰 등 모바일기기에서 생체인식기술에 대한 보안대책 제시로 모바일 생체인식제품의 안전신뢰성 보장 |
| 4 | *Telebiometric Authentication using Bio-signals ( X.tab )* | 생체신호를 이용한 텔레바이오인식 인증기술 | *2019.9월 제정* | 위변조에 강인한 차세대 바이오인식기술로 신규시장창출 및 **세계최초로 개발** |



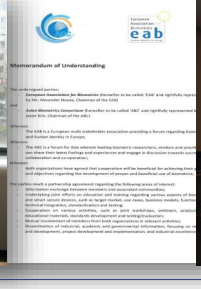
## /// 바이오인식분야 KISA 대응현황 – 국제협력 활동

**ABC2012** ('12.11, 제주)

**BBC2013** ('13.9, 미국 템파)



**MOU with EAB** ('13.2, 브뤼셀)




**ITU-T SG17** ('17.3, 스위스), **ISO/IEC SC37** ('17.1, 호주)

# Ⅳ 다중 생체신호 인증플랫폼 개발 – 국제공동연구(스페인, 미국)

## 심전도를 이용한 텔레바이오인식 인증기술개발

- Development of Telebiometric Authentication Technologies using ECG (ElectoCardioGram)
- 과제성격 : 표준화연계, 기술료징수, 기술사업화 활동기간 적용

### 주관기관 / 총괄책임자, 참여기관 / 총괄책임자

- 주관기관: *한국인터넷진흥원 / 공학박사 김재성 연구위원*
- 참여기관: *스페인 Univ.Carlos-III Madrid / Prof. Raul Sanchez-Reillo (ISO/IEC SC37 WG2 Secretariat)*
- 참여기관: *미국 Telebiometrics / CEO John Caras (ITU-T SG17 Q9 Rapporteur)*
- 참여기관: *한국 유파인스 / 강세진 대표이사 ( 생체신호센서용 웨어러블 디바이스 시제품 개발)*

### 사업기간

- 총사업기간: 2016. 06. 01 ~ 2018. 12. 31 (31개월)
- 당해년도 사업기간: 2018. 01. 01 ~ 2018. 12. 31 (2차년도)

### 사업비

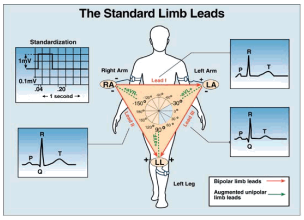
| 구 분 | | 1차년도 | 2차년도 | 3차년도 | 계 |
|---|---|---|---|---|---|
| 정부출연금 | | 400,000천원 | 400,000천원 | 500,000천원 | 1,300,000천원 |
| 민간 부담금 | 현금 | - | - | - | - |
| | 현물 | 73,000천원 | 146,000천원 | 146,000천원 | 365,000천원 |
| **합계** | | **473,000천원** | **546,000천원** | **646,000천원** | **1,665,000천원** |

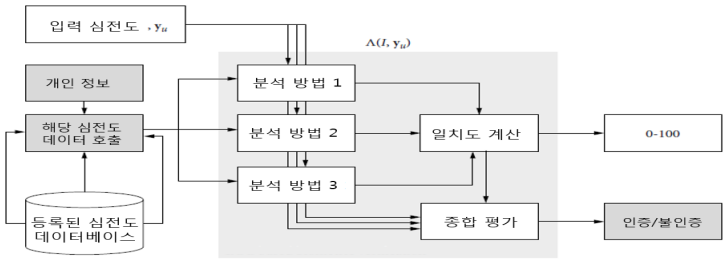
- 참여인력: 총 30명(7.75M/Y), 당해 연도 10명(1.55M/Y)



# Ⅳ 다중 생체신호 인증플랫폼 개발 – 국제공동연구(스페인, 미국)

## ▶ MILESTONES





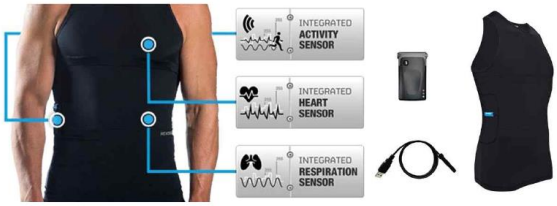

심전도 기반 생체 인증 구조

## IV 다중 생체신호 인증플랫폼 개발 – 웨어러블 디바이스

Lifetouch

AmpStrip

OmegaWave ECG Sensor




HexoSkin

Alive Bluetooth Heart & Activity Monitor

AliveCor Mobile ECG



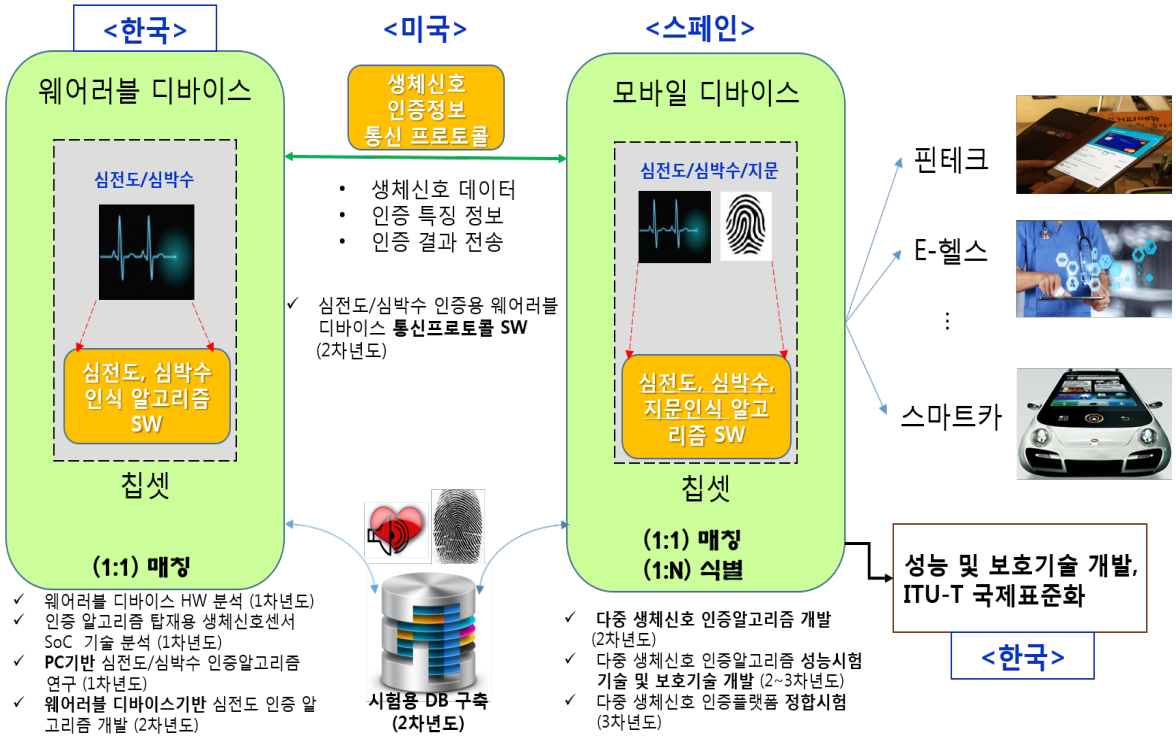
## IV 다중 생체신호 인증플랫폼 개발 – 웨어러블 디바이스

| | Accessary | | Clothing | Body attached/bio-transplanting | |
|---|---|---|---|---|---|
| | Band | watch | | | |
| Portability | ◎ | ◎ | ◎ | △ | |
| Low Power | ◎ | ○ | ◎ | △ | |
| Convenience | ◎ | ◎ | △/○ | △ | |
| Commodity | ○ | ◎ | △ | △ | |
| Competitive Price | ◎ | ○ | ○ | △ | |
| Marketability | ○ | ◎ | △ | △ | |

**Accessary Type, Especially Band Type(watch function) is more suitable for our target wearable device.** (ECG+ PPG + extra features)

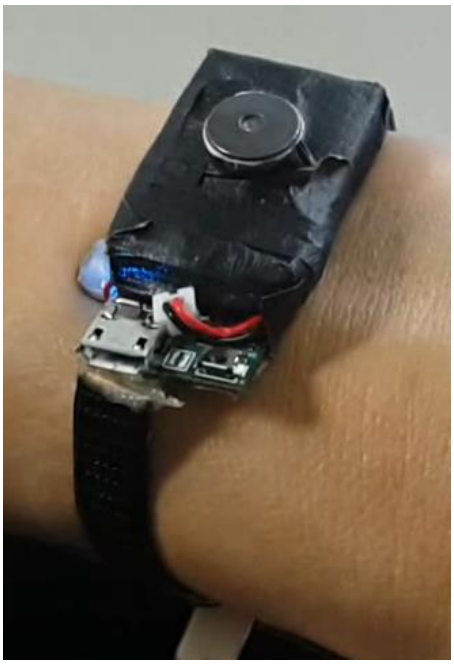
❖ 편의성, 정확성, 시장성, 안전성을 고려, 웨어러블 디바이스를 스마트 밴드형으로 개발 (2017년)

## IV 다중 생체신호 인증플랫폼 개발 – 국제공동연구(스페인, 미국)






## IV 다중 생체신호 인증플랫폼 개발 – 생체신호센서용 스마트밴드(유파인스 & KISA)

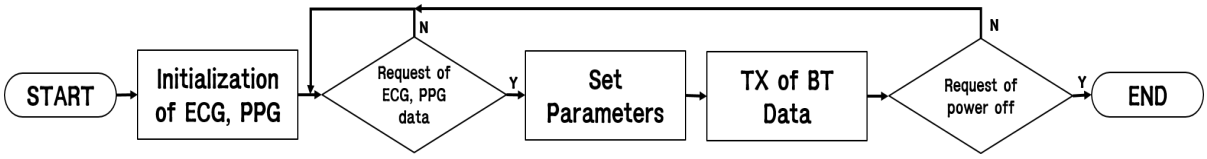


Smart-band wearable device for ECG & PPG bio-signals :

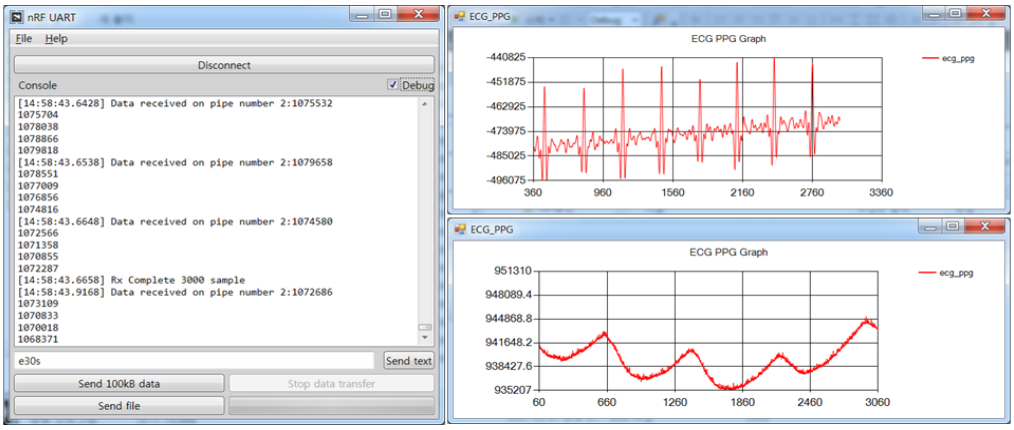
- TI AFE ADS1291(ECG) + TI AFE (PPG), individual chip
- Atmel 32bit ARM Coretex-M4 RISC based MCU or more high performance CPU (not decided yet)
- Built-in Flash Memory
- Two electrodes ( Lead I method)
- Nordic Bluetooth Smart SoC( nRF51822),
- Motion Sensor, Gyro Sensor, button, LED
- Chargeable battery
- LCD display (optional)

## IV 다중 생체신호 인증플랫폼 개발 – 생체신호센서용 스마트밴드(유파인스 & KISA)

### ❖ Firmware Flow Chart



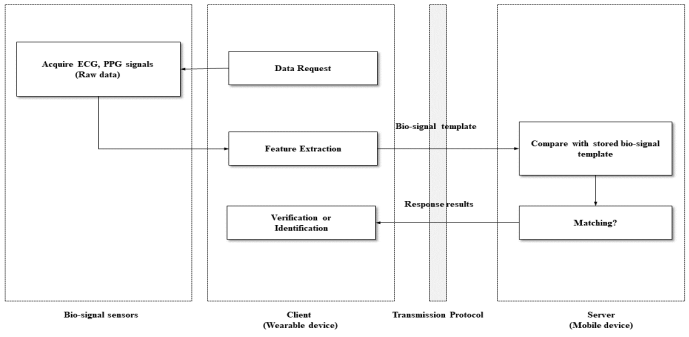

### ❖ Display SW for measured ECG, PPG Signals (check optimal sensing time for authentication)

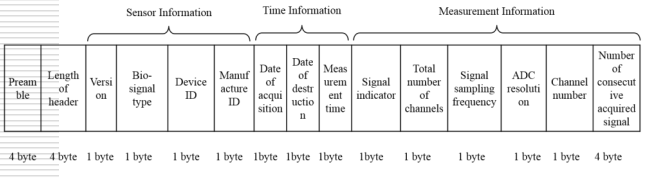





## IV 다중 생체신호 인증플랫폼 개발 – 통신프포토콜 (미국 Telebiometrics & KISA)

### ❖ Protocol Requirements

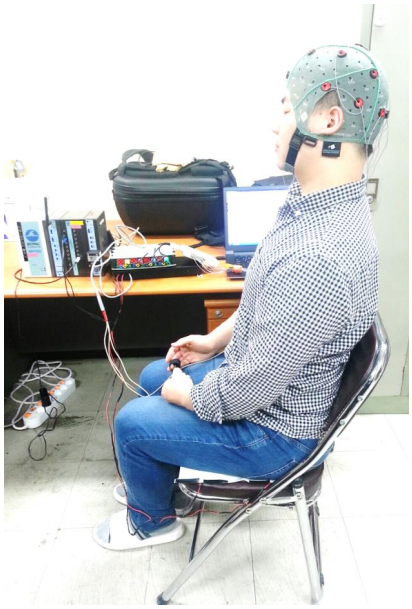


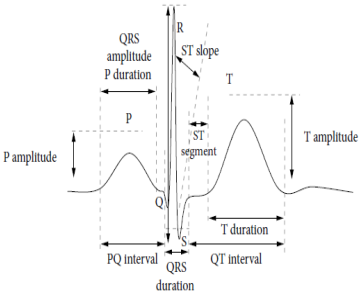




**Goals of the Communication Protocol:**

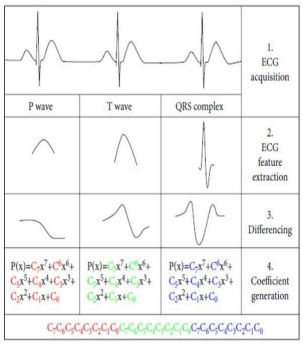
1. **Data Sequencing** – to detect loss or duplicate packets.
2. **Data Routing** – to find the most efficient path between source and a destination.
3. **Data Formatting** – defines a group of bits within a packet which constitutes data, control, addressing and other information.
4. **Flow Control** – ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.
5. **Error Control** – detect errors in messages. Method for correcting errors is to retransmit the erroneous message block.
6. **Precedence and order of transmission** – condition all nodes about when to transmit their data and when to receive data from other notes to use the communication channel.
7. **Connection** Establishment and termination.
8. **Data security** – prevents access of data by unauthorized users.

## IV 다중 생체신호 인증플랫폼 개발 – 생체신호 인증기술 연구






심전도 파형에서 사용 가능한 특징점




심전도 파형의 다항식 근사화 계수를 이용한 특징벡터

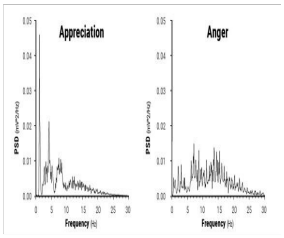
| | 심전도 (ECG) | 심박수(광용적맥파) (PPG) |
|---|---|---|
| 신호 샘플링 주파수 | 256Hz | 128Hz |
| 디지털 변환 해상도 | >10bit | >10bit |
| 주파수 성분 대역폭 | 0.5~35Hz | 1~5Hz |



## IV 다중 생체신호 인증플랫폼 개발– 생체신호 인증기술 연구

### 생체신호 DB 수집 대상분석

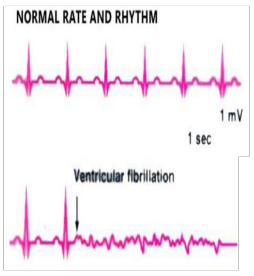
- Abnormal(10%), Normal(90%) DB 구축
- 나이, 성별, 국가별 정보수집
- 정상인 – 다양한 조건에서 시행 (신체, 감정 등 상태변화, 측정일수)




감정에 따른 ECG 스펙트럼 변화 (HeartMath Institute, 12명 평균)

### 신체 상태

- 운동/휴식
- 자세 (standing/sitting)
- 눈 개폐 (open eyes/closed eyes)




정상인과 환자(심방세동)의 심전도 파형 비교

### 감정상태

- 긴장(집중)/이완
- 기쁨/슬픔/분노/공포

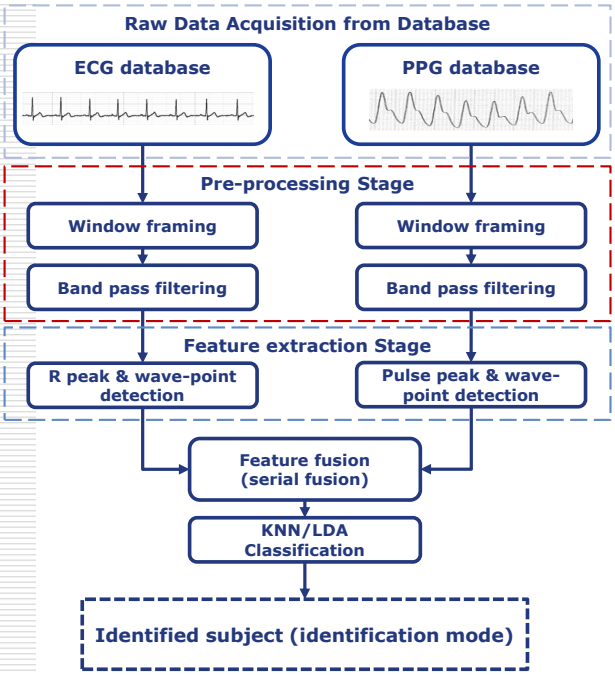
### 생체신호 측정방법

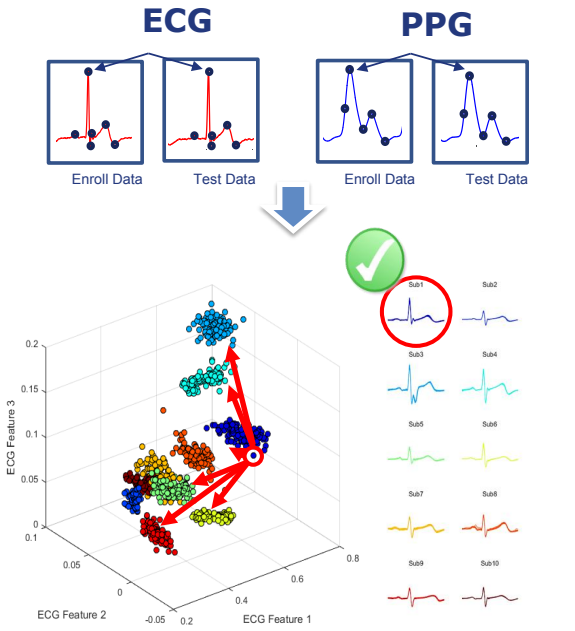
- 뇌파: 16채널 10-20 system 기반 표준 EEG 측정
- 심전도: 표준 LEAD I 방식으로 표준 ECG 측정
- 심박수(광용적맥파): 상용장비 이용 표준 PPG 측정
- 양손 지문: 상용 장비를 이용한 표준 지문영상 측정

### 웨어러블 디바이스를 이용한 생체신호 수집

- 악세사리형(스마트밴드, 스마트워치), 의류형, 신체부착형 생체신호센서 이용
- 광학식 지문인식센서를 이용

## IV 다중 생체신호 인증플랫폼 개발- 생체신호 인증메커니즘 개발




***CLOSEST Distance = MOST Reliable ID***

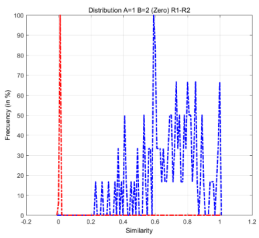


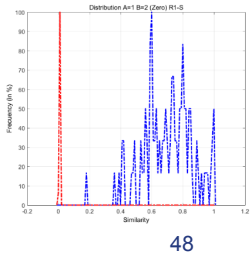
## IV 다중 생체신호 인증플랫폼 개발- 다중 생체신호 인증메커니즘(스페인 UC3M, KISA)

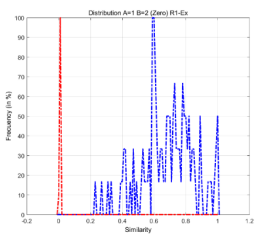
❖ ECG-Fingerprint Fusion

$$score_{global} = A * score_{ECG} + B * score_{fingerprint}$$

| ECG sample | A | B | EER |
|---|---|---|---|
| Sitting | 1 | 1 | 0.119% |
| Standing | 1 | 1 | 0.092% |
| Exercise | 1 | 1 | 0.137% |
| Sitting | 2 | 1 | 0.128% |
| Standing | 2 | 1 | 0.101% |
| Exercise | 2 | 1 | 0.147% |
| Sitting | 1 | 2 | 0.101% |
| Standing | 1 | 2 | 0.064% |
| Exercise | 1 | 2 | 0.128% |

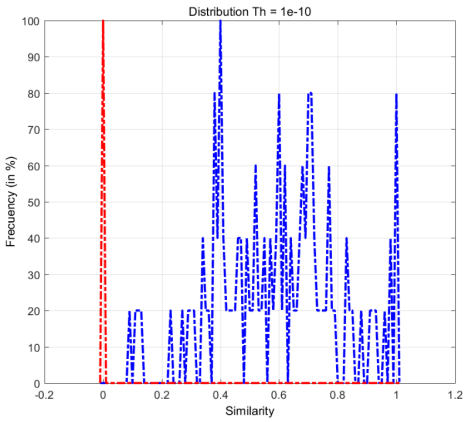


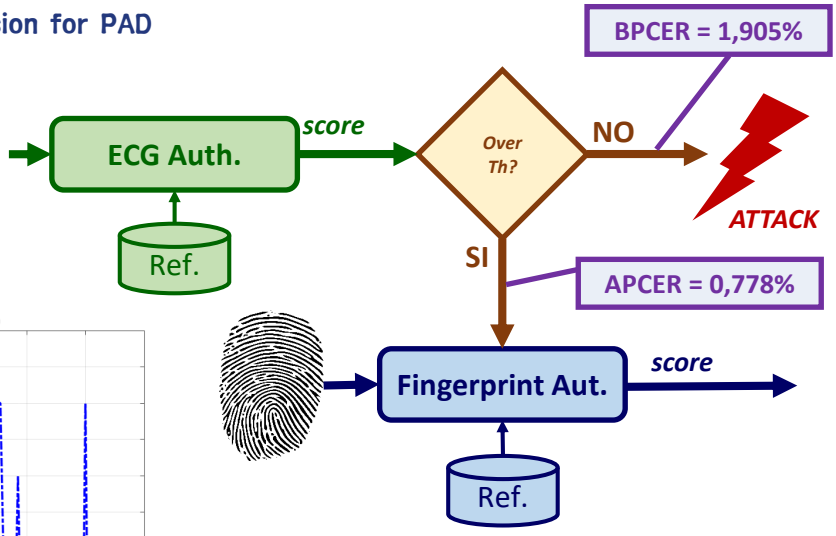




## IV 다중 생체신호 인증플랫폼 개발– 다중 생체신호 인증메커니즘(스페인 UC3M, KISA)

❖ ECG-Fingerprint Fusion for PAD

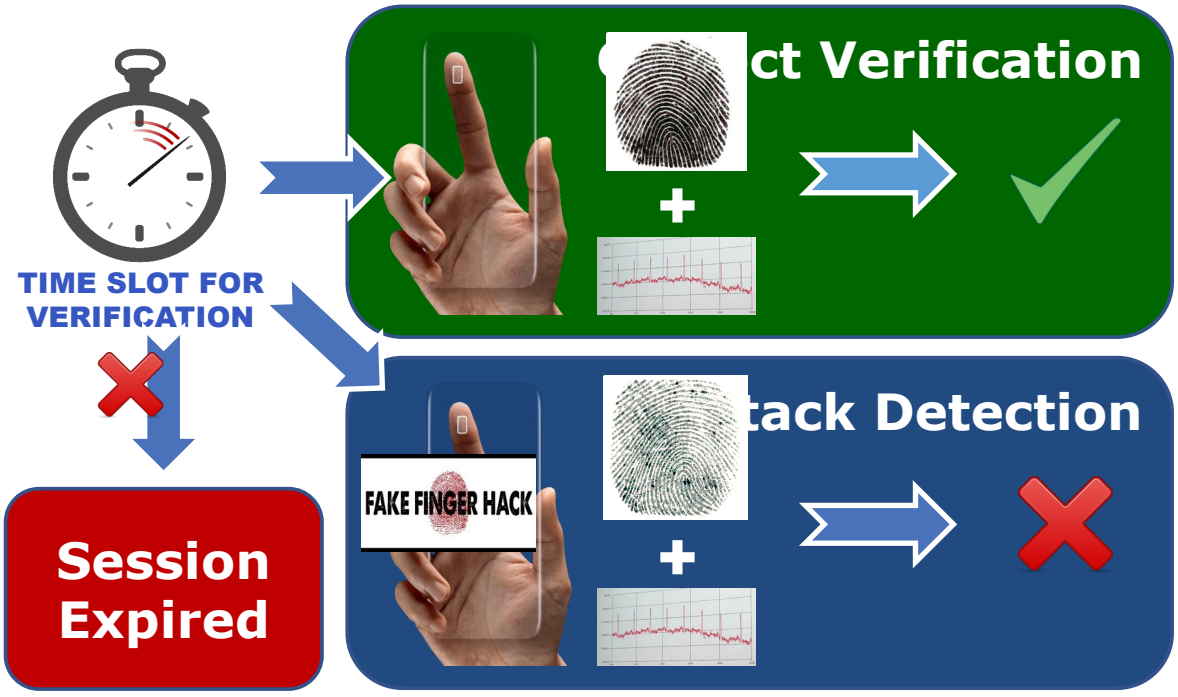





## IV 다중 생체신호 인증플랫폼 개발– 다중 생체신호 인증메커니즘(스페인 UC3M, KISA)

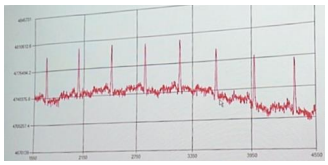
❖ Multi-biometric authentication (멀티모달로 인한 기능개선 사항추가)

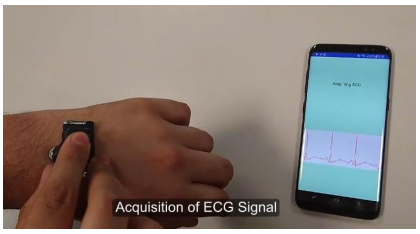


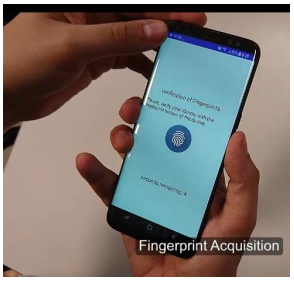
# IV 다중 생체신호 인증플랫폼 개발– 다중 생체신호 인증메커니즘(스페인 UC3M, KISA)

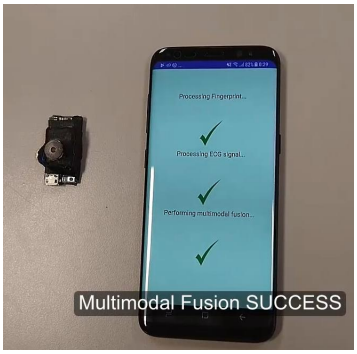
## ❖ Multi-biometric Authentication

Verification








# IV 다중 생체신호 인증플랫폼 개발– 언론홍보

**디지털타임스** 뉴스인쇄

기사 주소: http://www.dt.co.kr/contents.html?article_no=2017071702100351041001

### 뇌파·심전도로 본인인증 '텔레바이오인식' 상용화 속도

이경탁 기자 ki87@dt.co.kr | 입력: 2017-07-16 18:00

뇌파·심전도 등 생체신호 이용
지문·홍채보다 위·변조 어려워
알콜 마약 중독자 DB 추가 구축
KISA, 내년말 민간에 기술 이전

최근 지문·홍채 등 생체인식 기술이 확산하는 가운데 이보다 진화한 '텔레바이오인식(Telebiometrics)' 기술도 상용화에 속도를 내고 있다. 국내에선 한국인터넷진흥원이 내년 말까지 기술개발을 완료해 민간으로 기술을 이전, 상용화할 계획이다.

16일 한국인터넷진흥원(KISA)에 따르면 KISA는 서울대학교 의과대학과 함께 올해까지 200명(90% 일반인, 알콜 마약 중독자 등 환자 10%)에 대한 뇌파, 심전도 등을 테스트해 데이터베이스(DB)를 구축할 계획이다.

KISA와 서울대는 앞서 지난해 100명(일반인)에 대한 DB 구축을 완료했다. 그러나 뇌파와 심전도는 사람의 감성이나 알코올, 마약 등에 의해 달라질 수 있어 정확성을 높이기 위해 대량 테스트 DB를 통한 정교화된 알고리즘 개발에 나설 계획이다.

텔레바이오인식은 뇌파·심전도 등 생체 신호를 이용한 차세대 생체인식 기술이다. 뇌파, 심전도의 생체 신호는 전기신호로 감지되는 만큼 지문·얼굴·홍채·정맥 등 기존 생체정보에 비해 위·변조 공격이 상대적으로 어렵다는 게 전문가들의 설명이다.

최근 이슈로 떠오른 핀테크·스마트의료·웨어러블기기 등 ICT 융합서비스의 안전성을 높일 수 있을 것으로 KISA 측은 보고 있다.

실제 지난 5월 삼성전자 스마트폰 갤럭시S8에 탑재된 홍채인식 기능이 특일의 해킹그룹 '카오스 컴퓨터 클럽(CCC)'에 뚫렸다. 눈 부위를 확대한 사진을 프린터로 출력해 사진 위에 콘택트렌즈를 올려놓고 갤럭시S8 카메라 렌즈 앞에 대 홍채인식 잠금장치를 해제한 것. 또 목공용 본드를 이용해 지문을 위조하는 간단한 방법까지 인터넷에 떠돌고 있다. 생체정보는 한번 유출되면 재변경이 불가능하기 때문에 사용자들은 지속적으로 심각한 피해를 입을 수 있다.

김재성 KISA 정보보호R&D기술공유센터 보안기술확산팀 연구위원은 "모바일을 통해 생체인식 기술이 확산·보급되고 있지만, 지능화되는 해킹과 공격기법에 쉽게 노출될 우려가 있어 텔레바이오인식이 주목받고 있다"면서 "글로벌 표준화를 위해 미국, 스페인 등 세계 여러 기관 및 전문가그룹과 긴밀한 협력 체계를 구축하고 있다"고 밝혔다.

이어 김 연구위원은 "영국과 캐나다 은행권에선 이미 관련 시범 서비스를 진행 중인데, 심전도나 뇌파 신호는 음주 여부 같은 상황에 따라 인식 정확도가 떨어질 수 있는 만큼 인터넷진흥원은 기존의

http://www.dt.co.kr/etc/article_print.html?article_no=2017071702100351041001 2017-08-22

디지털시대 경제신문 디지털타임스 2의 2페이지

지문 등 전통적 생체인식과 결합하는 기술을 개발하는 것"이라고 전했다.

한편 KISA는 오는 9월 27일과 28일 부산에서 개최하는 국제전기통신연합(ITU-T) ABC2017 국제회의에 참석해 텔레바이오를 활용한 플랫폼을 설명할 계획이다.

이경탁기자 ki87@

[Herald Interview] KISA to unveil bio authentication for mobile banking in 2018-프... 1의 3페이지

The Korea Herald

[Herald Interview] KISA to unveil bio authentication for mobile banking in 2018

2017-06-12 13:46

The state-run Korea Internet & Security Agency is developing bio authentication for mobile banking to commercialize it by late 2018, KISA's chief researcher said.

"We are developing an algorithm for authenticating mobile banking with a combination of a fingerprint, heart rate and electrocardiogram. The technology is expected to be much safer than existing biometrics including iris sensor, fingerprint scanner and facial recognition," Jason Kim, chief of KISA's security technology dissemination team, told The Korea Herald in a recent interview.

Kim is also serving as vice chair of Korea Association for Biometric Identity Security and chair of Asian Biometrics Consortium.

Jason Kim, chief of KISA's security technology dissemination team (Korea Internet & Security Agency)

The biometric authentication reads heart rates and electrocardiogram on a user's smartwatch, which sends the information to their smartphone. The smartphone is then unlocked with the user's fingerprint which enables the use of mobile banking.

This is not the first time heart rate and electrocardiogram authentication is being used to unlock a device. The British bank Halifax and the Royal Bank of Canada are already using

[참고자료 별첨 5] – 생체홍보용 인터뷰(아리랑 TV, YTN 사이언스)

### YTN 사이언스 인터뷰 질의응답서

2017.8.16., 한국인터넷진흥원 공학박사 김재성 연구위원
아시아바이오인식협의회 의장, TTA 바이오인식 국내표준화 의장, 한국바이오인식협의회 수석부회장

☞ 아리랑 TV(8.17 방영), YTN 사이언스(10.12 방영예정)

## V 텔레바이오인식기술 표준화 추진현황 – TTA PG505, 국내표준화

| No. | 표준번호 | 표준명 | 제/개정일 |
|---|---|---|---|
| 48 | TTAE.IT-X.1085 | 바이오인식 보안토큰을 이용한 원격 바이오인증 프레임워크 | 2017-06-28 |
| 47 | TTAE.IT-X.1087 | 모바일 디바이스에서의 텔레바이오인식 보안지침 | 2017-06-28 |
| 46 | TTAK.KO-12.0303 | 개인인증을 위한 생체신호 정보 시험용 DB 구축지침 | 2016-12-27 |

| No. | 과제번호 | 초안명 | 프로젝트그룹 | 처리단계 | 처리일 | IPR |
|---|---|---|---|---|---|---|
| 12 | 2017-678 | [폐지]모바일 디바이스에서 텔레바이오인식 응용을 위한 기술 및 관리적 보안 지침 | PG505 | 과제채택 | 2017-09-06 | N |
| 11 | 2017-677 | [폐지]바이오인식 보안토큰을 이용한 텔레바이오인식 인증 프레임워크 | PG505 | 과제채택 | 2017-09-06 | N |
| 10 | 2017-415 | 일회용ID 기반 인증기술 | PG505 | 초안작성중 | 2017-06-29 | N |
| 9 | 2017-414 | 생체신호 인증알고리즘 성능시험기준 | PG505 | 초안작성중 | 2017-06-29 | N |
| 8 | 2017-050 | 모바일 바이오인식 제품의 위조샘플 탐지를 위한 시험 평가 지침 | PG505 | 초안작성중 | 2017-06-29 | N |
| 7 | 2017-049 | 바이오인식과 IC 카드를 이용한 접근제어용 개인확인시스템 | PG505 | 초안작성중 | 2017-04-07 | N |
| 6 | 2017-048 | 모바일 디바이스에서 전자건강기록의 보안 PART IV 보안표준 및 특성 비교 | PG505 | 초안작성중 | 2017-04-07 | N |
| 5 | 2017-047 | 모바일 디바이스에서 전자기록의 보안-엔지니어 가이드 | PG505 | 초안작성중 | 2017-04-07 | N |
| 4 | 2016-1904 | 생체신호 정보 프라이버시 보호지침 | PG505 | 초안작성중 | 2017-06-29 | N |
| 3 | 2016-1903 | 개인인증용 생체신호 데이터 포맷 | PG505 | 초안작성중 | 2017-06-29 | N |



## V 텔레바이오인식기술 표준화 추진현황 – ITU-T SG17 X.tab

INTERNATIONAL TELECOMMUNICATION UNION
**TELECOMMUNICATION STANDARDIZATION SECTOR**
STUDY PERIOD 2017-2020

**SG17-TD1087**
**STUDY GROUP 17**
**Original: English**

**Question(s):** 9/17 Geneva, 20-29 March 2018

**TD**

**Source:** Editor

**Title:** 3rd revised text for draft recommendation ITU-T X.tab: Telebiometric authentication using biosignals

**Purpose:** Proposal

**Contact:** Jason Kim Tel: +82 61 820 1251
Korea Internet & Security Agency E-mail: kimjs@kisa.or.kr

**Contact:** Sam Lee Tel: +82 61 820 1253
Korea Internet & Security Agency E-mail: sprout2@kisa.or.kr

**Summary**

This TD1087 proposes the 3rd revised text for ITU-T X.tab, Telebiometric authentication using biosignals, which is considered at the March 2018 SG17 meeting.

**Keywords**

biosignals, biosignal sensors, wearable devices, telebiometric authentication using biosignals

**Table of Contents**

1 Scope ..... 4
2 References ..... 4
3 Definitions ..... 4
3.1 Terms defined elsewhere ..... 4
3.2 Terms defined in this Recommendation ..... 5
4 Abbreviations and acronyms ..... 5
5 Conventions ..... 5
6 Prerequisites ..... 5
7 Overview of biosignals ..... 6
7.1 Types of biosignals ..... 6
7.2 Characteristics of biosignals for personal identification ..... 6
8 Requirements for biosignal sensors for authentication ..... 6
8.1 Types of biosignal sensor on wearable devices ..... 6
8.2 Functional requirements for authentication on biosignal sensor ..... 7
8.3 Data interchange format for biosignal sensors ..... 7
9 Architecture of telebiometric authentication platform using biosignals ..... 10
9.1 Overview ..... 10
9.2 Functional requirements for mechanism of biosignal authentication ..... 11
9.3 Functional requirements for biosignal transmission protocol ..... 11
9.4 Functional requirements for biosignal testing DB construction ..... 11
10 Performance testing methodology for biosignal authentication mechanisms ..... 11
11 PII protection for biosignal authentication model ..... 11
11.1 Vulnerabilites of biosignal authentication model applying ITU-T X.1086 ..... 11
Appendix I Use Cases of telebiometric authentication for biosignals ..... 13
I.1 Telebiometric authentication applications using multi-modal biosignals ..... 13
I.2 Case study for multi-modal biosignal authentication model ..... 14
Bibliography ..... 15

## V 텔레바이오인식기술 표준화 추진현황- ITU-T SG17 X.tab

**5.9.2 Relationships**

Questions: 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 and 12/17

Study Groups: ITU-T SGs 2, 5, 9, 11, 13 and 16; ITU-R SG 7, ITU-D SG2/2

Standardization bodies: ISO/IEC JTC 1/SC 17, 27, 37; ISO/TC's 68, 215; IETF, IEEE

Other bodies: International Bureau of Weights and Measures (BIPM), ICRU, FIDO Alliance, World Health Organization (WHO); International Labour Organization (ILO).

**5.9.3 Work programme and milestones**

| Draft Recommendation | First draft | Final draft | Consent | Determination |
|---|---|---|---|---|
| X.th2 | 2008-09 | 2018 | | 9/2018 |
| X.th3 | 2008-09 | 2018 | | 9/2018 |
| X.th4 | 2008-09 | 2018 | | 9/2018 |
| X.th5 | 2008-09 | 2018 | | 9/2018 |
| X.th6 | 2008-09 | 2018 | | 9/2018 |
| X.1080.1 (*) | 2016-09 | 2018 | 9/2018 | |
| X.tab | 2016-09 | 2018 | 3/2019 | |
| X.tac | 2017-03 | | 9/2018 | |

### ❖ 향후 추진계획

- *KISA 생체신호 인증기반 건강모니터링 서비스기술 표준개발 과제제안(IITP, 2018)*
  - *X.hsba(가칭) : Health-monitoring Services using Bio-signal Authentication (생체신호 인증을 이용한 건강정보 모니터링 서비스기술), NP 제안*
    - *ITU-T SG17 & ISO TC215 Common-Text로 Liaison statement 송부(Sept.2018)*

아시아

ASIAN BIOMETRIC CONSORTIUM

미국

the biometric CONSORTIUM

유럽

European Association for Biometrics eab Human Identity in Europe

➢ **KISA 보안기술확산팀 연구위원(공학박사)**
➢ *TTA PG505(바이오인식) 국내 표준화의장, 과기정통부 국립전파연구원 KS 국가표준 심의위원*
➢ *아시아바이오인식협의회(ABC) 의장, ISO/IEC SC37 & ITU-T SG17/Q9 국제표준전문가(에디터)*
➢ **kimjs@kisa.or.kr, +82-61-820-1251**

The 24th Network Security Conference -Korea

# 상황인지 기반의 범용 인증기술

**김승현** ETRI 선임

### 학력 및 경력사항

| | |
|---|---|
| 1998.03 ~ 2002.02 | 금오공과대학교 컴퓨터공학과 학사 |
| 2002.03 ~ 2004.02 | 포항공과대학교 컴퓨터공학과 석사 |
| 2004.01 ~ 현재 | 한국전자통신연구원 정보보호연구본부 |
| 2012.03 ~ 2017.06 | 카이스트 전산학부 박사 |

### 강연요약

2018년 1월, 정부가 공인인증서 제도를 폐지하기로 결정함으로써 다양한 본인인증 수단이 활성화되는 계기가 마련되었다. 최근들어 얼굴/음성/지문 등 생체인증 기술이 시장에 활발히 도입되고 있으며, 다양한 센서를 장착한 스마트폰의 보급 확대와 딥러닝 같은 인공지능 기술의 발달에 따라 더욱 활발한 연구가 진행될 것으로 예상된다.

단일 인증기술로 한번만 인증절차를 거쳤던 기존 방식에서 탈피하여, 여러 인증기술로 서비스 제공 도중에 지속적으로 인증 여부를 검증하는 연구가 시도되고 있다. 사용자의 편의성을 개선하기 위해서는, 매번 사용자에게 명시적인 인증을 요청하는 것이 아니라 사용자의 행위/환경 등의 특성을 바탕으로 묵시적인 인증을 수행하는 방안이 중요하다. 대표적인 국외연구로는 미국 DARPA의 Active Authentication 프로젝트, Google의 Abacus 프로젝트, NokNok Labs의 FIDO 인증 솔루션이 있다.

ETRI는 바이오, 행위, 환경 등 다양한 사용자 특성정보를 무자각/지속 모니터링하여 편리한 강화 인증을 제공하는 범용 인증 플랫폼 기술을 지난 3년 동안(2015년–2017년) 연구했다. 본 강연에서는 상황인지 요소를 고려한 다양한 행위/환경 기반 인증기술과 함께 FIDO 표준으로 이들 인증기술을 통합한 범용 인증 플랫폼을 설명한다.

좀 더 자세하게, 모바일 단말에서 사용자의 명시적 개입없이 인증할 수 있는 얼굴/화자 인식 기술, 서비스 이용 환경/행위 리스크를 분석하여 필요한 수준으로 사용자를 인증하는 지속인증 기술, FIDO 상호운용성 시험을 통과한 범용인증 플랫폼 기술, 몇 번의 클릭만으로 기존 앱에 범용인증 모듈을 적용할 수 있는 앱래핑 기술에 대한 설명과 함께 시연 영상을 보인다.

NETSEC-KR 2018

# 상황인지기반의 범용인증 기술

2018 년 4월 12일

한국전자통신연구원
정보보호연구본부

김승현

Smart & Green Technology Innovator
ETRI

## 목 차

Ⅰ. 연구 배경
1. 인증기술 현황 및 한계
2. 관련 연구동향

Ⅱ. 상황인지기반의 범용인증 기술
1. 가변 멀티팩터 인증
2. 리스크 기반 지속인증
3. FIDO 인증

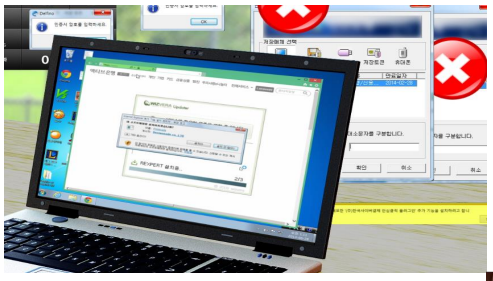
Ⅲ. 범용인증 기술의 검증 및 개선
1. 유저스터디
2. 레거시 연동 모듈

# Ⅰ. 연구 배경



## 연구 배경 – 인증기술 현황

### 문제 정의



☞ 공인인증/OTP 기술의
이용 편중 및 불편

패스워드 보안 취약성으로 ☜
유출 및 피해사례 증가

REUSED

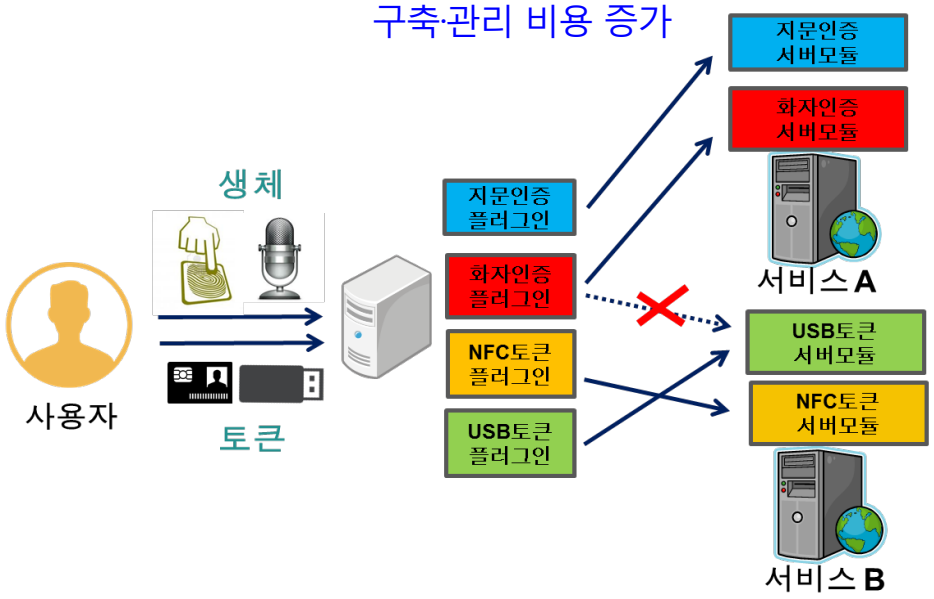
PHISHED

KEYLOGGED

# 연구 배경 – 인증기술 한계

## 문제 정의

☞ 새로운 인증 수단 도입 → 범용성 한계 &
구축·관리 비용 증가

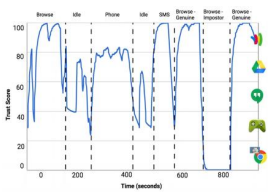



5

# 연구 배경 – 연구 동향

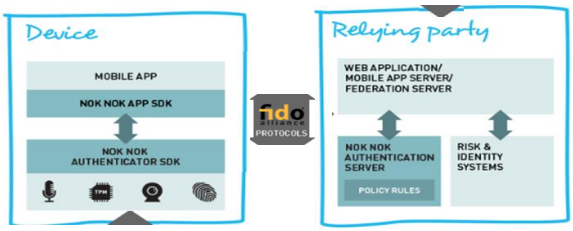
## Google

- Google ATAP(첨단기술프로젝트)팀에서 '14-'16년 연구 추진
- 다양한 행위요소들을 신뢰도 점수로 산정하여, 실제 사용자 본인 여부를 판단
  - 행위요소: 얼굴/음성패턴, 걸음걸이, 터치패턴, 키스트로크 패턴 등
- 지문인식보다 10배이상 안전한 인증 제공 주장(엔트로피: 16 bits(지문) vs. 21 bits(Abacus))
- '16년 말, Google Trust API 서비스로 오픈 예정



## Nok Nok Labs

- Nok Nok Labs가 '16.10월 발표한 FIDO기반 솔루션
- FIDO UAF의 추상화 계층에서 다양한 인증수단 수용 및 Federation 기술과 연동 지원
  - SAML, OpenID 등
- 리스크 분석 엔진을 탑재하여 인증 정책을 동적 적용
  - 사용자/디바이스/앱/세션/트랜잭션 별 정책 구분
  - 사용자의 현재 위치/디바이스 상태/이동 속도 등 고려
- NTT DOCOMO, PayPal, AliPay 등에 적용




6

# II. 상황인지 기반의 범용인증 기술

7

## 상황인지 기반의 범용인증 기술

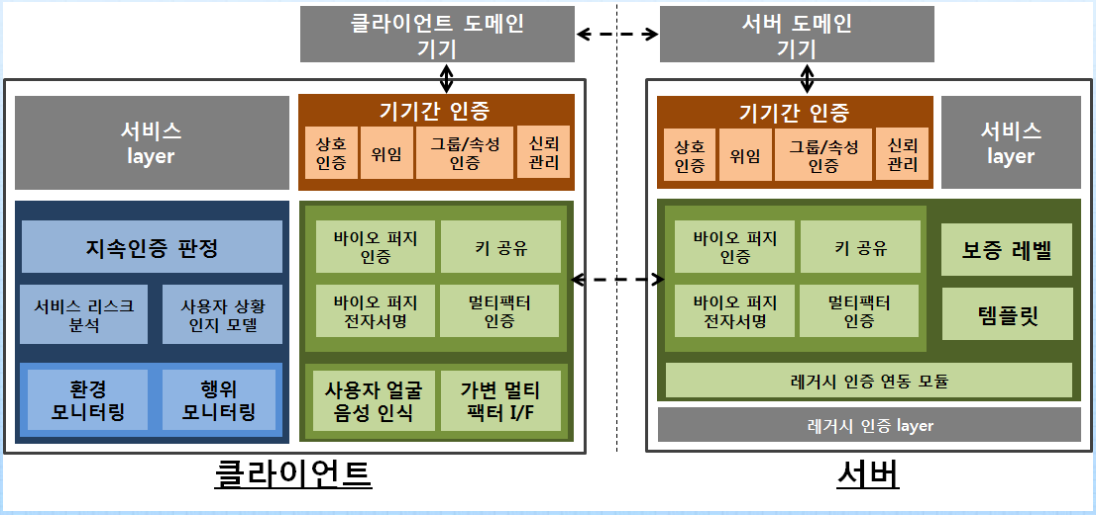
### 기술 개념

8

# 상황인지 기반의 범용인증 기술

## 범용인증플랫폼 개발

증명 가능한 가변 멀티팩터(4종) 인증과 환경/행위 정보 기반의 지속 인증 (명시적 인증 42% 절감) 및 고유정보 외부 노출 없는 부인방지 전자서명을 제공하는 유니버셜 인증 플랫폼 개발




9

# 범용인증 기술 – 가변 멀티팩터 인증

**전자금융서비스에 적용 가능한**
**4단계 인증 레벨 규정 및 신뢰승급 방안 제시**

### 연구 내용

- 인증 레벨 연구 및 표준화
  - 바이오인증을 포함한 4단계 인증 보증레벨 정의 및 근거 확보
  - 4단계 인증 보증레벨에 엔트로피, 인증강도 개념 반영

### 연구 성과

- 국내 표준 1건 : TTAK,KO-12.0313('17.12.13. 제정)
- 논문 1건 : "금융권에서 인증 보증 등급을 기반으로 한 신뢰 승급 방법", 정보보호학회지, '17.12.
- 국외 표준 기고서 3건
  - ISO/IEC : ISO-IECJTC1-SC27-WG5_N0836_DoC_DIS_29003_N16981
  - ISO/IEC : WG5_N935_Att7_CfC_SP_Req& outline_f_29115_Youm, Heung Youl Mr
  - ITU-T : T17-SG17-C-0115

| 방식 설명 | | 엔트로피 | 인증강도 |
|---|---|---|---|
| PIN(4자리) | | 13.2877 | 1 |
| PIN(6자리) | | 19.9319 | 1 |
| PIN(8자리) | | 26.5754 | 2 |
| 패스워드 (8자리) | 대문자 + 소문자 + 숫자 + 특수문자 | 52.4367 | 2 |
| 패스워드 (10자리) | 대문자 + 소문자 + 숫자 + 특수문자 | 64.5459 | 3 |
| 바이오 인증-안면 | | 9.9658 | 1 |
| 바이오 인증-지문 | | 9.9658 | 1 |
| 바이오 인증-홍채 | | 6.6439 | 1 |
| 바이오 인증 – 키스트로크 (키스와이핑) | | 6.6439 | 1 |
| OTP | | 19.9316 | 3 |
| SMS | 4자리 | 13.2877 | 2 |
| | 6자리 | 19.9316 | 3 |
| 공인인증서 | | 20 | 3 |

| | 인증수단 조합 예시 | 인증강도 | 인증레벨 | 사유 |
|---|---|---|---|---|
| 1 | 안면(1)+ PIN6(1) | 1+ | 2 | 2팩터 |
| 2 | 안면(1)+ PIN8(2) | 2+ | 2 | 인증강도2+ |
| 3 | PIN6(1) + 키스트로크(1) | 1+ | 2 | 2팩터 |
| 4 | PIN8(2) + 키스트로크(1) | 2+ | 2 | 인증강도2+ |
| 5 | 안면(1)+ 키스트로크(1)+ PIN6(1) | 2 | 2 | 인증강도2 |
| 6 | 안면(1)+ 키스트로크(1)+ PIN8(2) | 3 | 3 | 인증강도3 |
| 7 | 안면(1)+ 음성(1)+ 키스트로크(1)+ PIN6(1) | 2+ | 2 | 인증강도2+ |
| 8 | 안면(1)+ 음성(1)+ 키스트로크(1)+ PIN8(2) | 3+ | 3 | 인증강도3+ |

10

# 범용인증 기술 – 가변 멀티팩터 인증

## 모바일 라이브 얼굴 인식 EER: 0.79%
## – Liveness 탐지 EER: 3.38% –

### 연구 내용

- 모바일 단말용 실시간 얼굴 인식 기술 개발
  - 모바일 단말에서 얼굴인식 전과정 실시간 수행
  - 사용자 무자각/지속인증 수행 가능
  - 모바일 환경의 다양한 환경 변화에 강인한 얼굴 검출 및 인식 기술
  - 딥러닝 기반 얼굴 검출 및 인식 기술
- 모바일 단말용 얼굴 liveness 탐지 기술 개발
  - 모바일 환경에 최적화된 얼굴 liveness 탐지 기술

### 연구 성과

- 국내외 핵심 IPR 확보 및 학계 검증(SCI 2, 비SCI 5편)
- KISA 얼굴인식성능 시험인증 획득
- 모바일 얼굴인식 모듈 개발(EER: 0.79%@POSTECH, 0.18%@KNBTC)
- 모바일 얼굴 liveness 탐지 모듈 개발(EER: 3.33%@OULU-NPU)

<표 1> 시험용 얼굴 영상 데이터베이스의 구성

| 구분 | | 1 SET | | 2 SET | |
|---|---|---|---|---|---|
| 인원 | | 500명 | | 500명 | |
| | | 분류 | 영상수 | 분류 | 영상수 |
| ibset | 1 | 조명방향(8) | 4,000 | 조명방향(8) | 4,000 |
| | 2 | 표정변화(4) | 2,000 | 표정변화(4) | 2,000 |
| | 3 | 포즈(3) | 1,500 | 포즈(3) | 1,500 |
| | 4 | 액세서리(2) | 1,000 | 액세서리(2) | 1,000 |

<표 2> 얼굴 정합 횟수

| 분류 | 정합 방식 | 본인 대 본인 (genuine) | 본인 대 타인 (impostor) |
|---|---|---|---|
| 정합 횟수 (회) | 조명 | 4,000 | 1,996,000 |
| | 표정 | 2,000 | 998,000 |
| | 포즈 | 1,500 | 748,500 |
| | 액세서리 | 1,000 | 499,000 |

<표 3> K-NBTC의 본시험 결과 (Set-1, Set-2)

| 구분 | 조명 | 표정 | 포즈 | 액세서리 |
|---|---|---|---|---|
| Set-1 EER(%) | 0.20 | 0.20 | 0.15 | 0.37 |
| Set-2 EER(%) | 0.01 | 0.05 | 0.03 | 0.35 |
| 평균 | 0.11 | 0.12 | 0.09 | 0.41 |

KISA 바이오인식시스템 시험평가 결과



# 범용인증 기술 – 가변 멀티팩터 인증

## 모바일 라이브 화자인식 EER: 5.47%
## – Liveness 탐지 EER: 4.82% –

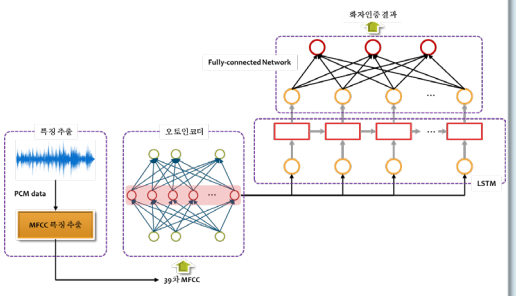
### 연구 내용

- 모바일 단말용 실시간 화자 인식 기술 개발
  - 모바일 단말에서 화자 인식 전과정 실시간 수행
  - 문장독립 화자인증 수행 가능
  - 모바일 환경의 다양한 환경 변화에 강인한 발화구간 검출 및 전처리 기술
  - 딥러닝 기반 음성특징 검출 및 화자 인식
- 모바일 단말용 화자 liveness 탐지 기술 개발
  - 딥러닝 기반 화자 liveness 탐지 기술 개발
  - 모바일 환경 화자 liveness 탐지 기술

### 연구 성과

- 딥러닝 기반 모바일 화자인식 모듈 개발 (EER: 5.47%, 모바일 문장독립 음성 DB, 30명)
- 딥러닝 기반 모바일 화자 liveness 탐지 모듈 개발 (EER: 4.82%, 합성/녹음 음성 DB)

화자 인식 기술 개요



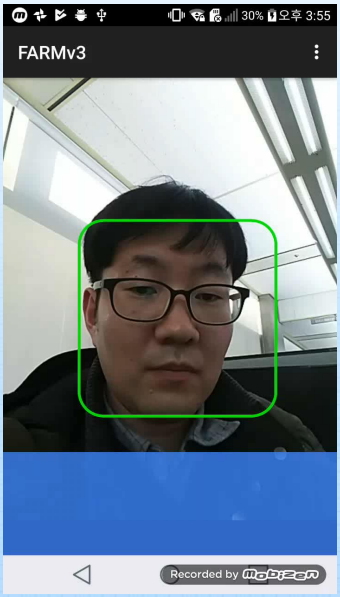

화자 Liveness 탐지 성능

| | Genuine | Imposter | 인식률 |
|---|---|---|---|
| Genuine | 30,087 | 275 | 99.1% |
| Imposter | 749 | 10,113 | 93.1% |

# 범용인증 기술 – 가변 멀티팩터 인증

시연

**모바일 사용자**
**얼굴/화자 인식 및 liveness 탐지**



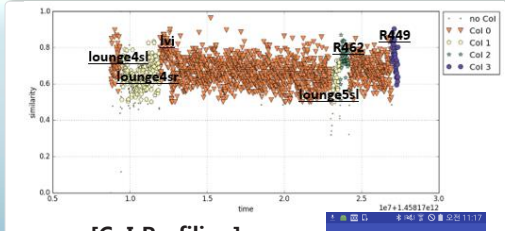

13

# 범용인증 기술 – 리스크 기반 지속인증

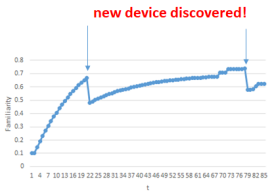
**환경/행위 정보 결합 상황인지 및**
**리스크 분석 모듈 개발**

## 연구 내용

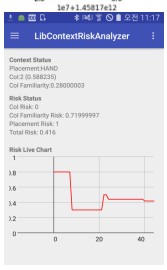
- **환경/행위 정보 결합 상황인지 모듈 개발**
  - WiFi AP 목록 기반의 CoI(Context of Interest) Profiling/Inference 모듈
  - Bluetooth 기기 스캔 정보를 이용한 CoI Familiarity Analyzer 모듈
  - Acc, Gyro, Orientation, Light 센서를 이용한 Placement Inference 모듈
- **Lunch time attack에 대응하는 상황인지 기반 리스크 분석 알고리즘 및 모듈 개발**
  - CoI: 자주 방문하는 장소 여부
  - Familiarity: 장소의 익숙함 정도를 수치화
  - Placement: 기기가 인증된 사용자의 주의력에서 벗어난 상황 여부




[CoI Profiling]




[CoI Familiarity]




[리스크 분석기]

## 연구 성과

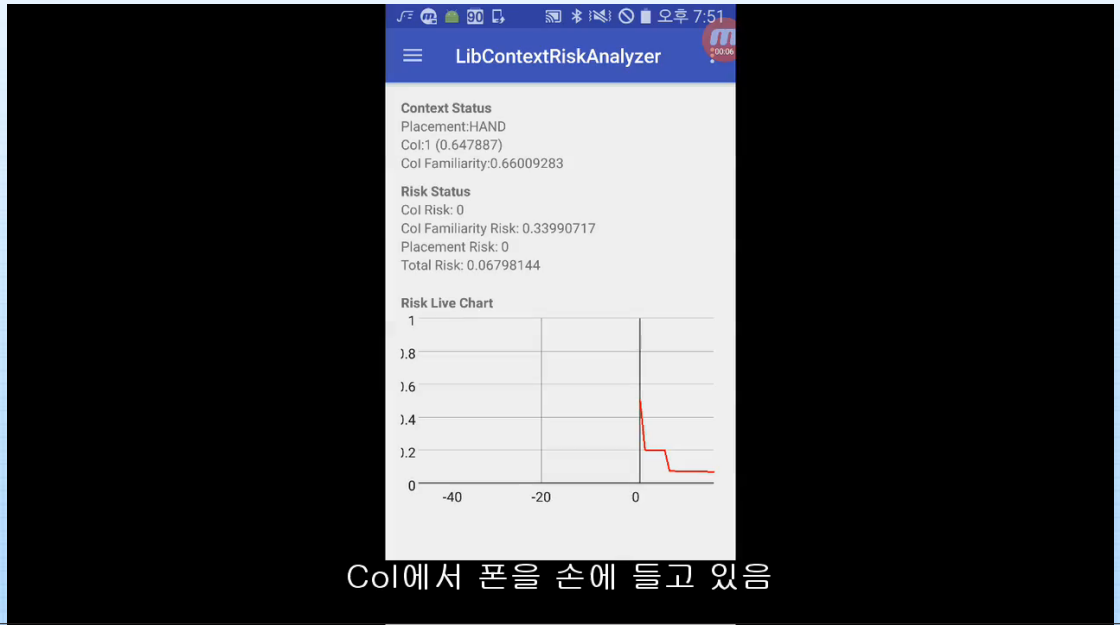
- Placement classification accuracy: 97.59%
- CoI profiling classification v-measure: 72.01%

14

# 범용인증 기술 – 리스크 기반 지속인증

시연

## 환경/행위 정보 결합 상황인지 및 리스크 분석 모듈




Col에서 폰을 손에 들고 있음



# 범용인증 기술 – FIDO 인증

## 상황인지 기반 무자각 지속인증을 지원하는 FIDO 시스템

### 연구 내용

- **환경/행위 정보 기반의 지속 인증 기술**
  - 4단계 인증 레벨에 따른 지속 인증 관리
    - 멀티팩터/멀티모달에 따른 지속 인증 관리
  - 지속 인증 모니터링 기술
    - Risk Score/요청 인증 레벨/인증 결과 등을 시각적으로 관리할 수 있는 모니터링 모듈
  - 상황 인지/인증 모듈 연결
    - 인증 수준 분석 및 요구 인증 레벨 만족을 위한 Risk 분석/PIN/Keystroke/Face 인증 모듈 연결

### 연구 성과

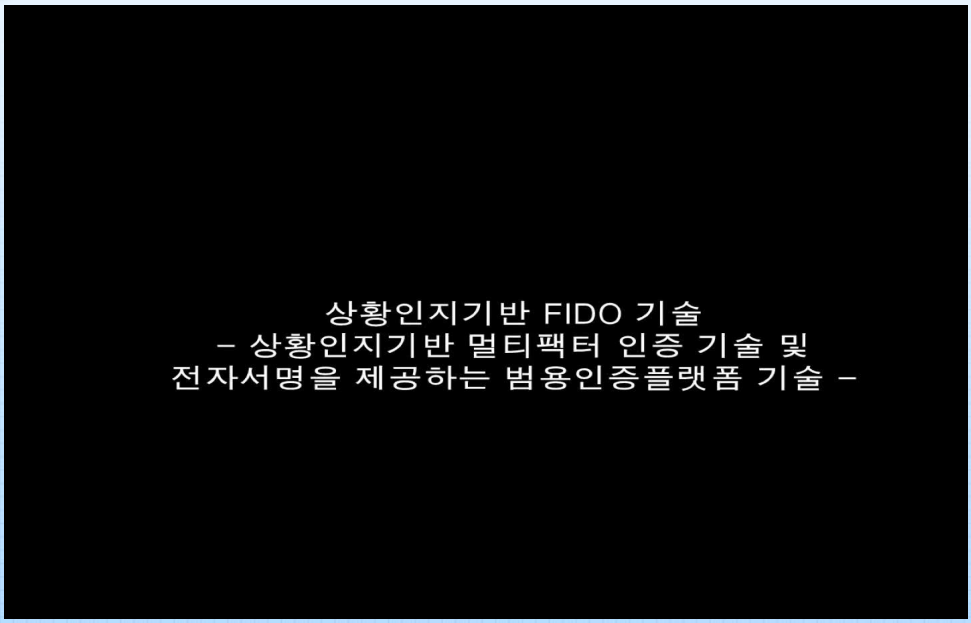
- FIDO UAF 표준 프로토콜을 준용한 4단계 인증 레벨 지원 프로토콜 개발
- 인증 레벨 지원이 가능한 은행 시연 시스템 개발
- 상황인지 기반의 FIDO 인증 시스템이 적용된 파일럿 서비스 구축(한국정보인증㈜)

[지속 인증 관리 시스템]

# 범용인증 기술 – FIDO 인증

시연

사용자 이용상황 및 서비스 보안 요구수준에 따라 명시적 인증을 생략하거나 추가 인증을 요청하는 서비스




17

## Ⅲ. 범용인증 기술의 검증 및 개선

# 성능 검증 – 유저 스터디

**실험**

**22명 평균 41.5일간 데이터 수집 및 시험 평가**
**– 20개 항목, 약 100GB –**

| 모니터링 앱 개발 | 사용자(일반인) 대상 데이터 수집 | 실험 데이터 가공 | 지속인증 적용 및 결과 분석 |
|---|---|---|---|
| 얼굴이미지특징, 각종센서정보, 이벤트로그, 앱사용 정보 등 20개 항목 (얼굴이미지는 프라이버시 이슈로 특징벡터만 저장) | 22명 대상으로 평균 41.5일간 데이터 수집<br><br>(약 100GB) | 수집된 데이터로 시계열 상 행위, 환경 모듈의 결과값 도출 및 기타 부가 정보 가공 | 가공데이터로 지속인증 모듈의 결과 도출 및 해당 시간의 실행앱에서 요구하는 인증 레벨의 부합 여부로 절감율 계산 |



# 성능 검증 – 유저 스터디

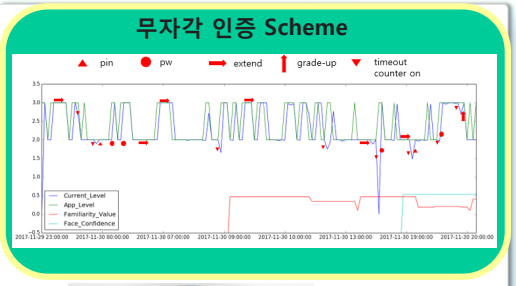
**얼굴/환경/행위 무자각 지속인증을 통한**
**명시적 인증 45% 절감 달성**

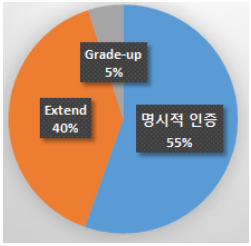
## 연구 내용

- Face, 환경, 행위 정보 기반 무자각 지속인증 Scheme 개발
  - Face 기반 인증레벨 승급 (Grade-up)
  - 환경/행위 리스크 분석 및 지속 인증
- 생체/환경/행위 High Level Features 사용
  - Face confidence, CoI, CoI Familiarity, Placement

## 연구 성과

- 무자각 지속인증을 통한 명시적 인증 45% 절감 달성
- Face, CoI, CoI Familiarity, Placement 기반의 무자각 지속인증 Scheme 제시




명시적 인증 45% 절감

# 성능 검증 – 레거시 연동

**레거시 앱에 FIDO 보안모듈을
패치할 수 있는 동적 바인딩 앱래핑 시스템 개발 완료**

## 연구 내용

- 액티비티 모니터링 기반의 보안정책 관리 모듈 개발
  - 앱의 주요 액티비티 식별 후 추적 코드 패치
  - 웹 인터페이스로 사용자 액션에 따른 앱 동작 실시간 모니터링 및 보안정책 관리
- 동적 보안정책을 지원하는 앱래핑 모듈 개발
  - 임의의 보안모듈을 패치할 수 있는 동적 바인딩 앱래핑 기술 개발

## 연구 성과

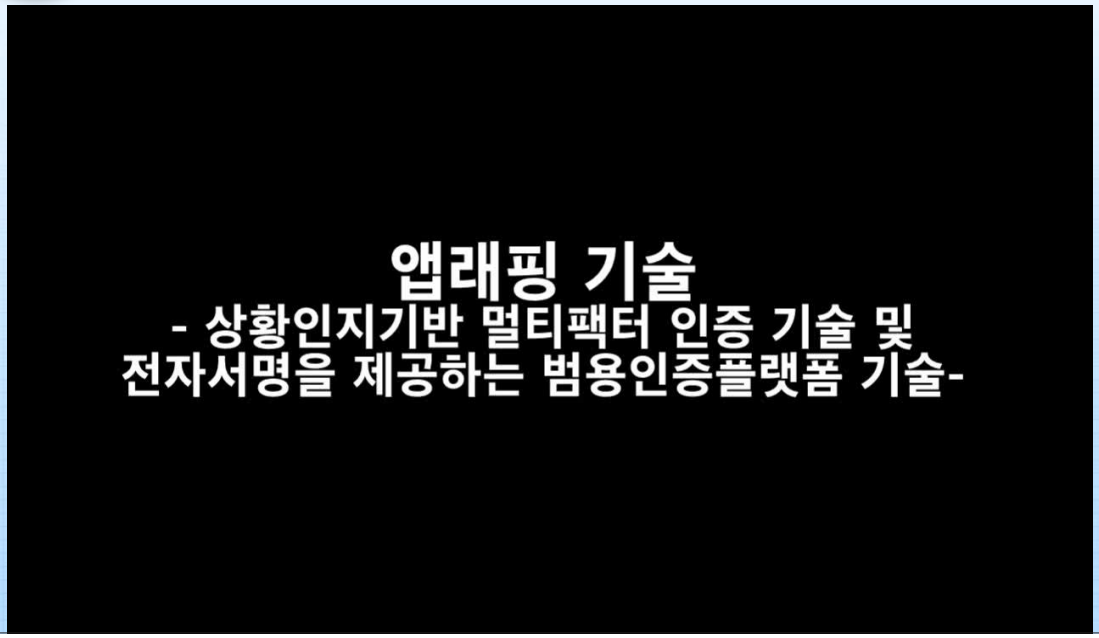
- 업계에서 실제 적용중인 그룹웨어 앱 5종, 안드로이드 마켓의 카테고리 별 top 3앱(99개) 대상 100% 성공
- 상용 MDM 솔루션 (라온시큐어) 의 보안 모듈을 적용하여 연동 확인



# 성능 검증 – 레거시 연동

시연

**일반 그룹웨어 앱을 대상으로 액티비티 모니터링 및
동적 보안정책을 지원하는 앱래핑 기술**



감사합니다

The 24th Network Security Conference -Korea

# 인공지능기반 차세대 인증 패러다임 변화 방향

**박정현** 금융결제원 팀장

### 학력 및 경력사항

KAIST 테크노경영대학원 석사 (2004)
서강대학교 경제학 학사 (1998)
現 금융결제원 차세대인증업무팀장
금융결제원 금융결제연구소 전문연구역

### 강연요약

현재 국내 인증시장은 다양한 인증서비스가 경쟁하는 소위 '춘추인증전국시대'로 고객의 서비스 선택 폭이 확장되는 양의 효과도 있지만 검증되지 않은 새로운 서비스에 대한 인증 공격 가능성과 서비스 이용자의 인증 피로감도 급격히 증가하는 부의 효과도 확대되는 상황

따라서, 서비스 이용자가 스스로를 인증하는 현재의 '서비스 이용자 능동형 인증체계'에서 인공지능기술을 기반으로 서비스 공급자가 이용자를 알아서 인증하는 '서비스 제공자 능동형 인증체계'로의 패러다임 전환을 통해 서비스 이용자 인증 피로감을 해소하고 인증서비스 이용자 공격에 대한 새로운 방어기제를 구성할 필요

강연자의 요청으로
발표자료를 공개해 드리지 못한 점
양해 부탁드립니다.

The 24th Network Security Conference -Korea

# 딥러닝을 적용한 서명행위 기반의 생체인증

**한승호** 시큐브 연구소장

### 학력 및 경력사항

| | |
|---|---|
| 2002.02 | 아주대학교 정보 및 컴퓨터공학과 학사 |
| 2001.08 ~ 현재 | (주)시큐브 정보보호기술연구소 |
| 2017.11 | 정보보호 산업부문 유공자 과학기술정보통신부 장관 표창 수상 |

### 강연요약

생체인증 기술은 사용자의 고유한 신체적 특징 및 행위적 특징을 인증요소로 사용하며, 기존의 소유기반/지식기반 인증 기술에 비해 높은 사용자 편의성을 제공하므로 핀테크 시대에 적합한 본인인증 기술로 각광받고 있다. 특히 행위정보 기반 인증기술은 생체정보 기반 인증기술의 해결과제로 이슈화되고 있는 개인정보 유출 및 이에 따른 도용 가능성이 상대적으로 낮아 국내외적으로 활발한 연구개발이 이루어지고 있다.

본 발표는 딥러닝을 적용한 사용자의 행위정보(걸음걸이, 음성, 입력패턴, 수기서명)에 기반한 생체인증 기술에 대한 연구동향을 분석하고, 행위정보 기반 생체인증 기술 중에서 다양한 특.장점을 지니고 있는 수기서명 인증기술에 대한 딥러닝 적용 방안을 제시한다.

KOSDAQ 코스닥상장법인

SECUVE 시큐브

# 딥러닝을 적용한 서명행위 기반의 생체 인증

2018. 4.

한 승 호 연구소장
㈜시 큐 브

Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved

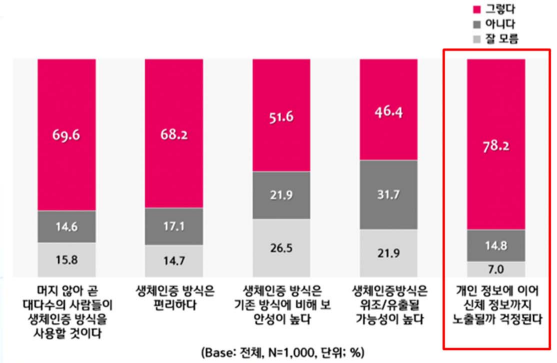
## 최근 생체 인증 기술 이슈

생체 인증

**다양한 인증기술 화두**
- 공인인증서 제도 폐지 (전자서명법 개정안 18.03)
- 스마트폰과 생체인증 기술의 융합

**생체인증 기술의 대중화**
- 개인정보보호에 대한 관심 증가
- 다양한 자동화된 장치를 통한 개인 식별

'생체인증' 방식 관련 전반적인 인식 평가



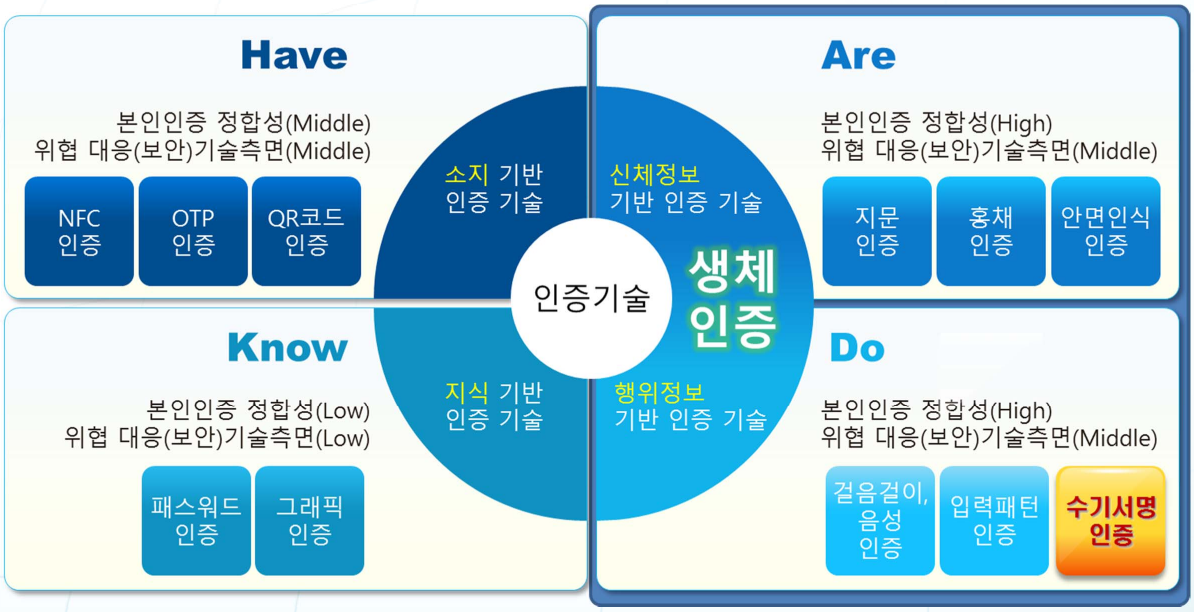

(Base: 전체, N=1,000, 단위: %)

시장조사전문기업 '엠브레인 트렌드모니터'

보안성과 편리성이 확보된 비대면 인증기술 필요


Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

## 비대면 인증 기술 분류





Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

## 생체인증 기술 정의 및 분류

사용자 고유의 **신체 정보** 또는 **행위 정보**를 추출하여 본인 여부를 판별하는 인증 기술

NIST Information Technology Laboratory
- Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011, NIST SP 500-290 Edition 3, 2016. 9.

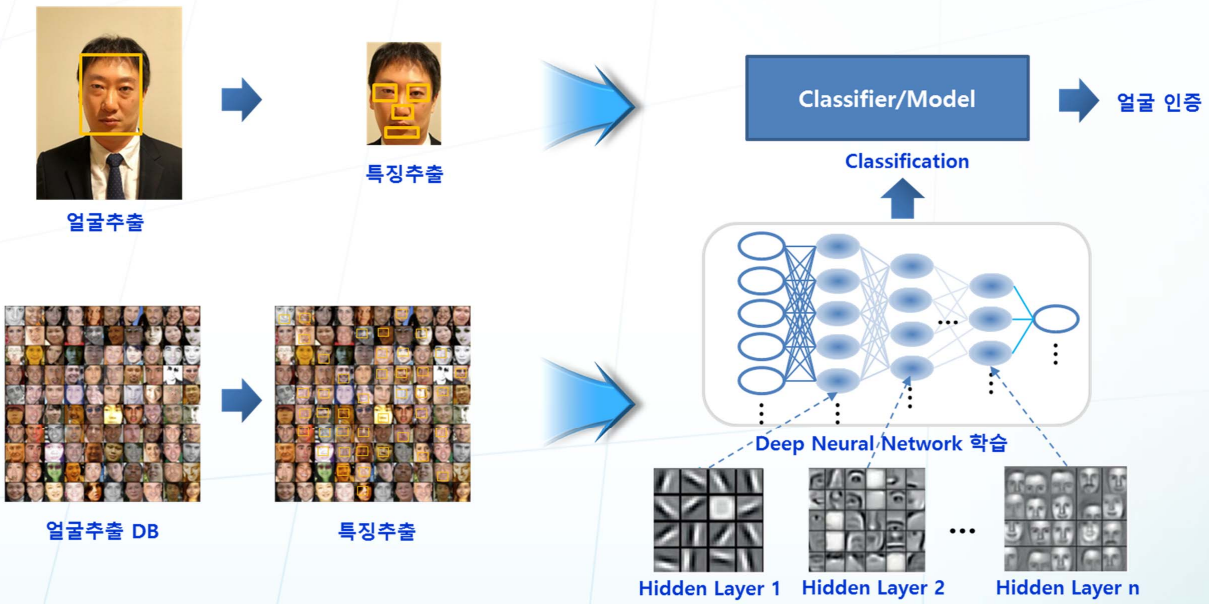
Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝 정의 및 응용분야

뇌 구조와 유사한 신경망 학습을 통해 데이터 간의 복잡한 관계를 이해하는 인공지능 분야

# 딥러닝을 활용한 생체인증 사례 [1] 얼굴 인증 (1/3)

- 영상 처리 장치로 얼굴 영상을 입력 받아 얼굴을 자동으로 검출하고 딥러닝 기술을 적용하여 조명, 표정 포즈 변화에 얼굴 인증을 제공하는 기술



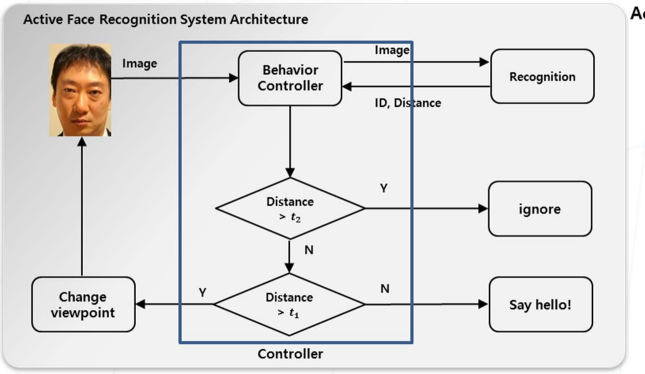


Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [1] 얼굴 인증 (2/3)

- 기술 연구 동향

## 딥러닝을 이용한 다각도의 사용자 얼굴 인식에 관한 연구




AcFR: Active Face Recognition Using Convolutional Neural Networks
- Masaki Nakada, 캘리포니아 대학교 (미국, 2017년)

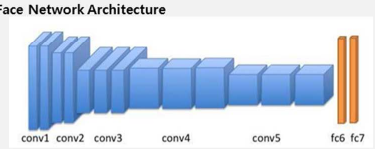
Behavior Modeling

$$Behavior = \begin{cases} Greet & if\ d \le t_1, \\ Ignore & if\ d \le t_2, \\ ChangeView & if\ t_1 < d < t_2 \end{cases}$$

$d : distance$
$t_1, t_2 : distance\ thresholds$

다각도의 사용자 이미지

VGG-Face Network Architecture




다각도 사용자 얼굴 이미지를 이용하여 딥러닝 적용

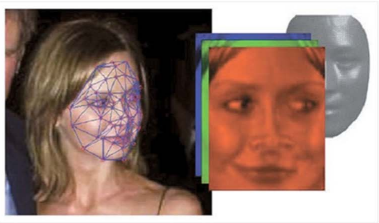

Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [1] 얼굴 인증 (3/3)

- 기술 적용 사례

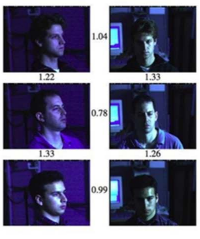
## Facebook 社(미국)

- 2014년 딥러닝이 적용된 '딥페이스(DeepFace)'라는 사진 얼굴 인식 알고리즘 발표
- 심층신경망 조합으로 얼굴을 인식하는 딥페이스는 정확도 97.25%
- 이미지의 얼굴을 인식하고 3차원으로 변환해 어떤 각도에서 보더라도 사진의 인물을 파악
- 페이스북 자동 태깅 성능 향상, 개인화된 맞춤형 광고 제공



## Google 社(미국)

- TensorFlow 라이브러리 사용하는 페이스넷(FaceNet)
- 인터넷에서 실험집단 데이터 1만 3천명의 데이터 이미지를 사용한 결과 99.96% 인식율
- 심층신경망을 구현하여 사람 이미지 인식
- 얼굴당 128바이트만 사용, 어두운 곳에서도 밝은 곳처럼 인식 가능





Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [2] 음성 인증 (1/3)

- 억양, 말의 빠르기, 목소리 톤 등 **언어적 특징 정보**를 이용하여 딥러닝을 적용한 인증 기술

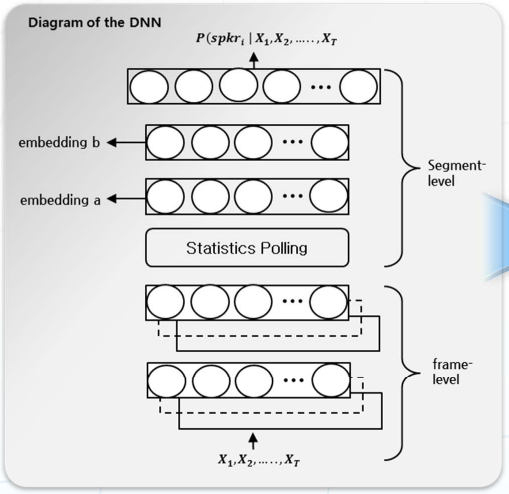
Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [2] 음성 인증 (2/3)

- 기술 연구 동향

## 문맥 독립 화자 인식을 위한 딥러닝 기반의 임베딩

Deep Neural Network Embeddings for Text-Independent Speakr Verification
- David Snyder, Johns Hopkins University(2017년)




성능 비교

NIST SER10 표준의 음성

English telephone speech

| | 10s-10s | 5s | 10s | 20s | 60s | Full |
|---|---|---|---|---|---|---|
| ivector | 11.0 | 9.1 | 6.0 | 3.9 | 2.3 | 1.9 |
| embedding a | 11.0 | 9.5 | 5.7 | 3.9 | 3.0 | 2.6 |
| embedding b | 9.2 | 8.8 | 6.6 | 5.5 | 4.4 | 3.9 |
| embeddings | 7.9 | 7.6 | 5.0 | 3.8 | 2.9 | 2.6 |
| fusion | 8.1 | 6.8 | 4.3 | 2.9 | 2.1 | 1.8 |

EER(%) on NIST SRE10

*fusion : ivector와 embeddings에 동일한 점수의 가중치를 합한 방식

i-vector 모델과 DNN기반의 embedding에 대한 성능 비교


Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [2] 음성 인증 (3/3)

- 기술 적용 사례

## Microsoft 社(미국)

- MS에서는 개발 화자를 인식하고 식별하는 API를 제공
- 화자가 특정 신원을 요청할 경우 학습된 음성을 사용하여 화자를 검증
- 이를 이용하여 '인보크'라고 하는 인공지능 스피커 출시

## 화자 인식 연구 및 도입 예정인 국내 기업

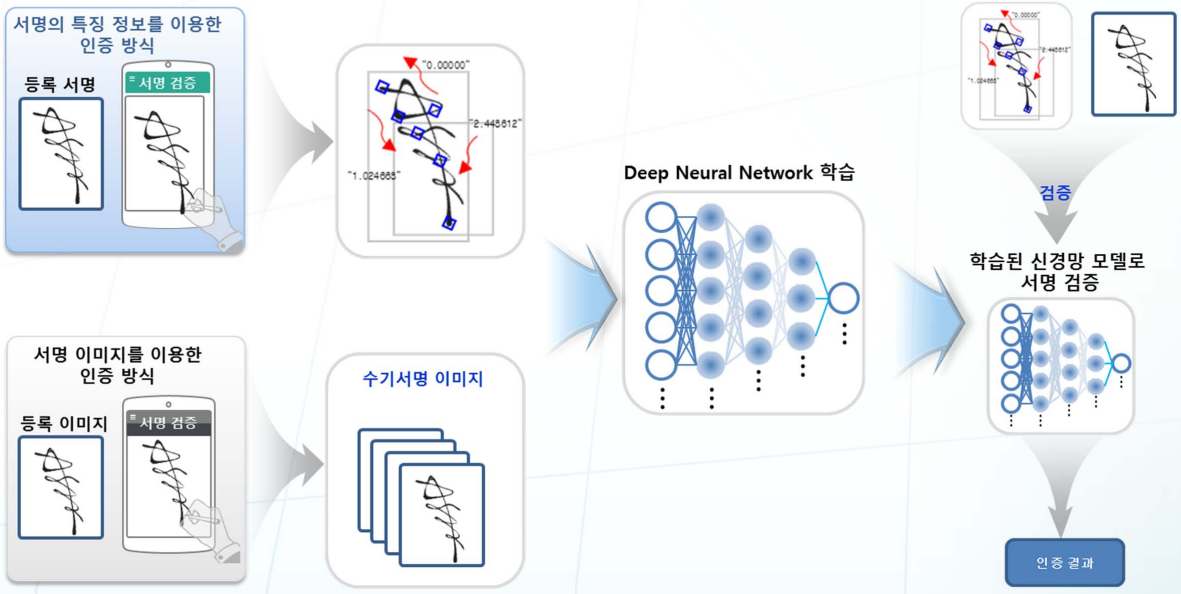
국내 AI 플랫폼

GiGA Genie
kt
kakao i
kakao
NUGU
SK telecom
Clova
NAVER


Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [3] 수기서명 인증 (1/3)

- 수기서명의 특징 정보 및 수기서명 이미지 학습, 학습된 모델 통한 인증 수행





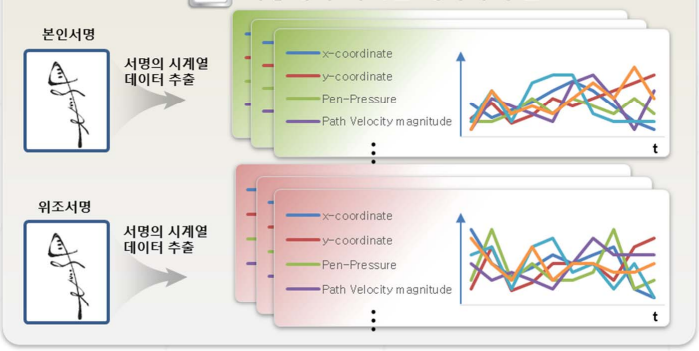
Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 활용한 생체인증 사례 [3] 수기서명 인증 (2/3)

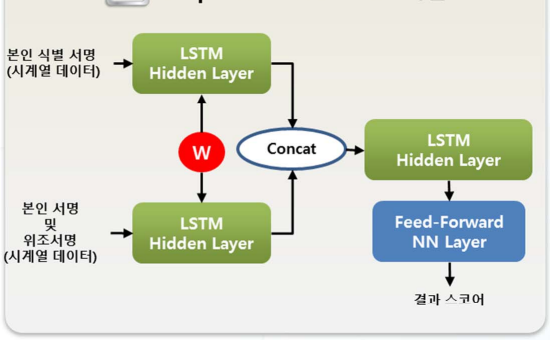
## 기술 연구 동향

Biometric Signature Verification Using Recurrent Neural Networks
Ruben Tolosana, BiDA Lab, 2017

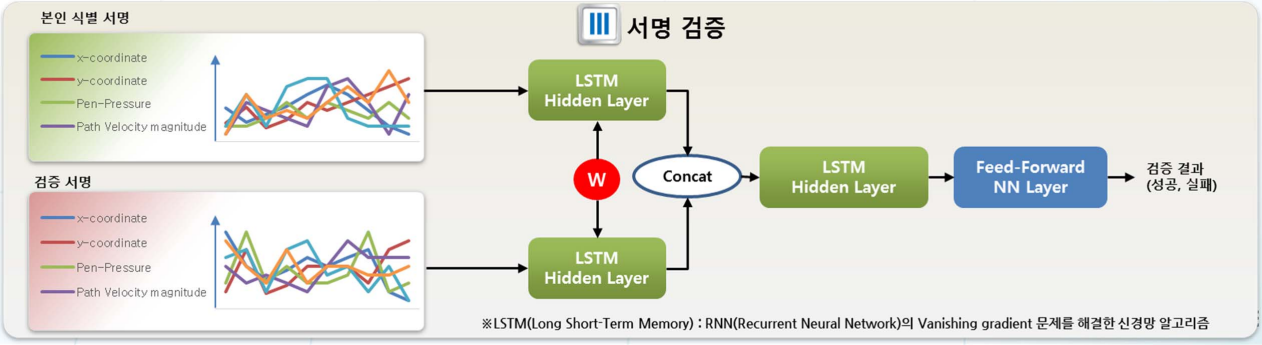
### I 서명에서 시계열 데이터 추출




### II Deep Neural Network 학습




### III 서명 검증



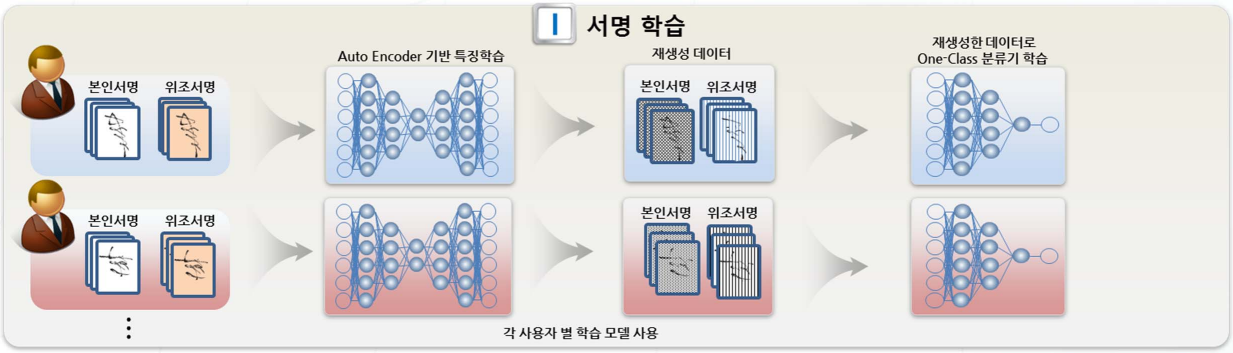

※LSTM(Long Short-Term Memory) : RNN(Recurrent Neural Network)의 Vanishing gradient 문제를 해결한 신경망 알고리즘

# 딥러닝을 활용한 생체인증 사례 [3] 수기서명 인증 (3/3)

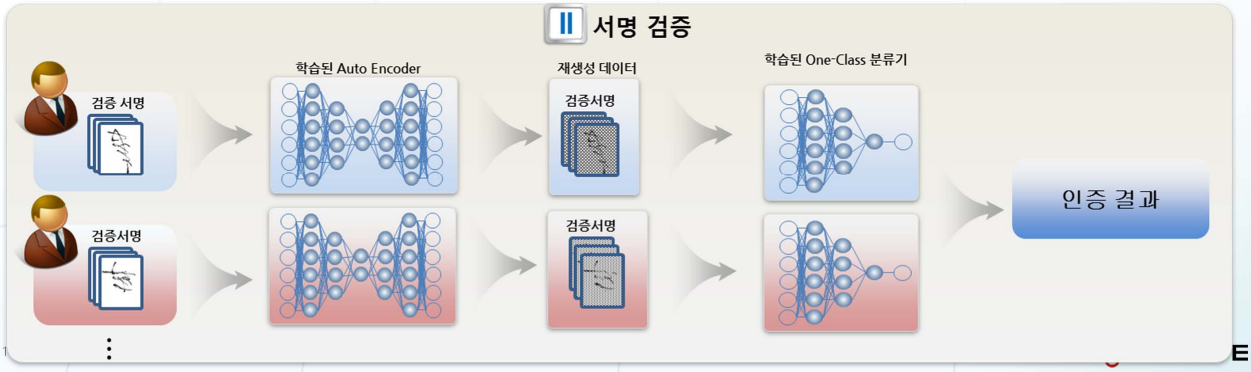
## 기술 연구 동향

Feature Representation for Online Signature Verification
Mohsen Fayyaz , Malek-Ashtar University , 2015

### I 서명 학습

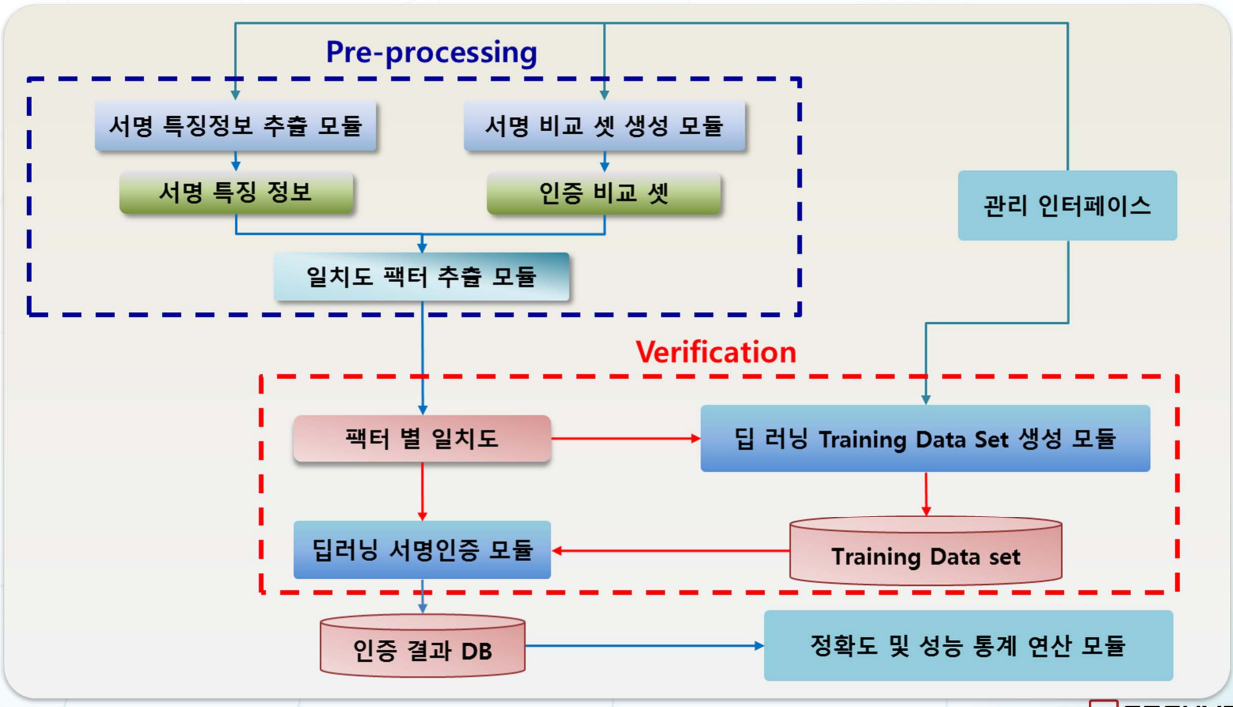



### II 서명 검증



# 딥러닝을 적용한 서명행위 기반의 생체인증 연구 방향 (1/3)

- 딥러닝 기술을 적용한 서명행위 생체 인증 기술 연구

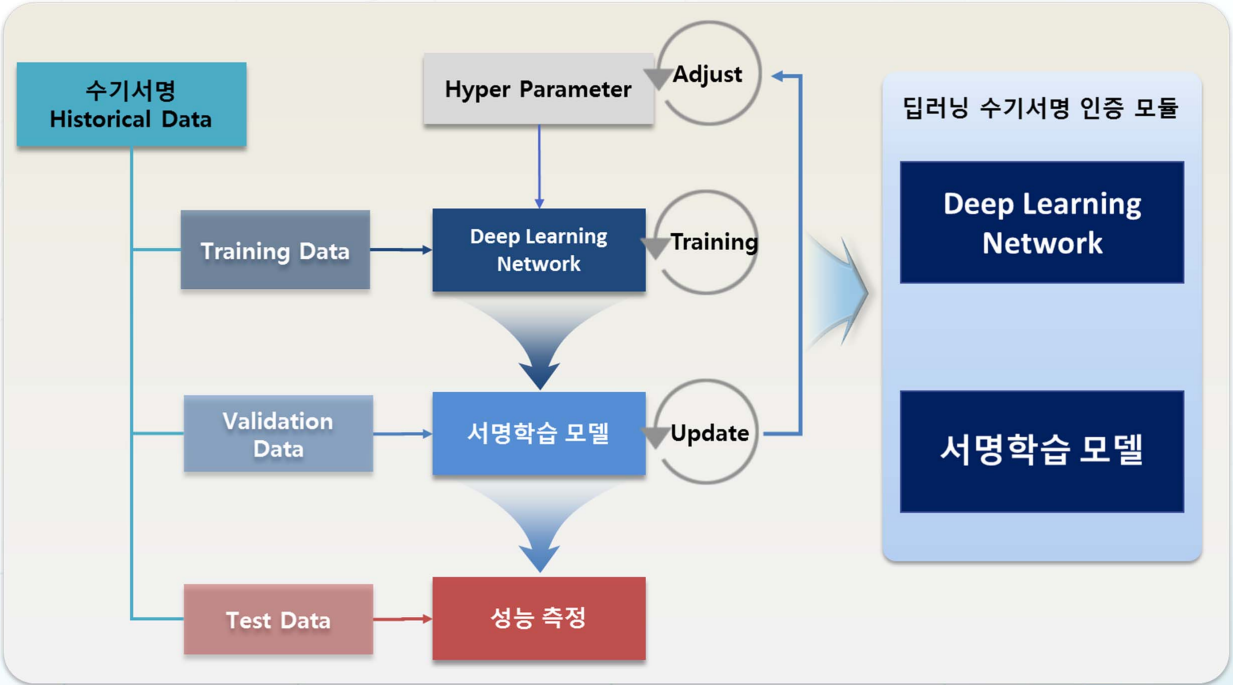




Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 적용한 서명행위 기반의 생체인증 연구 방향 (2/3)

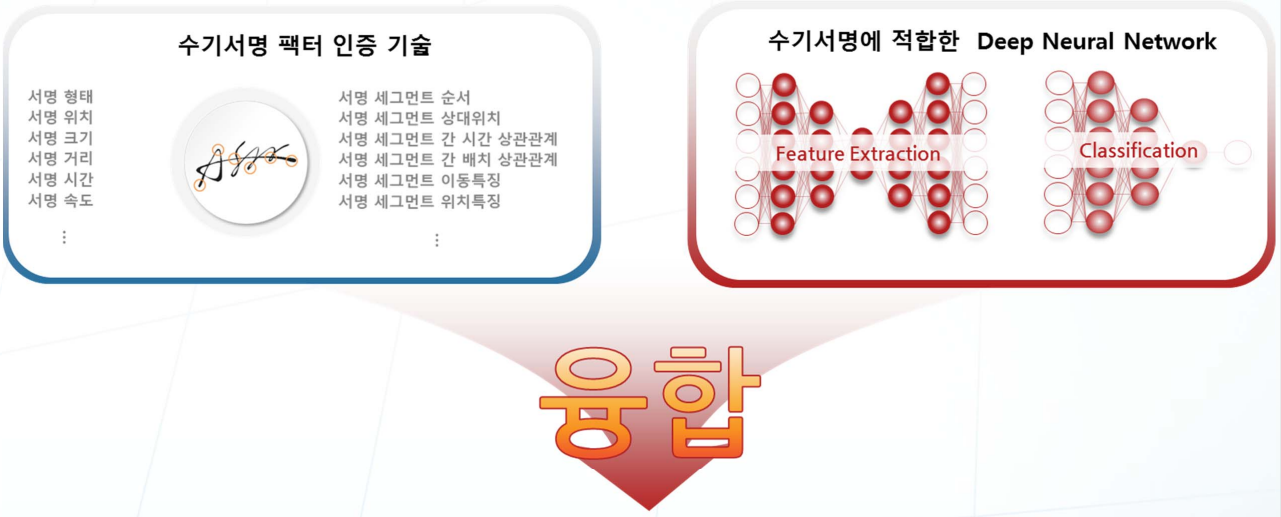
- 수기서명 딥러닝 모델 학습 절차





Copyright ⓒ SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 딥러닝을 적용한 서명행위 기반의 생체인증 연구 방향 (3/3)




팩터 인증기술과 딥러닝 학습 모델을 융합한 수기서명 인증 시스템


Copyright © SECUVE Co., Ltd. All Rights Reserved
SECUVE

# 수기서명 활용사례 (1/3)

- 수기서명 생체행위 특성정보 분석을 통한 본인인증

시큐브 **시큐사인(SecuSign)**은 사용자의 서명 행위 과정의
다양한 **동적인 행위 특징정보**를 추출/분석하여 사용자를 인증하는 기술

사용자 고유의
생체행위특성을 이용하여
서명 검증

서명 형태
서명 위치
서명 크기
서명 거리
서명 시간
서명 속도
⋮

서명 세그먼트 순서
서명 세그먼트 상대위치
서명 세그먼트 간 시간 상관관계
서명 세그먼트 간 배치 상관관계
서명 세그먼트 이동특징
서명 세그먼트 위치특징
⋮

수기서명 행위기반 인증기술
시큐사인 FIDO 인증 획득

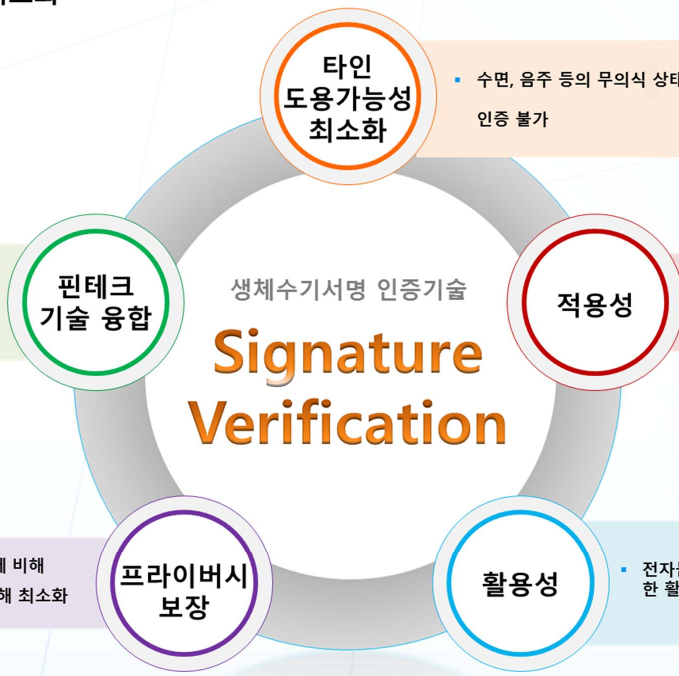
**SecuSign FIDO®**
Authenticator for
Android 1.0
FIDO UAF Certificate
UAF100020160322005
March 22, 2016

**SecuSign FIDO®**
Authenticator for
iOS 1.0
FIDO UAF Certificate
UAF100020160322006
March 22, 2016

Copyright © SECUVE Co., Ltd. All Rights Reserved
SECUVE

## 수기서명 활용사례 (2/3)

- 수기서명 인증 기대효과
  - 핀테크 서비스
  - 인터넷뱅킹
  - 스마트뱅킹
  - 인터넷전문은행

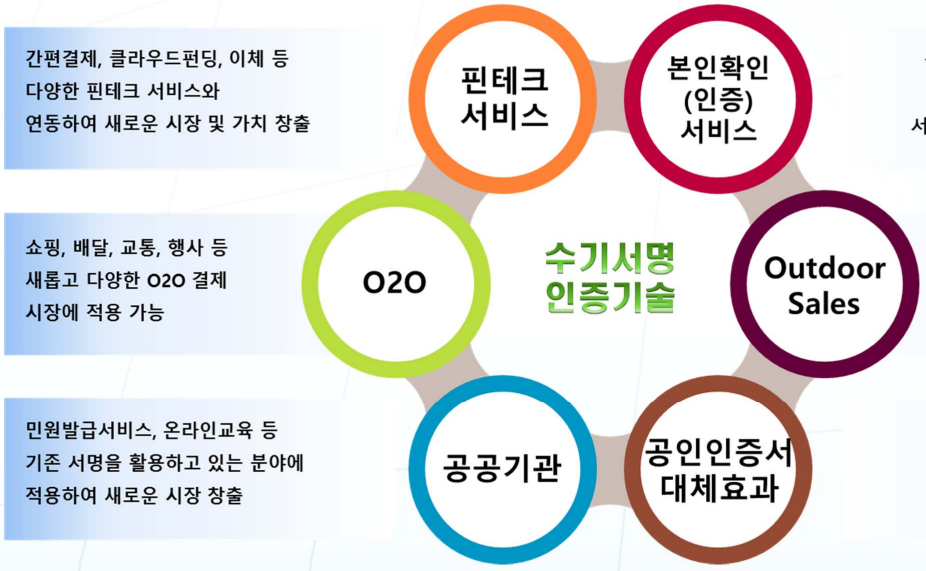




Copyright © SECUVE Co., Ltd. All Rights Reserved
SECUVE

## 수기서명 활용사례 (3/3)

- 수기서명 인증 활용 분야

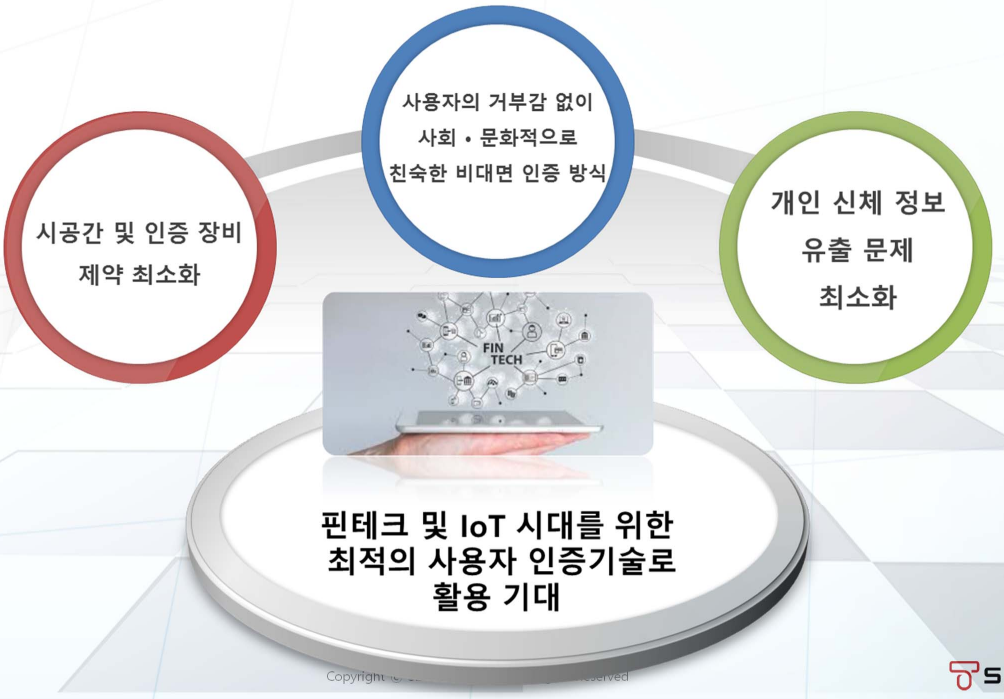




Copyright © SECUVE Co., Ltd. All Rights Reserved
SECUVE

## 결 론

행위정보 기반 생체 인증 기술은 보안성과 편리성이 확보된 비대면 인증기술




21

Copyright © SECUVE Co., Ltd. All Rights Reserved

KOSDAQ
코스닥상장법인

SECUVE
시큐브

# 감사합니다

Copyright © SECUVE Co., Ltd. All Rights Reserved

The 24th Network Security Conference -Korea

# 다크웹 및 불법 암호화폐 거래 분석 기술

**허준범** 고려대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2009.08 | KAIST 공학박사 (컴퓨터학) |
| 2005.08 | KAIST 공학석사 (컴퓨터학) |
| 2001.02 | 고려대학교 이학사 (컴퓨터학) |
| 2016.09 ~ 현재 | 고려대학교 컴퓨터학과 부교수 |
| 2015.03 ~ 2016.08 | 고려대학교 컴퓨터학과 조교수 |
| 2011.09 ~ 2015.02 | 중앙대학교 컴퓨터공학부 조교수 |
| 2009.09 ~ 2011.08 | University of Illinois at Urbana–Champaign 박사후연구원 |

### 강연요약

본 강연에서는 최근 수개월간 수집한 국내외 다크웹 데이터를 바탕으로 다크웹 운용현황 및 프로파일링 결과를 소개한다. 그리고 다크웹에서 불법적으로 거래되고 있는 암호화폐 흐름 분석을 위한 기초 클러스터링 기법의 소개와 상용 클러스터링 툴의 취약점을 분석한다. 그리고 불법자금 세탁에 활용되는 상용 믹싱서비스 분석 결과 및 믹싱된 암호화폐 거래에 대한 역추적 연구결과를 발표한다.

# 다크웹 및 불법 암호화폐 거래 분석 기술

NetSec - KR

2018년 4월 12일

고려대학교 컴퓨터학과
허준범 교수

KOREA UNIVERSITY ISSLAB Information System Security Laboratory

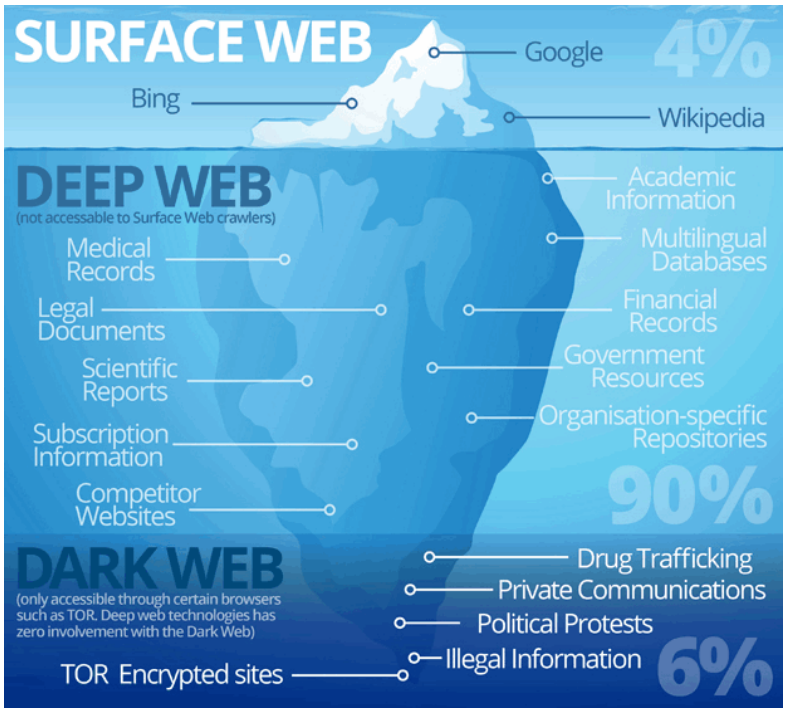
## 순서

- 다크웹과 암호화폐
- 다크웹 분석 및 프로파일링 (국내를 중심으로)
- 불법 암호화폐(비트코인) 거래 분석
  - Clustering
  - De-mixing (Helix)

# 서피스웹 / 딥웹 / 다크웹

4% of www contents

96% of www contents

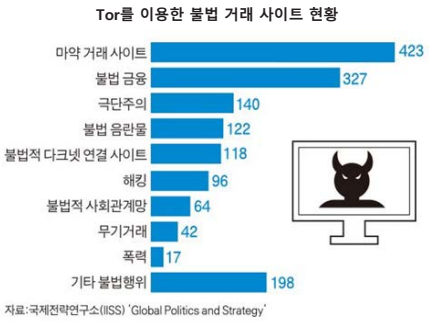



www.thedarkwebsites.com

# 다크웹 개요

**다크웹 내의 불법 사이트의 증가와 거래 비중의 급격한 증가**

- 2016년 기준 마약 거래 사이트가 약 450개, 불법금융 350개, 포르노 150개 등 순으로 이루어져 있음 (조사기관마다 일부 상이)
- 2016년 기준 다크웹에서 미국의 한 달간 마약 거래 금액은 약 57억원이며 판매자는 약 890명으로 이루어져 있음
- 익명네트워크 (e.g., Tor) 이용자 수가 200만명을 넘어서며 향후에도 꾸준히 다크웹을 통한 불법적인 거래가 지속적으로 확대 예상



# 다크웹과 암호화폐

**다크웹 불법사이트**

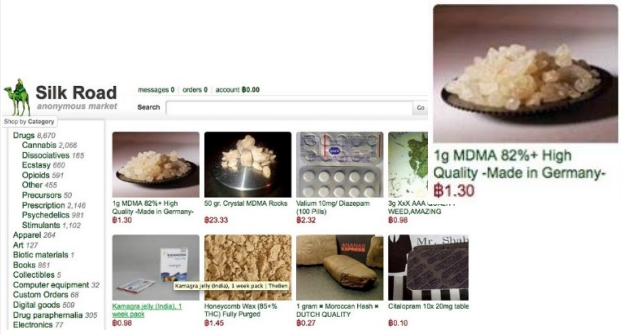
- 다크웹 불법사이트의 급격한 증가와 거래 비중의 증가
- 암호화폐(e.g., 비트코인)를 통한 불법 거래 증가

**범죄 정보 식별**

- 네트워크 익명화(e.g., Tor 등)에 따른 IP 추적의 어려움
- 다크웹 및 암호화폐 익명화에 따른 범죄자 정보 식별의 어려움

**암호화폐 거래 분석**

- 암호화폐 주소(wallet address)간 상관도(clustering) 분석의 어려움
- 암호화폐 거래 (transaction) 믹싱으로 인한 거래 추적의 어려움
- 불법 자금세탁으로 활용



# 연구 목표

- 다크웹 내 범죄 사이트 도메인 및 콘텐츠 색인 기술
- 범죄에 사용된 암호화폐(비트코인 등) 분석 기술
- 다크웹 이용 범죄자 프로파일링 기술

**다크웹 도메인/ 콘텐츠 색인**

- 다크웹 콘텐츠 크롤링용 웹로봇 개발 (한국어 콘텐츠)
- 다크웹 운용 서버 정보 분석 기술 개발
- 캐싱한 사이트 이미지 파일로 보관하는 기술 개발

**암호화폐 거래 분석 및 추적**

- 암호화폐(e.g., Bitcoin) 계좌 주소 클러스터링(clustering) 기술
- 믹싱서비스 분석 및 거래추적(de-mixing) 기술

**범죄활동 내역 수집 및 프로파일링**

- Tor 익명네트워크 내 다크웹 서버 및 사용자 IP 추적
- 범죄사이트 웹 분석 및 웹 범죄 정보 연동에 따른 범죄자 프로파일링 기술 개발

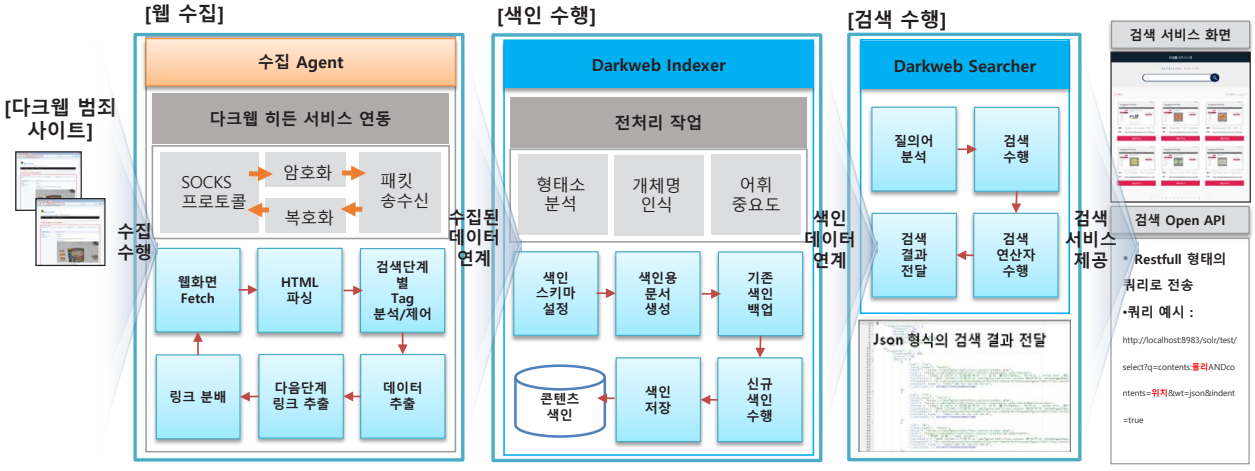
# 다크웹 분석 및 프로파일링 (국내를 중심으로)



## 다크웹 분석

### 다크웹 내 범죄 사이트 도메인 및 콘텐츠 수집/ 색인 / 검색 시스템

- 익명화 다크웹 콘텐츠 크롤링용 웹로봇 개발
  - 다크웹 히든 서비스 연동을 통한 **다크웹 범죄 사이트 수집**
  - 수집된 데이터를 이용한 **범죄 정보 색인 수행**
  - 색인 정보를 이용한 **검색 서비스 제공**



# 다크웹 범죄 사이트 유형 및 접근 패턴 분석

- 다크웹 범죄 사이트 유형 분석 및 접근 패턴 연구
  - 사이트 유형별 분류 및 인증 필요 및 URL 노출 패턴 분석
  - 초기 수집 대상 선정을 위한 접근 패턴 연구

## 사이트 유형별 분류

· 논문 및 관련 기사, 수집 결과 분석 등을 통하여 연구 수행

| Category | Websites |
|---|---|
| None | 3,503 |
| Drugs | 423 |
| Finance | 327 |
| Other illicit | 198 |
| Unknown | 155 |
| Extremism | 140 |
| Porno | 122 |
| Nexus | 118 |
| Hacking | 96 |
| Social | 64 |
| Arms | 42 |
| Violence | 17 |
| Total | 5,205 |
| Total active | 2,723 |
| Total illicit | 1,547 |

※ Cryptopolitik and the Darknet (Daniel Moore/Thomas Rid)

## 사이트 URL 노출 패턴 예시

· 약 300여 개이상의 다크웹 사이트들을 패턴을 분석하여 연구 수행

| 패턴 | 분류 | 패턴 |
|---|---|---|
| 인증 불필요 | Case1-1 (약 85%) | HTML 코드 상에서 URL 단순 노출 -> URL 판별 후 추출 |
| | Case1-2 (약 10%) | HTML 코드 상에서 Java Script 함수 URL 노출 -> JavaScript 렌더링 후 추출 |
| | Case1-3 (약 5%) | HTML 코드 상에서 URL이 암호화 되어 노출 -> 화면 렌더링 후 추출 |
| 인증 필요 | Case2-1 (약 40%) | 회원가입 패턴 -> 반자동 로그인 기능 지원 수집 활용 |
| | Case2-2 (약 60%) | 회원가입 + 회원자격 요건 충족 패턴(captcha) -> 인증 기능 지원 수집 활용 |

## 초기 수집 대상 선정 방식

| 접근 패턴 | 설명 |
|---|---|
| 히든위키 사이트 | 히든위키, 다크웹 광고 사이트에서 홍보되고 있는 범죄 사이트들을 수집하여 초기 수집에 사용 |
| 다크웹 광고 사이트 | |
| 다크웹 검색 사이트 | 다크웹 검색 사이트에서 검색되는 범죄 사이트들을 수집하여 초기 수집에 사용 |
| 수집 중 발견되는 링크 사이트 | 수집기를 통하여 발견되는 신규 사이트들을 수집하여 추가 수집 수행 |

[로그인 전 예시]

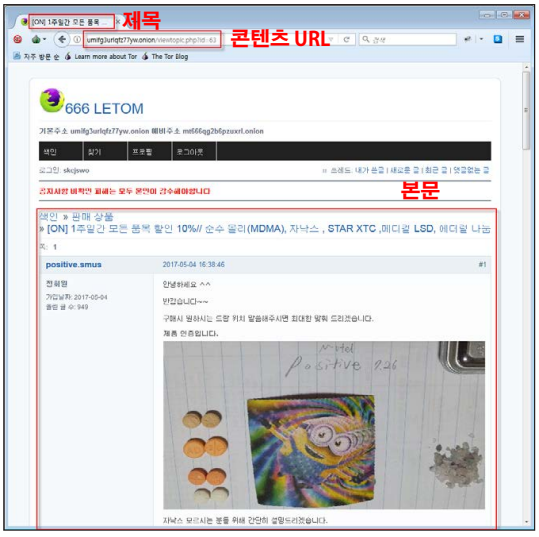
[로그인 후 예시]

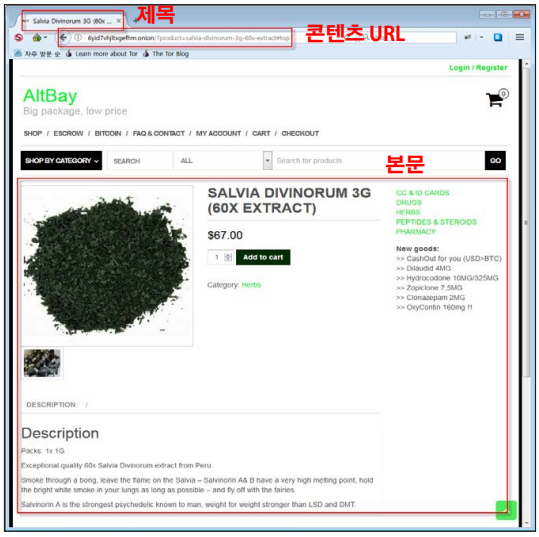
[히든위키 사이트 예시]

# 다크웹 범죄 사이트 유형 및 접근 패턴 분석

- 다크웹 범죄 사이트 유형 분석 및 접근 패턴 연구 – 콘텐츠 게시 패턴 분석
  - ➔ 콘텐츠 URL, 제목, 본문 등(기존 다크웹 검색 사이트 벤치마킹) 대상 정보 수집 (최종 3000여개 사이트 커버)

[사이트 콘텐츠 게시 패턴]

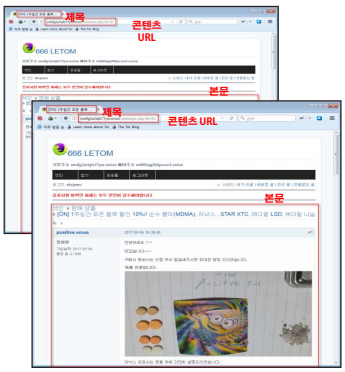


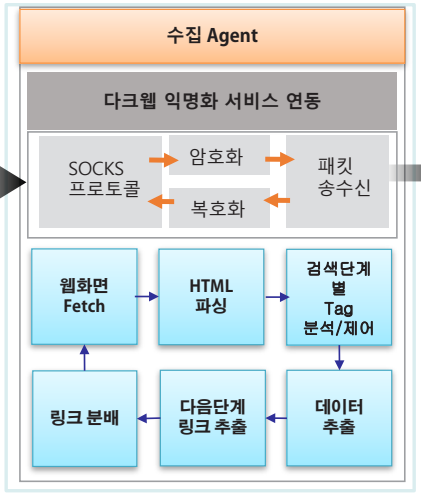
# 다크웹 수집 프로세스

- 다크웹 익명화 서비스 연동을 통한 다크웹 범죄 정보 Fetch
- Fetch 한 HTML 코드 파싱 후 내용 추출하여 저장
- 신규 추출한 URL을 재 수집 수행

[다크웹 범죄 정보]

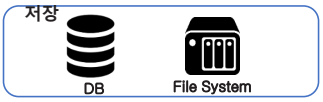



[웹 수집]




[내용 추출]

| | |
|---|---|
| 제목 | 1주일간 모든 품목 할인 10% 순수 몰리(DBMA) ... |
| 본문 | 안녕하세요. 구매시 원하는 드랍 위치를 말씀해 ... |
| URL | http://umlfg3urlqfz77yw.onion/viewtopic.php?id=63 |
| ... | ... |

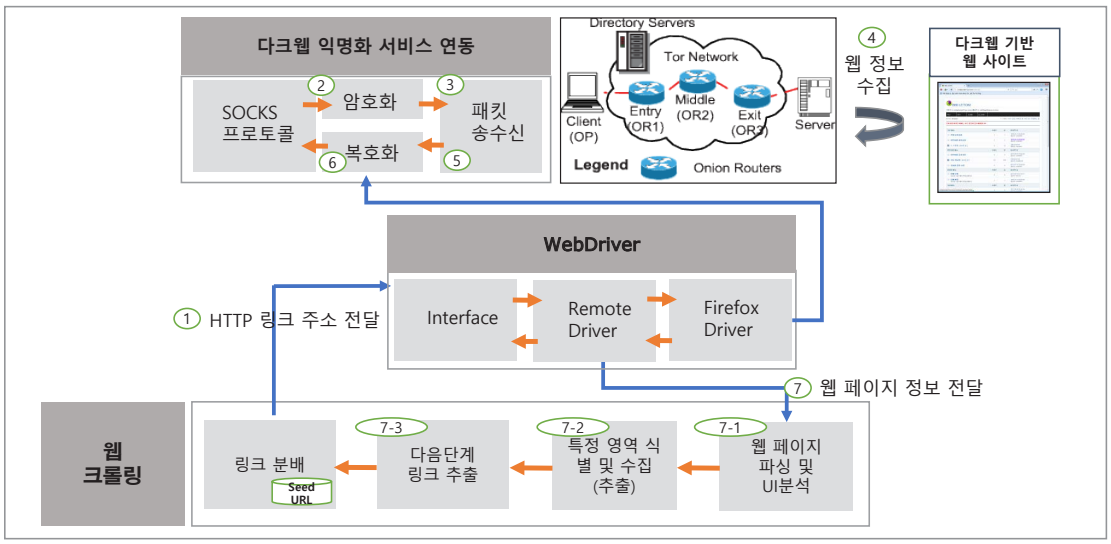





# 다크웹 수집 프로세스

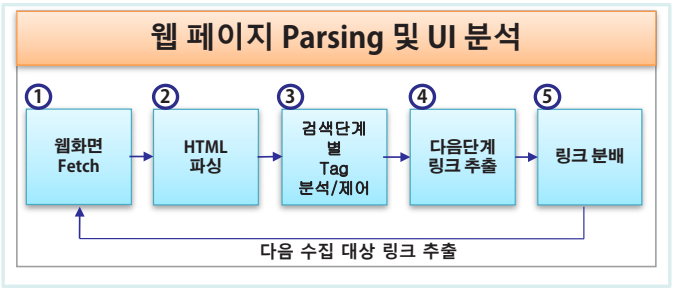
- 익명 네트워크 (Tor) 연동과정

→ Tor Network망에서 **Web Driver(Firefox)**를 이용하여 **익명화 서비스의 프로토콜/패킷 복호화** 수행

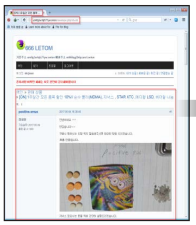


# 다크웹 페이지 파싱 (Parsing) 및 UI 분석

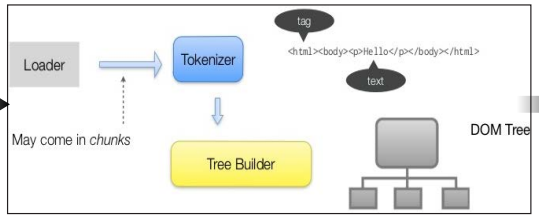
- 웹 화면 분석 후 웹 수집기를 이용하여 다크웹 사이트 화면을 렌더링, HTML 및 태그 정보 수집
- 웹 소스 분석을 위해 HTML 파싱 및 검색 단계 별 Tag 분석/제어 수행
  (Tokenizing 및 Tree Builder를 활용하여 HTML 파싱 및 검색 단계별 Tag 분석)
- DOM Tree 및 웹 페이지 UI를 자동 분석하여 콘텐츠 게시정보 및 신규 URL 링크를 추출




[웹화면 Fetch]



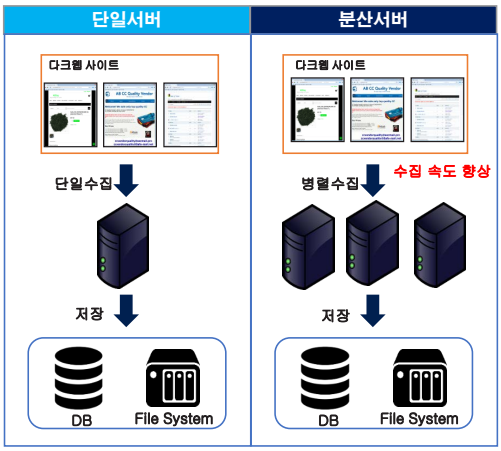
[HTML 파싱 및 Tag 분석]

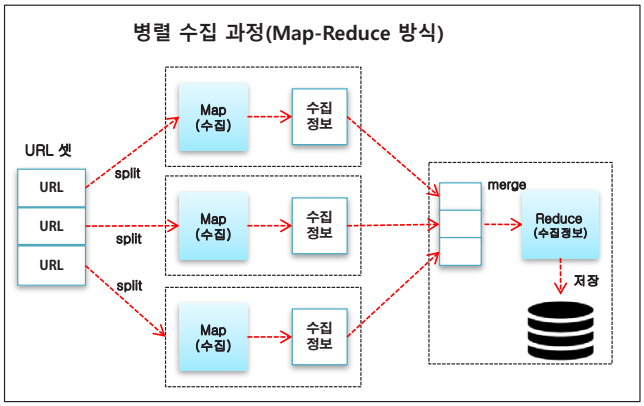



[신규 링크 URL 추출]

# 다크웹 사이트 병렬 수집

- 분산서버 기반으로 수집 수행
- 다크웹 내 범죄사이트 도메인/콘텐츠 수집 시스템에서 병렬수집 관리 수행
- 단일 서버들이 각자 대상 URL을 나눠서 수집 후 게시정보를 Merge하여 저장
- 수집 속도 및 안정성 개선

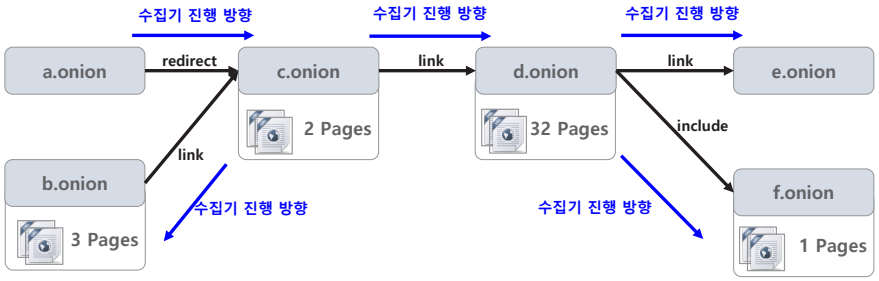


# 다크웹 사이트 이미지 변환

## 다크웹 사이트 히스토리 관리/저장 및 웹 화면 이미지 변환 기술

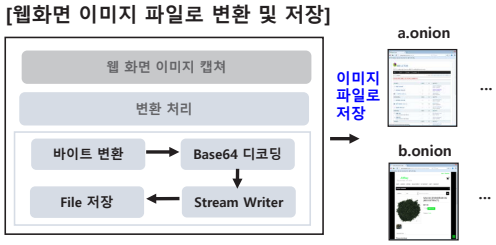
- **수집한 다크웹 사이트**들에 대하여 **DB에 저장 관리**
- 수집한 대상 **사이트 웹 화면**을 **이미지 파일**로 **변환**하여 File System에 **저장**




[방문 사이트 히스토리 관리 DB]

| 접근 사이트 | 사이트의 페이지 URL |
|---|---|
| a.onion | a.onion |
| b.onion | b.onion/1page, b.onion/2page, b.onion/3page |
| c.onion | c.onion/1page, c.onion/2page |
| d.onion | d.onion/1page ~ d.onion/32page |
| e.onion | e.onion |
| f.onion | f.onion/1page |

[웹화면 이미지 파일로 변환 및 저장]




# 다크웹 데이터 분석

## 다크웹 내 범죄 사이트 도메인 수집 현황

- 다크웹 수집기간: 2017. 7. ~ 10. (4개월)
- 다크웹 내 범죄 사이트 1,000개 수집 (총 페이지 수: 89,116 / 데이터 총량: 71GB)
- 전체 사이트의 Page 수집율 82%, 접속 가능한 한국어 사이트 8개 수집

### 다크웹 수집 건수 결과

· 카테고리 별 사이트 개수

| Category | 사이트 개수 |
|---|---|
| None | 68 |
| Drugs | **150** |
| Finance | **323** |
| Other illicit | 110 |
| Unknown | 41 |
| Extremism | 6 |
| Porno | 111 |
| Hacking | 67 |
| Social | 4 |
| Arms | 19 |
| Violence | 18 |
| Gambling | 38 |
| Community | 45 |
| **Total** | **1,000** |

· 수집한 1,000개 사이트의 결과 예시

| 전체 사이트 별 페이지 개수 비교를 통한 Page 수집율 현황 | | | | | |
|---|---|---|---|---|---|
| ID | 사이트 명 | Category | 전체 Page 개수 | 수집한 Page 개수 | Page 수집율 |
| 1 | [redacted] | Porno | 49건 | 41건 | 84% |
| 2 | | Finance | 13건 | 11건 | 85% |
| 3 | | Drugs | 5건 | 4건 | 80% |
| 4 | | Gambling | 377건 | 311건 | 82% |
| 5 | | Drugs | 74건 | 62건 | 84% |
| 6 | | Arms | 5건 | 4건 | 80% |
| 7 | | Hacking | 17건 | 13건 | 76% |
| 8 | | Unknown | 6건 | 54건 | 84% |
| 9 | | Porno | 602건 | 502건 | 83% |
| 10 | | Violence | 18건 | 14건 | 78% |
| .. | | ... | ... | ... | ... |
| 1000 | | Finance | 22건 | 18건 | 82% |
| 전체 1,000개 사이트 수집율 평균 | | | | | 82% |

· 한국어 사이트 별 수집율 결과

| 한국어 사이트 페이지 개수 비교를 통한 수집율 현황 | | | | |
|---|---|---|---|---|
| ID | 사이트 명 | 전체 Page 개수 | 수집한 Page 개수 | 수집율 |
| 1 | [redacted] | 1,675건 | 1,341건* | 80% |
| 2 | | 514건 | 334건 | 65% |
| 3 | | 1건 | 1건 | 100% |
| 4 | | 58건 | 47건 | 81% |
| 5 | | 483건 | 382건 | 79% |
| 6 | | 2,321건 | 1,841건 | 79% |
| 7 | | 43건 | 36건** | 84% |
| 8 | | 74건 | 67건 | 91% |
| 한국어 사이트 수집율 평균 | | | | 82% |

※ * 와 ** 의 경우 로그인 전 사이트 기준으로 수집율 측정 (인증 + 로그인 이전)

※ 다크웹 환경 자체가 접속 불안정, 서비스 중지, 일시적인 페이지 소멸 등 수시로 발생 가능

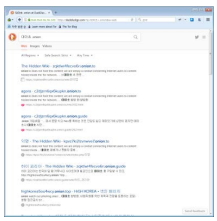
# 다크웹 데이터 분석

## 다크웹 내 범죄 한국어 사이트 재현율 측정

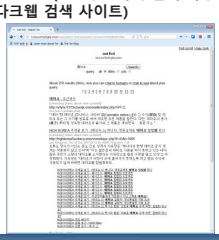
- 키워드 검색을 통한 다크웹 내 범죄 한국어 사이트 재현율 측정
  - **서비스 중인** 한국어 검색 가능한 **다크웹 검색 사이트**와 **검색 결과 상호 비교**를 통한 **재현율 측정**
  - 현재 접속 가능한 한국어 사이트 여부를 고려하여 재현율 측정
  - **한국어 사이트 검색 재현율 80% 이상 확보**

### 한국어 사이트 재현율 측정 절차

· 더덕고 (Tor 대표 검색 사이트)



· not Evil (Tor내 한국어 검색 가능한 다크웹 검색 사이트)



### 키워드 검색을 통한 한국어 사이트 재현율

| 검색 결과 비교를 통한 재현율 현황 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| No | 검색어 | 다크웹 검색 시스템 | 한국어 지원 검색 서비스 사이트 별 검색 건수 | | | | | |
| | | | 더덕고 | | | Not Evil | | |
| | | | 전체 건수 | 실패 건수 | 검색 재현율 | 전체 건수 | 실패 건수 | 검색 재현율 |
| 1 | 마약 | 626건 | 9건 | 1건 | 89% | 179건 | 33건 | 82% |
| 2 | 코카인 | 85건 | 7건 | 2건 | 71% | 31건 | 8건 | 74% |
| 3 | 대마초 | 702건 | 19건 | 3건 | 84% | 224건 | 26건 | 88% |
| 4 | 헤로인 | 62건 | 8건 | 1건 | 88% | 31건 | 9건 | 71% |
| 5 | 비트코인 | 596건 | 7건 | 2건 | 71% | 452건 | 9건 | 98% |
| 6 | 살인 | 340건 | 13건 | 3건 | 77% | 89건 | 24건 | 73% |
| 7 | 도박 | 145건 | 5건 | 2건 | 60% | 40건 | 11건 | 73% |
| 8 | 음란물 | 121건 | 13건 | 1건 | 92% | 53건 | 1건 | 98% |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 100 | 폭탄 | 127건 | 13건 | 1건 | 92% | 82건 | 22건 | 73% |
| 재현율 평균 | | | | | 82% | | | 81% |

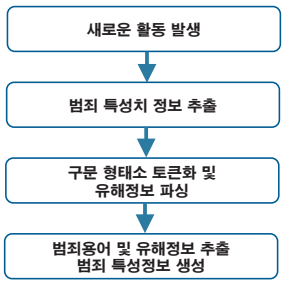
# 프로파일링

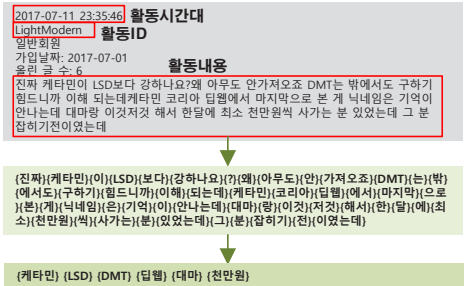
## 다크웹 범죄자 프로파일링 시스템 개발

### 연구 개발 내용

- Tor범죄와 연관된 '한영 복합 용어' 토큰화 기술 개발
- 유해 정보 파싱을 위한 **Tor 범죄사이트의 유해정보에 특화된 구문형태소 분석기** 개발
- 수학적 클러스터링 기반의 **범죄 특성 정보 추출 및 생성 기술** 개발
  (예: 분류되지 않은 행동정보에 대한 범죄영역 특성 정보 추출 및 분석 등)
- **행동 패턴 중심 프로파일링 기법**을 이용한 **범죄자 프로파일링 프로토타입 시스템** 개발

### 연구 개발 방법

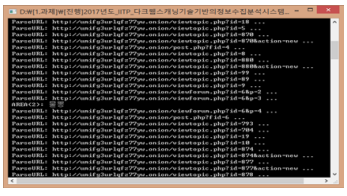


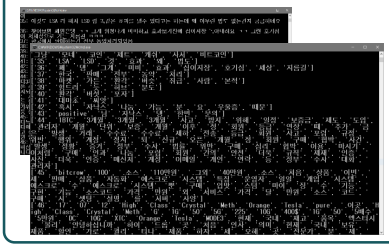

### 연구 개발 결과

- 다크웹 범죄자 프로파일링 모듈 DWCPA(DarkWeb Criminal Profile Analyzer)

- 범죄 특성치 정보 분석기



- 구문 형태소 분석기



# 프로파일링

## 다크웹 범죄 사이트별 기반 서비스 분석 기술 및 범죄자 프로파일링 기법 연구

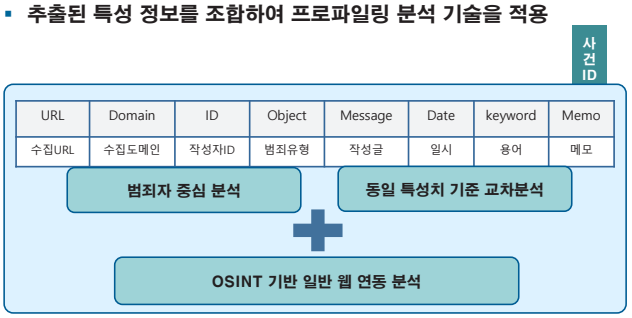
### 연구 개발 내용

- 현존하는 범죄 프로파일링 기법 및 사이버 범죄 프로파일링 기법 연구 (연역적/귀납적 범죄 프로파일링 방법, 수사심리학 프로파일링 방법, 행동증거분석 프로파일링 방법, OSINT, 사례추론기법을 이용한 프로파일링 방법)
- **행동 패턴 중심 프로파일링 기법** 연구
  (행동패턴 타입: 활동시간대, 범죄용어 등)
  - **범죄자 정보 중심 분석 기술** 연구
    - 범죄자의 범죄용어, 활동시간대, 활동사이트, 활동범죄영역, 상세활동 내용 분석
  - **동일 특성치에 대한 교차 분석 기술** 연구
    - 활동시간대 기준 교차분석 : 사이트별, 범죄영역별 활동시간대 분석
    - 범죄용어 기준 교차분석 : 사이트별, 범죄영역별, 활동시간대별 범죄용어 분석
- **일반웹 연동 분석을 통해서 (OSINT 기반) 수사관의 경험 및 노하우를 반영할 수 있는 프로파일링 기술** 연구 개발

※OSINT (Open Source Intelligence) : 공개출처정보

### 연구 개발 방법

- 추출된 특성 정보를 조합하여 프로파일링 분석 기술을 적용




### 연구 개발 결과

# 시스템 데모

1. 다크웹 자동 모니터링 시스템
2. 국내 다크웹 사용자 프로파일링 분석

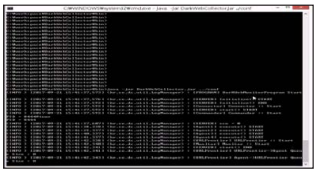
# 다크웹 자동 모니터링 시스템 데모

## 다크웹 자동 수집과정

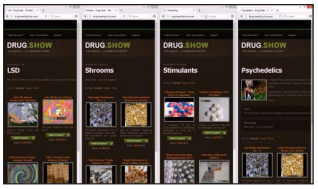
- 다크웹 내 범죄 사이트 도메인/콘텐츠 수집기
- 다크웹 내 범죄 사이트 도메인/콘텐츠 색인
- 다크웹 내 범죄 사이트 도메인/콘텐츠 검색 웹 UI

### 수집 수행 예시

· 수집기 시작 화면



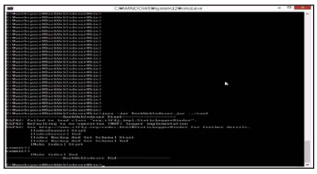
· 병렬 수집 과정 화면



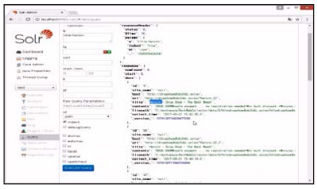

수집된 데이터 연계 (DB)

### 색인 수행 예시

· 색인 시작 화면



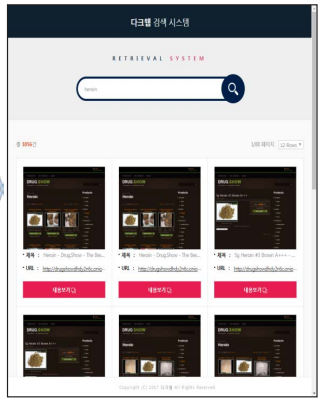
· 색인 결과 조회 화면




색인 데이터 연계 (Open API 검색)

### 검색 수행 예시

· 웹 UI 검색 화면




# 다크웹 범죄자 프로파일링 데모

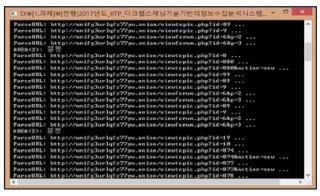
## 다크웹 범죄자 프로파일링 과정

- 다크웹 내 수집 콘텐츠의 범죄 특성치 정보 파싱 처리기
- 다크웹 내 범죄용어/유해정보의 추출 및 분석
- 다크웹 내 범죄자 행동 중심 프로파일링

### 범죄 특성치 정보 파싱 예시

다크웹(한국어) 수집 데이터 연계(DB)

· 범죄 특성치 정보 파싱 화면

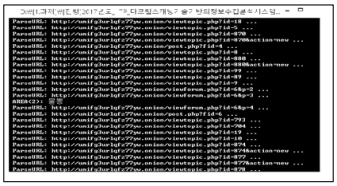


파싱 데이터 연계 (DB&File)

### 범죄용어 및 유해정보 추출 예시

· 구문 형태소 분석 화면

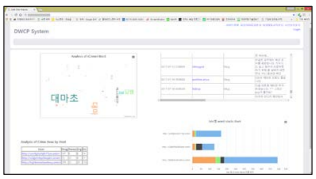
· 범죄용어 및 유해정보 추출 화면



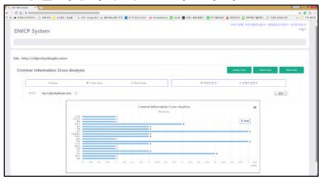
분석 데이터 연계 (DB)

### 행동 중심 프로파일링 예시

· 범죄자 정보 중심 분석 화면



· 동일 특성치에 대한 교차분석 화면

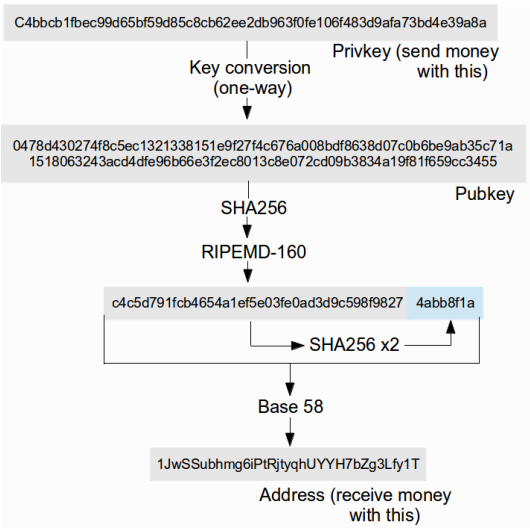


# 불법 암호화폐(비트코인) 거래분석

1. Clustering
2. De-mixing

## Clustering

### 개인 · 공개키 및 비트코인 주소 간의 관계




- ECDSA signature
  - private key : 32 bytes
- SHA256 * 2
  - 결과값의 MSB 4 bytes 추가

# Clustering

## 비트코인 주소

- 해쉬함수와 인코딩을 통해 생성된 주소를 가명(Pseudonym)으로 활용
- Shadow address
  - 자동으로 생성되어 사용자가 발급 한 거래로 인해 발생하는 " 잔액"을 회수하는 데 사용
  - 사용자의 개인 정보를 강화하기 위해 Bitcoin에서 채택한 메커니즘

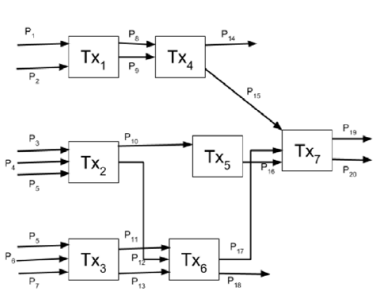
- 출력 주소중 하나는 “Shadow address”
- 개인키로 서명하여 계좌의 소유권을 증명

- 매 거래 시 Shadow address를 생성하기 때문에 한 사람이 많은 비트코인 주소를 관리

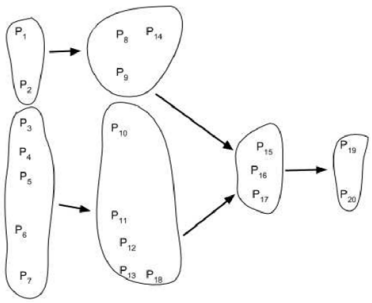
# Clustering

## 클러스터링

- 블록체인에 있는 모든 트랜잭션의 입력과 출력을 분석하여 비트코인 주소를 지갑단위로 분류




Transaction graph



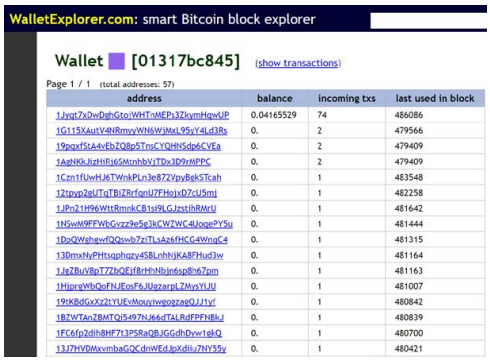
Entity/User graph

- 비트코인 자금 흐름 파악에 활용

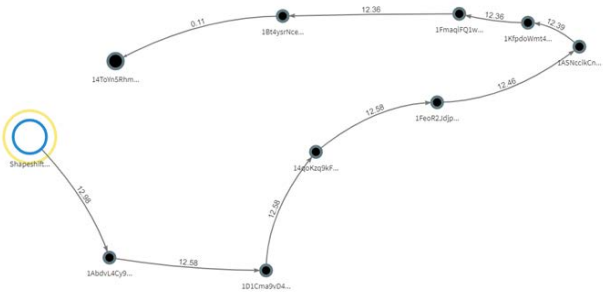
# Clustering

## 클러스터링 툴 목록

- **Elliptic** - https://www.elliptic.co/
- **Blockseer** - https://www.blockseer.com/
- **Chainalysis** - https://www.chainalysis.com/
- **Numisight** - http://numisight.com/
- **Ciphertrace** - https://ciphertrace.com/
- **Bitfury** - http://bitfury.com/




<WalletExplorer>



<Chainalysis>

# Clustering

## 클러스터링 알고리즘

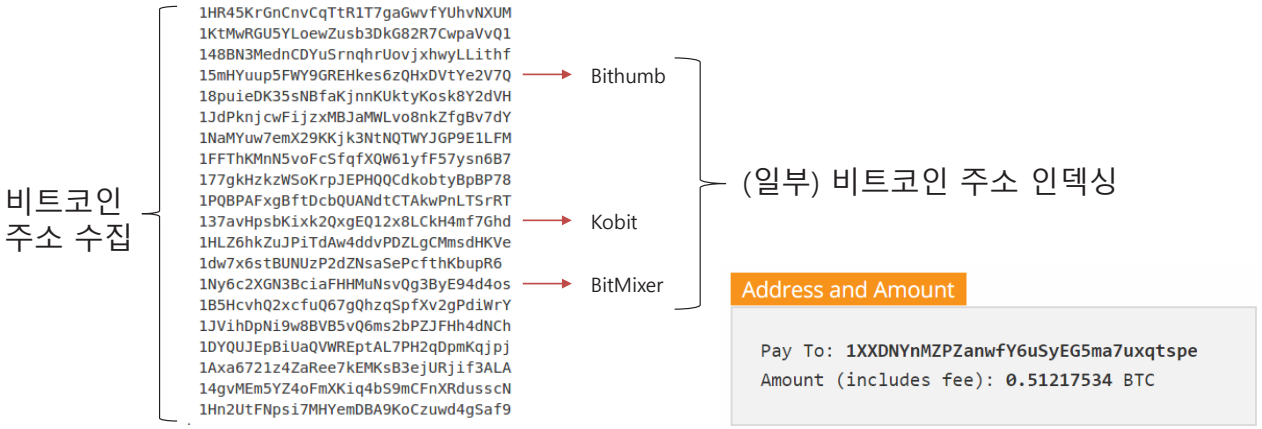
- Step 1. Data collection
- Step 2. Address clustering

References
[1] Evaluating User Privacy in Bitcoin (FC'13)
[2] A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (IMC'13)
[3] Bitlodine: Extracting Intelligence from the Bitcoin Network (FC'14)
[4] Bitconeview: visualization of flows in the bitcoin transaction graph (VIZSEC'15)

# Clustering

## Step 1. Data collection

- 분석대상 주소 분류를 위한 공개 정보 수집
  - 공개된 비트코인 주소 수집 (다양한 웹사이트 포럼 등)
    - ex) 비트코인 믹싱 서비스에서 주소 “1XXDNYnMZPZanwfY6uSyEG5ma7uxqtspe” 를 공개한 경우 해당 주소는 믹싱 서비스의 주소로 인덱싱




# Clustering

## Step 2. Address clustering

- Heuristic 알고리즘을 이용하여 주소를 클러스터링
  - **Heuristic I—Multi-input Transactions**
  - **Heuristic II— “Shadow” Addresses**
  - **Heuristic II— False positives reduction**
  - **Heuristic II— Performance improvement**

- 클러스터링한 주소들을 하나의 지갑(wallet)으로 매핑
  - 지갑에 인덱스가 있는 주소가 있을 경우 지갑을 해당 인덱스로 분류

# Clustering

## Heuristic I—Multi-input Transactions

- 단일 트랜잭션 주소를 동일한 사람의 지갑으로 클러스터링
  - 현재 비트코인 클라이언트의 경우 다수 사용자들 간의 단일 트랜잭션 생성을 미지원

→ 동일한 사람의 wallet에 클러스터링 되는 주소

[1] Evaluating User Privacy in Bitcoin (FC'13)

# Clustering

## Heuristic II— "Shadow" Addresses

- Shadow address 클러스터링
  - 비트코인 사용자들은 하나의 트랜잭션으로 두 명 이상의 사용자에게 코인을 전송하는 경우가 적음
  - 2개의 출력 주소 중 하나가 이전 거래 기록이 없다면, Shadow address일 확률 증가 → Shadow address는 같은 wallet으로 클러스터링

[1] Evaluating User Privacy in Bitcoin (FC'13)

# Clustering

## Heuristic II— Reduce false positives

- False positives 분석 결과 대부분이 Satoshi Dice(도박 사이트) 등과 연관 있다는 것을 보임
- Satoshi Dice와 관련된 트랜잭션은 전부 무시
  - False positives 1%대로 감소

[2] A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (IMC'13)

# Clustering

## Heuristic II— Performance improvements

- 2013년까지의 데이터는 구현 취약점으로 인해 "Shadow address" 판정률을 비약적으로 높일 수 있음을 보임
  - 출력 주소가 2개일때, GetRandInt() 함수는 항상 0을 return

  - 현재는 적용 불가

[3] Bitlodine: Extracting Intelligence from the Bitcoin Network (FC'14)

# Clustering

## Step 2. Address clustering

1HR45KrGnCnvCqTtR1T7gaGwvfYUhvNXUM
1KtMwRGU5YLoewZusb3DkG82R7CwpaVvQ1
148BN3MednCDYuSrnqhrUovjxhwyLLithf
15mHYuup5FWY9GREHkes6zQHxDVtYe2V7Q → Bithumb
18puieDK35sNBfaKjnnKUktyKosk8Y2dVH
1JdPknjcwFijzxMBJaMWLvo8nkZfgBv7dY
1NaMYuw7emX29KKjk3NtNQTWYJGP9E1LFM

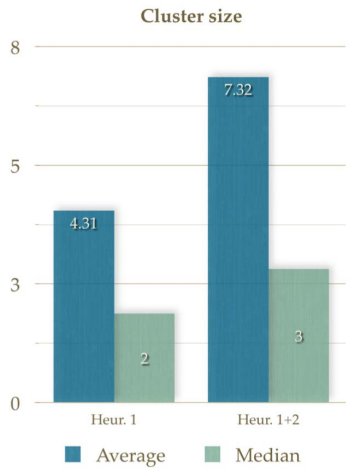
1FFThKMnN5voFcSfqfXQW61yfF57ysn6B7
177gkHzkzWSoKrpJEPHQQCdkobtyBpBP78
1PQBPAFxgBftDcbQUANdtCTAkwPnLTSrRT
137avHpsbKixk2QxgEQ12x8LCkH4mf7Ghd → Kobit
1HLZ6hkZuJPiTdAw4ddvPDZLgCMmsdHKVe
1dw7x6stBUNUzP2dZNsaSePcfthKbupR6

1Ny6c2XGN3BciaFHHMuNsvQg3ByE94d4os → BitMixer
1B5HcvhQ2xcfuQ67gQhzqSpfXv2gPdiWrY
1JVihDpNi9w8BVB5vQ6ms2bPZJFHh4dNCh

1DYQUJEpBiUaQVWREptAL7PH2qDpmKqjpj
1Axa6721z4ZaRee7kEMKsB3ejURjif3ALA
14gvMEm5YZ4oFmXKiq4bS9mCFnXRdusscN
1Hn2UtFNpsi7MHYemDBA9KoCzuwd4gSaf9

Wallet - c9cb18c6ed

→ 클러스터링 결과




→ 평균 7.32개의 주소가 하나의 지갑으로 클러스터링

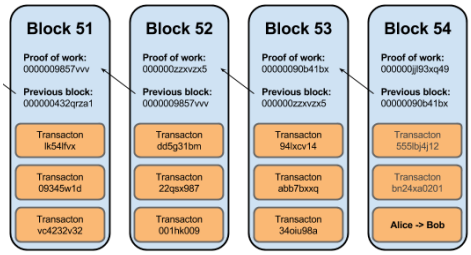
[3] Bitlodine: Extracting Intelligence from the Bitcoin Network (FC'14)

# De-mixing

## 비트코인 익명성

- 비트코인의 익명성
  - 해쉬함수와 인코딩을 통해 생성된 가명(Pseudonym)을 이용
  - 거래마다 새로운 주소(Shadow address)를 생성

- 익명성의 한계
  1. 트랜잭션 분석
     - 블록체인 트랜잭션의 투명성 => 거래 분석
  2. 중개거래소
     - 비트코인 거래를 위한 중개거래서 이용 시 휴대폰, 계좌 등 인증 절차 요구




coinone bithumb KORBIT

# De-mixing

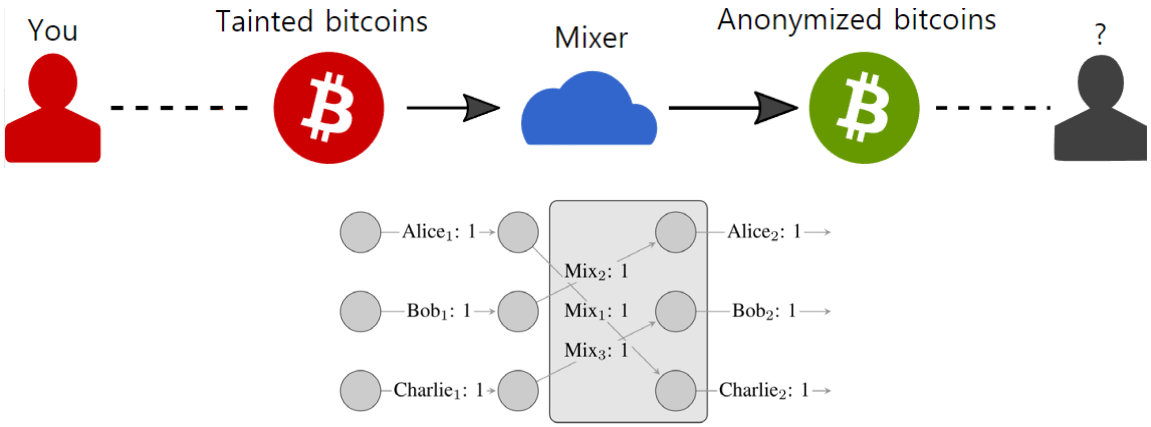
## 비트코인 익명성 분석 연구

- 비트코인 익명성 분석 연구
  - Deanonymisation of clients in Bitcoin P2P Network (ACM CCS'14)
    - 트랜잭션을 생성한 사용자의 IP 주소에 대한 유추 방안 연구
  - An Analysis of Anonymity in Bitcoin Using P2P Network Traffic (FC'14)
    - 5개월 동안 수집한 트랜잭션을 분석하여 비트코인 주소와 IP 데이터를 직접적으로 매핑
  - Bitcoin over Tor isn't a Good Idea (IEEE S&P'15)
    - Tor를 사용하는 bitcoin에 대한 user finger printing 가능성에 대한 연구

→ 부가 프로토콜을 활용한 익명성 확보의 필요성

# De-mixing

## 비트코인 믹싱 서비스




- Mixer를 통한 다수의 bitcoin shuffling service
- 입력과 출력 주소간의 상관관계를 감춤(unlinkability)으로써 익명성 강화
- 익명성은 참여자 수, 트랜잭션 수 등에 비례

# De-mixing

## 비트코인 믹싱 서비스 파라미터

1. 출력 주소 (forward address) 분할 (일부 서비스의 경우 최소 2개로 강제)
2. 지연 시간 (0~99h 범위에서 자유롭게 설정)
3. 수수료 (범위 내에서 랜덤하게 설정)

- 믹싱 서비스 거래정보에 대해 파라미터 분석을 통한 분석 가능성

Ex)

| Time | Type | Value | Unique transaction ID |
|---|---|---|---|
| 2013-06-24 15:56 | In | 0.332211 | 6078f4779354d3cd8902be6703c0f5bb2b13417f43c60e62ed0f6375acd66a09 |

- ✓ Time : 2013년 06월, 24일 3시 56분 ~ 25일 3시 56분
- ✓ Amount : 0.325566 BTC ~ 0.328888 BTC [n개의 출력의 합 (n = 분할한 주소 수)]

# De-mixing

## 비트코인 믹싱 서비스 이용현황 분석결과

| Mixing service | Url | Minimal deposit | Mixing service fee | Delay | Max_output_address |
|---|---|---|---|---|---|
| *CoinMixer* | coinmixibh45abn7.onion/ | 0.001 | 1 - 3% | ~120h | 5 |
| *BitcoinBlender* | bitblendervrfkzr.onion/ | 0.01 | 1 - 3% | ~99h | 10 |
| *CryptoMixer* | cryptomixns23scr.onion/ | 0.001 | 0.5 - 3% | ~48h | 10 |
| *BitMix* | bitmixbizymuphkc.onion/ | 0.01 | 0.4 - 4% | ~24h | 5 |
| *PrivCoin* | tr5ods7ncr6eznny.onion/ | 0.01 | 0.8 - 3.8% | ~24h | 10 |
| *Bitcoin Fog* | foggeddriztrcar2.onion/ | 0.005 | 1 - 3% | ~48h | 20 |
| *BitCloak* | bitcloak43blmhmn.onion/ | 0.015 | 1 - 3% | ~8h | 1 |
| *Bitcoin Mixer* | Bitcoin-mixer.org/ | 0.01 | 1.5% | ~24h | 10 |
| *Helix* | grams7eu3phkfrt3.onion/helix/ | 0.02 | 2.5% | ~24h | 5 |
| *Helix light* | grams7eu3phkfrt3.onion/helix/light/ | 0.02 | 2.5% | ~6h | 5 |

1. BitMixer.io
   – 발생 트랜잭션 수 17만개 → 하루 평균 350개
   – 기간 : 2016년 3월 ~ 2017년 7월 (현재 중단)
2. Helix Mixer
   – 발생 트랜잭션 수 84만개 → 하루 평균 910개 (가장 많은 사용자가 이용)
   – 기간 : 2015년 4월 ~ 현재

(Chainalysis를 이용한 분석 결과)

# De-mixing

## De-mixing 알고리즘

- Y. Hong, H. Kwon, J. Lee, J. Hur, "A practical de-mixing algorithm for Bitcoin mixing services", ACM Workshop on Blockchains, Cryptocurrencies and Contracts (BCC'18), 2018. 6. 4.

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

1. 필터링 단계
   - 거래 시간 필터링
   - 비트코인 값 필터링
2. Combination 계산 단계
3. Combination 선택 단계
4. 매칭 거래 제거 단계
   - 입력 제거 단계
   - 출력 제거 단계
   - 알고리즘 반복
5. 비매칭 거래 처리 단계

# De-mixing

## De-mixing 알고리즘 – 믹싱 서비스 입출력 거래 수집 (예제)

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| Input | 6/4 1:11 | 0.02772853 |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:14 | 0.03362579 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 19:49 | 0.32639444 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

# De-mixing

## De-mixing 알고리즘 – input 선택

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| **Input** | **6/4 1:11** | **0.02772853** |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

→ **첫번째 input 선택**

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| **Output** | **6/3 1:50** | **0.05172631** |
| **Output** | **6/4 0:27** | **0.00434362** |
| **Output** | **6/4 11:48** | **0.01081412** |
| **Output** | **6/4 16:14** | **0.03362579** |
| **Output** | **6/4 16:42** | **0.01359976** |
| **Output** | **6/4 19:49** | **0.32639444** |
| **Output** | **6/4 20:7** | **0.0108682** |
| **Output** | **6/4 20:39** | **0.00535299** |
| **Output** | **6/5 3:31** | **0.04358188** |
| **Output** | **6/5 7:17** | **0.10169106** |

# De-mixing

## De-mixing 알고리즘 - 필터링

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| **Input** | **6/4 1:11** | **0.02772853** |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| **Output** | **6/4 11:48** | **0.01081412** |
| Output | 6/4 16:14 | 0.03362579 |
| **Output** | **6/4 16:42** | **0.01359976** |
| Output | 6/4 19:49 | 0.32639444 |
| **Output** | **6/4 20:7** | **0.0108682** |
| **Output** | **6/4 20:39** | **0.00535299** |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

→ **입력에 대한 출력 시간**(delay), **비트코인 값**(mixing service fee)**을 기준으로 연관성 없는 출력 거래 제거**

# De-mixing

## De-mixing 알고리즘 – Combination 계산

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to *Result* set.
4: If the size of the *Result* set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the *Result* set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| Input | 6/4 1:11 | 0.02772853 |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:14 | 0.03362579 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 19:49 | 0.32639444 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

→ 조건을 만족하는 출력 거래들로 가능한 조합 (combination) 계산

# De-mixing

## De-mixing 알고리즘 – Combination 계산

1

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

2

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:39 | 0.00535299 |

3

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

4

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

→ 조건을 만족하는 출력 거래들로 가능한 조합 (combination) 계산

# De-mixing

## De-mixing 알고리즘 – Combination 선택

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| Input | 6/4 1:11 | 0.02772853 |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:14 | 0.03362579 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 19:49 | 0.32639444 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

→ 입력값으로 부터 매칭 가능한 조합 확인

# De-mixing

## De-mixing 알고리즘 – Combination 선택

1

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

2

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:39 | 0.00535299 |

3

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

4

| | | |
|---|---|---|
| Output | 6/4 11:48 | 0.01081412 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 20:7 | 0.0108682 |
| Output | 6/4 20:39 | 0.00535299 |

→ Only one case matched

→ 입력값으로 부터 매칭 가능한 조합 선택

# De-mixing

## De-mixing 알고리즘 – 매칭거래 제거

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to *Result* set.
4: If the size of the *Result* set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the *Result* set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| | | |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| | | |
| Output | 6/4 16:14 | 0.03362579 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 19:49 | 0.32639444 |
| | | |
| | | |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

→ 1개만 매칭 될 경우 (성공) 해당 입출력을 제거하고
다음 입력에 대해 모든 입출력이 제거될 때 까지 반복 수행

# De-mixing

## De-mixing 알고리즘 – 비매칭 거래 처리

**Algorithm** De-mixing

For $i$ = 1 to $N$, repeat the follow

1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i * (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to *Result* set.
4: If the size of the *Result* set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the *Result* set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

<믹싱 서비스 입력>

| Type | Time | Value |
|---|---|---|
| | | |
| Input | 6/4 1:21 | 0.3832 |
| Input | 6/4 4:56 | 0.14899789 |
| Input | 6/5 2:32 | 0.13676388 |

<믹싱 서비스 출력>

| Type | Time | Value |
|---|---|---|
| Output | 6/3 1:50 | 0.05172631 |
| Output | 6/4 0:27 | 0.00434362 |
| | | |
| Output | 6/4 16:14 | 0.03362579 |
| Output | 6/4 16:42 | 0.01359976 |
| Output | 6/4 19:49 | 0.32639444 |
| | | |
| | | |
| Output | 6/5 3:31 | 0.04358188 |
| Output | 6/5 7:17 | 0.10169106 |

→ 매칭되는 경우가 더 이상 존재하지 않는 경우 알고리즘 종료
(해당 입력에 대해 연결 가능한 다수의 출력 조합이 있는 경우)

# De-mixing

## 비매칭 거래 분석

<입력값이 같은 경우>

| | Type | Time | Value |
|---|---|---|---|
| $t_{A_1}$ | In | 2017-6-4 9:42 | 0.1 |
| $t_{A_2}$ | Out | 2017-6-4 14:20 | 0.05703751 |
| $t_{A_3}$ | Out | 2017-6-5 2:36 | 0.024375 |
| $t_{A_4}$ | Out | 2017-6-5 4:14 | 0.01608749 |
| $t_{B_1}$ | In | 2017-6-4 9:42 | 0.1 |
| $t_{B_2}$ | Out | 2017-6-4 23:43 | 0.07605 |
| $t_{B_3}$ | Out | 2017-6-5 0:40 | 0.02145 |

$$t_{A_2} + t_{A_3} + t_{A_4} = t_{B_2} + t_{B_3}$$

<출력 부분집합의 합이 같은 경우>

| | Type | Time | Value |
|---|---|---|---|
| $t_{C_1}$ | In | 2017-6-4 12:5 | 0.1 |
| $t_{C_2}$ | Out | 2017-6-4 14:38 | 0.03217499 |
| $t_{C_3}$ | Out | 2017-6-4 19:14 | 0.024375 |
| $t_{C_4}$ | Out | 2017-6-5 6:36 | 0.04095001 |
| $t_{D_1}$ | In | 2017-6-4 12:5 | 0.075 |
| $t_{D_2}$ | Out | 2017-6-4 14:16 | 0.03598892 |
| $t_{D_3}$ | Out | 2017-6-4 15:59 | 0.00501637 |
| $t_{D_4}$ | Out | 2017-6-4 22:58 | 0.00146249 |
| $t_{D_5}$ | Out | 2017-6-4 23:25 | 0.03065722 |

$$t_{C_2} + t_{C_4} = t_{D_2} + t_{D_3} + t_{D_4} + t_{D_5}$$

- Delay 범위 안에 위 경우와 같은 입출력이 존재할 경우 알고리즘을 반복해도 입력에 대해 유일한 출력 조합을 결정할 수 없음 (indeterministic)
- 1 BTC 단위가 크기 때문에 실제 환경에서는 흔히 발생하지 않으며, 믹싱 입력과 연결 가능한(linkable) 조합의 경우의 수를 크게 줄일 수 있음

# De-mixing

## Helix 믹싱 서비스에 대한 De-mixing 실험 과정

1 CHAINALYSIS → 클러스터링 툴(Chainalysis)을 이용하여 Helix 믹싱 서비스의 실제 입력 데이터를 추출

2

| Mixing service | Url | Minimal deposit | Mixing service fee | Delay | Max_output_address |
|---|---|---|---|---|---|
| *Helix* | grams7eu3phkfrt3.onion/helix/ | 0.02 | 2.5% | ~24h | 5 |

→ 분석한 파라미터 (Fee, Delay, Max_output_address)를 적용하여 Output 데이터 생성

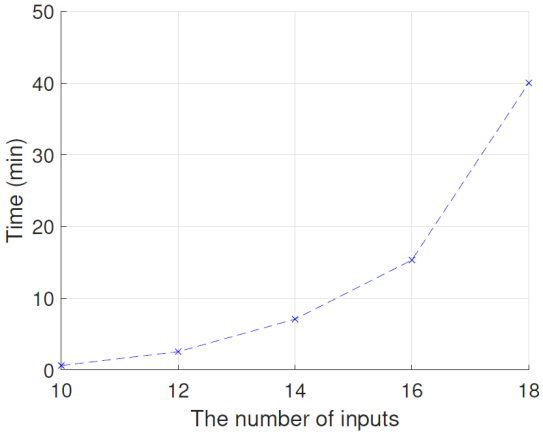
3

**Algorithm** De-mixing.
For $I$ = 1 to N, repeat the follow
1: $OUTPUT'$ ← Extract the output set satisfying the following conditions.
(1) The time range is between $Input_i.time$ and $Input_i.time$ + $Max\_delay$.
(2) The Bitcoin value is less than $Input_i.value$.
2: $OUTPUT_{subset}$ ← Stores all combinations in $OUTPUT'$ that can be made up to $Max\_out$ or less.
3: Compare the Bitcoin values of the $input_i \times (1 - fee)$ and each $OUTPUT_{subset}$. If the values are the same, add to $Result$ set.
4: If the size of the $Result$ set is 1 (determines output).
(a) Remove $input_i$ from set INPUT.
(b) Remove corresponding $OUTPUT_{subset}$ from set OUTPUT.
(c) The algorithm is repeated from the first input.
5: If the size of the $Result$ set is not 1 for all inputs (cannot determine output).
(a) Print the number of cases for each input.

→ 1,2번 과정을 통해 얻은 데이터에 De-mixing 알고리즘 적용 후 결과 분석

# De-mixing

## Helix 믹싱 서비스에 대한 De-mixing 실험 결과




- 각 입력마다 10개의 데이터를 생성하여 평균 소요시간을 계산
- 총 700개의 테스트 데이터에 De-mixing 알고리즘 적용 결과 694개의 데이터 매칭 성공
- De-mixing 정확도: 99.14%

# Q & A

The 24th Network Security Conference -Korea

# 블록체인 취약점 연구 동향

**김용대** KAIST 교수

### 학력 및 경력사항

| | |
|---|---|
| 2012 ~ 현재 | 카이스트 전기및전자공학부 교수 |
| 2012 ~ 현재 | 카이스트 정보보호대학원 겸임교수 |
| 2017 ~ 현재 | 카이스트 사이버보안연구센터 센터장 |
| 2018 ~ 현재 | 한국블록체인협회 정보보호위원회 위원장 |
| 2013 ~ 2016 | 카이스트 지정 석좌교수 |
| 2002 ~ 2012 | Univ. of Minnesota 교수 |
| 1993 ~ 1998 | 한국전자통신연구소 연구원 |
| 2002 | Univ. of Southern California 박사 |

### 강연요약

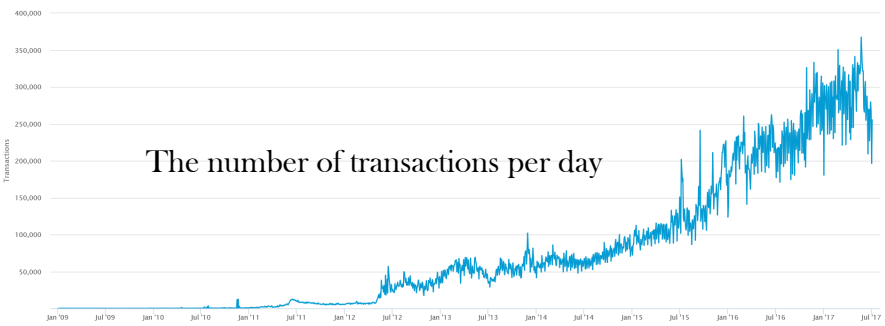
전 세계에 1500 종 이상의 암호화폐가 개발되고 있고 블록체인들 또한 꾸준히 개발되고 있다. 블록체인과 암호화폐는 그 성격 상 보안이 가장 중요한 요구조건 중의 하나라고 할 수 있다. 그럼에도 불구하고 현재 사용중인 블록체인과 암호화폐는 많은 취약점들이 존재하고 있고, 계속해서 고쳐져 나가고 있다. 본 강의에서는 아직까지 알려진 블록체인과 암호화폐의 취약점들에 대해서 살펴봄으로써 새롭게 블록체인과 암호화폐를 개발하는 회사들이 주의해야 할 취약점들에 대하여 살펴보기로 한다.

# 블록체인 취약점 연구 동향

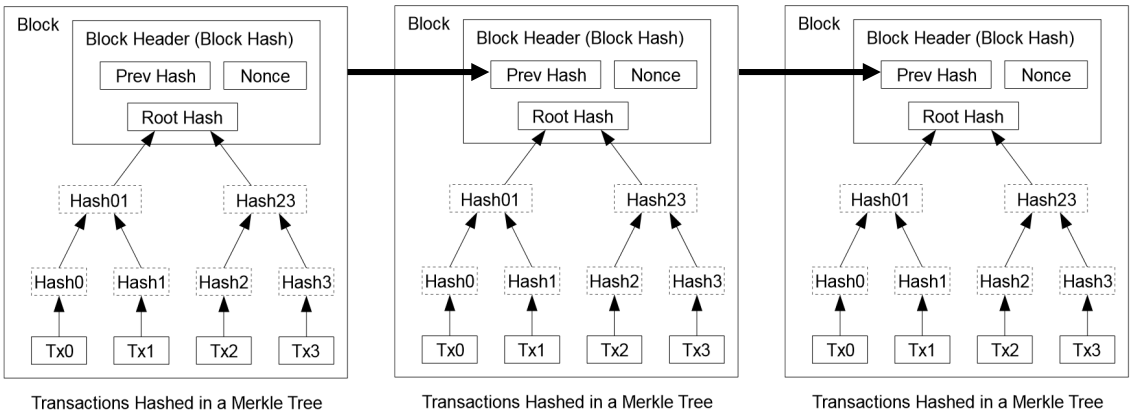
**Yongdae Kim**
**Korea Advanced Institute of Science and Technology**
**School of Electrical Engineering**
**System Security Lab.**

## What is Bitcoin?

- Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.
- Bitcoin is a first cryptocurrency based on a peer-to-peer network.
- Bitcoin as a form of payment for products and services has grown, and users are



# Blockchain

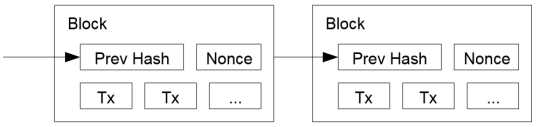



- Blocks connect as a chain.
- Each header of blocks includes the previous block's hash.



# Proof-of-Work

- Proof-of-work scheme is based on SHA-256
- Proof-of-work is to find a valid Nonce by incrementing the Nonce in the block header until the block's hash value has the required prefix zero bits.




Contents

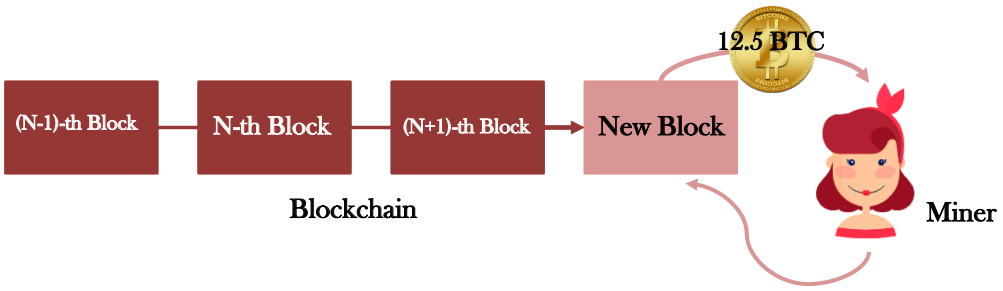
Nonce

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Valid nonce

# Reward

- Performing proof-of-work is called **Mining.**
- A person which do mining is called **Miner.**
- A miner can earn 12.5 BTC (≈ $ 32.5k) as a reward when she succeeds to find a valid nonce.

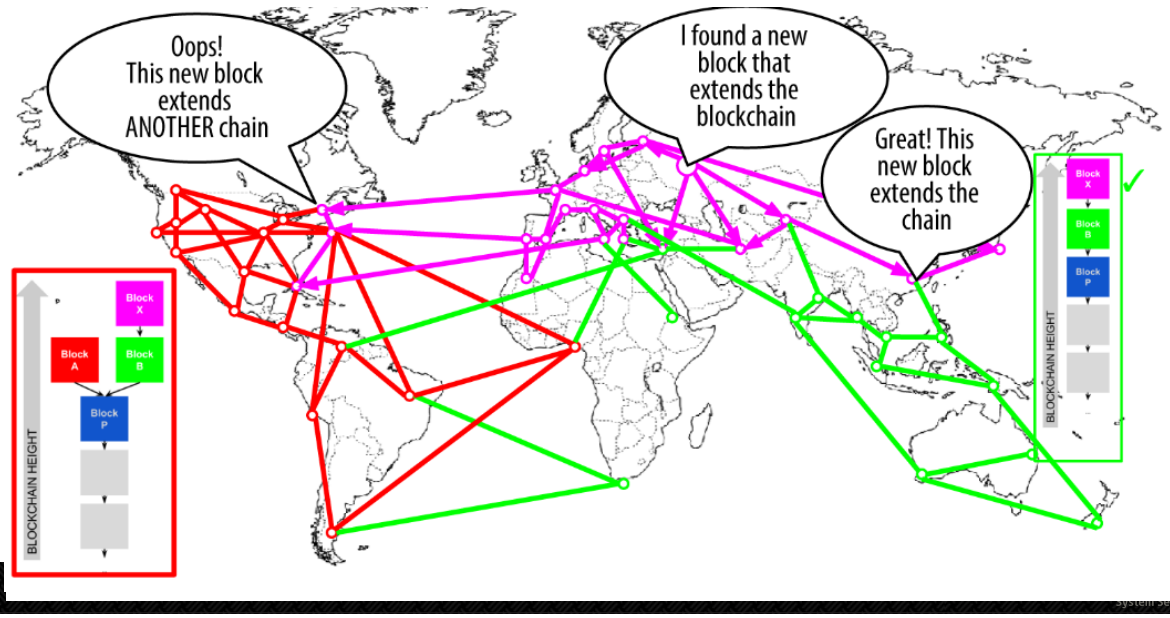





# Step (Miner)

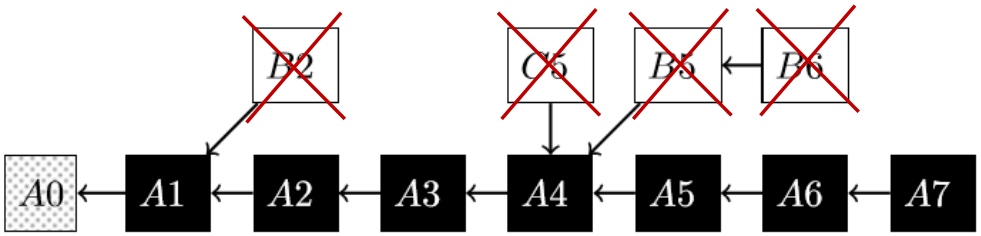
- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes express their acceptance of the block by working on creating the next chain, using the hash of the accepted block as the previous hash.

# Forks



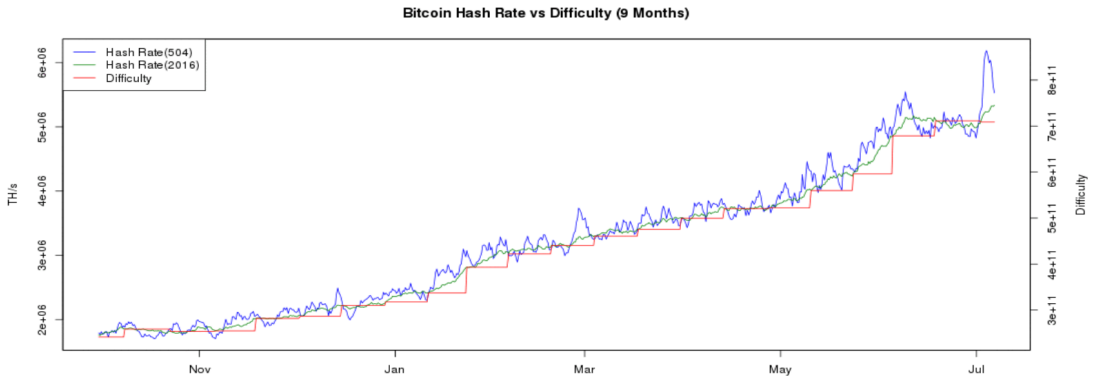



# Forks




- Only one head is accepted as a valid one among heads.
- An attacker can generate forks intentionally by holding his found block for a while.

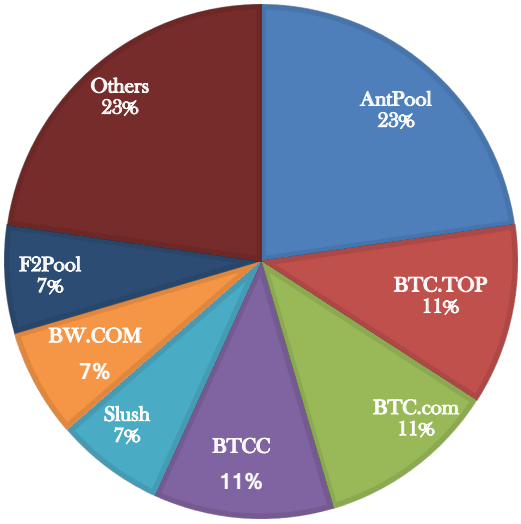
# Mining Difficulty




- ❖ Bitcoin adjusts automatically the mining difficulty to be an average one round period 10mins.
- ❖ The difficulty increases continuously as computing power increases.



# Mining Pool




- ❖ Many miners started to do mining together.
- ❖ Most mining pools consist of a manager and miners.
- ❖ Currently, most computational power is possessed in mining pools.

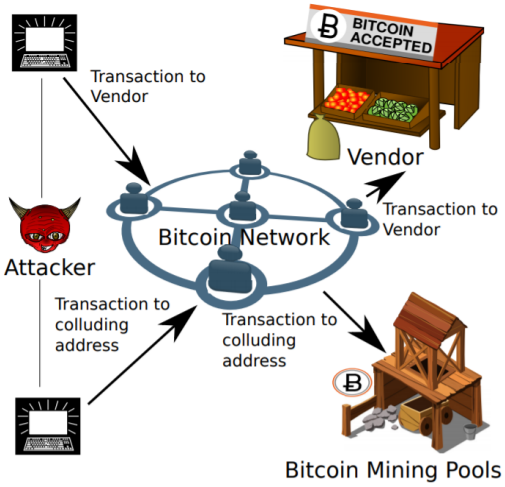
# Security of Cryptocurrency

- Double spending
  - Double-Spending Fast Payments in Bitcoin: CCS 2012
- Anonymity (이전 발표)
  - Quantitative Analysis of the Full Bitcoin Transaction Graph: FC 2013
- (Peer-to-Peer) Network
  - Eclipse Attacks on Bitcoin's Peer-to-Peer Network: Usenix 2015
  - Low-Resource Eclipse Attackson Ethereum's Peer-to-Peer Network: ePrint 2018
  - Hijacking Bitcoin: Routing Attacks on Cryptocurrencies: SP 2017
- Mining
  - Miner's Dilemma: SP 2015
  - Fork after withholding (FAW) attacks: CCS 2017 (KAIST 논문)
- Scalability vs Security
  - Security and Performance of Proof of Work Blockchains: CCS 2016

# Double Spending Attack

# How Can We Launch Double Spending?

- Key Point: Generate Forks
- In order that an attacker spends spent Bitcoin, the vendor should consider the Bitcoin is unspent.






# Necessary Conditions for Double-Spending

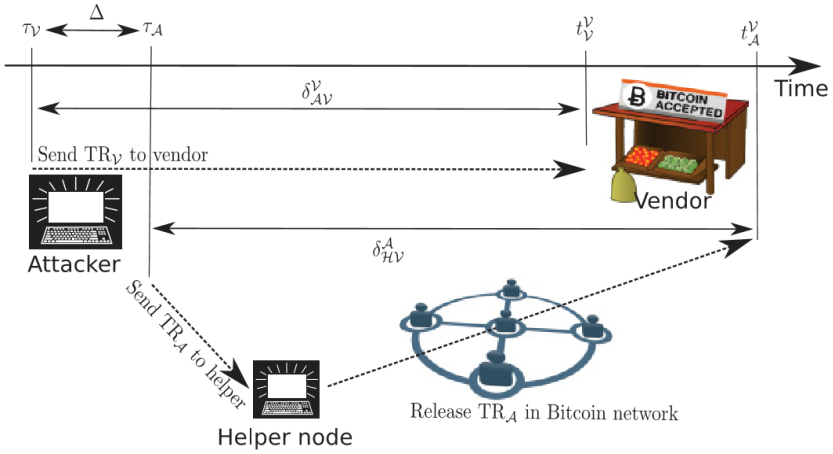
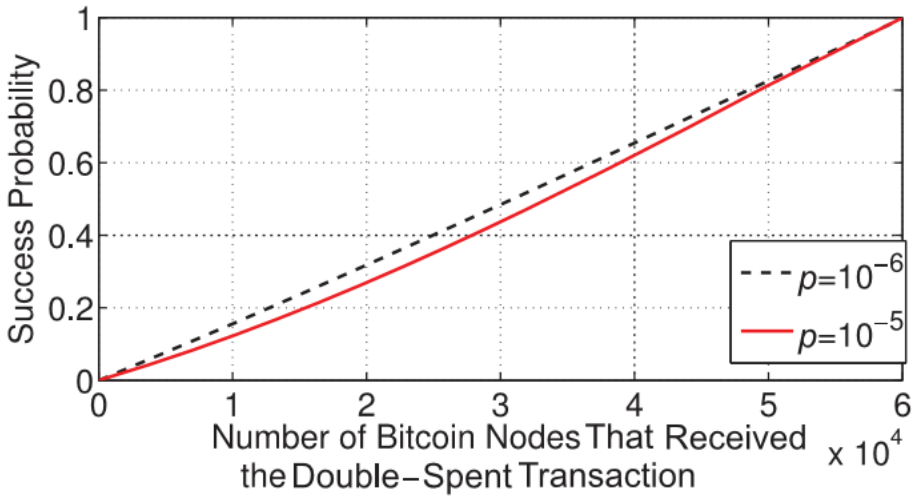



Fig. 3. Sketch of a double-spending attack on fast payments in Bitcoin. Here, the attacker $\mathcal{A}$ dispatches two transactions that use the same BTCs in the Bitcoin network. The double-spending attack is successful if the BTCs that $\mathcal{A}$ used to pay for $\mathcal{V}$ cannot be redeemed (i.e., when the second transaction is included in the upcoming Bitcoin block).

# Performing Double Spending Attack




SysSec System Security Lab

# Eclipse Attack

# Bitcoin Network

- Cryptographic authentication between peers is not used, and nodes are identified by their IP addresses.
- Each node uses a randomized protocol to select eight peers with which it forms long-lived outgoing connections, and to propagate and store addresses of other potential peers in the network.
- Nodes with public IPs also accept up to 117 unsolicited incoming connections from any IP address.



# Propagating Network Information

- A DNS seeder is a server that responds to DNS queries from bitcoin nodes with a list of IP addresses for bitcoin nodes.
- ADDR messages, containing up to 1000 IP address and their timestamps, are used to obtain network information from peers.
- Nodes accept unsolicited ADDR messages.
- Peers store Public IPs in *tried* and *new* table.
  - Tried: unique addresses for peers to whom the node has successfully established an incoming or outgoing connection.
  - New: addresses for peers to whom the node has not yet initiated a successful connection.

# Eclipse Attack

- Populates the tried table with addresses for its attack nodes
- Overwrites addresses in the new table with "trash" IP
- The attack continues until the victim node restarts and chooses new outgoing connections from the tried and new tables in its persistent storage
- With high probability, the victim establishes all eight outgoing connections to attacker addresses;
- Finally, the attacker occupies the victim's remaining 117 incoming connections.

# The BWH Attack

# The History of the BWH Attack

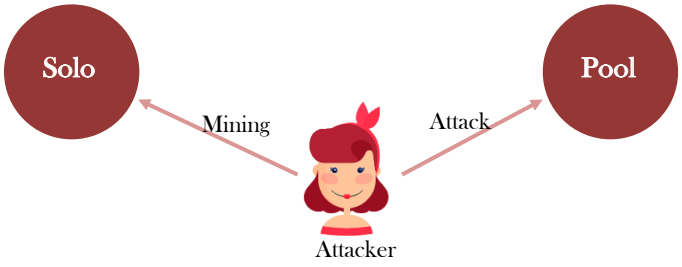
- 2011: Analysis of Bitcoin Pooled Mining Reward Systems
  - "This has no direct benefit for the attacker, only causing harm to the pool operator or participants. "
- 2014 : On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency
  - "They showed that an attacker can earn profit by this attack"
  - In june 2014, Eligius pool made a loss because of the BWH attack.
- 2015 : The miner's dilemma

  On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining
  - Attack strategy && game theory

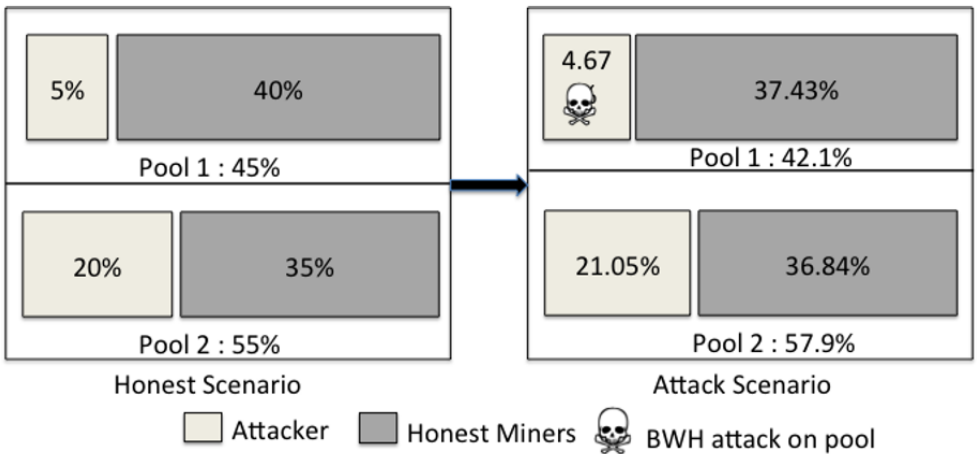


# BWH Attack

- An attacker joins the target pool.
- She receives unearned wages while only pretending to contribute work in the pool.
- She submits the share which contains only partial solution but not the perfect solution.
- She should split her computational power into solo mining and malicious pool mining.

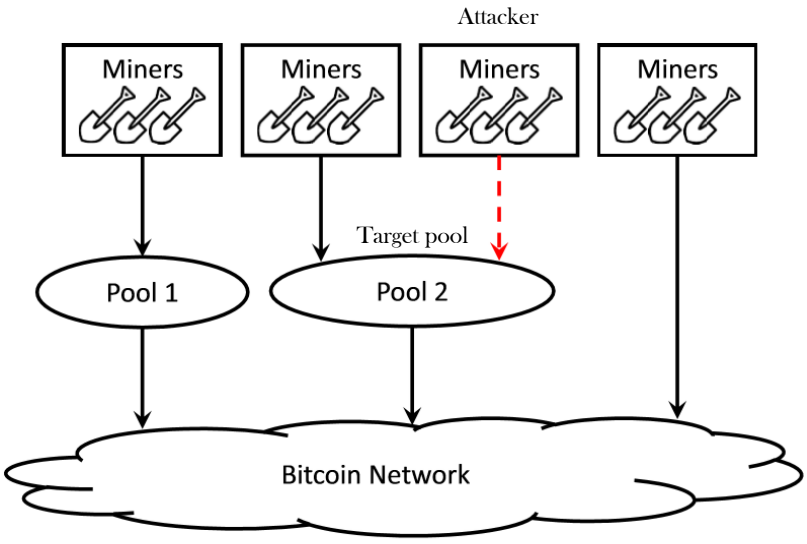


# BWH Attack

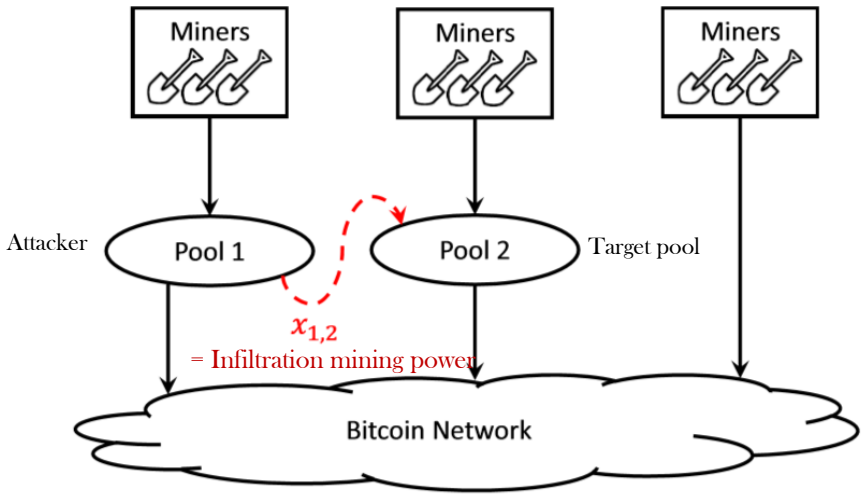





# Classical BWH attack

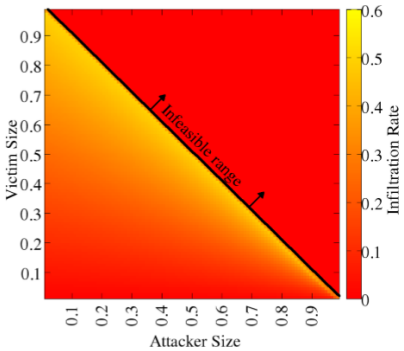


# BWH attack among pools



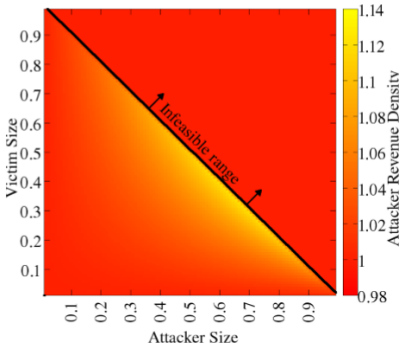

SysSec System Security Lab

# Result



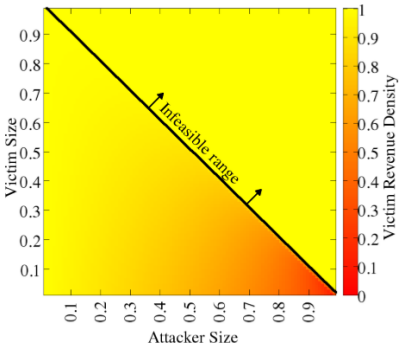

(a) $x_{1,2}$

Infiltration mining power




(b) $r_1$

Attacker relative reward




(c) $r_2$

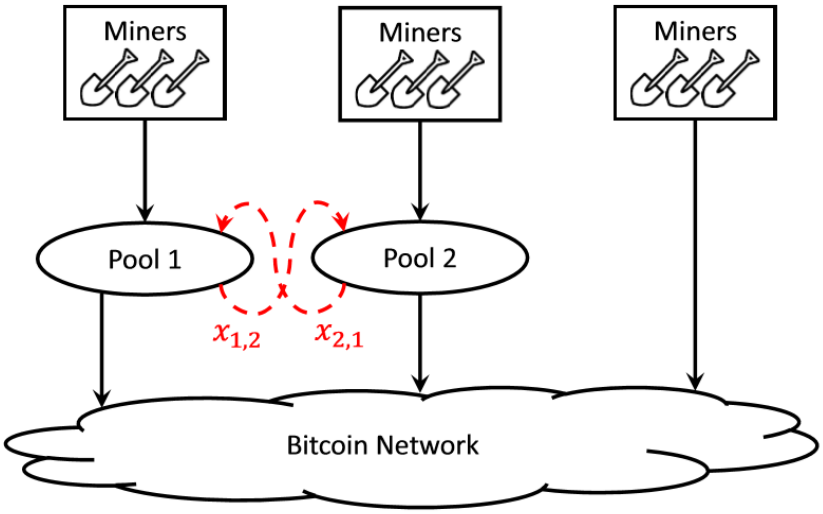
Victim relative reward

❖ The BWH attack is always profitable.

SysSec System Security Lab

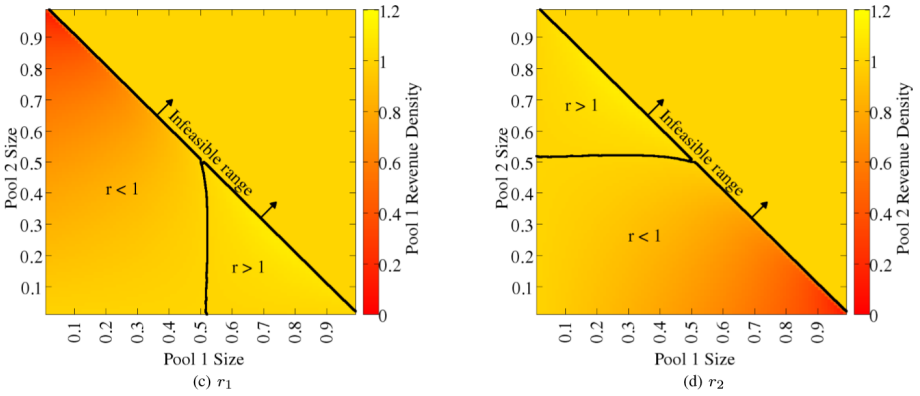
# Between Two Pools

- Rational two pools can launch the BWH attack each other.
- It leads to a BWH attack game.






# Result




- When they executes the BWH attack each other, both of them make a loss.

# Miners' dilemma

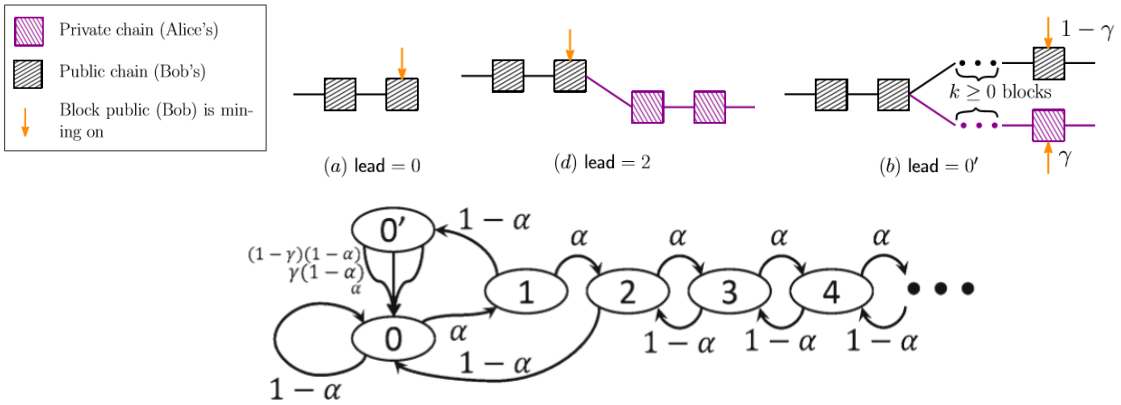
| Pool 1 / Pool 2 | no attack | attack |
|---|---|---|
| no attack | $(r_1 = 1, r_2 = 1)$ | $(r_1 > 1, r_2 = \tilde{r}_2 < 1)$ |
| attack | $(r_1 = \tilde{r}_1 < 1, r_2 > 1)$ | $(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$ |

- The equilibrium revenue of the pool is inferior compared to the no-pool attacks scenario.
- This is equivalent to the prisoner's dilemma.
- The fact that the BWH attack is not common may be explained by modeling the attack decisions as an iterative prisoner's dilemma.

SysSec System Security Lab

# The FAW Attack

# Selfish Mining




❖ Generate intentional forks adaptively.
❖ Force the honest miners into performing wasted computations on the stale public branch.

Eyal and Sirer. "Majority is not enough: Bitcoin mining is vulnerable." Financial Crypto, 2014.

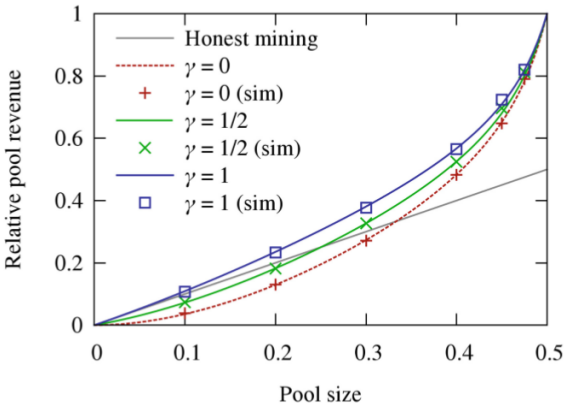


# Selfish Mining

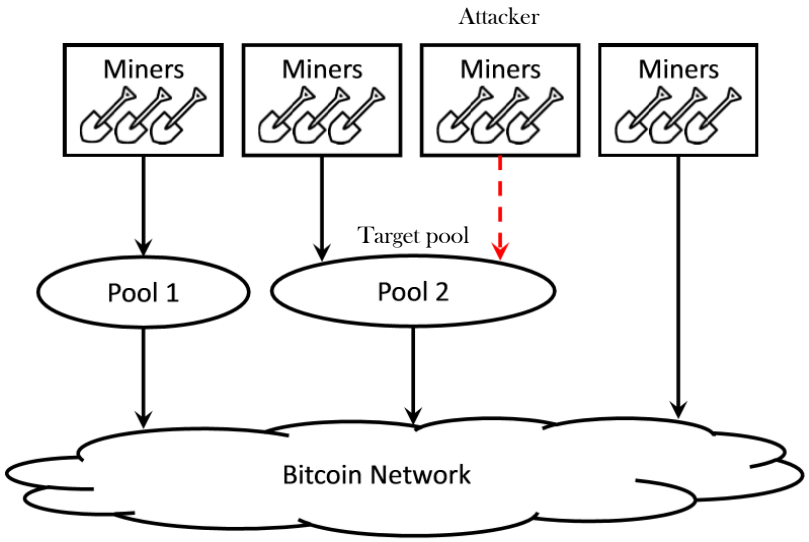
❖An attacker can earn the extra reward according to her network capability.

❖For example, if an attacker possesses 20% computational power, she can earn the extra reward $6M at most.

❖However, it is not practical.

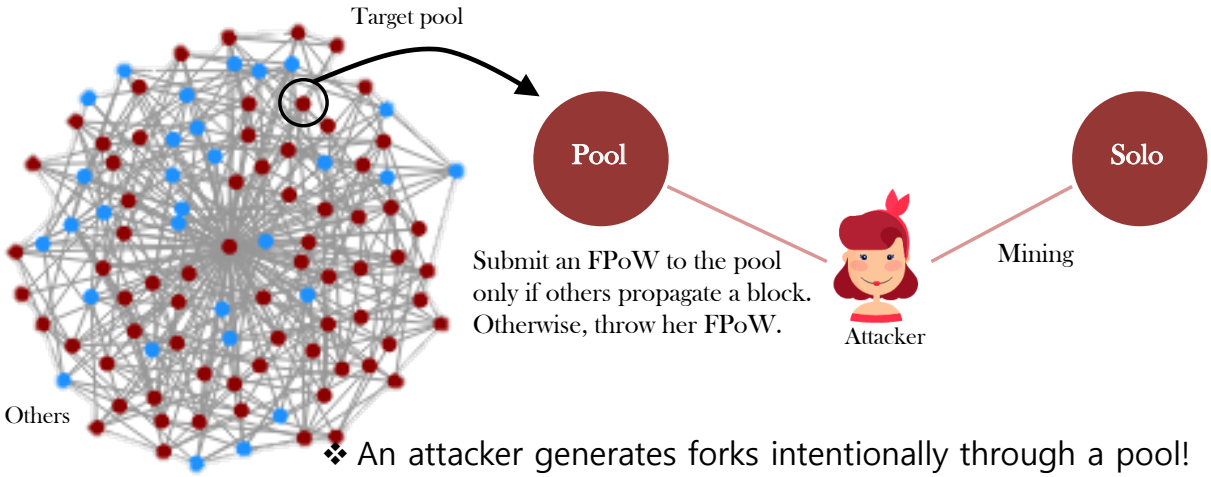


# FAW Attack



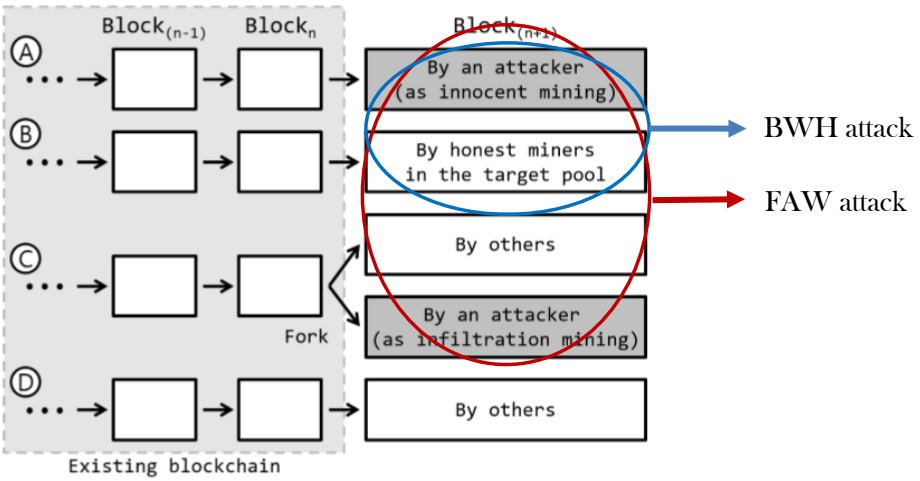



# FAW Attack



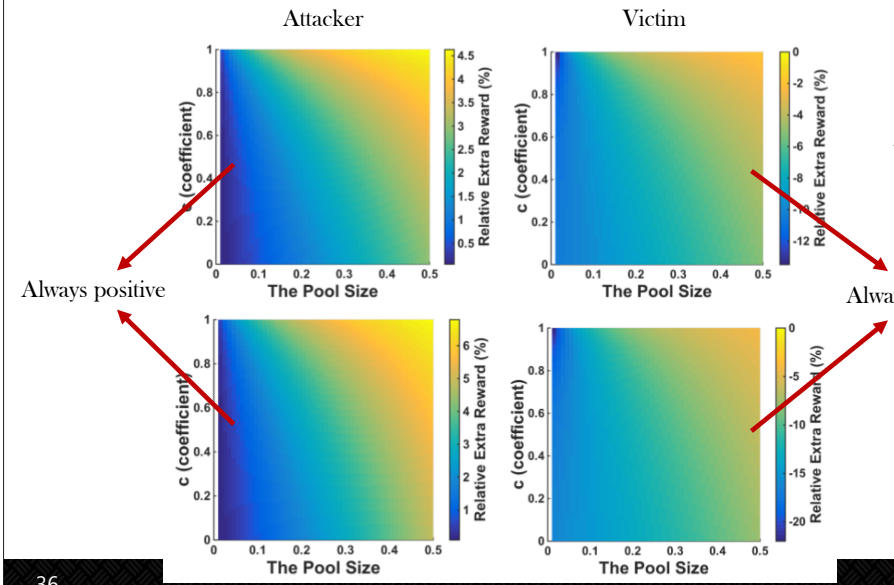

❖ An attacker generates forks intentionally through a pool!

# FAW Attack Against One Pool






# Result




❖ An attacker with 0.2 power

❖ An attacker with 0.3 power

# Result

Increasing

| c \ α | 0.1 | 0.2 | 0.3 | 0.4 |
|---|---|---|---|---|
| 0 | 0.53 (0.53) | 1.14 (1.14) | 1.85 (1.85) | 2.70 (2.70) |
| 0.25 | 0.65 (0.67) | 1.38 (1.38) | 2.20 (2.20) | 3.1 (3.13) |
| 0.5 | 0.85 (0.85) | 1.74 (1.74) | 2.70 (2.70) | 3.75 (3.75) |
| 0.75 | 1.21 (1.22) | 2.37 (2.37) | 3.52 (3.52) | 4.69 (4.70) |
| 1 | 2.12 (2.12) | 3.75 (3.75) | 5.13 (5.13) | 6.37 (6.36) |

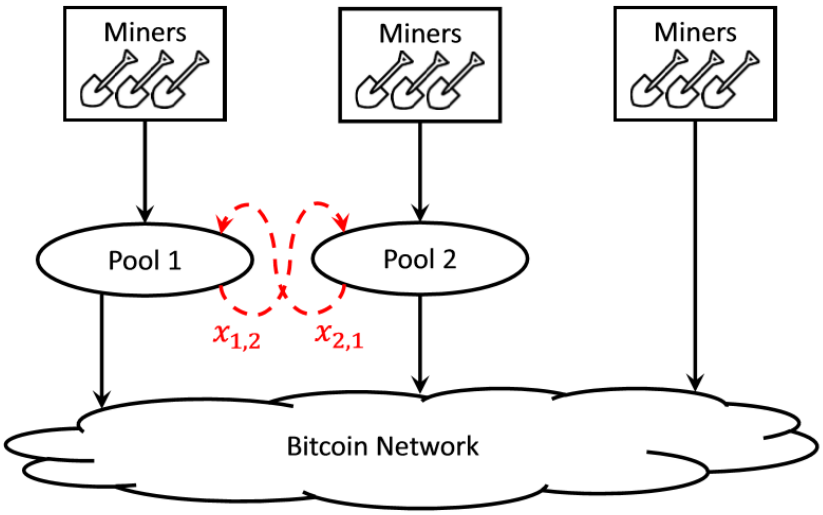
The case is equivalent to the case of the BWH attack

Increasing

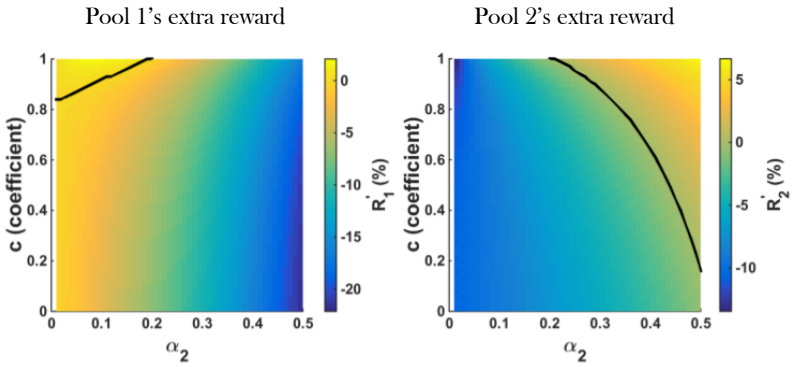
❖ We simulated an FAW attack against one pool which possesses a computational power of 0.2, using a Monte Carlo method.



# FAW Attack Game



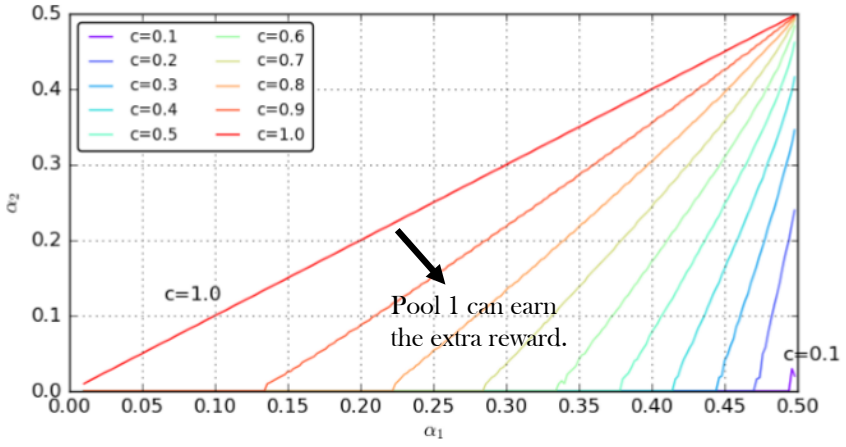
# Result




- Pool 1 possesses 0.2 computational power.
- The bigger pool can earn the extra reward unlike the miner's dilemma.



# Break Dilemma




- The FAW attack game leads to a pool size game: the larger pool can always earn the extra reward.

# The DAO 공격 사례

- The DAO : 탈중앙화 자율조직을 구현한 스마트 컨트랙트
  - 투자자들이 보유한 DAO Token을 바탕으로 의결권 행사
  - 전세계에서 약 2천억원의 투자금 모집
  - DAO Token을 Ether(이더리움 화폐)로 환급하는 코드에 취약점 존재 (약 750억 상당의 해킹 피해)

- Attack Example 1
  1. DAO 출금 기능을 악용하는 스마트 컨트랙트 작성 및 호출
  2. 공격자 계좌에 입금 발생 시, DAO에 출금 요청
  3. DAO 출금으로 공격자 계좌에 입금 발생
  4. 잔액 업데이트 전에 2) 3) 과정의 무한 Loop 생성되어 무한 출금

- Attack Example 2
  1. 공격자 계좌에 1 wei 입금
  2. 'Attack Example 1' 응용하여 1 wei 두번 출금
  3. Underflow에 의해서 잔고가 2^256 – 1 wei 로 변환
  4. 잔고 출금



# 스마트 컨트랙트 취약점 연구

| 연구명 | Making Smart Contracts Smarter | ZEUS: Analyzing Safety of Smart Contracts |
|---|---|---|
| 출처 | CCS 2016 | NDSS 2018 |
| 목적 | 자동화 도구를 이용하여 이더리움의 취약한 스마트 컨트랙트 탐지 | 자동화 도구를 이용하여 이더리움의 취약한 스마트 컨트랙트 탐지 |
| 공격 | 4 종류 공격<br>- Reentrancy<br>- Unchecked send<br>- Block state dependence<br>- Transaction order dependence | 7 종류 공격<br>- (기존 4종류)<br>- Failed send<br>- Integer overflow/underflow<br>- Transaction state dependence |
| 취약점 점검결과 | 8,833 / 19,366 (46%) 취약 | 21,281 / 22,493 (94.6%) 취약<br>(1524 unique contract) |

# Thank You!

https://syssec.kaist.ac.kr

The 24th Network Security Conference -Korea

# 스마트 컨트랙트와 보안

**이종협** 가천대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2009 | 연세대학교 컴퓨터과학 공학박사 |
| 2004 | 연세대학교 컴퓨터과학 공학석사 |
| 2002 | 연세대학교 전기전자 학사 |
| 2015 ~ | 가천대학교 금융수학과 조교수 |
| 2012 ~ 2015 | 한국교통대학교 소프트웨어학과 조교수 |
| 2009 ~ 2012 | 미국 카네기멜론대학교 CyLab 박사후연구원 |

### 강연요약

스마트 컨트랙트는 단순히 생각하면 블록체인 위에서 동작하는 프로그램 코드라 할 수 있지만, 블록체인만의 새로운 응용 분야를 만드는 과정에서 필수 요소로서 역할을 하고 있다. 하지만 블록체인 자체의 보안성과는 별개로 스마트 컨트랙트를 적용하는 과정은 익숙하지 않은 실행 환경에서 새롭게 경험하는 버그들에 의하여 심각한 보안의 문제를 겪고 있다. 본 강연에서는 스마트 컨트랙트에서 발생하는 보안의 문제점과 이유에 대하여 살펴보고, 안전한 스마트 컨트랙트를 작성하고 활용하기 위한 방법과 한계점에 대해서 이야기하고자 한다.

# Smart Contract & Security

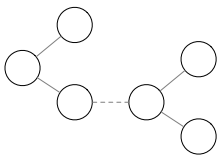
2018-04-12
NetsecKR

이종협

# Blockchain intro

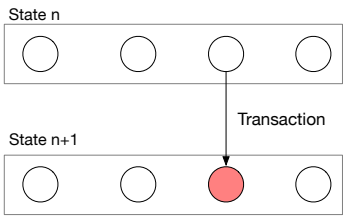
## Bitcoin

Transaction Model



## Ethereum

State + account model




+ EVM
(Ethereum Virtual Machine)

## Hyperledger

Framework

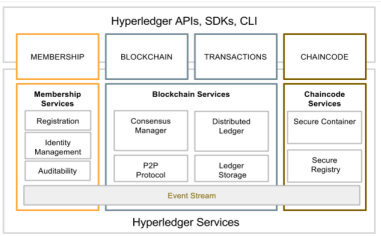
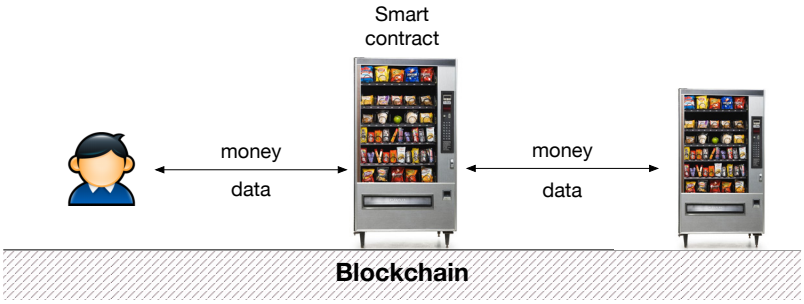



Figure 2: Hyperledger reference architecture

# Smart contract

"Contract를 구현하고, 강제하고, 실행시켜 주는 code"

- 믿지 않는 사용자간의 agreement + coordination
- 블록체인에 복잡한 기능을 제공




# Solidity code

Storage

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;
```

Constructor

```
    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }
```

Function (Public)

```
    /* Send coins */
    function transfer(address _to, uint256 _value) public {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
```

Fallback function

```
    /* Fallback */
    function () payable {
        ...
    }
}
```

# Smart contracts

어떻게 볼 것인가?

Vending machine

Balance (Money!)

Storage

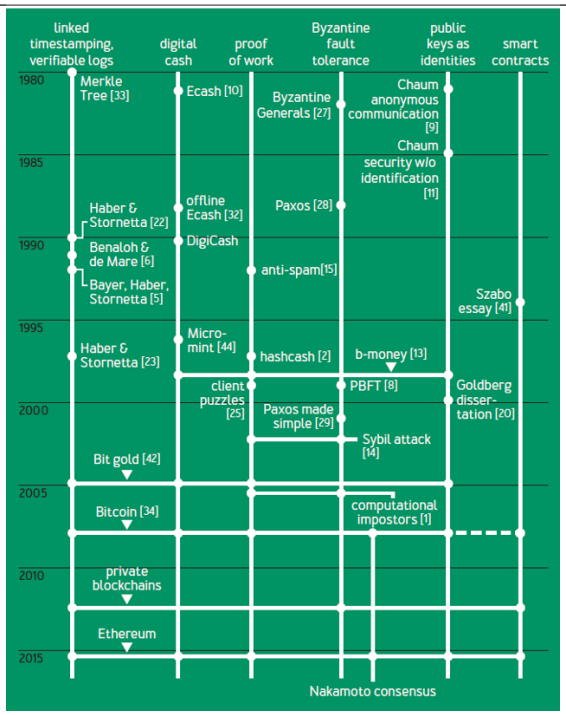
Distributed objects

Threads using concurrent objects in shared memory

Secure execution (External)

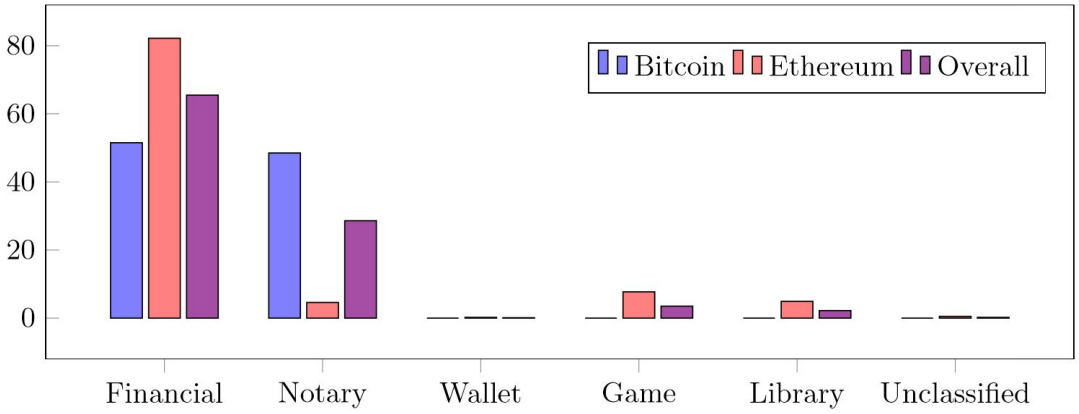
어떠한 의미를 가지는가?

# Academic Pedigree




from “Bitcoin’s academic pedigree” Narayanan *et al.*

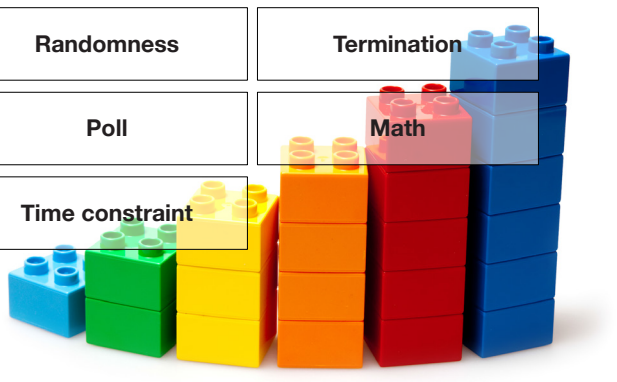
# Smart contracts - category




from “an empirical analysis of smart contracts” Bartoletti *et al.*

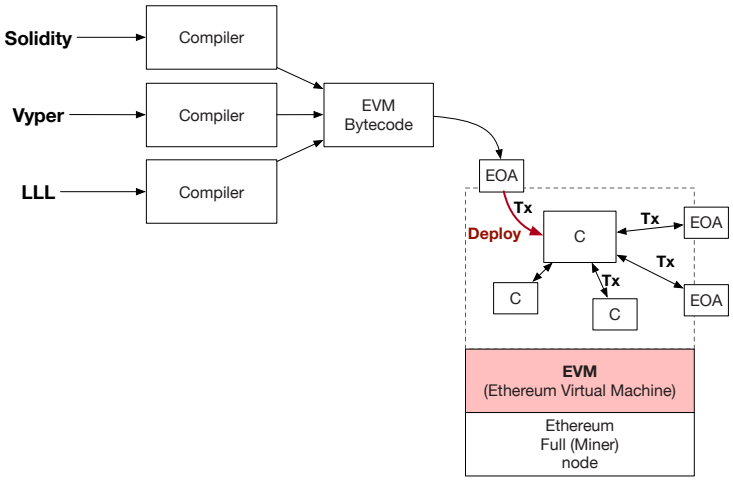
# Smart contracts - Design patterns

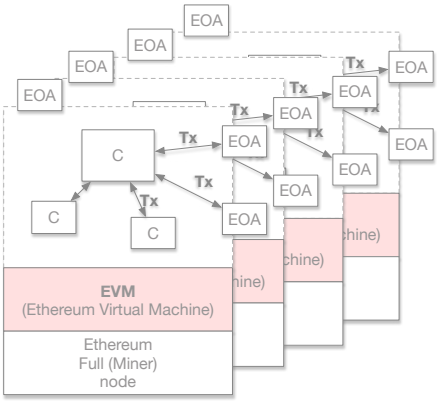
| | | |
|---|---|---|
| Token | Randomness | Termination |
| Authorization | Poll | Math |
| Oracle | Time constraint | |



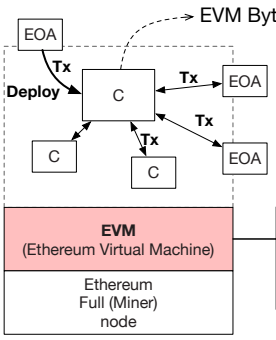
from “an empirical analysis of smart contracts” Bartoletti *et al.*

# Smart contract lifecycle



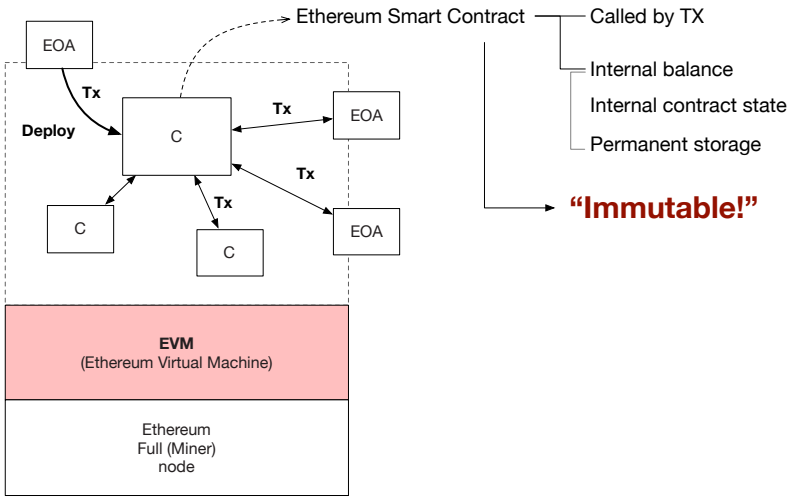




# Ethereum Virtual Machine



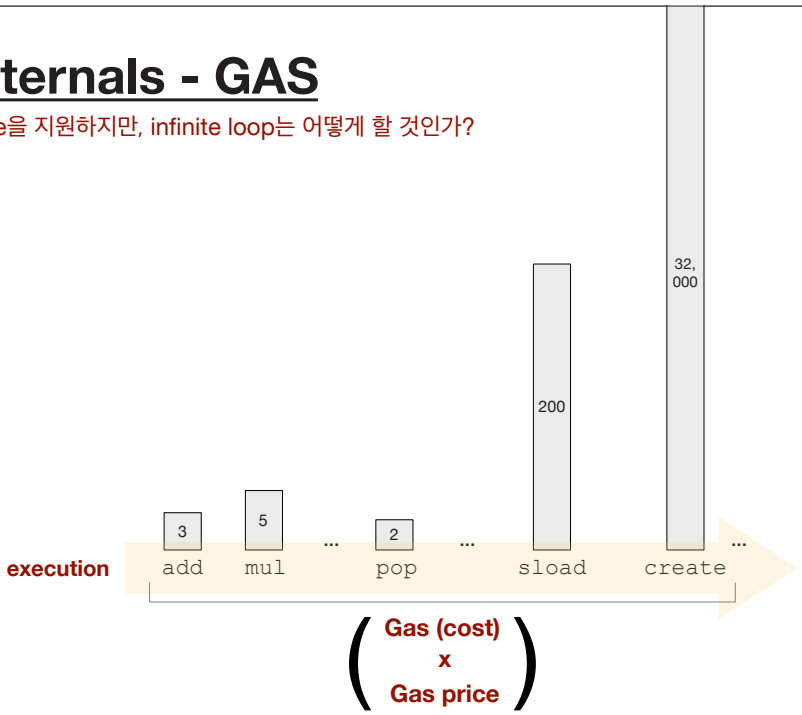

- Smart contract를 위한 execution model
  - Redundantly parallel
  - Turing complete! → GAS
- Design Goal
  - Simplicity
  - Space efficiency
  - Determinism?
  - Specialization
  - Security

# Ethereum Virtual Machine



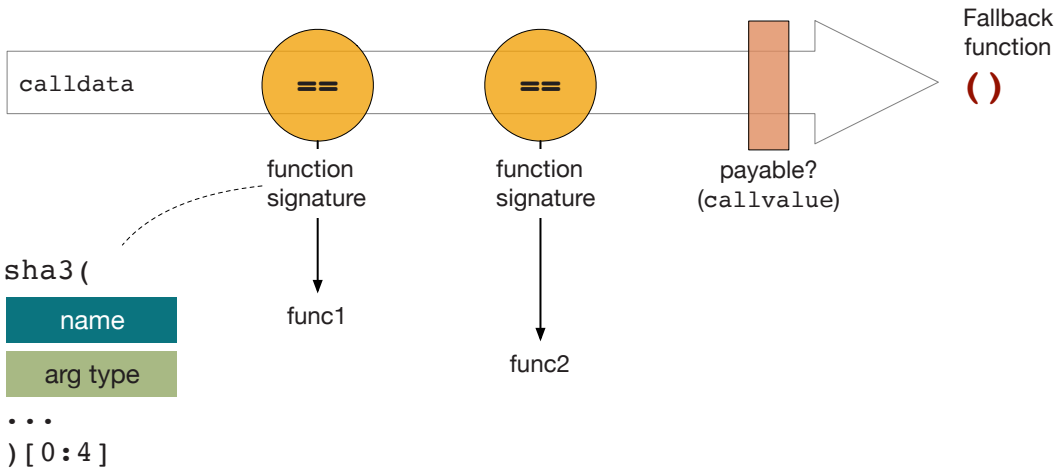

# EVM internals - GAS

Turing complete을 지원하지만, infinite loop는 어떻게 할 것인가?



# Function call handling in Solidity ( ≠ EVM)

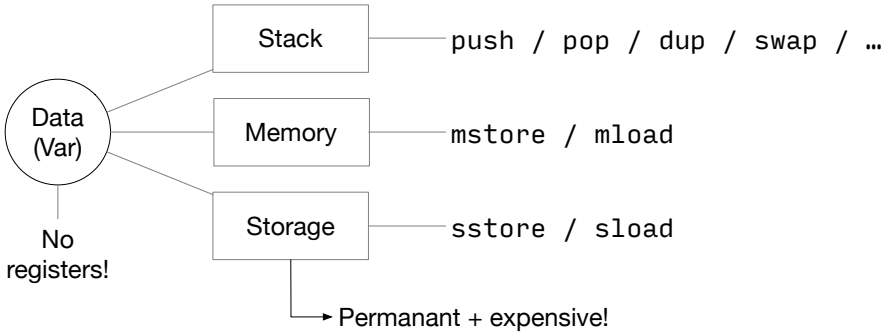
Function call과 fall back



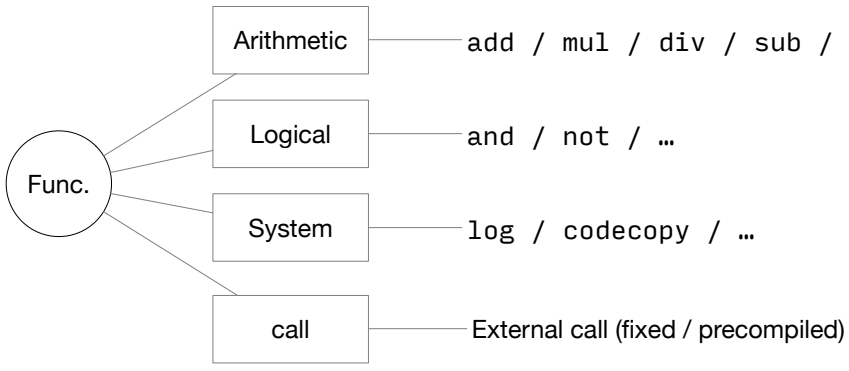

# EVM assembly code

```
PUSH 0
DUP1
PUSH 100
EXP
DUP2
SLOAD
DUP2
PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
MUL
NOT
AND
SWAP1
DUP4
PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
AND
MUL
OR
SWAP1
SSTORE
POP
```

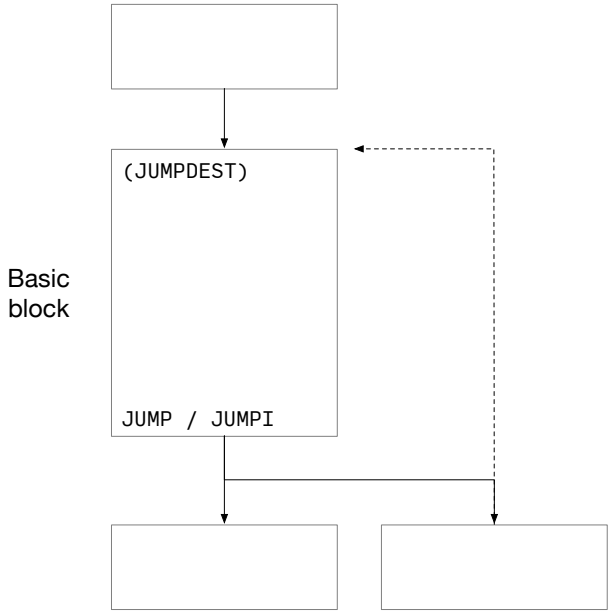
# EVM internals - data




# EVM internals - data



# EVM internals - control



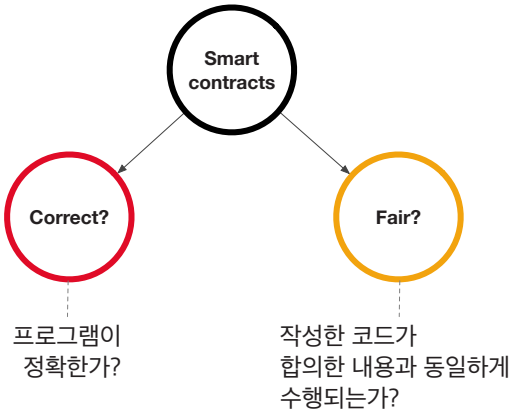

## Smart contract security

# 왜 해킹의 대상이 되는가?

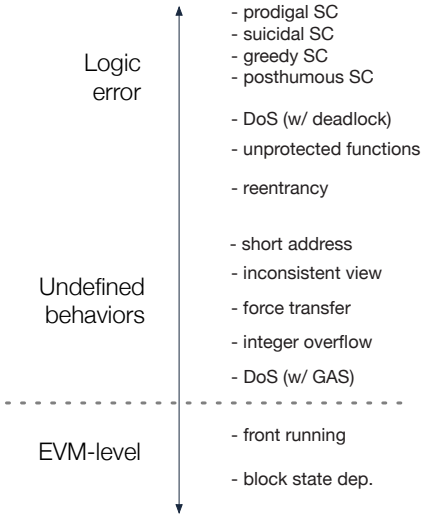
- Smart contract는 기본적으로 항상 online + open
- 공격자가 즉각적인 reward를 얻는다.
- Immutable!
- 개발자들에게도 생소한 execution model
- Solidity의 abstraction과 실제 EVM과의 mismatch

⋮

# Smart contract의 문제




# Smart contract 취약점



# Examples

Integer overflow

```
(1)  uint payout = balance/participants.length;
(2)  for (var i = 0; i < participants.length; i++)
(3)    participants[i].send(payout);
```

Prodigal contract

```
1  function payout(address[] recipients,
2                  uint256[] amounts) {
3   require(recipients.length==amounts.length);
4   for (uint i = 0; i < recipients.length; i++) {
5      /* ... */
6      recipients[i].send(amounts[i]);
7    }}
```

from “ZEUS: Analyzing Safety of Smart Contracts” Kalra *et al.*, “Finding the greedy, prodigal, ad suicidal contracts at scale” Nikolic *et al.*

# Examples

```
(1)  contract Wallet {
(2)    mapping(address => uint) private userBalances;
(3)    function withdrawBalance() {
(4)      uint amountToWithdraw = userBalances[msg.sender];
(5)      if (amountToWithdraw > 0) {
(6)        msg.sender.call(userBalances[msg.sender]);
(7)        userBalances[msg.sender] = 0;
(8)      }
(9)    }
(9)    ...
(10)  }
```

```
(1)  contract AttackerContract {
(2)    function () {
(3)      Wallet wallet;
(4)      wallet.withdrawBalance();
(5)    }
(6)  }
```

Re-entrancy

1. 조건을 확인하고
2. state를 변경하고
3. action

Unchecked send

```
(1)  if(gameHasEnded && !prizePaidOut) {
(2)    winner.send(1000); // send a prize to the winner
(3)    prizePaidOut = True;
(4)  }
```

```
(1)  while (balance >
           persons[payoutCursor_Id_].deposit/100*115) {
(2)    payout = persons[payoutCursor_Id_].deposit/100*115;
(3)    persons[payoutCursor_Id].EtherAddress.send(payout);
(4)    balance -= payout;
(5)    payoutCursor_Id_++;
(6)  }
```

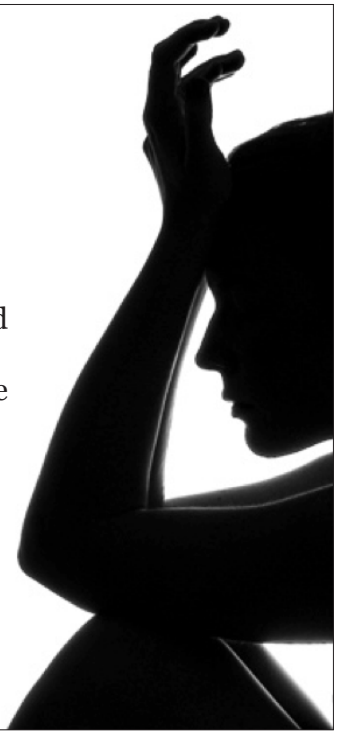
Incorrect logic

from “ZEUS: Analyzing Safety of Smart Contracts” Kalra *et al.*

## Smart contract를 작성한다는 것은..

"I want you to write a program that has to run in a concurrent environment under Byzantine circumstances where any adversary can invoke your program with any arguments of their choosing. The environment in which your program executes (and hence any direct or indirect environmental dependencies) is also under adversary control. If you make a single exploitable mistake or oversight in the implementation, or even in the logical design of the program, then either you personally or perhaps the users of your program could lose a substantial amount of money. Where your program will run, there is no legal recourse if things go wrong. Oh, and once you release the first version of your program, you can never change it. It has be right first time.

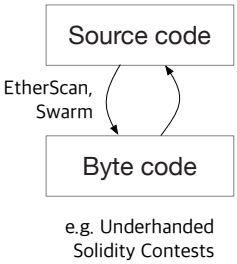
from *blog.acolyer.org*



## 어떠한 고민이 필요한가?

### 믿을 수 있는가?

Bi-directional한
분석이 필요한가?




e.g. Underhanded
Solidity Contests

### 취약점 분석

- integer overflow
- delegate call
- reentrancy
- DoS (revert / GAS limit)
- force transfer
- inconsistent view
- short address
- front running
- randomness

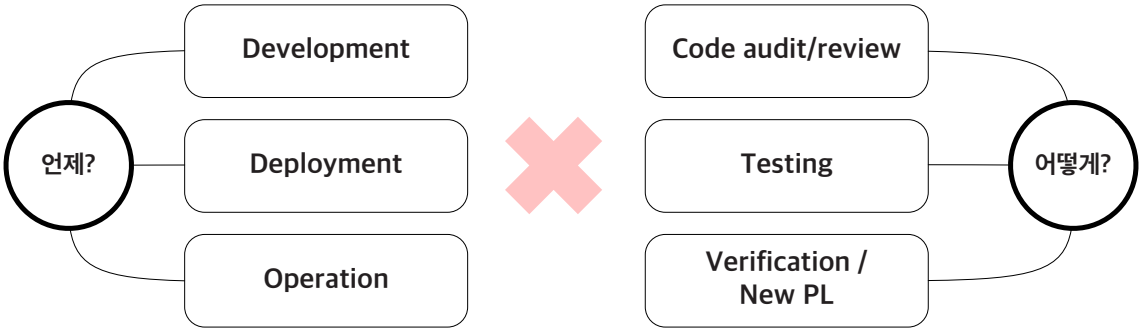
⋮

### Solidity의 한계

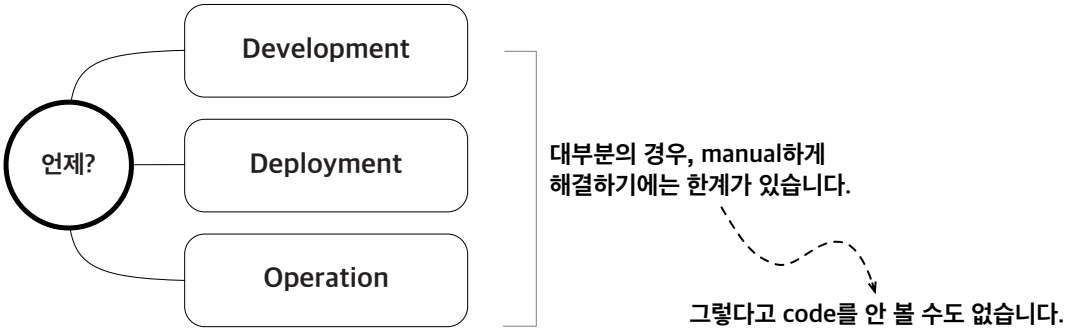
언어의 미성숙

과연 contract에
맞는 프로그래밍
방식인가?

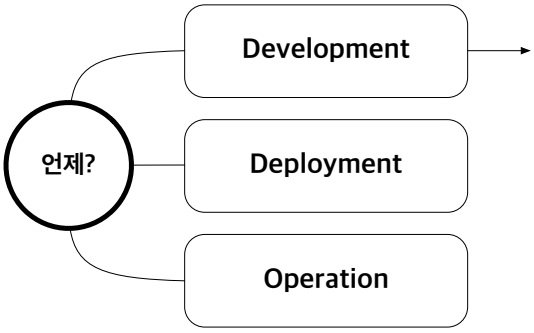
## 해결 방안?


Development
Deployment
Operation
언제?
Code audit/review
Testing
Verification / New PL
어떻게?

## 해결 방안?

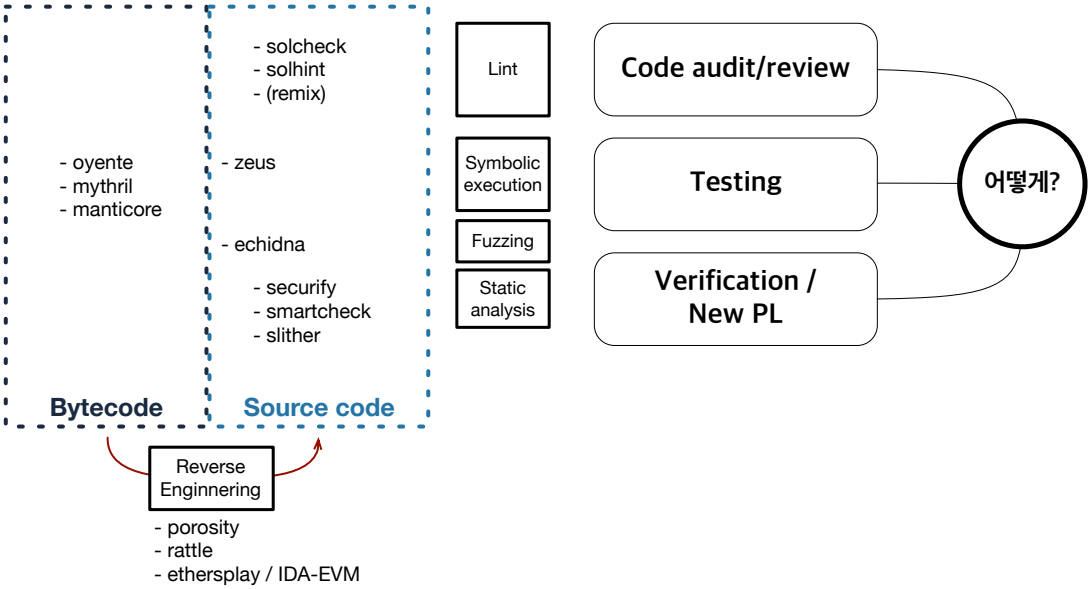

Development
Deployment
Operation
언제?
대부분의 경우, manual하게
해결하기에는 한계가 있습니다.
그렇다고 code를 안 볼 수도 없습니다.

# 해결 방안?

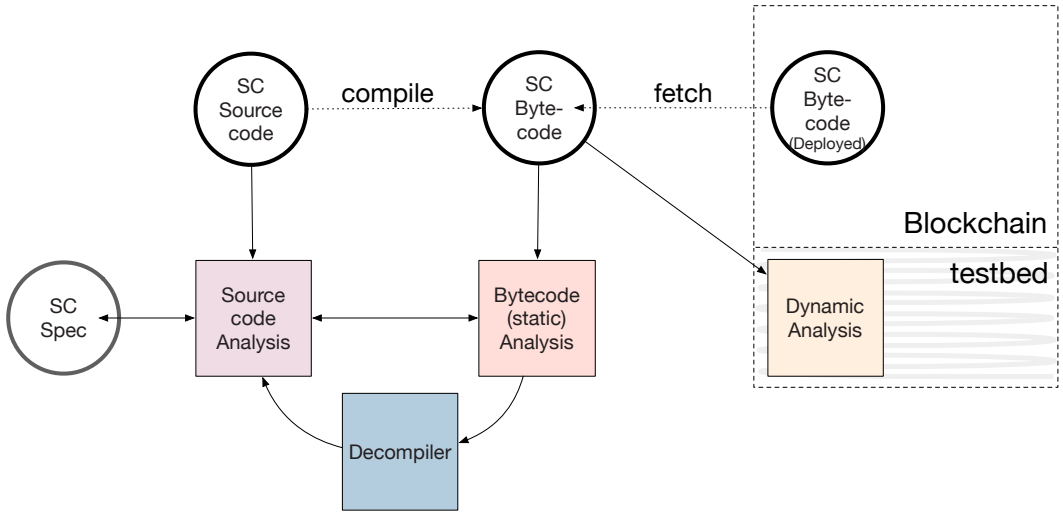



- OpenZeppelin
- "Good code patterns"
  - Enforce invariants with assert()
  - Use assert() and require() properly
  - Beware rounding with integer division
  - Keep fallback functions simple
  - Explicitly mark visibility in functions and state variables
  - …

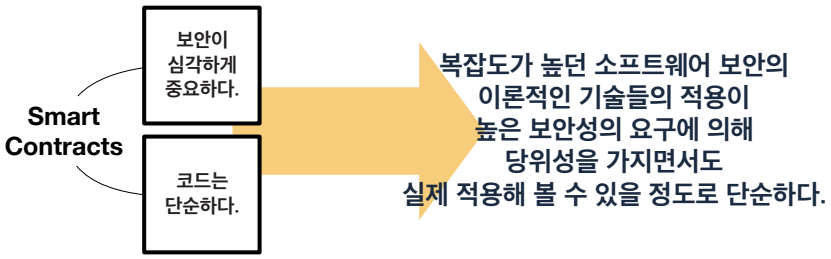
# 해결 방안?



# Automated smart contract analysis




# PL 기반의 자동화된 접근 방식의 적용



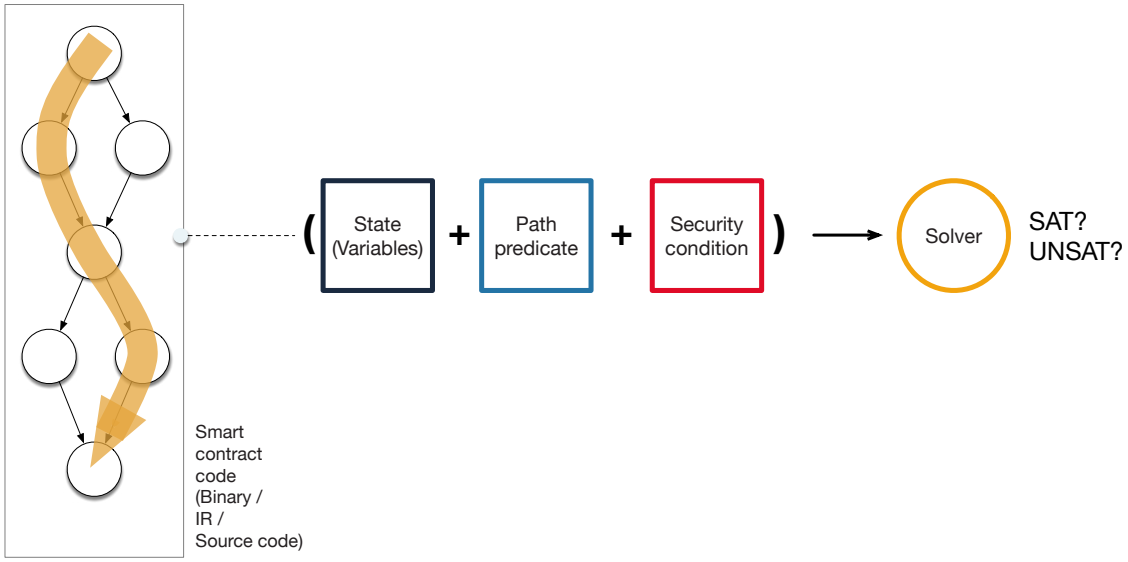

## Advantages

- 코드가 짧다.
- Bytecode instruction이 단순하다.

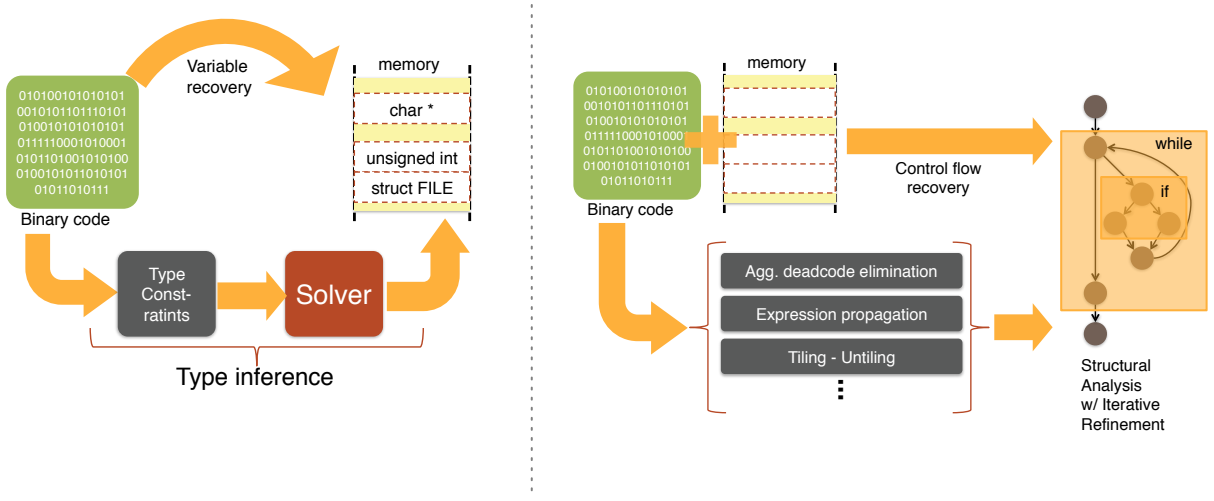
## Challenges

- 코드가 짧다.
- inter-prodecural -> inter-contract (High dependency)
- Execution model의 가정이 필요하다.

# 대표 기술1 - Symbolic execution approach




# 대표 기술2 - Automated reverse engineering

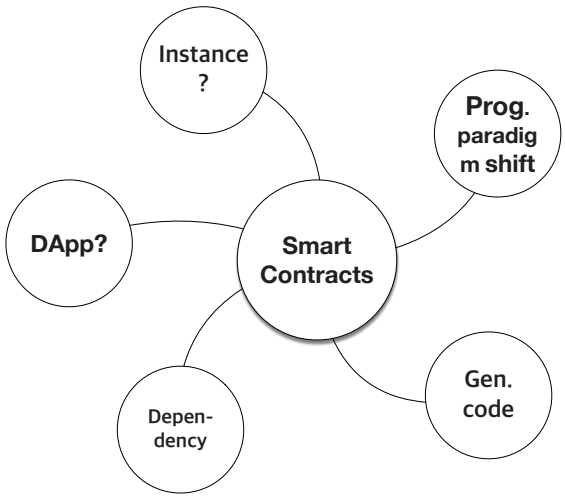


# Mythril vs. Oyente

| Vulnerable Contracts | Source | Oyente Analysis | Mythril Analysis |
|---|---|---|---|
| coinflip.sol | Hack This Contract | Callstack Depth Attack Vulnerability<br>Transaction-Ordering Dependence<br>Re-Entrancy Vulnerability | CALL with gas to dynamic address<br>Integer Underflow<br>Unchecked CALL return value<br>Weak random |
| erc20.sol | Hack This Contract | Callstack Depth Attack Vulnerability<br>Re-Entrancy Vulnerability | CALL with gas to dynamic address<br>Integer Underflow<br>Unchecked CALL return value |
| lostether.sol | Hack This Contract | Callstack Depth Attack Vulnerability | Integer Underflow<br>Unchecked CALL return value |
| naive.sol | Hack This Contract | | |

| Vulnerable Contracts | Source | Oyente Analysis | Mythril Analysis |
|---|---|---|---|
| delegation.sol | Zethernaut | | |
| fallback.sol | Zethernaut | | |
| fallout.sol | Zethernaut | Transaction-Ordering Dependence | Ether send |
| force.sol | Zethernaut | | |
| king.sol | Zethernaut | | |
| reentrancy_3.sol | Zethernaut | Re-Entrancy Vulnerability<br>Callstack Depth Attack Vulnerability | Unchecked CALL return value<br>CALL with gas to dynamic address |
| token.sol | Zethernaut | | Integer Underflow |

# New beginning



# 감사합니다.

jonghyup@gachon.ac.kr

The 24th Network Security Conference -Korea

# 암호화폐 거래소 보안 전략

**이은준** 라온시큐어 이사

### 학력 및 경력사항

경희 경영대학원 e-Business 석사
라온시큐어 이사

### 강연요약

최근 암호화폐 거래소에 대한 해킹 사고가 끊이지 않고 일어나고 있다.
암호화폐 거래소는 안전한 블록체인의 기술과 검증된 현실세계의 경제 체제의 고리로서 그 역할을 수행하고 있다. 암호화폐 거래소는 금융과 기술 사이의 새로운 비즈니스 영역이고 정책적으로나 기술적으로 많은 부분이 미흡한 상태로 서비스가 진행되고 있다.
향후 안정적인 암호화폐 생태계로서의 정착을 위해서 안전한 보안환경을 구축해야 하고, 그에 대하여 거래소에서 준비해야 할 사항과 참여자로서 수행해야 할 사항에 대한 구체적인 예를 제시하고자 한다.

# 가상화폐 거래소의 보안전략

2018.04.12 CP팀 이은준 이사

RAONSECURE

RAONSECURE

## 목차

I 회사 소개
II 암호화폐 생태계의 현주소
III 암호화폐 거래소의 보안전략

# Ⅰ. 회사 소개

RAON Secure

## 1. 일반현황

Ⅰ

### All about ICT Security, ICT 통합 보안 선도기업

| | | | |
|---|---|---|---|
| 회사명 | 라온시큐어(주) KOSDAQ 코스닥상장법인 | 대표이사 | 이순형 대표 |
| 설립연도 | 2012년 : 라온시큐어㈜ 공식 출범 | 직원수 | 150명 |
| 주요채널 | 홈페이지 : http://www.raonsecure.com<br>라온 화이트햇 센터 : http://www.whitehat.co.kr | | USIM 스마트인증 : http://www.usimcert.com<br>휴대폰 전자서명 서비스 : http://www.mobisign.co.kr |

Security First
**차세대 보안 선도기업**

FIDO 생체인증 기반
**통합 인증 플랫폼**

USIM 기반 본인확인 서비스
**보안 서비스 사업**

ISMS 인증 컨설팅과 모의해킹
**보안 인텔리전스**

**스마트하고 안전한 정보 사회 구현**

| | |
|---|---|
| 2016 | - **국민건강보험공단 장기요양 모바일정보시스템 사업 구축**<br>- 국민생활체육회 모바일 농업재해현장조사시스템 iOS 보안솔루션 구축<br>- 금융결제원 바이오정보 분산관리 시스템 구축사업 수주<br>- 롯데캐피탈㈜ 모바일뱅킹 구축<br>- 라온화이트햇 보안인텔리전스 서비스 론칭<br>- **미래에셋증권㈜ 스마트폰 앱 난독화 구축**<br>- 서울시도시철도공사 모바일망 사업<br>- **롯데제과 모바일 보안솔루션(MDM, 앱위변조 방지솔루션) 도입 사업**<br>- FIDO 생체인증 공급 확대(KT, LGU+, 부산/경남은행, 씨티은행, 현대카드, 신한카드 등)<br>- 광주소방본부 모바일 보안구축 도입 사업 |
| 2015 | - CJ Only One R&D Park MDM 구축<br>- **㈜한국스마트카드 고속버스 모바일앱 위변조 솔루션 구매**<br>- **근로복지공단 통합퇴직연금시스템 구축**<br>- 롯데손해보험 CM시스템 구축<br>- FIDO 생체인증기반 간편인증/결제 솔루션 출시, 국제 FIDO Certified 제품 인증 획득<br>- CC인증 : 모바일 단말관리(MDM/MAM) 솔루션 TouchEn mGuard |
| 2014 | - **동양생명보험 모바일 및 홈페이지 보안 솔루션 구축**<br>- **신한카드 모바일 소스코드 보호 솔루션 구축**<br>- 제 3회 정보보호의날 기념식 미래창조과학부 장관상 수상<br>- **KB생명보험 앱 난독화 및 보안솔루션 구축**<br>- KT 기업용 모바일 보안 사업 공동 추진 협약 체결<br>- 한국모바일인증 앱위변조방지 솔루션 구축<br>- 한국전자통신연구원(ETRI) 앱위변조 방지 솔루션 구축 |
| 2013 | - GS인증 : 모바일 단말관리(MDM/MAM) 솔루션 TouchEn mGuard |

RAONSECURE

## 2. 주요 사업영역

회사소개 I

RAON Line-up

ICT 보안에 필수적인 다양한 솔루션과 보안 서비스를 제공하는 통합 보안 선도 기업입니다.

### 01 보안 솔루션

**모바일 보안**
- 앱위변조 방지
- 보안 키패드
- 모바일 백신
- 암호/인증/단일인증(mSSO)
- 일회용 패스워드(mOTP)

**온라인 PC 보안**
- 키보드 보안
- 가상 키보드
- 웹페이지 보안
- 개인 PC보안
- 자동 가입 방지

**유비쿼터스/PKI**
- 모바일웹 전자서명
- 네트워크 암호/인증
- 기기 인증 보안
- XML 암호/인증
- 어플리케이션 인증

**통합계정관리**
- 단일인증(SSO)
- 권한관리(EAM)
- 계정관리(IM)

### 02 보안 서비스

**OnePass 간편인증**
- 명의인증 서비스
- 패스워드 필요 없는 간편인증

**USIM스마트인증**
- USIM 기반 인증 서비스
- USIM에 공인인증서 저장/발급 및 인증

**MobiSign**
- 휴대폰 전자서명 서비스
- 금결원 공동 서비스

**TOUCH 웹프린**
- 스마트폰 웹 브라우저에서 공인인증서 서비스 제공
- 서비스별 관리비용 절감 및 인증 편의성 제공

### 03 차세대 보안

**통합인증보안(FIDO)**
- FIDO 기반의 생체인증
- 공인인증서 패스워드 대체
- FIDO 기반의 mOTP/ PKI / SSO
- 이상 인증 탐지를 위한 FDS

**모바일 보안(EMM)**
- 모바일 단말관리 (MDM)
- 모바일 앱관리 (MAM)
- 모바일 컨텐츠관리 (MCM)
- 모바일 계정관리 (MIM)
- 모바일 위협관리 (MTM)

**보안 인텔리전스**
- 취약점 점검
- 국내 최정예 화이트해커에 의한 모의해킹 및 보안 감사 서비스 제공
- ISMS 인증 컨설팅



## 3. 핵심 역량

회사소개 I

핵심역량 및 고객사

주요 금융, 공공 분야 40% 이상의 시장에서 RAON SECURE 가 함께하고 있습니다.

### 1 핵심 기술력 확보
- 인증 및 특허 다수 획득, 검증된 보안 기술력 확보
  - 특허 등록 및 출원 : **총 45건** 원천 기술 특허 보유
  - 상표 등록 및 출원 : **총 18건** 상표권 보유
- 국정원 CMVP, CC 인증 등
- 차세대 보안 기술 확보
  - FIDO 기반 통합인증 플랫폼
  - TEE 기반의 보안 인증기술 (USIM, Trust Zone, HSM 등)

### 2 정보보안 컨설팅
- 국내 최고 화이트햇으로 구성된 해커 그룹 보유
- 선행 보안기술 연구, R&D 역량 강화
- ISMS 인증 / 컨설팅
- 국제 해킹 대회 참가 및 우승, 국위선양

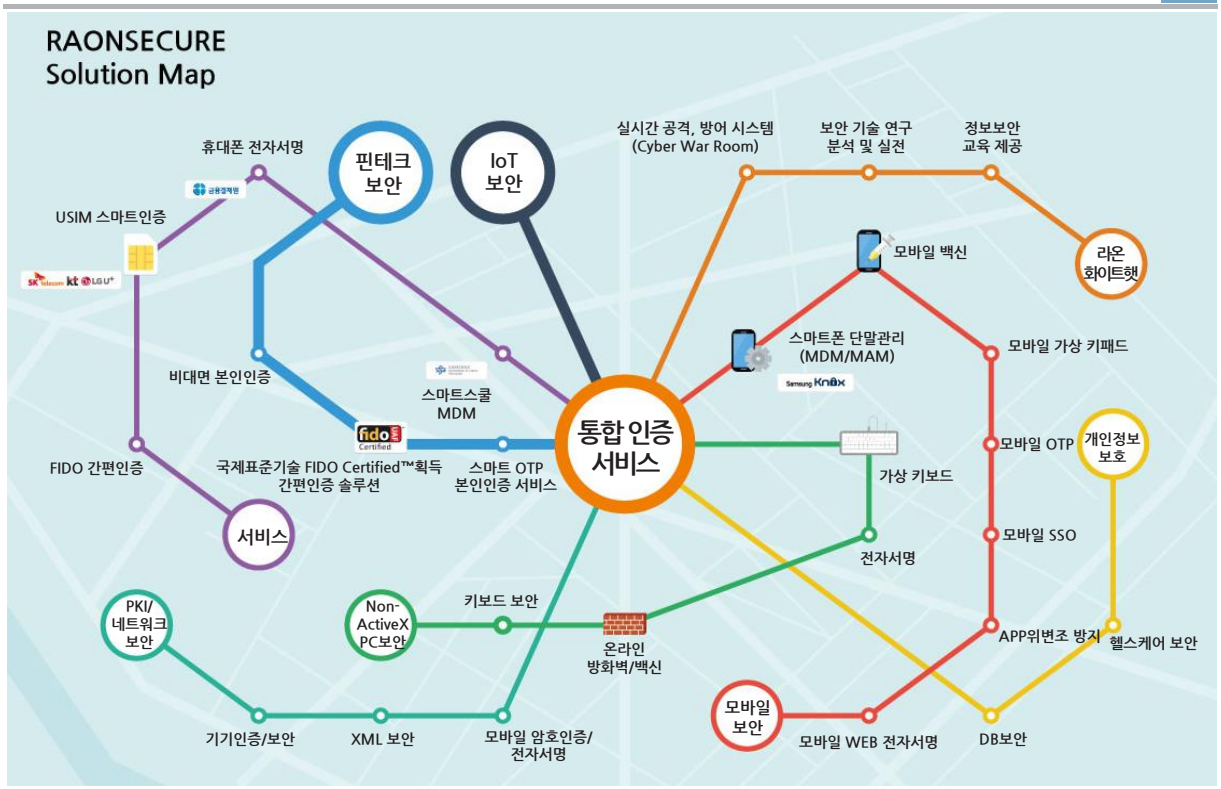
### 3 제조사 및 인증기관과의 기술/사업 협력
- 국내 최초 미국 애플社, MDM 공식 파트너
- 삼성전자 S.E.A.P 공식 파트너 (기술 제휴)
- LG전자 MDM 공식 파트너 (API 공유 협력)
- 휴대폰 전자서명, 인증서 이동 및 저장 제휴

### 4 플랫폼 변화에 따른 보안 신기술 표준 선도
- FIDO 기반의 통합인증 플랫폼 (세계 최초 FIDO certified 인증 획득)
- Window8 공인인증 PKI 기술 상용화
- 통신사 연계 모바일 보안토큰 'USIM스마트인증' 서비스
- 국내 통신사를 통한 SaaS형 MDM 플랫폼

| 금융기관 | 정부기관 | 일반기업 |
|---|---|---|
| 금융결제원, 우리은행, 신한은행 | 국세청, 안전행정부, 외교통상부 | SAMSUNG, LG U+, kt |
| IBK기업은행, KB국민은행, NH농협 | 보건복지가족부, 검찰, 대법원 | nhn, HYUNDAI, SK 케미칼 |
| KEB 하나은행, citibank, 하나HSBC생명 | 행정자치부, 국민건강보험공단, NPS 국민연금 | Hanwha, CJ 대한통운, 현대중공업 |
| Hyundai Card, LIG 손해보험, 롯데손해보험 | innovation21 함께하는병무청, 한국고용정보원, 대한주택공사 | GS 홈쇼핑, KISA 한국인터넷진흥원, 흥국생명 |
| think Next 삼성화재, Prudential, 동양생명 | 질병관리본부, 한국토지공사, 한국수출보험공사 | 현대제철, 신세계 인터내셔날, Gmarket |
| 삼성생명 SAMSUNG, IBK Insurance, SAMSUNG 삼성카드 | 국민건강보험공단, 기획재정부, 대한민국 국방부 | 인터파크, SNUH 서울대학교병원, ASIANA AIRLINES |

## 4. 솔루션 맵








# II. 암호화폐 생태계의 현주소

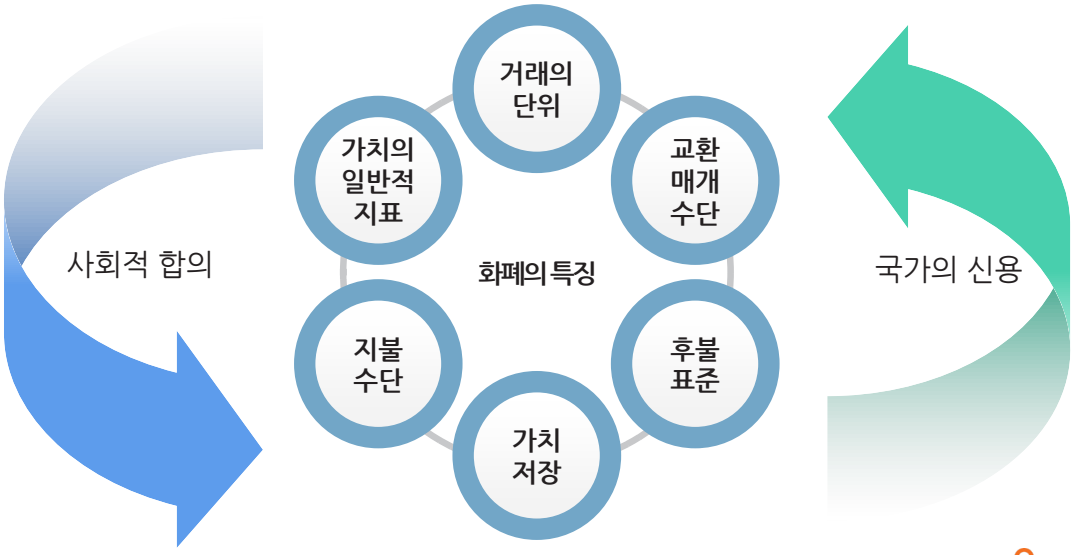
## 암호화폐

암호화폐 생태계의 현주소 II

### 화폐(Currency)란?

화폐는 국가의 주권 및 힘과 매우 긴밀한 관계를 맺고 있습니다. 현재 각국의 화폐는 모두 불환화폐-금이나 현물로 교환이 보장되지 않는 화폐-로 국가의 신용이 화폐의 가치를 말해주고 있습니다.

새로운 디지털화폐의 한 종류인 암호화폐-가상화폐, 비트코인 등-는 국가가 담보하는 신용이 존재하지 않습니다.




9

RAONSECURE

## 암호화폐

II

### 암호화폐(Cryptocurrency)의 탄생

▶ **미국발 금융위기가 한창이던 2008년에 나카모토 사토시라는 익명의 컴퓨터 프로그래머가 창안한 것이 암호화폐-비트코인의 시작.**

▶ **목표**

금융 기관을 거치지 않고 온라인 지불을 한 쪽에서 다른 쪽에게 직접 보낼 수 있는 "피어 투 피 어 (peer to peer) 현금 시스템" 을 만드는 것

▶ **시대적 배경**

- 2008년 금융위기
  복잡한 파생상품과 무분별한 A등급의 신용 승인
  서브프라임 모기지론의 붕괴로 인해 기존 은행 및 화폐 시스템은 한계

- 2009년 양적완화
  FED가 막대한 양의 달러를 찍어내면서 시장에 공급하는 양적완화가 시작
  돈-달라-의 가치 하락 : 더 큰 위기의 시작

▶ **암호화폐의 기존 발행체계에 지배되지 않는다.**

- 신용카드 회사와 같이 제 3자를 배제하고 구매자와 판매자가 직접 결제를 진행하는 방식
- 거래의 비용이 거의 발생하지 않는다와
- 누구나 계정을 쉽게 만들어 참여할 수 있다는 장점을 가지고 있음

bitcoin
ethereum
ethereum classic
Bitcoin Cash
Peer-to-Peer Electronic Cash
ripple

10

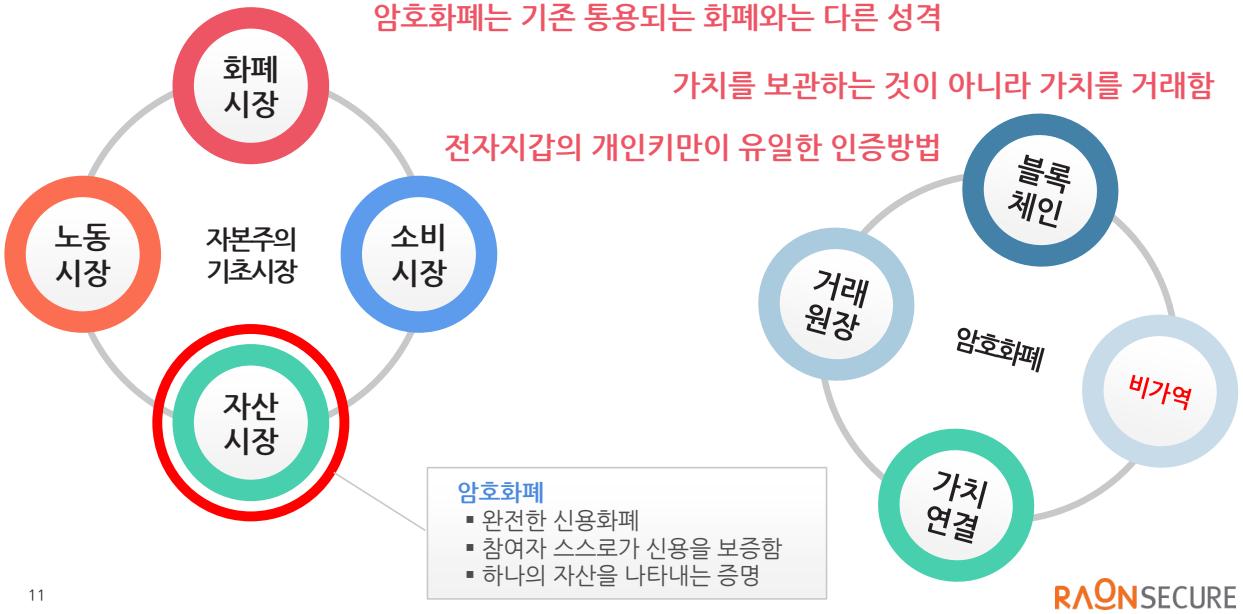
RAONSECURE

## 암호화폐 II

### 자본시장의 관점에서 본 자본과 암호화폐의 차이점

*자본주의란 무엇보다도 '화폐에 의해 생산이 일어나는 경제' 이다.* [출처] 자본주의특강_화폐, 권력, 자본주의 역사의 재구성

*돈은 이윤을 남기며 되팔기 위해 상품이나 노동을 사는 데 사용할 때만 자본이 된다.* [출처] 자본주의 바로알기




암호화폐는 기존 통용되는 화폐와는 다른 성격

가치를 보관하는 것이 아니라 가치를 거래함

전자지갑의 개인키만이 유일한 인증방법




**암호화폐**
- 완전한 신용화폐
- 참여자 스스로가 신용을 보증함
- 하나의 자산을 나타내는 증명



## 암호화폐 생태계의 위협 II

### 지금도 사기(Fraud)는 진행중이다

**2017년도 국내**

거래소 3곳에서 4차례 해킹

총 248억 원의 손실

개인정보도 3만건이나 유출

**2018년도 전세계**

들어 40만 달러 이상 암호화폐 사기 사건만 22차례 발생

첫 두 달간 암호화폐 사기 피해만 13억 6천만 달러
(1조 5천억)

트위터나 텔레그램에서 매일 발생하는 소규모 사기 건 제외
(최저피해액 40만 달러 미만)

[비트코인뉴스닷컴 인용]

**지난 10년 동안**

해커들이 훔친 비트코인과 이더리움

12억 달러(1조3천억원)정도로 추정

[금융정보 업체 오토노머스리서치]

**2018년도 전세계 예상**

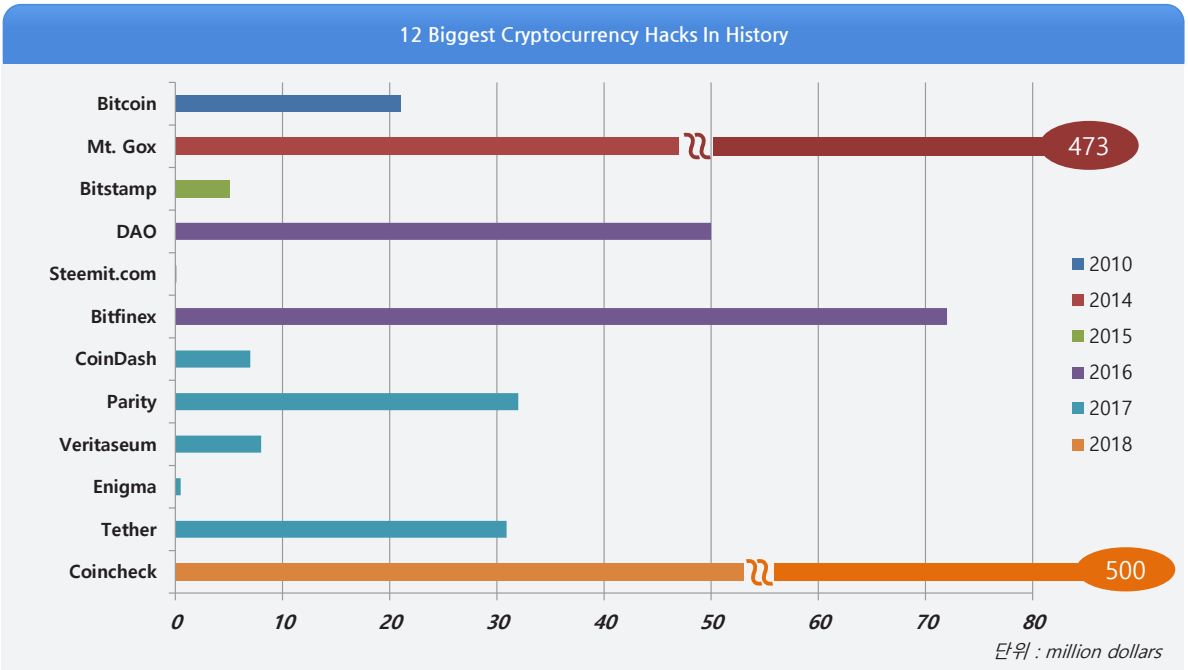
암호화폐 사기 피해액을 매일 정확하게 측정하는 것은 불가능

현 추세 유지시
사기 피해액은 32억 5천만 달러으로 추정
(3조 5천억)

## 암호화폐 생태계의 위협

II

### 주요 해킹사건 및 피해규모






## 암호화폐 생태계의 위협

II

### Why? 위협과 사고가 끊이지 않는가?

**구체적인 대상**

거래소라는 구체적인 해킹의 대상

암호화폐는 실체가 없다

**중앙집중식 시스템**

증권거래소 형식의 중앙집중식 거래 방식

계좌에 암호화폐를 보관

거래소의 전자지갑을 이용

**풍부한 유동성**

하루 거래 금액 10조가 넘는 유동성
(3/19 기준 업비트, 빗썸 합계 14조 8천억)

익명거래를 통하여 훔친 암호화폐의 현금화가 용이

**새로운 비즈니스 모델**

공격자가 좀 더 모델에 대한 공부를 많이 한다

새로운 공격형태

## 암호화폐 거래소의 중요성

II

### 거래소는 어떤 가치를 지니고 있는가?

**암호화폐의 현실화**

암호화폐는 거래를 나타내는 허상

가치를 화폐로 표현하고 그 가치를 거래할 수 있음

**사이버세상과 현실세상의 연결점**

가상의 통화를 현실의 통화와 연결시킴

다양한 암호화폐 간의 연결

중세 시장에서 지역화폐가 통용되던 시장에의 환시장 역할

**과거 디지털화폐와의 차이점**

화폐의 보조수단

기존 화폐와 교환을 통해서만 가치 존재

발행된 금액으로만 가치가 유지

**미래가치**

자립적으로 존재할 수 있는 모델

산업별로 특성화된 거래 기준으로서의 모델



## 주요 해킹사례와 시사점

II

### Mountain Gox사례

2010년 7월
제드 맥칼렙(Jed McCaleb)은 비트코인과 실제 통화 간 거래할 수 있는 웹사이트를 개발
세계 최초의 비트코인 거래소인' 마운트 곡스(Mt. Gox)'가 탄생
2014년 해킹으로 파산 신청하기 전까지 전 세계 비트코인 거래의 70~80%를 담당하는 세계 최대의 비트코인 거래소

2011년 3월
일본에 거주하는 프랑스인 개발자 마크 카펠레스(Mark Karpelès)가 마운트 곡스를 인수
2011년 6월
첫 번째 해킹이 발생하여 개인정보 유출로 875만 달러 피해

2014년 2월
두 번째 해킹으로 고객 비트코인 75만 개와 자사 비트코인 10만 개가 도난(당시 시세 4억 7,400만 달러 손실) - 파산

일본은 전자화폐 시장관리를 강화했고, 현재 코인체크와 같은 가상화폐 거래소는 금융당국에 등록하도록 돼 있다.

## 주요 해킹사례와 시사점 II

### 유ㅇ파산사례

2017년 4월
해커의 공격으로, 야ㅇㅇ 거래소의 Hot-Wallet(인터넷망에 연결된 코인지갑) 4개가 탈취
총 피해규모는 3831비트코인(당시 시세 55억 상당)이며, 이는 야ㅇㅇ이 보유하고 있는 회원의 총자산의 37.08%에 해당하는 규모

원화예치금은 100% 은행에, 암호화폐 예치금은 70%를 콜드월렛에 예치하여야 하는 예치자산 보호장치 마련

2017년 12월
거래소 '유ㅇ'이 해킹 공격을 받아 고객자산 17%가량을 도난 당한 후 파산을 선언
핫월렛에 있던 코인만을 도난 당함



## 주요 해킹사례와 시사점 II

### NEM 해킹 사례

2018년 1월
일본 최대 암호화폐(가상화폐) 거래소인 코인체크에서 580억엔(약 5700억원)어치 가상 화폐 뉴이코노미무브먼트(NEM)가 해킹
해킹 당시 네트워크에 접속된 '핫 월렛(Hot wallet)'에서 NEM을 관리

[기술적인 어려움과 그 기술을 가진 인재가 부족]해서 콜드 월렛에 보관하지 않았다고 해명

익명화폐
익명화폐는 송금하는 쪽 주소를 일회 용 주소로 하거나 거래할 때의 데이터를 섞어서
보내는 사람과 받는 사람이 누구인지 추적할 수 없는 거래 특징
익명화폐는 자금세탁과 세금도피에 사용되기 쉬운 점

## 주요 해킹사례와 시사점 II

### 관심을 가질만한 사례

암호화폐 거래소인 폴로닉스(Poloniex)를 흉내 낸 사이버 범죄 행위
- 범죄자들은 폴로닉스의 공식 모바일 앱이 없다는 것을 발견
- 자신들이 폴로닉스라는 이름의 앱을 만들어 앱스토어인 구글 플레이에 등록
- 2017년도 8월부터 9월까지 약 5천 건이 다운로드

크리덴셜만 보안의 중점이 아님. 다양한 채널을 통한 사기가 진행될 수 있음

빗썸의 개인정보 유출
- 회원들의 개인정보를 직원PC에 저장했다가 벌어진 해킹
- 전체 회원 수의 3% 수준에 달하는 이용자들의 개인정보가 해킹
- 1인당 10만원의 피해 보상 결정

개인정보 관리 체계의 부재. 서버 해킹을 위해서 직원의 PC를 우선적으로 해킹 시도함

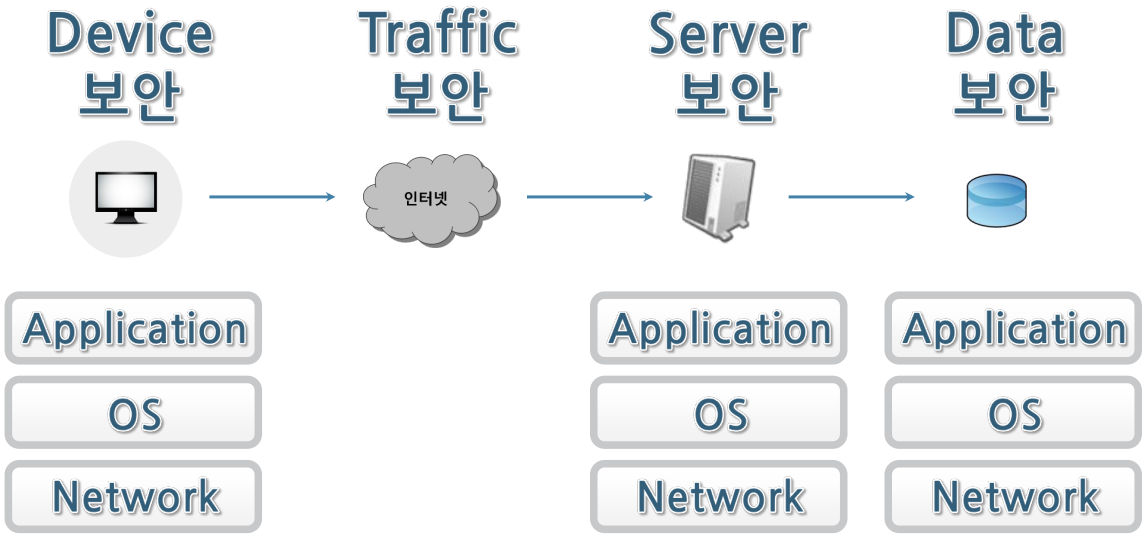


# III. 암호화폐 거래소의 보안전략

## 보안관련 검토 사항

III

### 보안맵






## 보안관련 검토 사항

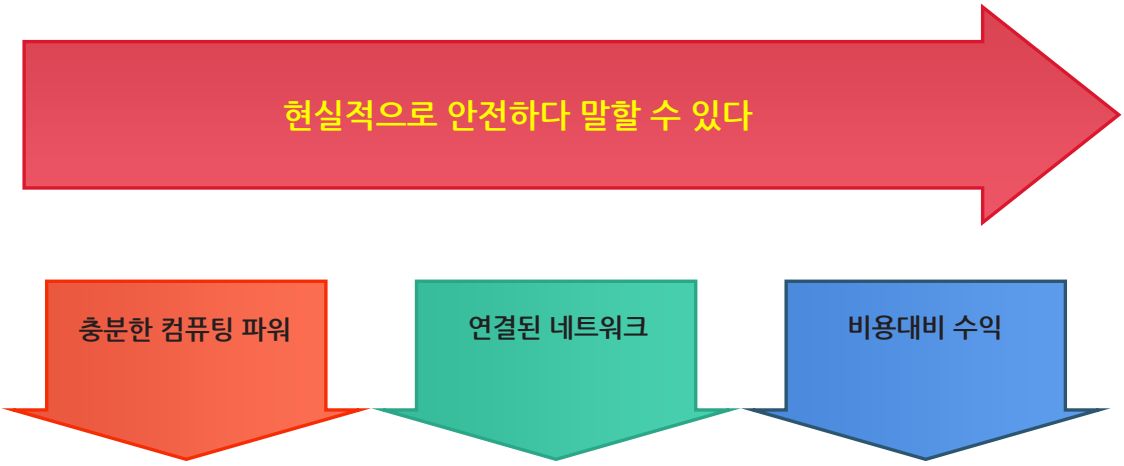
III

### 정보보안 시스템구성 다이어그램

## 과연 블록체인은 안전한가

III

### 현실적인 안전성




- 참여자가 줄어들 경우
- 고속연산 기술의 도입의 경우

**스텔라루멘(XML)**

블랙 월렛(BlackWallet)을 해킹

40만 달러 무단 인출

관리자 계정을 탈취 DNS 조작

- 대상 코인의 전체 가격이 관리비용보다 커진다면?



## 과연 블록체인은 안전한가

III

### 거래소 모델은 블록체인이 아니다

**평균적으로 높은 보안수준**

일반 기업대비 높은 보안수준

다양한 보안 기술의 습득 및 적용에 노력

**금융권에 미치지 못하는 보안수준**

전자상거래업으로 고객자산 보호 불가

금융권과 비교하면 현저히 떨어지는 보안 환경
(수십년간 준비한 보안환경)

**기존 방식의 거래소 시스템**

증권거래소 형식의 중앙집중식 거래 방식

이미 해커에게 익숙한 대상 시스템 구성

**전자지갑 개인키의 탈취**

블록체인을 공격하는 것이 아니라 거래소의 지갑을 공격

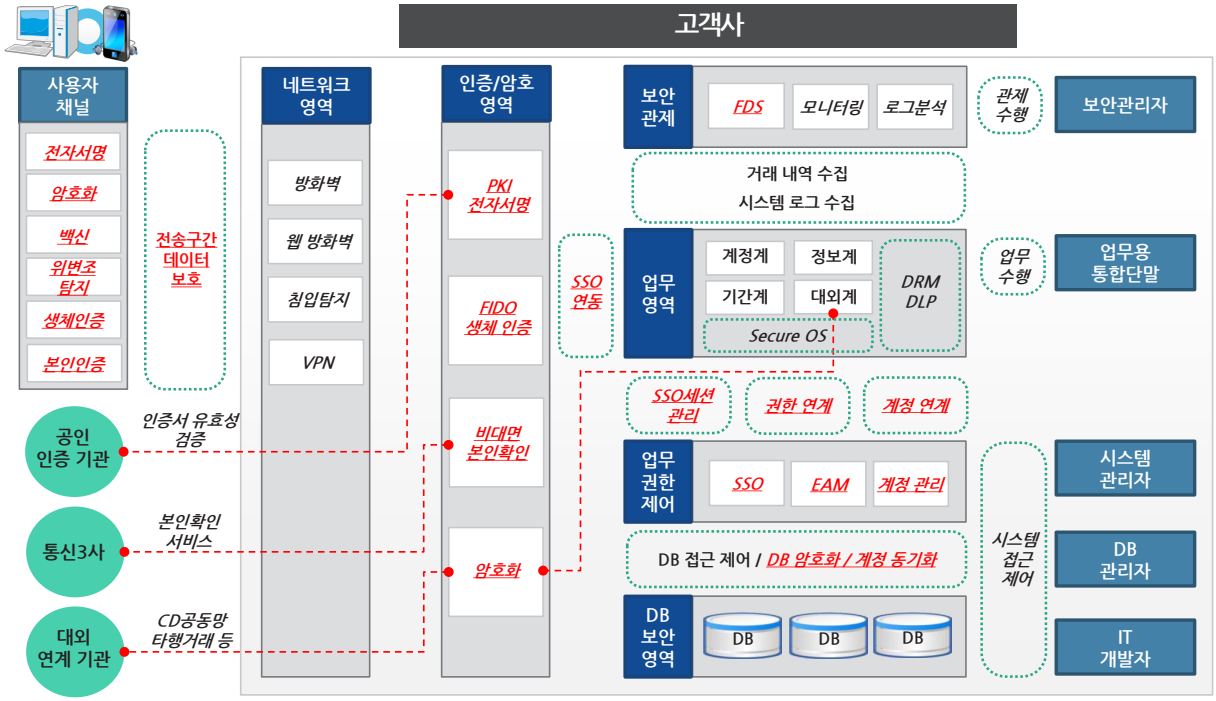
지갑의 비밀키를 탈취하면 암호화폐의 거래 가능

콜드월렛 적용 의무화

## 암호화폐거래소 모델로 구성된 보안솔루션 도입

III

### 유사 비즈니스 모델 검토 - PG(Payment Gateway)






## 현실은 그렇지 않다

III

### 암호화폐 거래소의 보안수준 향상은 왜 어려운가

01

**규모가 작다**

- 거래규모에 비하여 자본금 등 회사 규모가 상대적으로 작업 (금융권 기준)
- 조직적인 대응 등이 어려움
- 침입차단 시스템, 위협관리시스템, 보안관제시스템 등 보안 구축을 위한 리소스 확보가 어려움

02

**인력이 부족하다**

- 신기술을 이용한 서비스로 숙련도 높은 개발인력이 부족
- 시장의 확대와 더불어 개발 인력 확대가 되지 않고 있음(기술적 난이도 높음)

03

**신규사업 모델에 대하여 경험이 부족하다**

- 다양한 리스크에 대한 분석 및 대응방안이 미흡
- 매일 매일 새롭게 변화하는 사업환경
- 정부 규제 등에 대하여도 아직 정립되지 않은 상황

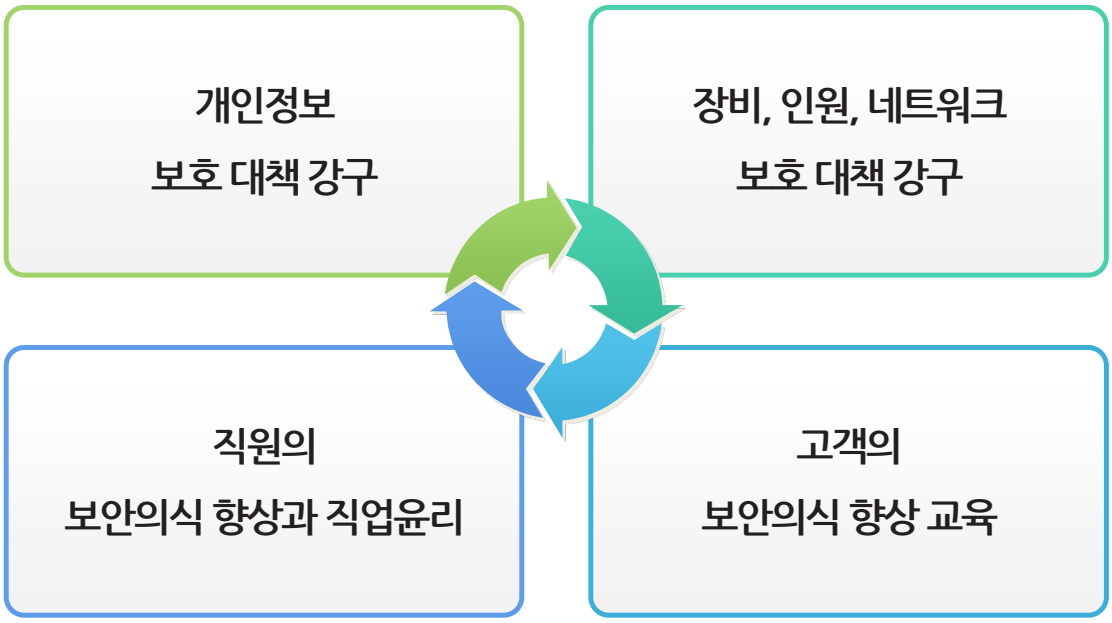
04

**공격자에게 매력적이다**

- 한 도둑을 열사람이 막을 수 없다
- 자체 개발자가 보안을 공부하는 속도보다 공격자가 보안을 공부하는 속도가 더 빠르다
- 공격자가 일단 성공하면 상당한 금액이 보장된다

## 지금 당장 해야할 일

III




27

RAONSECURE

## 방향성

III

암호화폐 거래소는 앞으로 어떻게 해야 하는가?

- 해외 사례에 대한 꾸준한 관심과 대처
- 유사 업종의 보안 수준으로 보안성 확보
- 상시 모니터링 체계 구축
- IT Compliance 준수

28

RAONSECURE

## 방향성

III

암호화폐를 사용하려는 사용자는 앞으로 어떻게 해야 하는가?

- 개인키의 안전한 보관
- 암호화폐 계좌의 분산 관리
- 안전한 디바이스 환경 유지 - 백신 등
- 추가적인 인증수단의 선택 및 비밀번호 관리 철저

29

RAONSECURE

# 감사합니다.

라온시큐어 이은준 이사 / ejlee@raonsecure.com

fido UAF Certified
FIDO 생체/간편 인증
raonsecure.com/onepass

USIM 스마트인증
www.usimcert.com

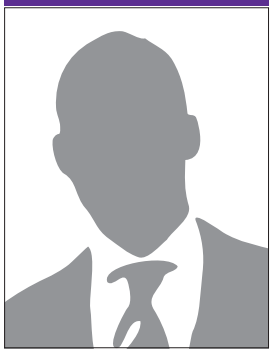
터치엔샘
touchen.raonsecure.com

화이트햇센터
whitehat.co.kr

주소 : 서울시 강남구 봉은사로 86길 6(삼성동, 레베쌍트빌딩 6~7층)
Tel. 02-561-4545 / Fax. 02-561-5343

RAONSECURE

The 24th Network Security Conference -Korea



# 제어시스템 보안 기술 동향

**민병길** NSR 선임

### 학력 및 경력사항

2002.03 ~ 2004.02 포항공과대학교 컴퓨터공학 석사
1994.03 ~ 2002.02 충북대학교 컴퓨터공학 학사
2004.02 ~ 현재 국가보안기술연구소 선임연구원
원자력시설 설계기준위협 설정회의 자문위원
인천국제공항공사 사이버보안 자문협의회 자문위원
ISO27001 선임심사원

### 강연요약

국가기반시설 및 산업 현장 설비를 감시, 운영하는 제어시스템에 대한 사이버 위협과 공격은 계속 증가 추세에 있습니다. 2015, 2016년의 우크라이나 대규모 정전 사태는 제어시스템에 대한 사이버공격에 의한 피해라는 분석도 잘 알려진 사실입니다. 이에 따라 다양한 제어시스템 보안기술 개발 노력이 이루어지고 있습니다. 본 발표에서는 제어시스템 보안위협 동향과 보안기술 개발의 어려운 점을 살펴보고, 국내외에서 수행되고 있는 제어시스템 보안기술 개발 현황과 발전 방향들을 살펴보고자 합니다.

## 제어시스템 보안 위협

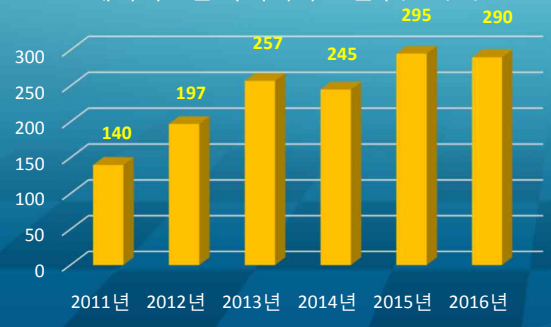
### 제어시스템 사이버사고 신고 건수 지속 증가

- 2011년 140건에서 2016년 290건으로 100%이상 증가

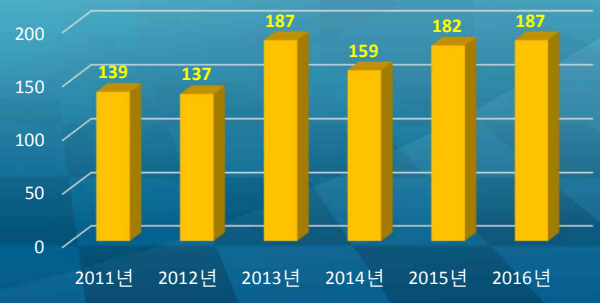
### 제어시스템 보안취약점도 지속적으로 발견

- 공개된 제어시스템 관련 취약점은 실제 취약점 규모의 1%에 불과한 것으로 추정(Macaulay & Singer)
  - 제어시스템 보급률, 제조사 등을 고려 시 전체 CVE중 10%가 취약점이어야 함(현재 0.1%불과)

제어시스템 사이버사고 건수(FY 기준)




제어시스템 취약점 건수(FY 기준)




* 출처: ICS-CERT Monitor(2011-2016), DHS

# 제어시스템 보안 위협(cont.)

## 제어시스템 사이버보안 침해 사고 주요 사례

**2010. 7.**
이란 원전 시설에 제어시스템 최초의 악성코드(Stuxnet) 감염

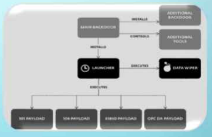
**2012. 7.**
사우디아라비아 아람코社에 악성코드(Shamoon) 감염

**2014. 7.**
미국과 유럽의 에너지분야 제어시스템의 기밀정보 탈취를 위한 스파이 활동 포착

**2014. 1.**
일본 몬주 원자력발전소 악성코드 감염으로 내부정보 유출

**2014. 12.**
독일 철강회사 용광로 제어시스템 공격으로 물리적 피해 유발

# 제어시스템 보안 위협(cont.)



**2015. 12.**
우크라이나 사이버공격으로 대규모 정전 (Black Energy 3)

**2016. 4.**
독일 원자력 발전소 악성코드(Ramnit, Conficker) 감염

**2016. 12.**
전력 제어시스템 특화 악성코드로 우크라이나 키예프 정전 (Industroyer)

**2016. 3.**
제어기기(PLC)상에서 감염·전파되는 악성코드 출현 (PLC Blaster)

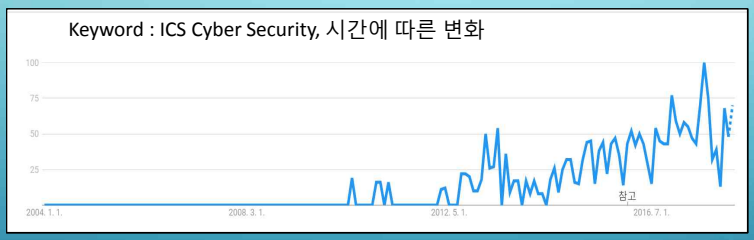
**2017. 2.**
제어시스템 특화 랜섬웨어 출현 (LogicLocker)

# 제어시스템 보안 관심

## 제어시스템 사이버보안 관심도(度) 변화

### 제어시스템 사이버보안 관심도 지속 증가 추세

- 제어시스템 사이버보안 키워드는 2010년 등장 이후 지속적 관심 증가 추세



Keyword : Industrial Control System, 지역 관심도

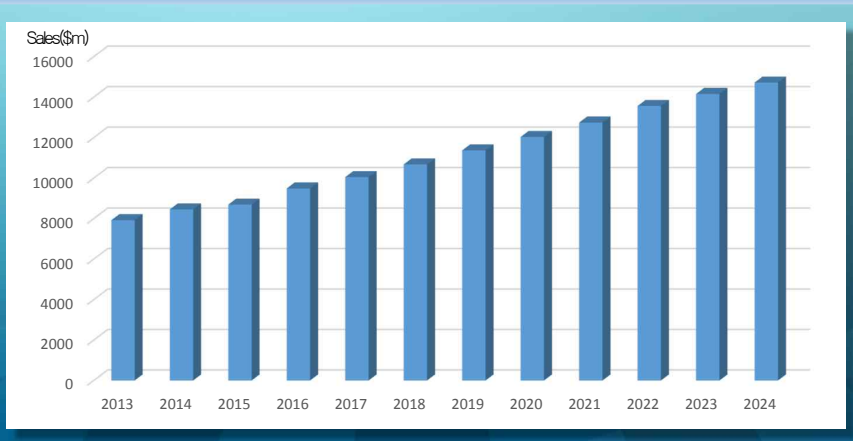
* 출처: Google trends

# 제어시스템 보안 시장(예측)

## 제어시스템 보안 글로벌 시장 규모

### 제어시스템 보안기술은 연평균 6%의 높은 성장 추세

- 연평규 성장률(CAGR) 6%, 2024년 140억$ 규모로 성장 예측




* 출처: Utilities Infrastructure Security Market Forecast(2014-2024), Visiongain

# 제어시스템 보안기술 동향(주요 기술들)

| 분류 | 기술명 | 제어 레벨 | 적용 범위 | IT 보안 기술 | 제어 보안 기술 | 비고 |
|---|---|---|---|---|---|---|
| 취약점 분석 (예방, 분석) | Scanner(S사이트) | L4, 3, 2 | TCP, DNP3, Modbus 등 | O | O | 제어기기 스캐닝 |
| | Scanner(C제품) | L2, 1 | TCP, Ethernet 기반 | O | O | 취약점 스캐닝 |
| | Nessus | L2, 1 | TCP, Ethernet 기반 | O | O | 취약점 스캐닝 |
| 접점 보안 기술 (예방, Unidirectional G/W) | 물리적 일방향 장치 | L2, 1 | TCP, DNP3, Modbus TCP등 Ethernet 기반 | O | O | |
| | W社, O社 등(외산) | L2, 1 | TCP, DNP3, Modbus TCP등 Ethernet 기반 | O | O | |
| | K社, N社 등(국산) | L2, 1 | TCP, DNP3, Modbus TCP등 Ethernet 기반 | O | O | |
| 산업용 방화벽 (예방) | T社 add-on F/W | L2, 1 | TCP, DNP3, Modbus 등 | X | O | 비표준 제어 프로토콜 미지원 |
| | I제품(국내개발) | L2, 1 | DNP3, Modbus 등 Ethernet 기반 | X | O | 비표준 제어 프로토콜 미지원 |
| | F제품(국내개발) | L2 | Ethernet 기반 | X | O | |

# 제어시스템 보안기술 동향(주요 기술들)

| 분류 | 기술명 | 제어 레벨 | 적용 범위 | IT 보안 기술 | 제어 보안 기술 | 비고 |
|---|---|---|---|---|---|---|
| 산업용 침입탐지 시스템 (탐지) | Q제품 | L2, 1 | DNP3, Modbus TCP등 Ethernet 기반 | O | O | Snort Add-on |
| | 이상징후탐지(W/L) (국내개발) | L2 | Ethernet 기반 | X | O | |
| | R社 ICS ID | L2, 1 | DNP3, Modbus 등 Ethernet 기반 | X | O | |
| | G社 O제품 | L2 | DNP3, Modbus 등 Ethernet 기반 | X | O | FW, IDS, IPS 기능 |
| Host-based 제어 시스템 보안기술 (예방) | M社(외산), A社 T제품(국산) | L2 | Windows 기반 | X | Δ | |
| 통합 분석 기술 (분석, 대응) | G社 S제품 | L2, 1 | 자사 제어기기 | O | O | 상용보안기술 통합&커스터마이징 |
| | E社 O제품 | L2 | 자사 제어기기 | O | O | 상용보안기술 통합&커스터마이징 |
| | S제품 | L1, 0 | 제휴 PLC | O | O | 제어시스템 별 분석 필요 |
| | A제품 | L2 | - | O | X | LOGIIC, NIST 1800-7 사례활용 |

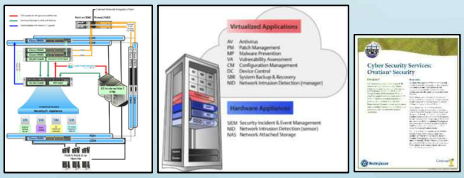
# 제어시스템 보안기술 동향(cont.)

## 정부·연구기관 주도에서 운영기관·공급社로 연구 주체 확대

- 제어시스템 위협·취약점 분석, 테스트베드 구축(정부·연구기관 주도)에서 제어시스템·기기 개발 시 보안기술 적용으로 확대

- 美 에너지부(DOE) 국가제어시스템 테스트베드(NSTB) 구축
  - 6개 국립연구소 중심으로 17개 테스트베드 구축(2003~)
  - 2011년까지 38개 제어시스템 취약성 분석
- 美 에너지부(DOE) CEDS(Cybersecurity for Energy Delivery Systems), TCIPG(Trustworthy Cyber Infrastructure for the Power Grid) 프로그램
  - 국립연구소, 학계, 산업계, 운영기관이 참여하여 실증 단계 까지 추진(2006~)
  - 트래픽 시각화(Sophia), 방화벽(Padlock), 게이트웨이(SIEGate) 등 개발
- EU FP7 프로그램 (2007~2013)
  - 보안위협 분석과 관리를 위한 ESCoRTS, VIKING, CockpitCI, PRECYSE, SPARK 등의 세부 프로젝트 수행
- 일본 제어시스템 보안센터(CSSC : Control System Security Center) 설립(2012~)

- IT 기반 제어시스템(서버, HMI 등)에 상용 보안기술 적용
  - LOGIIC 프로젝트(2006~2016, 10개 프로젝트 수행)
- 운영기관 차원에서의 트래픽 분석, 탐지 방안 연구, 적용(2016)
- 제어시스템, 기기 공급社에서 자사 검증을 통한 보안 솔루션 개발, 제어기기 개발 시, 보안기능 적용
  - SIEMENS TIA Portal, S7CommPlus Protocol에 암호화, 인증기능 적용
  - Westinghouse, 원전 계측제어시스템에 보안기술 적용(2013)
  - Emerson, Ovation 시스템에 보안 솔루션 구현(Ovation Security Center)
  - GE, Mark 시리즈에 보안기능 연동 솔루션 개발(GE Security ST)(2013)



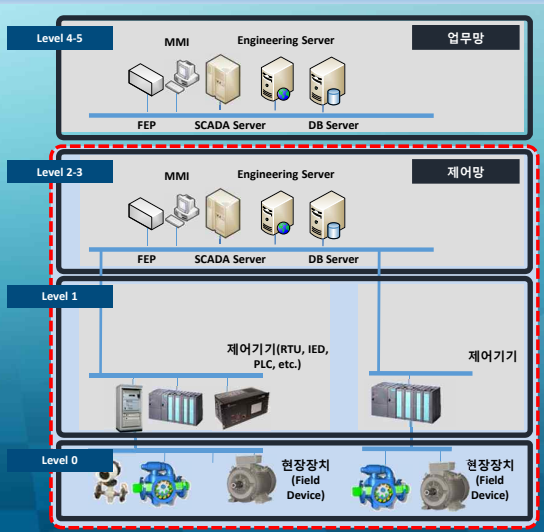

# 제어시스템 보안기술 동향(cont.)

## 제어기기, 제어시스템 특화 보안 기술 개발로 연구 영역 확대

- 네트워크 접점 보안, Level 2-3 보안기술에서 제어시스템 특화, Level 1-0 보안 기술로 영역 확대

- 네트워크 접점 보안기술, Level 2-3 보안 기술
  - Unidirectional gateway/일방향 자료전달 시스템 (Waterfall社, Owl社, NSR, KDN社, NNSP社 등)
  - 산업제어시스템 방화벽(Tofino社, ETRI, NSR 등)
  - 네트워크 이상 징후 감시 시스템
  - Whitelisting 백신(McAfee社, AhnLab社 등)

- 제어시스템 프로토콜, 운영정보 분석 기술, Level 1-0 보안 기술
  - DPBI(Deep Packet Behavior Inspection) 기반 탐지 기술
  - 제어시스템 운영 정보 분석 및 탐지




* 출처: ISA ICS model 참조

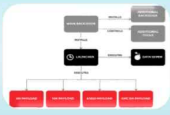
# 제어시스템 보안기술 동향(cont.)

## 새로운 보안위협 등장, 새로운 보안기술 접근

- 제어기기 간 감염 가능한 PLC worm, 제어시스템 랜섬웨어, 모듈화된 악성 코드 등장
- 인공지능, 클라우드 기반 제어시스템 플랫폼 및 보안서비스·기술 개발

- **PLC Blaster Worm(2016 Black Hat Asia)**
  - SIEMENS PLC를 대상으로 PLC 전이되는 Worm 시연

- **Industroyer(CrashOverride, 2016)**
  - 2016년 우크라이나 대규모 정전 사태에 이용
  - 전력제어시스템 타겟 모듈(IEC 60870, 61850, OPC DA)



- **LogicLocker Ransomware(2017)**
  - Schneider, Allen Bradley PLC를 대상으로 하는 랜섬웨어(PoC)

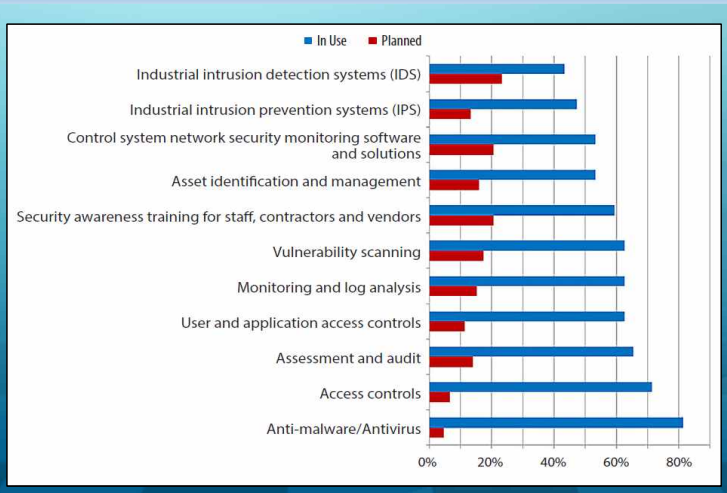
- **Machine Learning, AI 기반 제어시스템 보안기술 개발**
  - 제어 트래픽, 운영 정보에 대한 학습 및 이상 행위 탐지
  - 제어시스템 운영 현황 예측 시스템

- **Cloud 기반 제어시스템 서비스 및 보안기술 개발**
  - IT, OT 빅데이터 수집 및 분석을 통한 관리 및 보안

# 제어시스템 보안기술 동향(cont.)

## 탐지, 예방(Intrusion prevention) 기술 수요가 확대될 것으로 예상

- 백신(Anti-malware), 접근통제, 취약점 점검 기술에서 신속한 탐지, 예방 기술로 제어시스템 보안기술 적용이 확대될 것으로 예상




* 출처: Securing Industrial Control Systems 2017(SANS Institute InforSec Reading Room)

NSR
국가보안기술연구소
감사합니다

The 24th Network Security Conference -Korea

# Is it ICS Malware or No–malware?

**손태식** 아주대 교수

### 학력 및 경력사항

한국전력 정보보안 자문위원
IEEE Senior Member, 한국정보보호학회 이사
한국정보처리학회, 한국산업보안학회, 디지털포렌식학회 이사
Illinois Institute of Technology, Visiting Professor, 2017
국가정보원 정보보안 실태평가 평가위원, 2016
스마트그리드 핵심 보안기술 개발 자문위원 2016
원전 사이버보안 워킹그룹 운영위원 2016
삼성전자 통신연구소, DMC연구소 책임연구원, 2011
University of Minnesota, Research Scholar, 2004
고려대학교 정보보호학 공학박사

### 강연요약

지난 2010년 Kaspersky Lab에 의해 처음 알려졌던 Stuxnet 악성코드는 이란 원자력발전소의 PLCs(Programmable Logic Controllers)를 포함한 원전 내부 시스템들을 대상으로 사이버공격을 수행하였었고, 이후 발전을 포함한 다양한 산업제어시스템(Industrial Control System: ICS)을 대상으로 하는 Duqu, Flame(Flamer, sKyWIper), Gauss, Shamoon, Havex, Blackenergy2, Blackenergy3, Duqu2.0와 같은 여러 종류의 악성코드들이 나타나고 있다. 특히 2015년 12월 우크라이나 정전 사태와 같이 실제 ICS 시스템에 대한 사이버공격을 위해 만들어진 악성코드들에 의해 전력제어시스템이 영향을 받는 사례들이 최근 보고되고 있으며, 본 강연에서는 2015–2016년 우크라이나 사태에 영향을 준 Crashoverride와 또한 최근 제어시스템 악성코드로 알려진 Trisis/Triton 악성코드에 대한 분석, ransomware로 잘 알려진 Wannacry/Petya의 제어시스템에서의 위험성에 대한 분석, 그리고 Mining 관련 malware를 분석하여 그들의 특성에 기반한 탐지 및 대응방법에 대해 논의해 본다.

# Is it ICS Malware or No-Malware?

- Malware or not?
- Malware for ICS?

- ICS Malware Trends
- Malware Analysis I
  - Crashoverride / Industroyer
- Malware Analysis II
  - TRITON
- Malware Analysis III
  - WannaCry & Petya
  - Cryptojacking
- How to Predict/Prevent, Detect and Response?

## US Power Company Fined $2.7 Million Over Data Exposure - Two violations of the NERC CIP

### VIOLATION DESCRIPTIONS

- **A third-party PG&E contractor exceeded its authorized access by improperly copying certain PG&E data from PG&E's network environment to the contractor's network environment.**
  - While the data was on the contractor's network, a subset of live PG&E data was accessible online without the need to enter a user ID or password.
- **CIP-003-3 R4. Information Protection**
  **CIP-003-3 R5. Access Control**

US Power Company Fined $2.7 Million Over Data Exposure

Grid Regulator Says Company Left Critical Data Exposed for 70 Days

Mathew J. Schwartz (@euroinfosec) · March 14, 2018 · 0 Comments

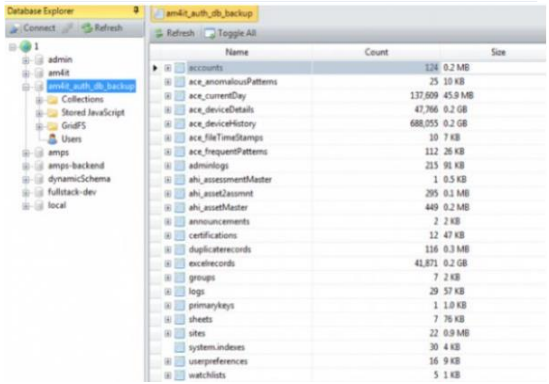
| Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation | | | | | | |
|---|---|---|---|---|---|---|
| **NERC Violation ID** | **Standard** | **Req.** | **VRF/VSL** | **Discovery Method*** | **Risk** | **Penalty Amount** |
| WECC2016016233 | CIP-003-3 | R4 | Medium/ Severe | SR | Serious | $2.7M |
| WECC2016016234 | CIP-003-3 | R5 | Lower/ Severe | | | |

출처 : NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No.NP18-_-000

Pacific Gas and Electric Claims Recent Data Breach Only Exposed Fake Details *UPDATED*

PG&E denies any wrongdoing, says it was only a test server

May 31, 2016 01:55 GMT · By Catalin Cimpanu · Share:

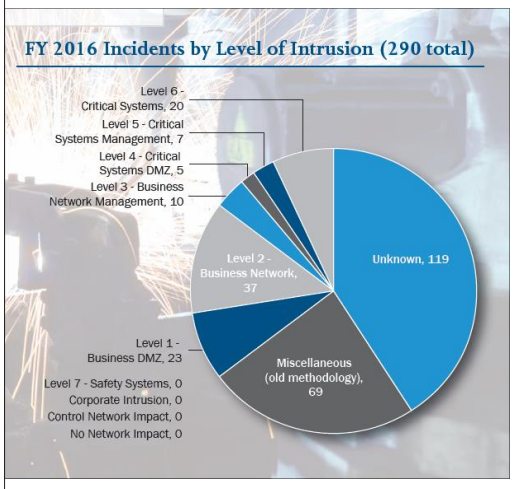


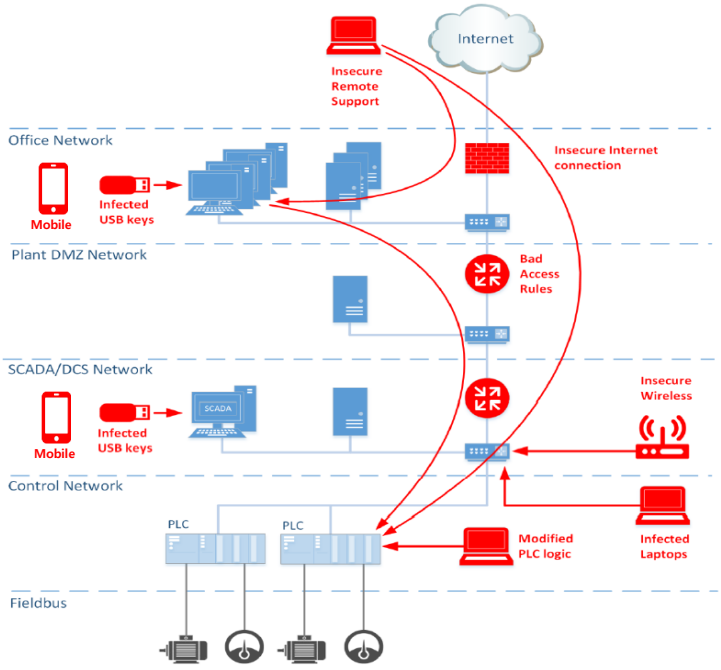
출처 : SOFTPEDIA NEWS, 2016.May.31

# ICS Malware Trends



ICS Malware Trends

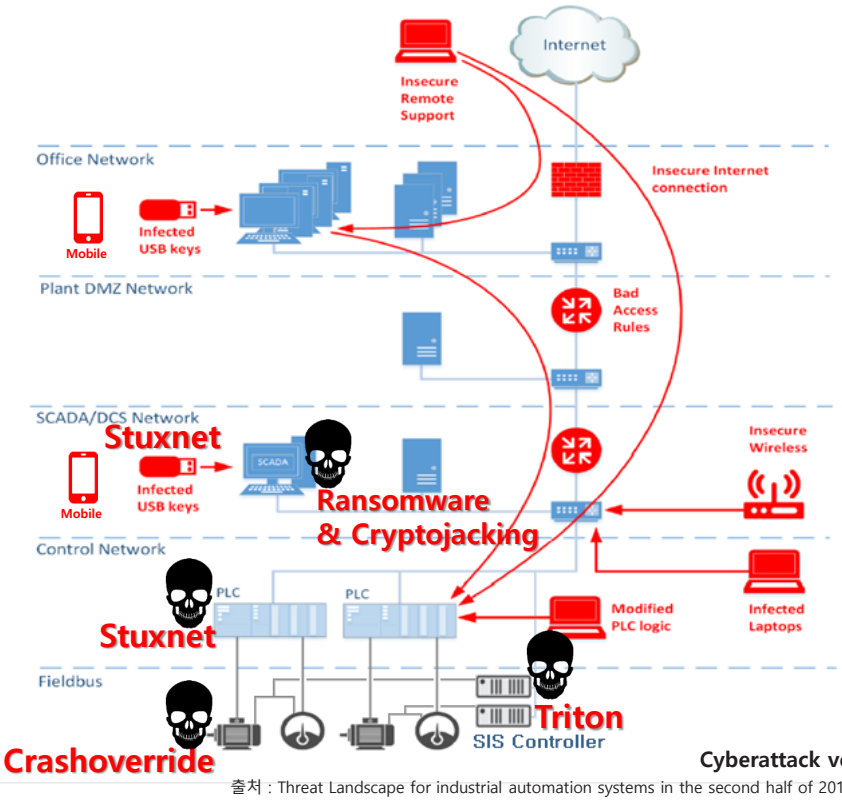



Cyberattack vector

출처 : Threat Landscape for industrial automation systems in the second half of 2016, Kaspersky lab – ICS CERT

# ICS Malware Trends



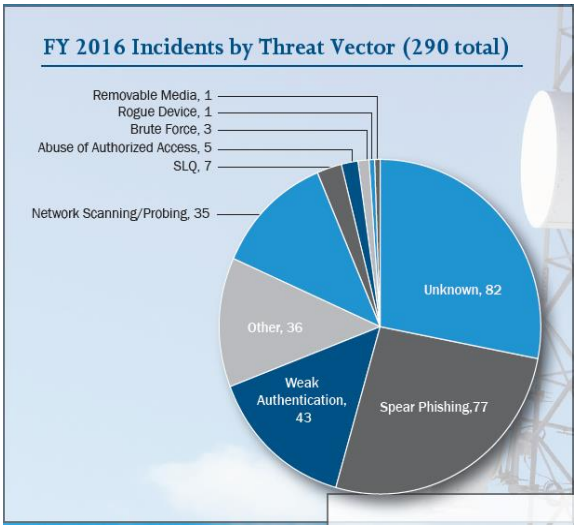

Cyberattack vector

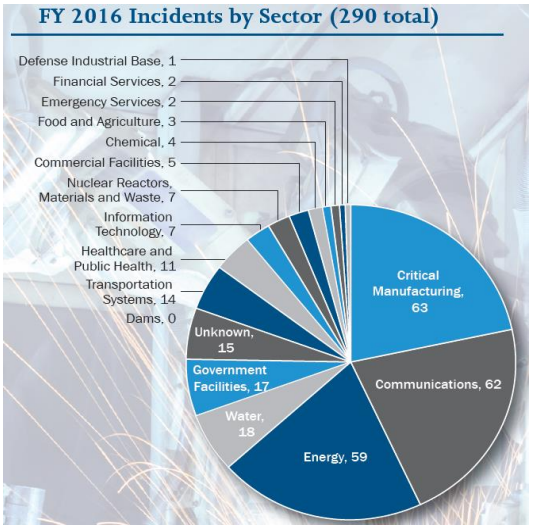
출처 : Threat Landscape for industrial automation systems in the second half of 2016, Kaspersky lab – ICS CERT



# ICS Malware Trends

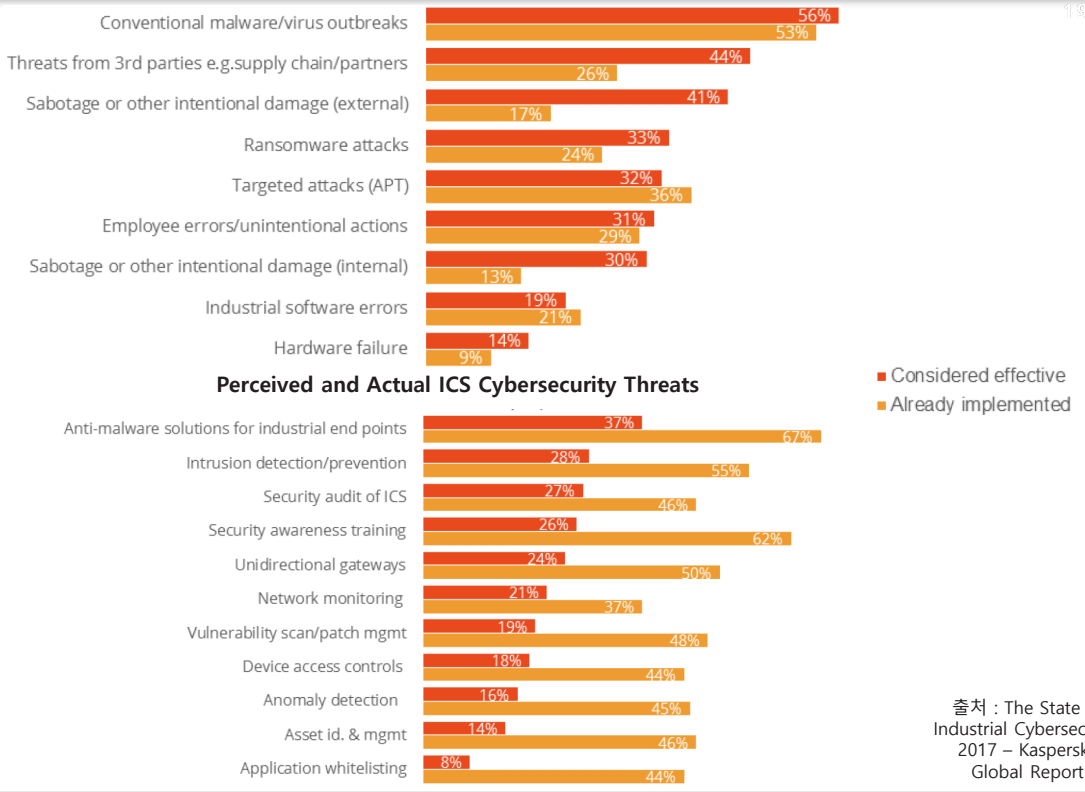
- **In FY 2016, the ICS-CERT Incident Response team completed work on 290 incidents.**
  - **The Critical Manufacturing Sector accounted for 63 of these incidents, while the Communications Sector had 62 and the Energy Sector had 59. Spear phishing represented 26 percent of these incidents, making it the leading access vector for ICS-CERT's FY 2016 incidents. Network scanning and probing accounted for 12 percent.**




출처 : Fact Sheet_IR Pie Chart FY2016 - ICS-CERT

# ICS Malware Trends




**Perceived and Actual ICS Cybersecurity Threats**




출처 : The State of Industrial Cybersecurity 2017 – Kaspersky Global Report

**Perceived Effectiveness and Implementation of ICS Security Measures**



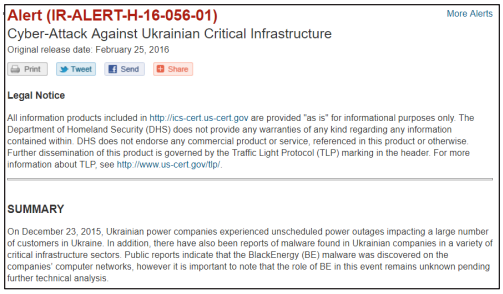
# Malware Analysis I

# - BlackEnergy / Crashoverride(Industroyer)

# Ukraine Blackout 2015 - BlackEnergy

## '15 Ukraine Blackout (BlackEnergy, KillDisk)

- **(2015. 12. 23.) Massive Blackout occurred in Ukraine**
- **BlackEnergy Malware is founded during investigation**
  - Infected with BlackEnergy Malware through malicious documents sent via spear phishing
  - Destroy the availability by deleting the files and terminating the process
  - Target : General Electric's Complicity HMI, Siemens's SIMATIC WinCC, Advantech/BroadWin's WebAccess
- **Up to 6 hours of power supply disruption**



Alert (IR-ALERT-H-16-056-01) More Alerts

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Print Tweet Send Share

**Legal Notice**

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

**SUMMARY**

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

TECHNOLOGY NEWS FEBRUARY 26, 2016 / 8:52 AM / 2 YEARS AGO

**U.S. government concludes cyber attack caused Ukraine power outage**

Dustin Volz 2 MIN READ

WASHINGTON (Reuters) - A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognized the blackout as caused by a malicious hack.

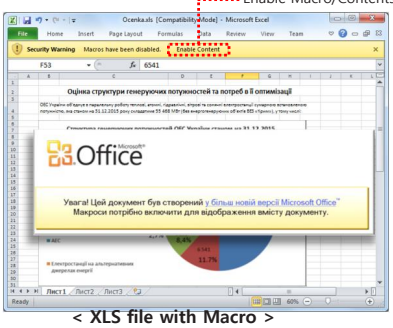


# Ukraine Blackout 2015 - BlackEnergy

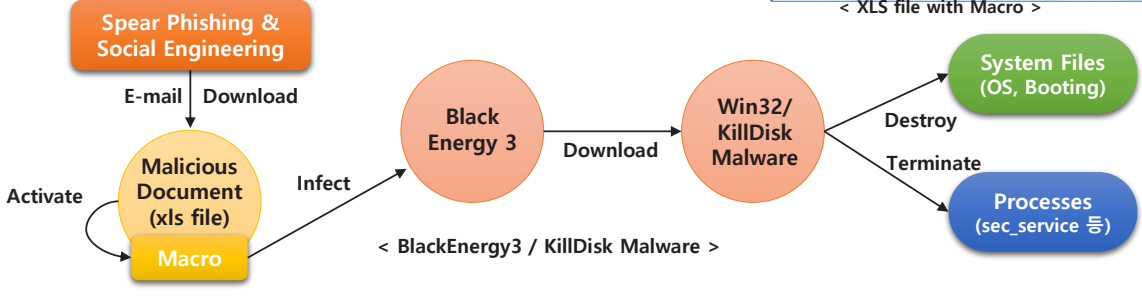
참고 : https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered
http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/
https://www.sans.org/webcasts/analysis-sandworm-team-ukraine-101597

## BlackEnergy3 / KillDisk Malware

- **Step1 : Spear phising email with MS XLS documents(Macro)**
- **Step2 : BE3 Malware is installed and then downloading Win32/KillDisk**
- **Step3 : Destroy system files and Terminate process**
  - OS system files, MBR booting info.
  - sec_service process (**S**erial-to-**E**thernet **C**onnector) by ASEM & Eltima




< XLS file with Macro >



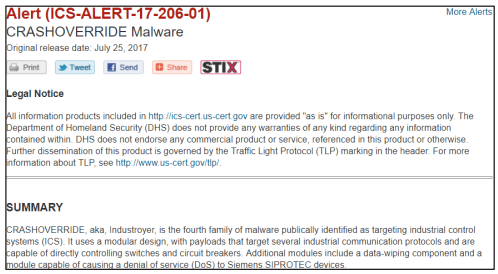

< BlackEnergy3 / KillDisk Malware >

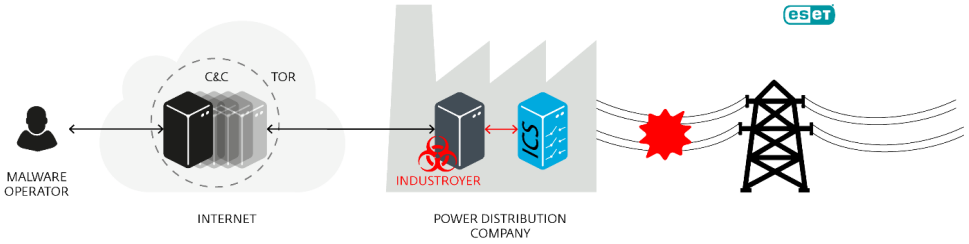
*http://www.asem.it/en/products/industrial-automation/remote-assistance/ubiquity/setup-downloads/
*http://www.eltima.com/products/serial-over-ethernet/

# Ukraine Blackout 2016 - Crashoverride/Industroyer

## ''16 Kiev Blackout (Crashoverride)

- **(2016.12.17.) 15 minutes outage at Kiev City**
- **Crashoverride malware is founded during investigation**
  - First grid operation enabled malware
  - Single Substation is affected, different with '15 Cyberattack
- **Cyber attacks on various areas of Ukraine**
  - Approximately 6,500 attacks performed for 2months
  - Attacks on 5 institutions and 31 information resources

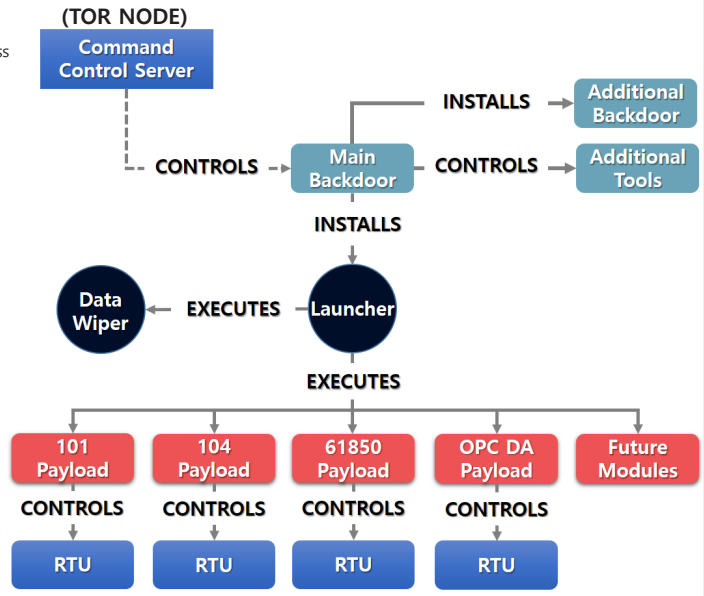

Alert (ICS-ALERT-17-206-01) More Alerts
CRASHOVERRIDE Malware
Original release date: July 25, 2017
Print Tweet Send Share STIX
Legal Notice
All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.
SUMMARY
CRASHOVERRIDE, aka, Industroyer, is the fourth family of malware publically identified as targeting industrial control systems (ICS). It uses a modular design, with payloads that target several industrial communication protocols and are capable of directly controlling switches and circuit breakers. Additional modules include a data-wiping component and a module capable of causing a denial of service (DoS) to Siemens SIPROTEC devices.



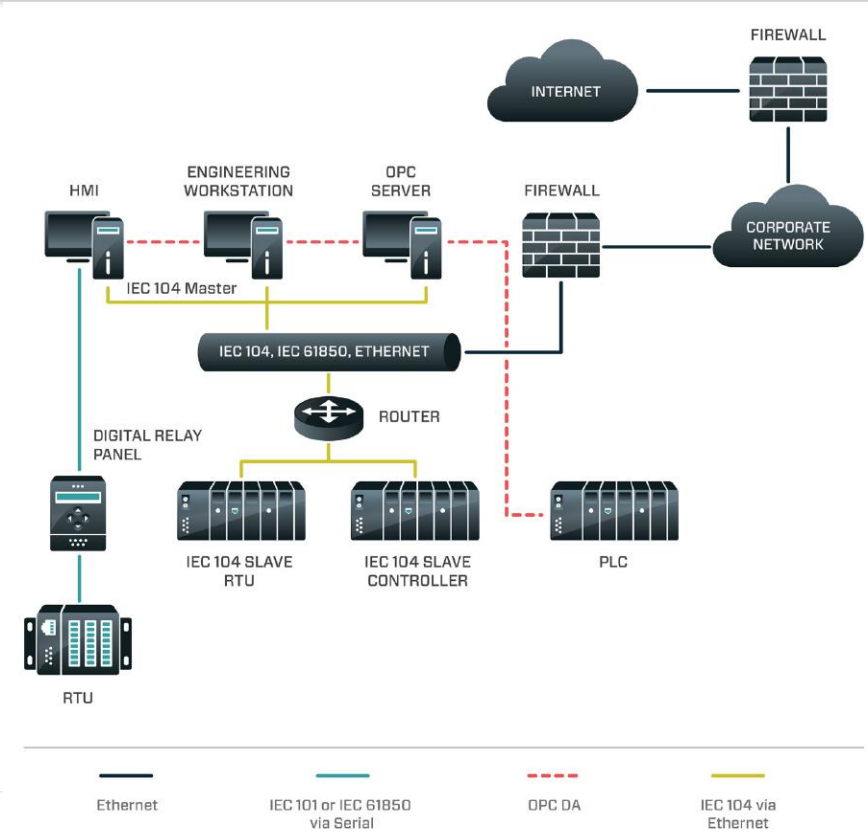
# Ukraine Blackout 2016 - Crashoverride/Industroyer

## Module Overview

- **Backdoors**
  - Main Backdoor
    - Directly communicated to hard-coded proxy address
    - HTTP Connect to C2 Server
  - Additional Backdoor
    - Trojanized version of the **Windows Notepad**
  - Data Wiper
  - Erase ICS Configuration Files
    - ABB PCM600 Configuration Files(.pcmp, .CIN, ...)
    - IEC 61850 Configuration Files (SCL, cid, scd etc)
    - PLC Files (.PL, .paf)
- **Payload Modules**
  - IEC 60870-5-101
  - IEC 60870-5-104
  - IEC 61850
  - OPC DA
- **Additional Tools**
  - Port Scanner
  - DoS tool (Target : Siemens protective relays)



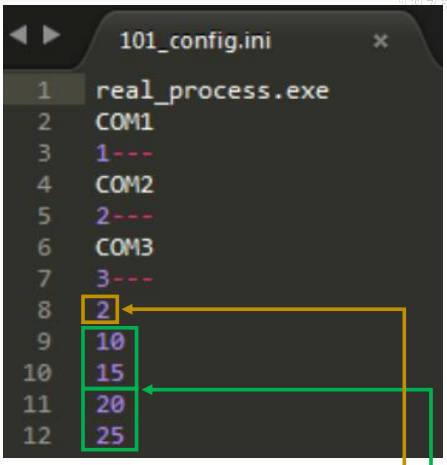
# Ukraine Blackout 2016 - Crashoverride/Industroyer




# Crashoverride/Industroyer payload : - IEC 60870-5-101 (1/2)

## Payload Modules (IEC 60870-5-101)

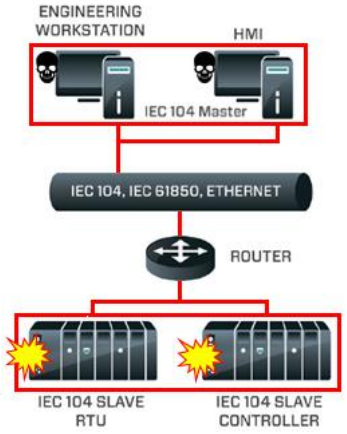
- **If attack execute in victim machine, the 101 payload component parses the configuration stored in its INI file(ex: 101_config.ini)**
- **Several entries in INI file**
  - Process name
    - specified belongs to an application the attackers suspect is running on the victim machine
  - Windows device names (usually COM ports)
    - The first COM port is used for the actual communication
    - The two other COM ports are just opened to prevent other processes accessing them
  - The number of Information Object Address(IOA) ranges
  - The beginning and ending IOA values for the specified number of IOA ranges
    - For each such IOA it constructs two "select and execute" packets
    - One with a single command (C_SC_NA_1) and the other with a double command (C_DC_NA_1)




**101 payload DLL configuration**

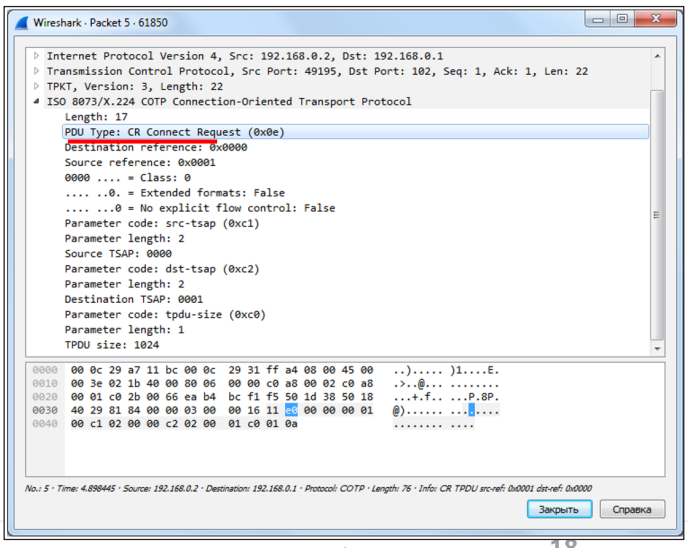
# Crashoverride/Industroyer payload : - IEC 60870-5-104 (1/3)

- IEC 60870-5-104 is used for communication between industrial control systems and Remote Terminal Units (RTUs) through a TCP/IP network.
- IEC 60870-5-104 module's main targets are IEC 60870-5-104 slave devices.
  - IEC 60870-5-104 is TCP/IP based protocol, so it is possible to cause malfunction to multiple device simultaneously.
- The 104 payload attempts to terminate the normal communication process and starts to communicate with the specified devices to cause malfunction to them.




# Crashoverride/Industroyer payload : IEC 61850

- Payload Modules (IEC 61850)
  - 61850 payload component exists as a standalone malicious tool (61850.exe and DLL 61850.dll)
  - Read the configuration file (i.ini)
    - Configuration file is expected to contain a list of IP address which communicating via IEC 61850
  - Auto-Discovery
    - Enumerates all possible IP address and try to connect to port 102
    - Sends a IEC 61850 Connection Request packet to target host

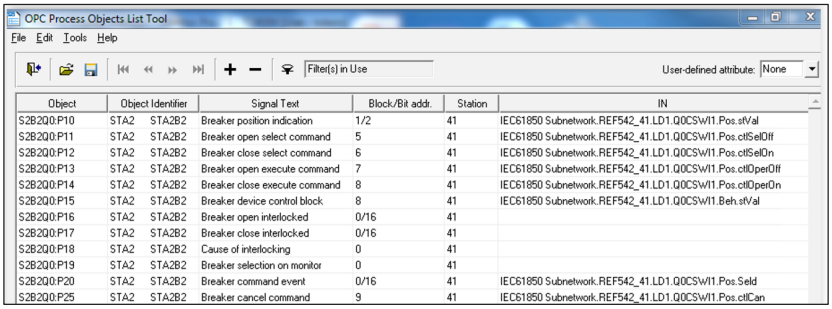



<IEC 61850 Connection Request>

# Crashoverride/Industroyer payload : OPC DA

## Payload Module (OPC DA)

- **Enumerates all OPC server and OPC items on the server**
  - ctlSelOn
  - ctlOperOn
  - ctlSelOff
  - ctlOperOff
  - ₩Pos and stVal
- **Change the state of discovered OPC items**




| Object | Object Identifier | | Signal Text | Block/Bit addr. | Station | IN |
|---|---|---|---|---|---|---|
| S2B2Q0:P10 | STA2 | STA2B2 | Breaker position indication | 1/2 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.stVal |
| S2B2Q0:P11 | STA2 | STA2B2 | Breaker open select command | 5 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOff |
| S2B2Q0:P12 | STA2 | STA2B2 | Breaker close select command | 6 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOn |
| S2B2Q0:P13 | STA2 | STA2B2 | Breaker open execute command | 7 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOff |
| S2B2Q0:P14 | STA2 | STA2B2 | Breaker close execute command | 8 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOn |
| S2B2Q0:P15 | STA2 | STA2B2 | Breaker device control block | 8 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Beh.stVal |
| S2B2Q0:P16 | STA2 | STA2B2 | Breaker open interlocked | 0/16 | 41 | |
| S2B2Q0:P17 | STA2 | STA2B2 | Breaker close interlocked | 0/16 | 41 | |
| S2B2Q0:P18 | STA2 | STA2B2 | Cause of interlocking | 0 | 41 | |
| S2B2Q0:P19 | STA2 | STA2B2 | Breaker selection on monitor | 0 | 41 | |
| S2B2Q0:P20 | STA2 | STA2B2 | Breaker command event | 0/16 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.SeId |
| S2B2Q0:P25 | STA2 | STA2B2 | Breaker cancel command | 9 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlCan |

<Example list of OPC items that contain names with similar strings>



# Malware Analysis II
# - TRITON

# TRITON Malware Overview (1/3)

- "The attack was not designed to simply destroy data or shut down the plant … It was meant to sabotage the firm's operations and trigger an explosion."
- TRITON may be linked to string of cyberattacks on Saudi Arabia petrochemical facilities; experts suggest Iran, perhaps with help from Russia & North Korea
  - https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
  - Anatomy of the TRITON ICS Cyberattack by CyberX

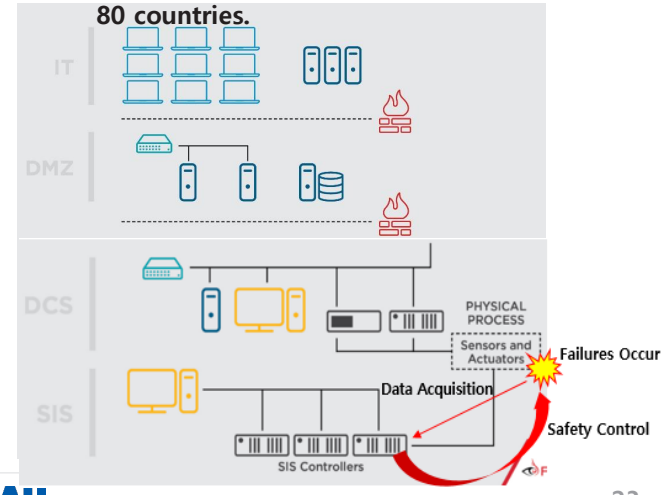
# TRITON Malware Overview (2/3)

- "*Trisis is the first ever to specifically target safety instrumented systems and it is the one that gives me the most concern," said Lee, a former Air Force cyberwarfare operator. "CrashOverride was an alarming event for power grid operators and should be taken very seriously, but Trisis specifically targeted a system that is designed to protect human life. To me that is outrageous and infuriating. I expect this will be a watershed moment for the engineering community.*" ref by Cyberscoop

- ICS-CERT MAR-17-532-01, 2017.12.18 ICS-CERT
  - Malware Analysis Report "HATMAN-SAFETY SYSTEM TARGETED MALWARE"
- In mid-November 2017, the Dragos, Inc. team discovered ICS-tailored malware TRISIS deployed against at least one victim in the Middle East.
  - East-Petrochemical facility in Saudi Arabia infected.
  - It also called as TRITON(FireEye) and HatMan(US NCCIC).

# TRITON Malware Overview (3/3)

- The TRITON's main target is, SIS(Safety Instrumented Systems/안전계장(安全計裝)시스템/)product, Schneider Electric's Triconex.
  - Safety systems are those control systems, often identified as Safety Instrumented Systems (SIS), maintaining safe conditions if other failures occur.
    - TRITON affect only Triconex products not others.
  - Triconex leads SIS market, there are more than 13,000 products in ICS environments over the 80 countries.




<SIS Controllers function>

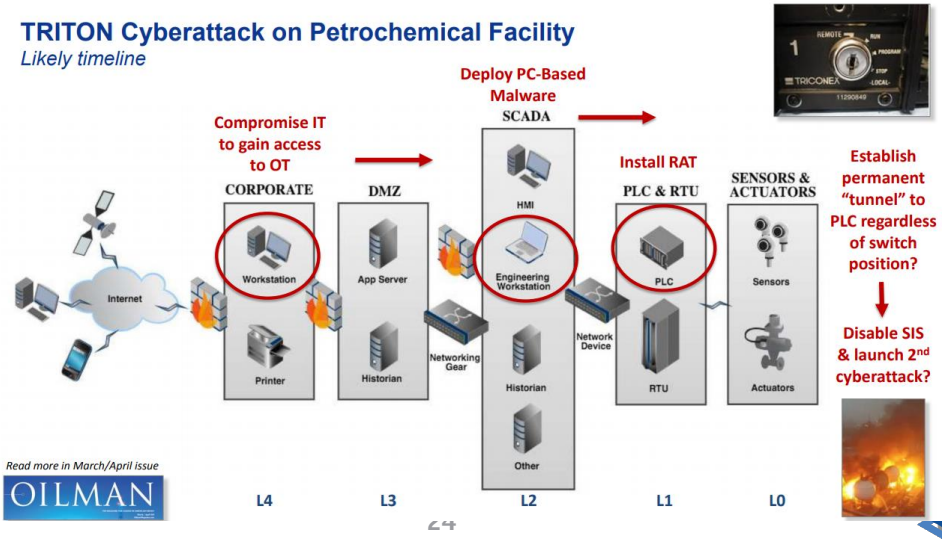
<Triconex SIS Controllers H/W products>

출처 : Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FireEye, 2017.12.14



# TRITON Architecture and Attack Scenario, but failed - I

- According to the Schneider Electric Analysis and Disclosure, released on Jan 23, it seems that the attackers were trying to implant a remote access Trojan (RAT) inside the Triconex SIS.
- A common practice at many sites is to allow engineers to access the operational network via Remote Desktop Protocol (RDP). Compromise of the engineer's RDP credentials will allow an attacker access to both the industrial process devices and the safety network, further increasing the attack surface.



# TRITON Architecture and Attack Scenario, but failed - II

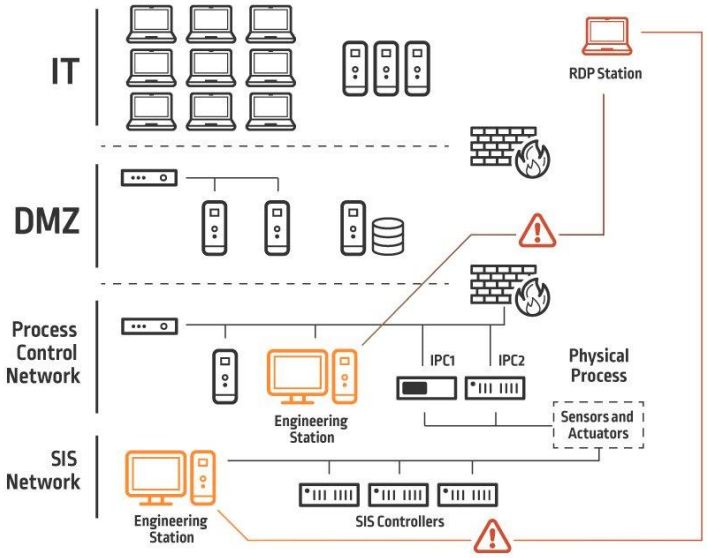
## Attackers' Weak Point in Triconex SIS

- The Triconex SIS firmware will only accept new SW when this keyswitch is in the 'program' position.
- The byte code downloaded by the TriStation protocol is not persistent.

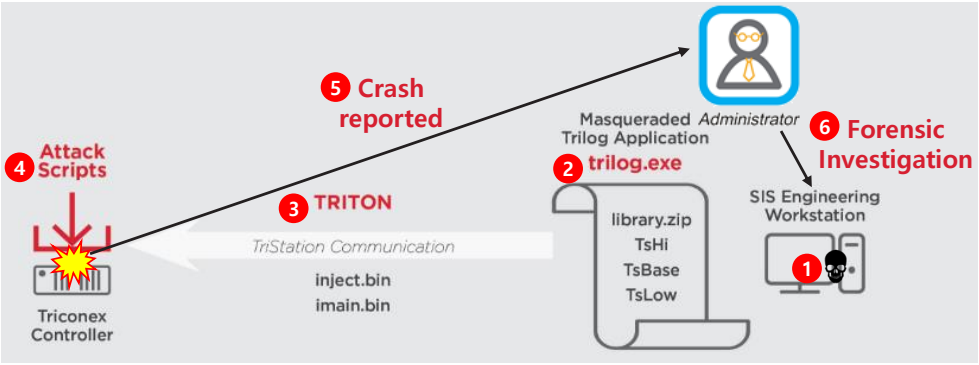
## Attackers' Persistence

- **Zero-day vulnerability in the Triconex OS**
  - allows the malware code to elevate from user to supervisor, obtain read/write/execute privileges and then copy itself into the firmware memory.

**During the incident, some SIS controllers crashed and entered a failed safe state, which automatically shutdown the industrial process and prompted the asset owner to initiate an review controller diagnostic log and TRITON was found, however, we don't know who/why/how???**




# TRITON Architecture and Attack Scenario, but failed - III




<TRITON was detected!>

## TRITON Program Structure

- **trilog.exe — Main executable py2exe compile that executes python script**
- **library.zip — Contains all libraries including TriStation communication libraries**
- **inject.bin — Places imain.bin in the right place**
- **imain.bin — Main backdoor**

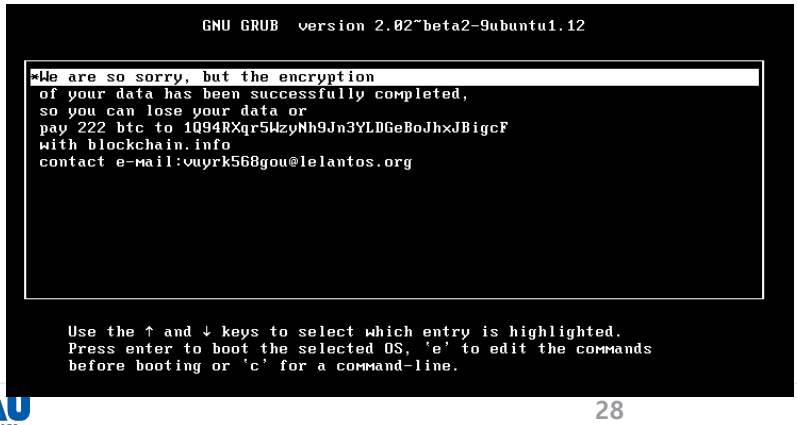
출처 : Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FireEye, 2017.12.14

# Malware Analysis III
# - WannaCry & Petya / Cryptojacking



## The First Ransomware in ICS? - KillDisk

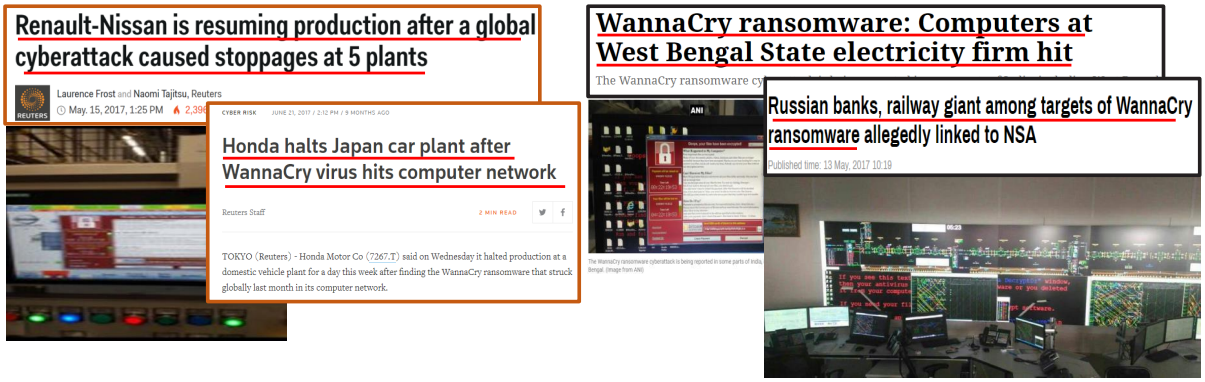
- KillDisk, a disk-wiping malware previously used in the cyberattacks against the Ukrainian power grid has now evolved into ransomware(by CyberX)
  - 5 months before WannaCry and 6 months before NotPetya



# Ransomware in ICS - Wannacry & Petya

## "WannaCry(WannaCrypt)"

- WannaCry is a wormable ransomware exploiting MS17-010(SMB*v1 Vulnerability) and spread using leaked NSA* exploit EthernalBlue and DoublePulsar
- Exploit conditions : 1) Listening on TCP 445, 2) Running SMBv1, 3) Unpatched Window OS
- Impacting ICS : Railway systems, Automobile manufactures, Power companies, Airlines, Hospital systems ... (just on week)




**SMB*:** Server Message Block, **NSA*:** National Security Agency

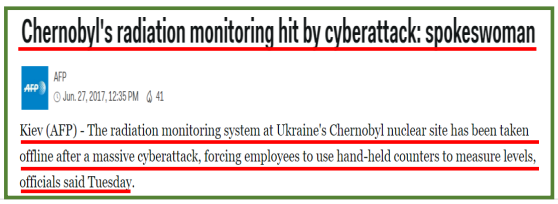
출처*: Reuter News, Chronicle Live, Indianexpress, Technoloman, RT



# Ransomware in ICS - Wannacry & Petya

## "Petya(Petya 2.0, NotPetya, ExPetr)"

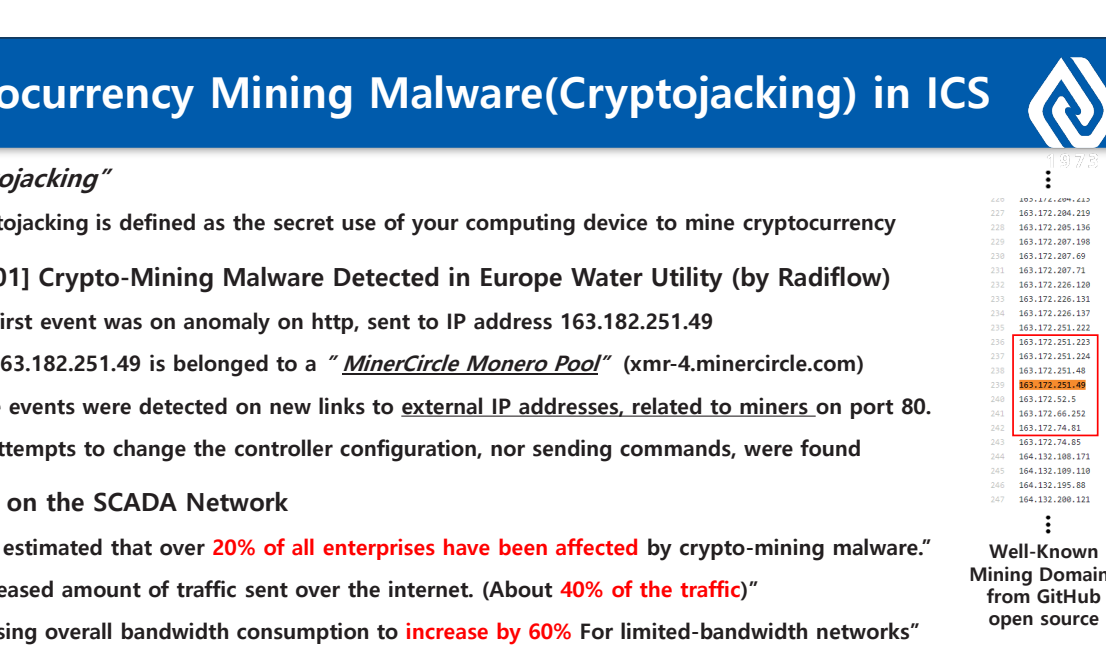
- Petya is similar to Wannacry but have several difference
  - Is a Wiper, Not Ransomware (intent to system destruction)
  - Encrypted about MFT*, not victim's whole file
  - Spread using multiple propagation method( EthernalBlue, EthernalRomance, PsExec and WMI*)
  - Spread and encrypt without connecting out to the attacker's C2*
- Exploit conditions : Wannacry exploit conditions or weak protection of privileges(Credentials)
- Impacting ICS : At least 50 % of the companies being attacked are manufacturing and oil & gas enterprises




**WMI*:** Windows Management Instrumentation, **MFT*:** Master File Table, **C2*:** Command and Control server 출처*: Zdnet, CNN, CNBC, Asia

# Cryptocurrency Mining Malware(Cryptojacking) in ICS

- *"Cryptojacking"*
  - Cryptojacking is defined as the secret use of your computing device to mine cryptocurrency
- [2018.01] Crypto-Mining Malware Detected in Europe Water Utility (by Radiflow)
  - The first event was on anomaly on http, sent to IP address 163.182.251.49
    - 163.182.251.49 is belonged to a *"MinerCircle Monero Pool"* (xmr-4.minercircle.com)
  - More events were detected on new links to external IP addresses, related to miners on port 80.
  - No attempts to change the controller configuration, nor sending commands, were found
- Effects on the SCADA Network
  - "It is estimated that over 20% of all enterprises have been affected by crypto-mining malware."
  - "Increased amount of traffic sent over the internet. (About 40% of the traffic)"
  - "Causing overall bandwidth consumption to increase by 60% For limited-bandwidth networks"




Well-Known Mining Domains from GitHub open source

| Port | Src IP | Dst IP | Hostname | First Seen |
|---|---|---|---|---|
| 80 | IP1 | 163.172.251.49 | xmr-4.minercircle.com | Jan 21, 2018 18:48 |
| 80 | IP1 | 163.172.52.5 | xmr-1.minercircle.com | Jan 21, 2018 18:48 |
| 80 | IP1 | 163.172.103.175 | xmr-2.minercircle.com | Jan 22, 2018 1:04 |
| 80 | IP1 | 163.172.251.224 | xmr-7.minercircle.com | Jan 22, 2018 1:04 |
| 80 | IP2 | 163.172.52.5 | xmr-1.minercircle.com | Jan 22, 2018 14:11 |
| 80 | IP2 | 163.172.74.81 | xmr-9.minercircle.com | Jan 22, 2018 14:11 |
| 80 | IP3 | 163.172.251.223 | xmr-6.minercircle.com | Jan 22, 2018 14:41 |

First Time Seen for Monero-miner IP Address



# How to Predict/Prevent, Detect, and Response?

# YARA Rule and Usage

- YARA is a tool aimed at helping malware researchers to identify and classify malware samples.
  - YARA is open source multi-platform, running on Windows, Linux and Mac OS X.
  - Binary/Pattern/String/Signature based
- Plenty of organizations are using YARA.
  - Avast, FireEye, Kaspersky Lab, McAfee, Symantec ...
- How to use?
  - Download YARA and rules or make rules
    - https://github.com/VirusTotal/yara/releases
  - Run YARA with YARA rules
    - yara [OPTIONS] RULES_FILE TARGET
  - Results show matching files with YARA rules.

```
[+] File : 01.exe, Matched :[UPX_rule, CrackMe01]
[+] File : 05.exe, Matched :[UPX_rule]
[+] File : 19.exe, Matched :[UPX_rule]
[+] File : Reverse_L01.exe, Matched :[CrackMe01]
```

```
rule coi_backdoor
{
    meta:
        description = "Detect CRASHOVERRIDE/Industroyer backdoors"
                author = "NCCIC ICS-CERT"

    strings:
        $co0 = {6a 43 ff 15}
        $co1 = {50 57 57 6a 2e 57 ff 15 ?? ?? ?? 00}
        $co2 = {5? 5? 5? 5? 5? 5? FF ?? ?? 6a ff 6a ff 6a ff 5? ff

        $st1 = {4f 62 74 61 69 6e 55 73 65 72 41 67 65 6e 74 53 74
        $st2 = "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;

    condition:
        filesize < 1MB and all of them
}
```

<Crashoverride YARA Rule 중 일부>



# YARA Rule for Detection

- Black Energy 2,3
  - https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-17-206-01.yara
- Crashoverride
  - https://github.com/dragosinc/CRASHOVERRIDE/blob/master/CRASHOVERRIDE%202016-06-12.yara
- TRITON / TRISIS / HATMAN
  - https://ics-cert.us-cert.gov/sites/default/files/file_attach/MAR-17-352-01.yara
- Wannacry
  - https://www.us-cert.gov/ncas/alerts/TA17-132A
- Petya
  - https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html

# Snort Rule

## Crashoverride

- **IEC 61850 Module (Sid 1-43252, 1-43253)**
  - https://www.snort.org/rule_docs/1-43252
  - https://www.snort.org/rule_docs/1-43253

• 1:43252 <-> DISABLED <-> PROTOCOL-SCADA IEC 61850 device connection enumeration attempt (protocol-scada.rules)

* 1:43253 <-> DISABLED <-> PROTOCOL-SCADA IEC 61850 virtual manufacturing device domain variable enumeration attempt (protocol-scada.rules)

- **IEC 60870-5-104 Module (Sid 1-43227, 1-43228)**
  - https://www.snort.org/rule_docs/1-43228
  - https://www.snort.org/rule_docs/1-43227

* 1:43227 <-> DISABLED <-> PROTOCOL-SCADA IEC 104 force off denial of service attempt (protocol-scada.rules)

* 1:43228 <-> DISABLED <-> PROTOCOL-SCADA IEC 104 force on denial of service attempt (protocol-scada.rules)



# References

# References


- Industrial Control system threats, Dragos, 2018.03
- The State of Industrial Cybersecurity 2017, kaspersky, 2017
- ICS-CERT Year in Review 2016, ICS-CERT, 2016

- Brad D. Williams. (2017.01.29.), "Hackers' Methods feel familiar in Ukraine power grid cyberattack", *FIFTH DOMAIN CYBER*, http://fifthdomain.com/2017/01/29/how-a-power-grid-got-hacked/ (Accessed Feb 21, 2017)
- Natalia Zinets. (2017.02.15.), "Ukraine charges Russia with new cyber attacks on infrastructure", *REUTERS*, http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN (Accessed Feb 21, 2017)
- Marina Krotofil. (2017.01.10), "Security Analysis of Cyber Attacks in Ukraine)", Youtube, https://youtu.be/ITwsDLO3C44 (Accessed Feb 21, 2017)
- Marina Krotofil. (2017.01.10), "Security Analysis of Cyber Attacks in Ukraine)", SlideShare, https://www.slideshare.net/MarinaKrotofil?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview (Accessed Feb 21, 2017)
- WIN32/INDUSTROYER : A new threat for industrial control systems, ESST, 2017.06.12
- CrashOverride : Analysis of the Threat to Electric Grid Operations, DRAGOS, 2017.06.12
- (SANS ICS) Set the Stage – ICS Attacks: Ukraine 2015 & 2016 Power, DRAGOS, 2017.07.07

- TRISIS Malware, Dragos, 2017.12.14
- Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FireEye, 2017.12.14
- MALWARE ANALYSIS REPORT HATMAN-SAFETY SYSTEM TARGETED MALWARE, NCCIC, 2017.12.18
- TRITON – Mandiant Analysis at S4x18, FireEye, 2018.01.23
- TRITON - Schneider Electric Analysis and Disclosure, Schneider Electric, 2018.01.23
- TRITON - Reverse Engineering the Tricon Controller, Dragos, 2018.01.24
- Decompiled TRITON code - https://github.com/ICSrepo/TRITON-TRITON-HATMAN




# References


- THE WANNACRYRANSOMWARE, CERT-MU, 2017.05
- #WannaCry Report, Panda security, 2017.05.22
- 워너크립터 랜섬웨어 분석 보고서, Ahnlab, 2017.05.12
- WannaCry 랜섬웨어 분석, Somansa, 2017.06.08
- WannaCry Ransomware Threat : What we know so far - SANS SANS DFIR, 2017.05.13, WannaCry Malware Profile, fireeye, 2017.05.23
- WannaCry ransomware massively attacks computer systems all over the world, Malwareless, 2017.05.12
- How did the WannaCry ransomworm spread?, Malwarebytes Labs, 2017.05.19
- WannaCry on industrial networks: error correction, KASPERSKY LAB ICS CERT, 2017.06.22
- Customer Guidance for WannaCrypt attacks, Microsoft, 2017.05.12
- Defending the ICS Ahead of the Patch WannaCry Lessons Learned/SANS/2017.05.26
- Lessons from the WannaCry ICS Trenches/SANS/2017.05.15
- QnA형식으로 알아보는 WannaCry 랜섬웨어 대응 가이드/KISA/2017.05.15

- Detection of a Crypto-Mining Malware Attack at a Water Utility, Radiflow, 2018.02.23
- Cybersecurity: Malware infects wastewater utility SCADA system, WaterWorld, 2018.02.12
- What is Cryptojacking?, hackerbits, 2018.01.24
- Increased Use of Browser Cryptojacking, CERT-EU, 2017.11.15
- Well-Known Mining Domains, GitHub(ZeroDot1), 2018.03.19
- Smominru Monero mining botnet making millions for operators, Proofpoint, 2018.01.31
- ADB.Miner: More Information, Netlab360, 2018.02.06
- New Monero mining malware discovered in Google Play, Avast Blog, 2018.03.15

The 24th Network Security Conference -Korea

# 발전제어시스템 이상징후 탐지를 위한 화이트리스트 개발 및 현장적용 사례

**강형구** 온시큐리티 대표

### 학력 및 경력사항

건국대학교 정보통신대학원 정보보안전공(석사)

| | |
|---|---|
| 1993 ~ 2000 | 삼성전자 / 삼성SDS S/W개발 |
| 2001 ~ 2005 | 마이엔진 / 넥시드텔레콤 S/W개발 |
| 2005 ~ 2010 | 프랑스텔레콤 R&D Researcher |
| 2011 ~ | 온시큐리티 대표이사 |

### 강연요약

국내 발전제어시스템은 기반시설로서 관리가 되며, 폐쇄망으로 구성되어 집니다. 그러나, 외부에서 접근이 허용될 수 밖에 없는 현실에서 이에 대한 보안 대책이 시급한 상황입니다.

본 강연에서는 국내 5개 발전사는 이에 대한 대책의 일환으로 발전제어시스템에 대한 보안스템을 구축중이며, 이에 대하여 진행된 내용을 알려드리고자 합니다.

A발전사의 경우, 발전제어시스템 보안 강화를 위하여 포렌식시스템을 활용하여 발전제어시스템 내부에서 외부로 연결되는 부분에 설치하여 운영 중입니다. B발전사의 경우, A사와 동일하게 구축을 하였으나, 연결부분의 차이가 있습니다. A사는 스위치에서 네트워크 탭을 이용하였고, B사는 스위치에서 미러링을 하였습니다. 하지만, 데이터 분석 범위, 발전제어시스템 제조사, 시스템 운영 담당부서, 보안부서의 협력에서 많은 차이점이 있습니다. 또 다른 C발전사의 경우는, 발전제어시스템의 보안강화를 위하여 B사와 같이 구성된 기반에 화이트리스트를 적용하는 방안을 모색하고 있습니다. 하이브리드형 보안관제 시스템을 구축하고자 함입니다. 지금까지 발전제어시스템을 포함한 국내 기반시설에 대하여 보안을 적용하기에 많은 어려움이 있었고, 앞으로도 많을 것으로 판단되지만, 이러한 노력 하나하나가 실현될 때 기반시설에 대한 보안이 강화될 것으로 판단됩니다.

# 발전제어시스템 이상징후 탐지를 위한 화이트리스트 개발 및 현장적용 사례

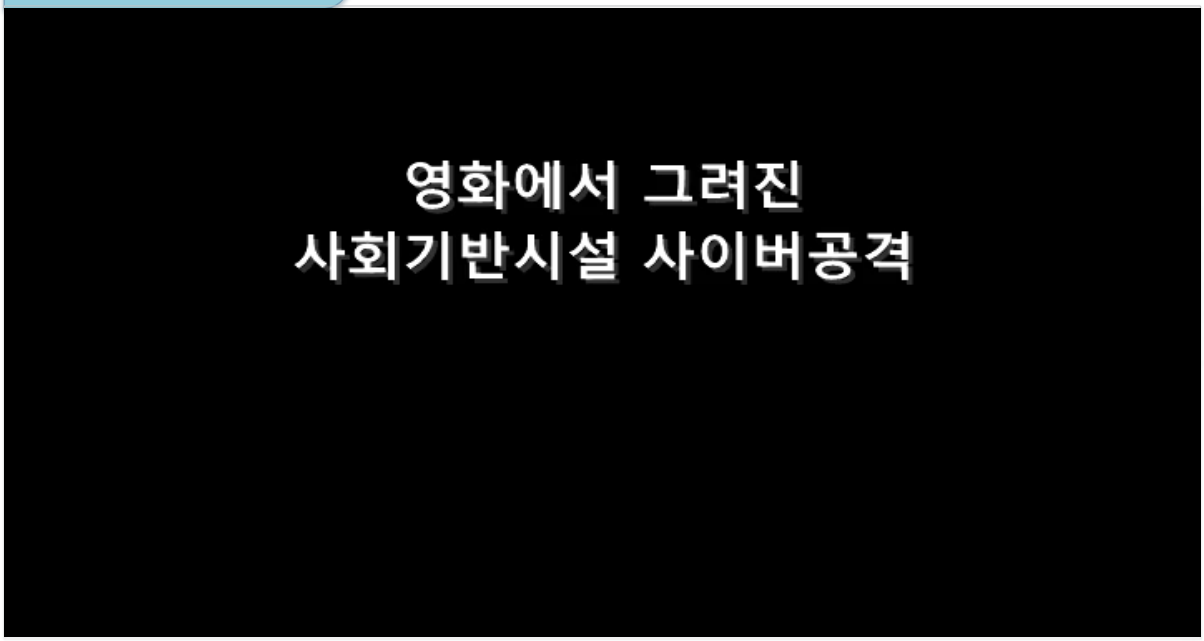
ON Security
온시큐리티(주)

## Contents

Ⅰ. ICS(Industrial Control System)
Ⅱ. 발전제어시스템 화이트리스트 개발사례
Ⅲ. 발전제어시스템 보안관제 구축사례
Ⅳ. 발전제어시스템 보안관제 전략
Ⅴ. Q&A

# 1. ICS(Industrial Control System)

## ICS 사이버 공격 영상



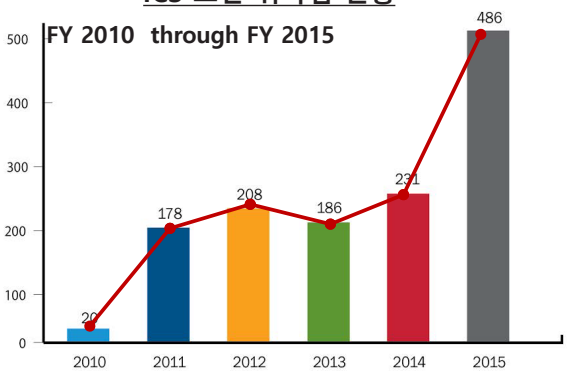



# 1. ICS(Industrial Control System)

## ICS 보안위협의 증가

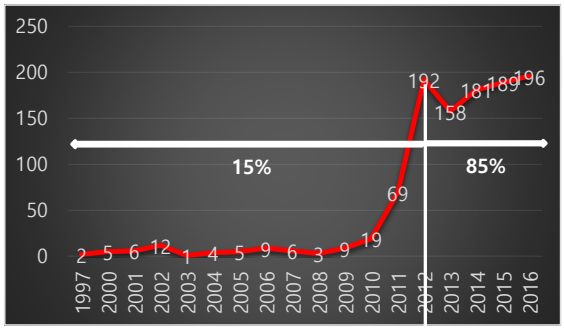
ICS 보안 취약점 노출 증가, 실제 ICS Cyber 공격이 2012년을 정점으로 급격히 증가

ICS 보안 취약점 현황



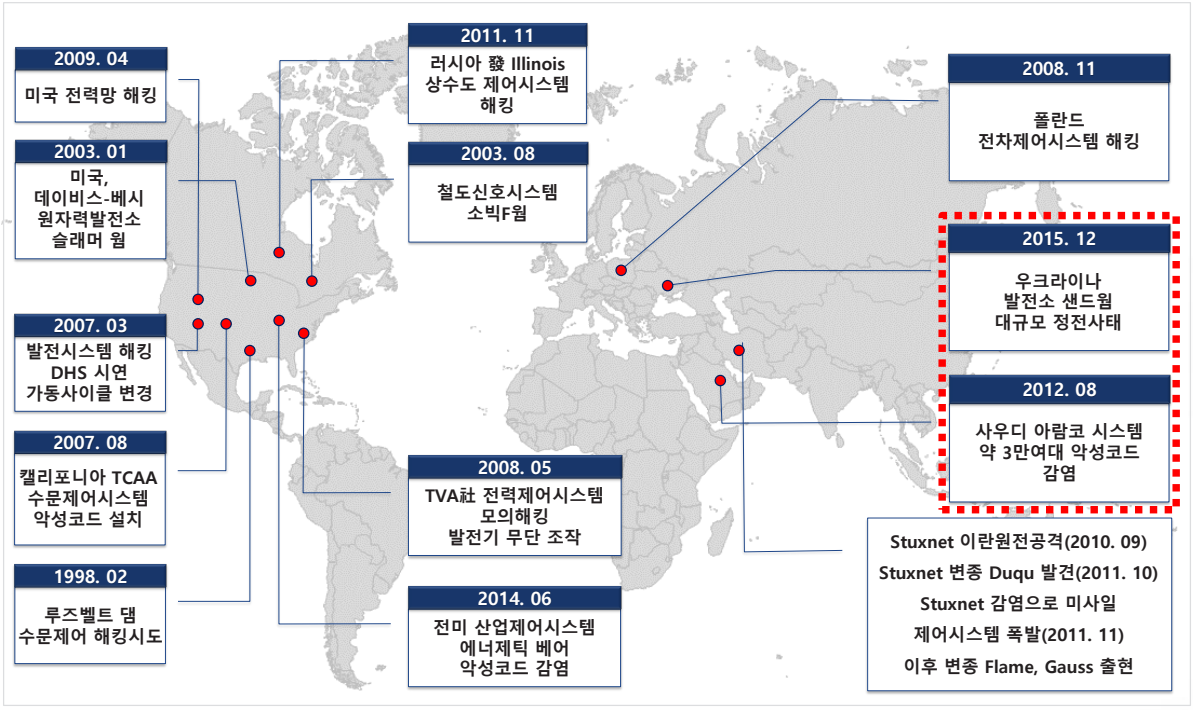

[출처 : 미국 ICS CERT, ICS CERT Year Review 2015]

ICS Cyber 공격 현황




[출처 : 국제 사이버 범죄 학회(ICACC), 2017]

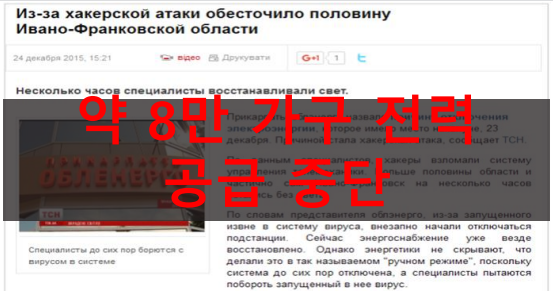
# 1. ICS(Industrial Control System)



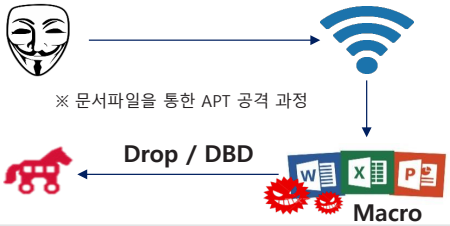



# 1. ICS(Industrial Control System)

## 우크라이나 정전 사태

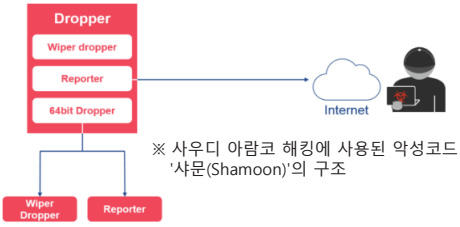



- 2015년 12월 23일, 우크라이나의 kyivoblenergo 발전소에 문제가 발생하여 3시간동안 약 8만여 가구에 전력 공급이 중단되었음




## 사우디 아람코 시스템 파괴

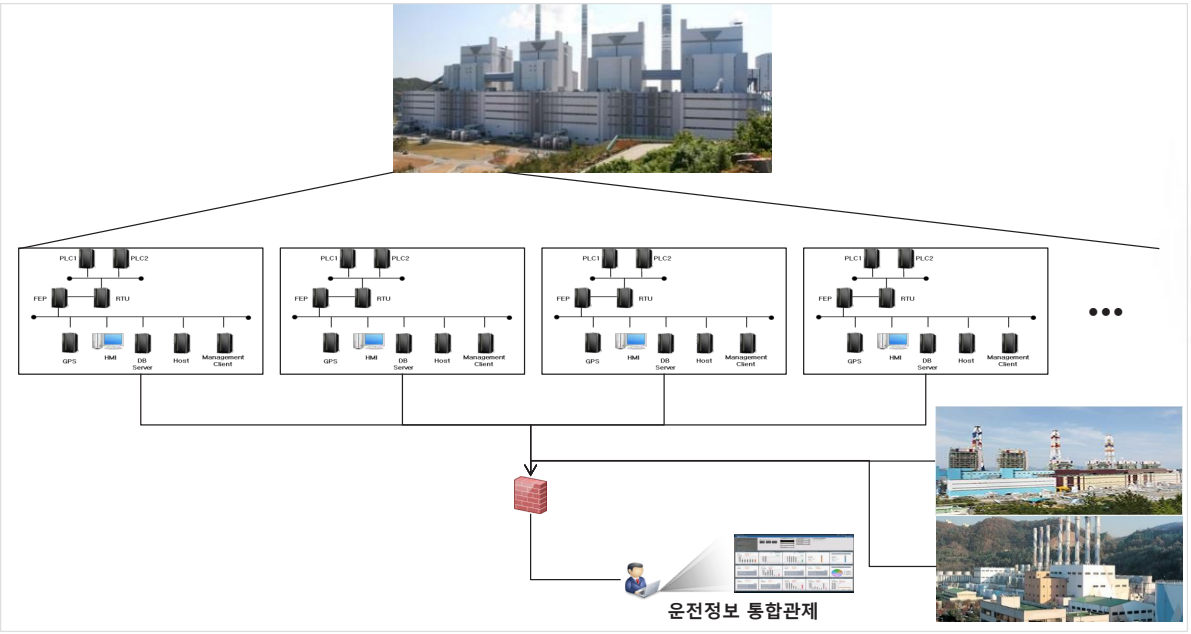
- 2012년 8월 15일 사우디 아람코의 컴퓨터 3만 여대의 데이터가 파괴되는 사건 발생
- 같은 날 '정의의 검(Cutting Sword of Justice)'이라고 자칭하는 단체가 아람코 해킹이 자신들의 소행이라고 주장함




※ 사우디 아람코 해킹에 사용된 악성코드 '샤문(Shamoon)'의 구조

## 2. 발전제어시스템 화이트리스트 개발사례

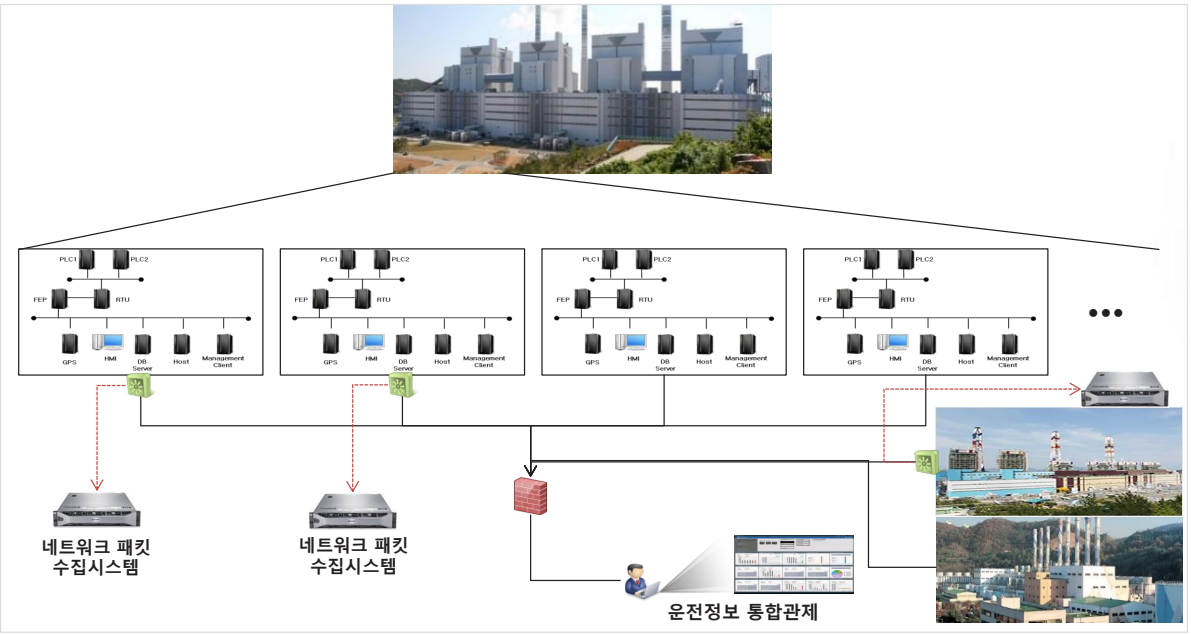
### 발전제어시스템 운전정보 통합관제




6

## 2. 발전제어시스템 화이트리스트 개발사례

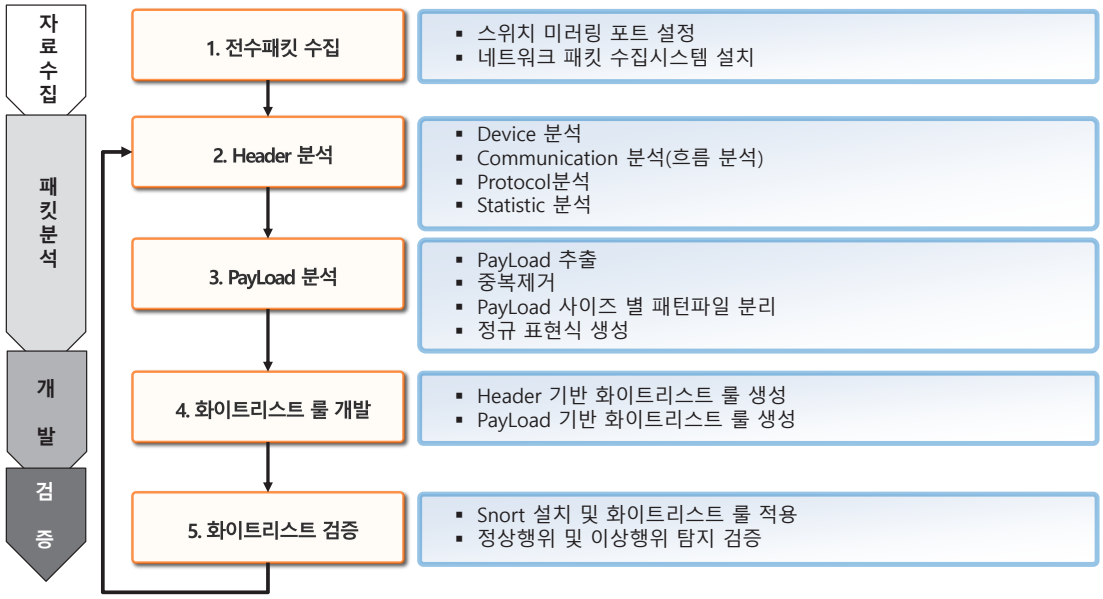
### 발전제어시스템 네트워크 수집




7

# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 개발 절차




8

# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 개발 환경

| 구 분 | 소프트웨어 | 비 고 |
|---|---|---|
| 운영체제 | Ubuntu 16.04.2 | 패킷 분석용 서버의 운영체제 |
| 분석도구 | tshark | 패킷 데이터를 분석하기 위한 S/W |
| | wireshark-common : capinfos | 수집된 Pcap파일 정보를 조회하는 S/W |
| 개발언어 | Perl : Net::Pcap, Net::Packet | 패킷 분석을 위한 프로그램 언어로 Pcap과 Packet 라이브러리를 사용 |
| 검증도구 | snort | 화이트리스트 검증 S/W |
| | tcpreplay | 화이트리스트 서버에 패킷을 전송하기 위한 S/W로 화이트리스트 검증을 위해 사용 |
| | WireEdit | 비정상 Payload에 대한 오탐을 검증하기 위한 도구로 Payload의 값을 임의로 변경 시 사용(패킷 위/변조용 TOOL) |
| 수집도구 | NIKSUN | 패킷 수집용 장비 |

9

# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 개발 예시

| 프로토콜 | Source | | 흐름 | Destination | | 페이로드 크기 | 페이로드데이터 |
|---|---|---|---|---|---|---|---|
| | IP | PORT | | IP | PORT | | |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 01 00 00 00 06 01 03 00 45 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 01 00 00 00 06 01 03 00 45 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 03 00 00 00 06 01 03 41 00 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 03 00 00 00 06 01 03 41 00 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 03 00 00 00 06 01 03 41 00 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 05 00 00 00 06 01 03 00 00 31 38 |

| 프로토콜 | Source | | 흐름 | Destination | | 페이로드 크기 | 페이로드데이터 |
|---|---|---|---|---|---|---|---|
| | IP | PORT | | IP | PORT | | |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 01 00 00 00 06 01 03 00 45 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 03 00 00 00 06 01 03 41 00 00 38 |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 05 00 00 00 06 01 03 00 00 31 38 |

| 프로토콜 | Source | | 흐름 | Destination | | 페이로드 크기 | 페이로드데이터 |
|---|---|---|---|---|---|---|---|
| | IP | PORT | | IP | PORT | | |
| TCP | 192.168.2.10 | 4767 | -> | 192.9.209.100 | 502 | 12 | 00 .. 00 00 00 06 01 03 .. .. .. 38 |

| 구분 | 데이터 |
|---|---|
| 경고메시지 | alert TCP 192.168.2.10 4767 -> 192.9.209.100 502(msg:"[warning]192.168.2.10 4767 ->192.9.209.100 502 Unknown pattern data has occurred"; dsize:12; pcr!"/ |
| 페이로드 | ₩x00.*₩x00₩x00₩x00₩x06₩x01₩x03.*₩x38 |
| 식별자 및 버전정보 | SID : 1478724 , rev : 1 |

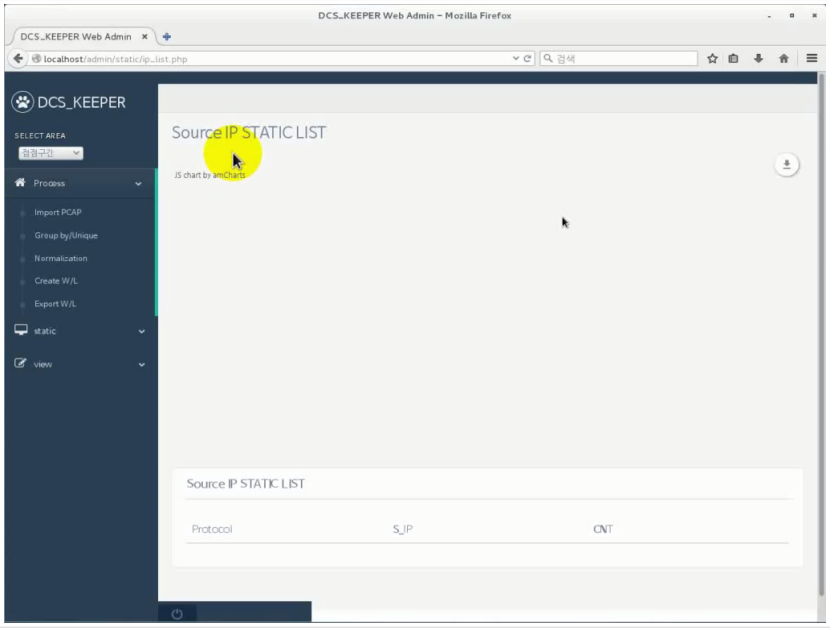
중복 데이터 → Unique 데이터 → 정규 표현식 생성 → 화이트 리스트

※ 본 자료에 사용된 자료(Data)는 이해를 돕기 위한 가상 Data입니다.



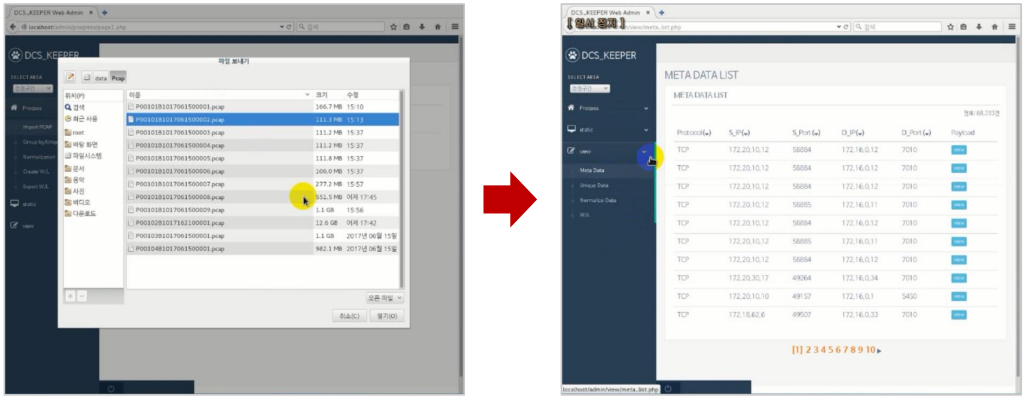
# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 프로그램 영상



# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 – import PCAP




- Import Pcap 화면에서 PCAP 파일을 선택합니다.

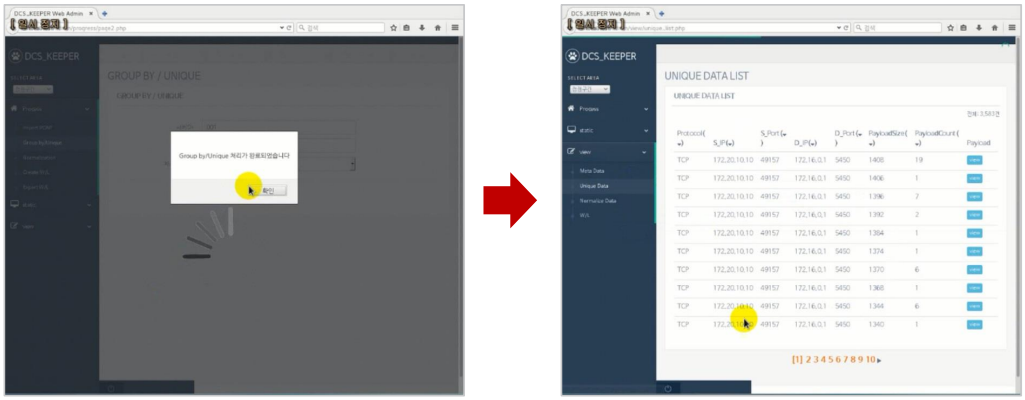
  분석 시스템이 Pcap 파일을 분석하여 대상 패킷을 METADATA 데이터베이스로 입력합니다.

  분석된 내용은 View 메뉴의 Meta Data 항목에서 확인 할 수 있습니다.



# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 – Group by / Unique



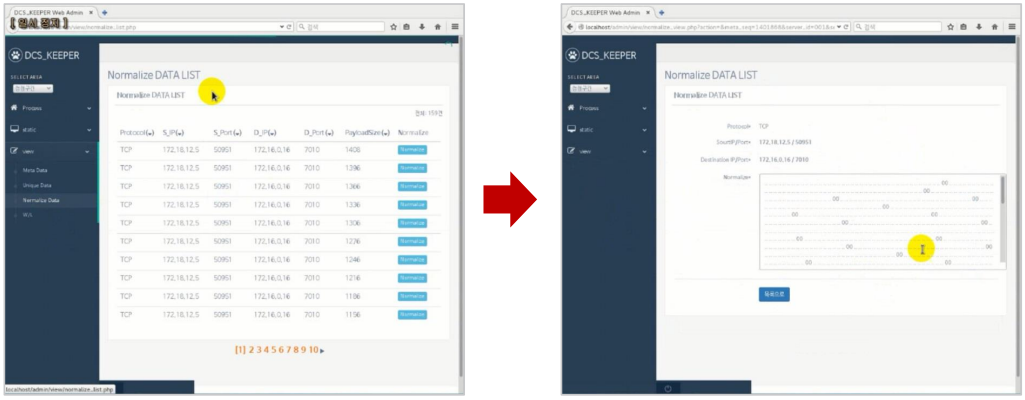

- Groupby/Unique 메뉴를 클릭하면 동일 패킷을 그룹화하고, 유일 데이터를 생성합니다.

  METADATA를 분석하여 중복된 패킷이 검출되면 PatternCnt를 증가시킵니다.

  분석된 내용은 View 메뉴의 Unique Data 항목에서 확인 할 수 있습니다.

# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 –Normalization




- Normalization 메뉴에서는 Payload 분석을 실행하여 정규표현식을 도출합니다.

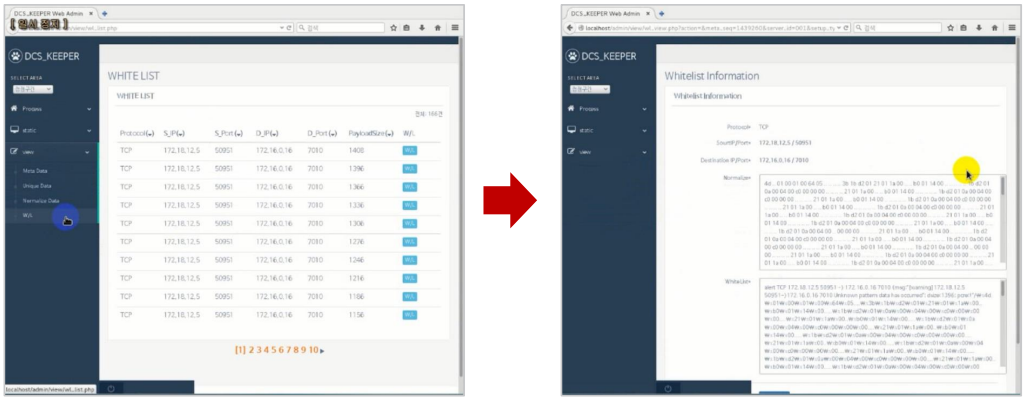
  Unique 데이터의 Payload Size를 기준으로 분석하여 Payload의 정규화 Pattern을 분석합니다.

  분석된 내용은 View 메뉴의 Nomalize Data 항목에서 확인 할 수 있습니다.



# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 – Create W/L



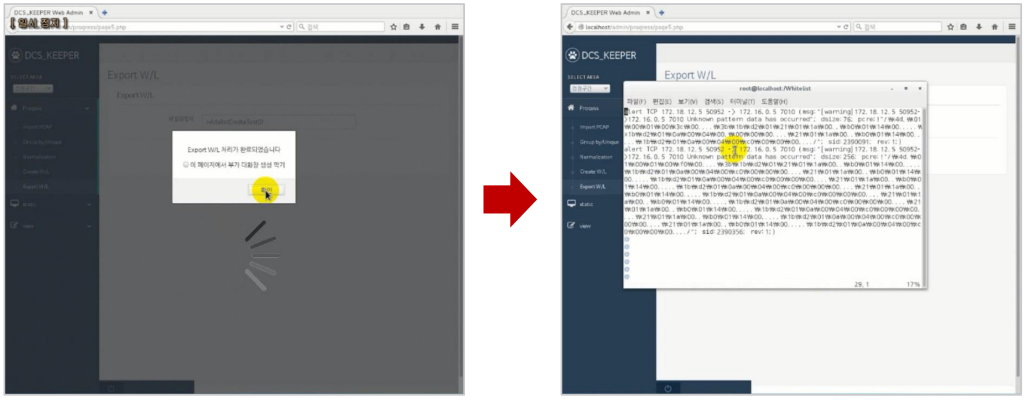

- Create W/L 메뉴에서는 IDS에 적용 가능한 화이트리스트를 생성합니다..

  Header 정보를 포함한 Payload 정규표현식을 IDS 탐지 규칙에 맞게 변환합니다.

  분석된 내용은 View 메뉴의 W/L Data 항목에서 확인 할 수 있습니다.

# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 – Export W/L



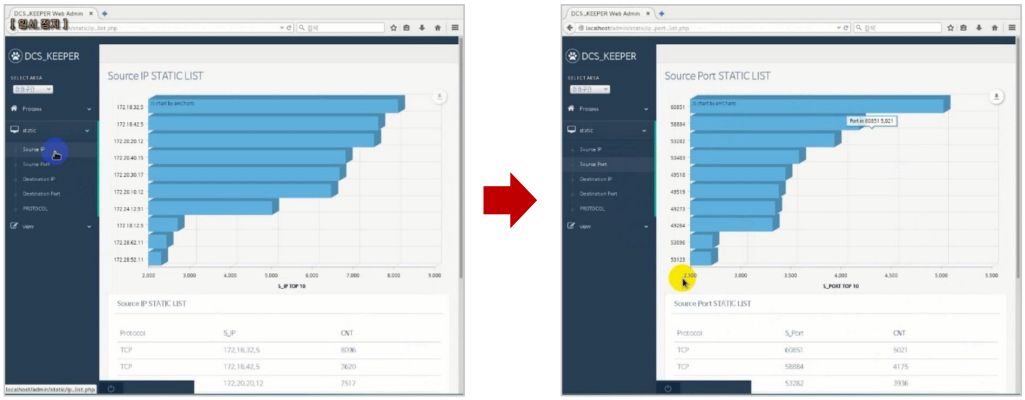

- 이전 단계에서 생성된 W/L를 파일로 저장합니다.

  IDS에 탐지 Rule에 적용하기 위한 화이트리스트 Rule 파일을 생성합니다.



# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 분석 – 통계정보

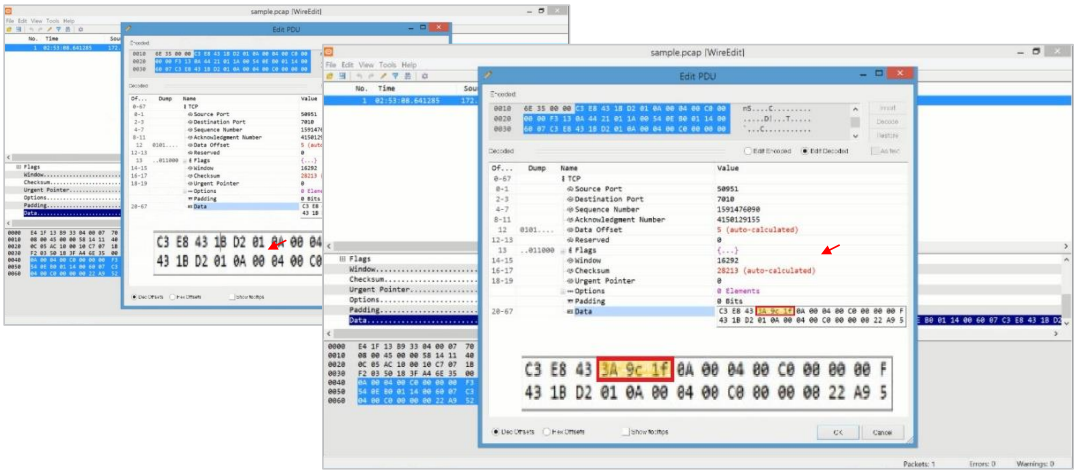



- Static 메뉴는 통계정보를 제공합니다.

  Source IP, Source Port, Destination IP, Destination Port, Protocol 별 세부 통계정보를 확인할 수 있습니다.

# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 수집 패킷 검증 – 위/변조 검증 데이터 준비




- 생성된 화이트리스트의 검증을 위한 위/변조 데이터 준비단계입니다.

  WireEdit 도구를 사용하여 정상 패킷의 페이로드 값 일부를 임의로 변경합니다.



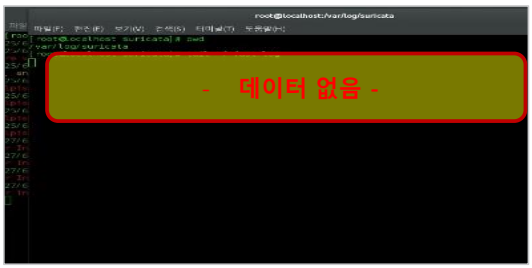
# 2. 발전제어시스템 화이트리스트 개발사례

## ☑ 화이트리스트(WhiteList) 적용 후 위/변조 행위 탐지 로그

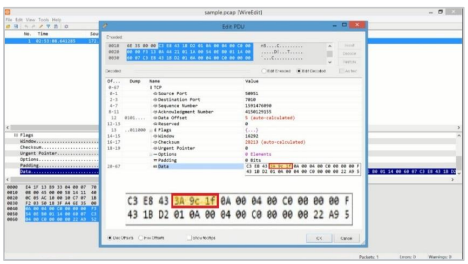
위/변조 행위 탐지

- 정상 패킷 데이터

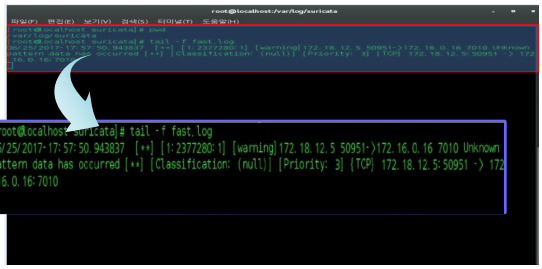
- 탐지 LOG -




- 위/변조 데이터 -



- 탐지 LOG -



# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 생성 결과

| NO | 구분 | 수집기간 | 원본데이터 | 분석 용량 | 메타 건수 | 화이트리스트 건수 | |
|---|---|---|---|---|---|---|---|
| | | | | | | 건수 | 압축률 |
| 1 | A구간 | 2016.05.10 ~ 2016.08.22 | 8.4 TB | 100 GB | 67,138,714 | 33,504 | 99.9% |
| 2 | B구간 | 2016.08.03 ~ 2016.09.01 | 11.7 GB | 11.7 GB | 2,439 | 1,655 | 32.1% |
| 3 | C구간 | 2017.02.13 ~ 2017.04.21 | 1.82 TB | 1.82 TB | 11,061,600 | 2,623 | 99.9% |
| 4 | D구간 | 2017.04.05 ~ 2017.05.10 | 1.45 TB | 1.45 TB | 17,958,295 | 591,723 | 96.7% |
| 총 계 | | | 11.68 TB | 3.38 TB | 96,161,048 | 629,505 | 99.3% |

시사점

✓ 생성된 PayLoad기반 화이트리스트는 압축률 평균이 약 99.3%를 차지하나 전체 화이트리스트 건수가 629,505건으로 파악되어, 기존 IDS 시스템으로는 PayLoad기반의 화이트리스트 적용이 어려움



# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 특징

EMERSON Process Management
SIEMENS
ABB
YOKOGAWA
Rockwell Automation
Honeywell THE POWER OF CONNECTED

발전소 지속 운영

제조사 다양

비표준 프로토콜

365일 24간 지속 운영을 해야 하는 발전제어시스템의 특성상 데이터 수집 및 제조사별 독자 프로토콜 분석의 한계가 존재

# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 개선방향

| | 한계점 | 핵심기술 | 개선방향 |
|---|---|---|---|
| 기술 관점 | ▪ **시그니처 기반 BlackList 기법의 한계**<br>- 단순 내부자 실수 등 알려지지 않은 보안 위협에 대응 불가<br>- 폐쇄망 구조로 인하여 신규 보안 Patch 적용이 어려움<br>▪ **국내 보안 기술의 한계**<br>- 표준 프로토콜(Modbus, DNP3)에 초점이 맞춰짐<br>- 비표준 기반 WhiteList기반 보안 탐지 제품이 전무함<br>▪ **IDS 탐지 엔진의 한계**<br>- 적용 가능한 화이트리스트 개수의 제한이 존재 | WhiteList 탐지기술 | ✓ **WhiteList 기반 기술 적용**<br>- 단순 내부자의 실수 및 알려지지 않은 보안 위협 대응 필요<br>- 보안 Patch 적용 불가 기간을 고려한 대응 방안 필요 |
| 운영 관점 | ▪ **실시간 보안위협 대응의 어려움**<br>- 제조사별 독자적 패킷의 분석 한계로 인하여 악성코드 발생여부의 파악이 어려워 보안위협에 대한 실시간 대응이 어려움<br>▪ **보안관제 유지보수 업무의 어려움**<br>- 외산 제품 운용에 따른 기술지원의 한계 존재<br>- 국내 발전사 업무 편의성을 고려한 기능 및 UI 구성 미흡<br>- 외산 제품 숙련공의 부족에 따른 즉시 기술 지원의 한계 | AI 기반 기술 | ✓ **비 표준 프로토콜 지원**<br>- 독자 프로토콜 분석 지원기능 필요<br>- 오탐을 고려한 사용자 예외처리 기능 필요<br>✓ **인공지능 기반 분석 엔진 적용**<br>- 이상행위 사전 예측 필요<br>- 화이트리스트 개수 제약을 해소 |
| | | BigData 기반기술 | ✓ **BigData 기반 네트워크 수집 기술 적용**<br>- 발전소 내부의 대량 네트워크 데이터 수집<br>- 실시간 분석을 통한 즉시 대응 가능 |



# 2. 발전제어시스템 화이트리스트 개발사례

## 발전제어시스템 화이트리스트 2차 개발

**전수 수집모듈 개발**

빅데이터 플랫폼 기반 구축
- 빅데이터 기반 플랫폼 구축
- 플랫폼 모니터링 구축
- 플랫폼 성능 검증 및 보완

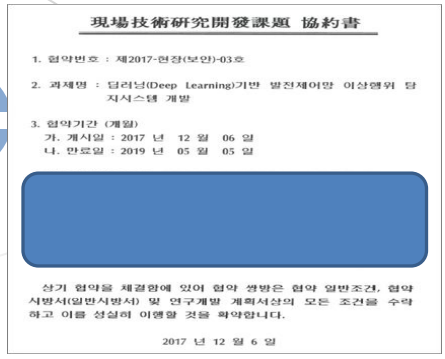
전수수집 기반 네트워크 패킷 수집 모듈 개발
- 모듈 개발/검증을 위한 초기 데이터 수집
- 모듈 검증 시나리오
- 검증용 데이터 준비

**분석/탐지/모니터링 모듈 개발**

인공지능 기반 패킷 분석/탐지 모듈 개발
- 인공지능 알고리즘 개발
- 네트워크 패킷 분석(Header/PayLoad) 및 학습수행

모니터링 시스템 개발
- 사용자 알람, 통계 분석 등

범위


現場技術研究開發課題 協約書

1. 협약번호 : 제2017-현장(보안)-03호
2. 과제명 : 딥러닝(Deep Learning)기반 발전제어망 이상행위 탐지시스템 개발
3. 협약기간 (개월)
가. 개시일 : 2017 년 12 월 06 일
나. 완료일 : 2019 년 05 월 05 일

상기 협약을 체결함에 있어 협약 상방은 협약 일반조건, 협약시방서(일반시방서) 및 연구개발 계획서상의 모든 조건을 수락하고 이를 성실히 이행할 것을 확약합니다.

2017 년 12 월 6 일

**현장검증**

현장 검증 및 보완
- 성능 검증 테스트 데이터/시나리오 준비
- 현장 설치 및 검증/보완 수행
- 결과 보고서 작성

# 2. 발전제어시스템 화이트리스트 개발사례

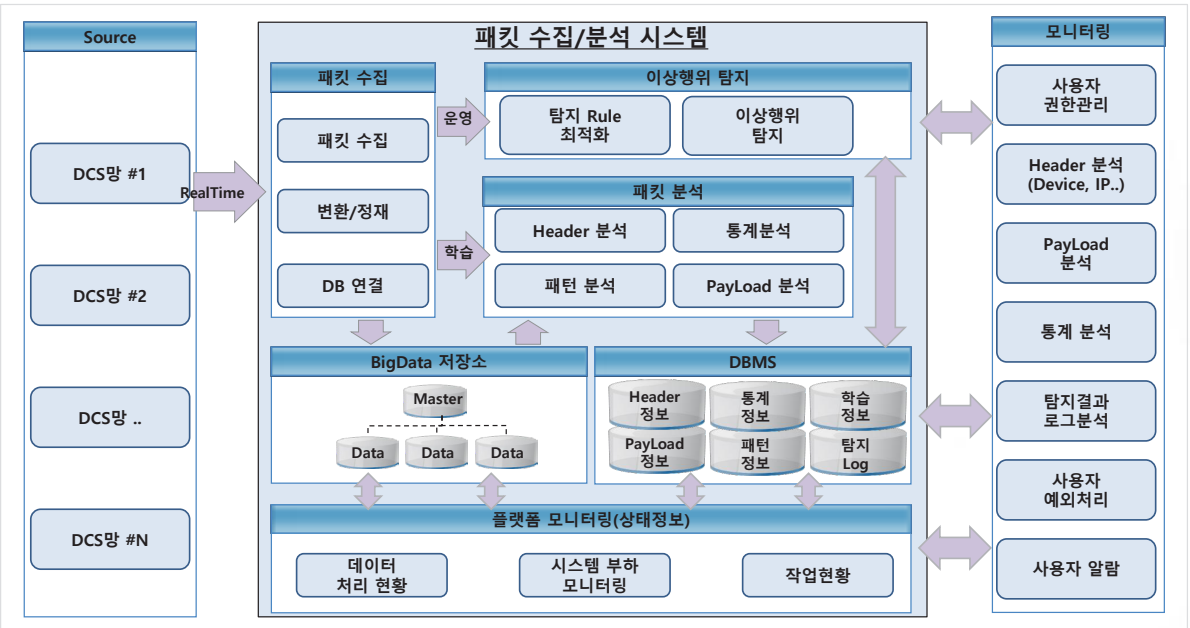
## 발전제어시스템 화이트리스트 목표 시스템

| 구 분 | 기존 IDS | 목표 시스템 | 주요 차이점 |
|---|---|---|---|
| 주요역할 | 탐지(Detection) | 탐지(Detection) | |
| 물리적 위치 | 내부에서 보안 위협 감시 | 내부에서 이상 행위 감시 | |
| 네트워크 부하 | 부하 적음 | 부하 많음 | 전수 수집에 따른 부하 증가 |
| 설계정책 | 명백하게 금지하는 것만 금지 | 이상 흐름이 예상되는 행위를 알림 (사용자가 이상여부의 최종 판단) | 사용자 판단 개입 |
| 패킷 데이터 적재량 | 없음(또는 일부 메타 데이터) | 전수 수집 | 빅데이터 기술 적용 |
| 탐지 엔진/방식 | IDS 엔진/BlackList 방식 | 인공지능 엔진/WhiteList 방식 | 탐지 엔진 및 기법 |
| 탐지범위 | 알려지지 않은 이상행위 탐지 불가 | 알려지지 않은 이상행위 탐지 가능 | Abnormally 분석 |
| 프로토콜 지원범위 | 표준 프로토콜만 지원 | 비표준 프로토콜 지원 (패킷 상세분석 미지원) | Header + Payload 분석 |



# 2. 발전제어시스템 화이트리스트 개발사례

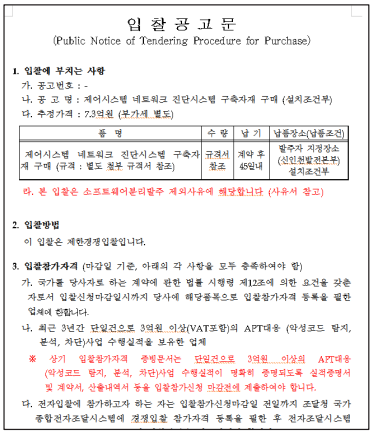
## 발전제어시스템 화이트리스트 목표 시스템 구성도



# 3. 발전제어시스템 보안관제 구축사례

## 발전사별 보안관제 추진현황

### 한국남부발전



입 찰 공 고 문
(Public Notice of Tendering Procedure for Purchase)

1. 입찰에 부치는 사항
가. 공고번호 : -
나. 공 고 명 : 제어시스템 네트워크 진단시스템 구축자재 구매 (설치조건부)
다. 추정가격 : 7.3억원 (부가세 별도)

| 품 명 | 수 량 | 납 기 | 납품장소(납품조건) |
|---|---|---|---|
| 제어시스템 네트워크 진단시스템 구축자재 구매 (규격 : 별도 첨부 규격서 참조) | 규격서 참조 | 계약 후 45일내 | 발주자 지정장소 (신인천발전본부) 설치조건부 |

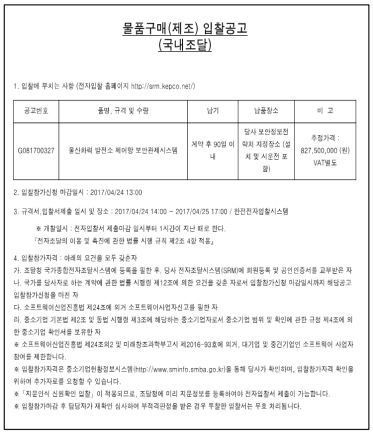
라. 본 입찰은 소프트웨어분리발주 제외사유에 해당합니다 (사유서 참조)

2. 입찰방법
이 입찰은 제한경쟁입찰입니다.

3. 입찰참가자격 (마감일 기준, 아래의 각 사항을 모두 충족하여야 함)
가. 국가를 당사자로 하는 계약에 관한 법률 시행령 제12조에 의한 요건을 갖춘 자로서 입찰신청마감일시까지 당사에 해당종목으로 입찰참가자격 등록을 필한 업체에 한합니다.
나. 최근 3년간 단일건으로 3억원 이상(VAT포함)의 APT대응 (악성코드 탐지, 분석, 차단)사업 수행실적을 보유한 업체
※ 상기 입찰참가자격 증빙문서는 단일건으로 3억원 이상의 APT대응 (악성코드 탐지, 분석, 차단)사업 수행실적이 명확히 증명되도록 실적증명서 및 계약서, 산출내역서 등을 입찰참가신청 마감전에 제출하여야 합니다.
다. 전자입찰에 참가하고자 하는 자는 입찰참가신청마감일 전일까지 조달청 국가종합전자조달시스템에 갱생입찰 참가자격 등록을 필한 후 전자조달시스템

제어시스템 네트워크 진단시스템 구축 공고(16.11)
신인천 발전본부 2017.05 구축 완료

### 한국동서발전



물품구매(제조) 입찰공고
(국내조달)

1. 입찰에 부치는 사항 (전자입찰 홈페이지 http://srm.kepco.net/)

| 공고번호 | 품명, 규격 및 수량 | 납기 | 납품장소 | 비 고 |
|---|---|---|---|---|
| G081700327 | 울산화력 발전소 제어망 보안관제시스템 | 계약 후 90일 이내 | 당사 보안정보전략처 지정장소 (설치 및 시운전 포함) | 추정가격 : 827,500,000 (원) VAT별도 |

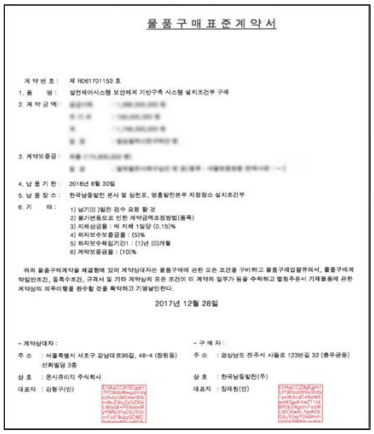
2. 입찰참가신청 마감일시 : 2017/04/24 13:00

3. 규격서 입찰서제출 일시 및 장소 : 2017/04/24 14:00 ~ 2017/04/25 17:00 / 한전전자입찰시스템
※ 개찰일시 : 전자입찰서 제출마감 일시부터 1시간이 지난 때로 한다.
[1]전자조달의 이용 및 촉진에 관한 법률 시행 규칙 제2조 4항 적요」

4. 입찰참가자격 : 아래의 요건을 모두 갖춘자
가. 조달청 국가종합전자조달시스템에 등록을 필한 후, 당사 전자조달시스템(ISRM)에 회원등록 및 공인인증서를 교부받은 자
나. 국가를 당사자로 하는 계약에 관한 법률 시행령 제12조에 의한 요건을 갖춘 자로서 입찰참가신청 마감일시까지 당사에 해당종목으로 입찰참가자격 등록을 필한 업체에 한합니다.
다. 소프트웨어산업진흥법 제24조에 의거 소프트웨어사업자신고를 필한 자
라. 중소기업 기본법 제2조 및 동법 시행령 제3조에 해당하는 중소기업자로서 중소기업 범위 및 확인에 관한 규정 제4조에 의한 중소기업 확인서를 보유한 자
※ 소프트웨어산업진흥법 제24조제2 및 미래창조과학부고시 제2016-93호에 의거, 대기업 및 중견기업인 소프트웨어 사업자 참여를 제한합니다.
※ 입찰참가자격은 중소기업현황정보시스템(http://www.sminfo.smba.go.kr)을 통해 당사가 확인하며, 입찰참가자격 확인을 위하여 추가자료를 요청할 수 있습니다.
※ 「지문인식 신원확인 입찰」이 적용되므로, 조달청에 미리 지문정보를 등록하여야 전자입찰서 제출이 가능합니다.
※ 입찰참가하려 후 입찰자가 재확인 심사하여 부적격판정을 받은 경우 무찰한 입찰서는 무효 처리됩니다.

제어망 보안관제시스템 구축 공고(17.04)
울산 발전본부 구축 완료

### 한국남동발전



물 품 구 매 표 준 계 약 서

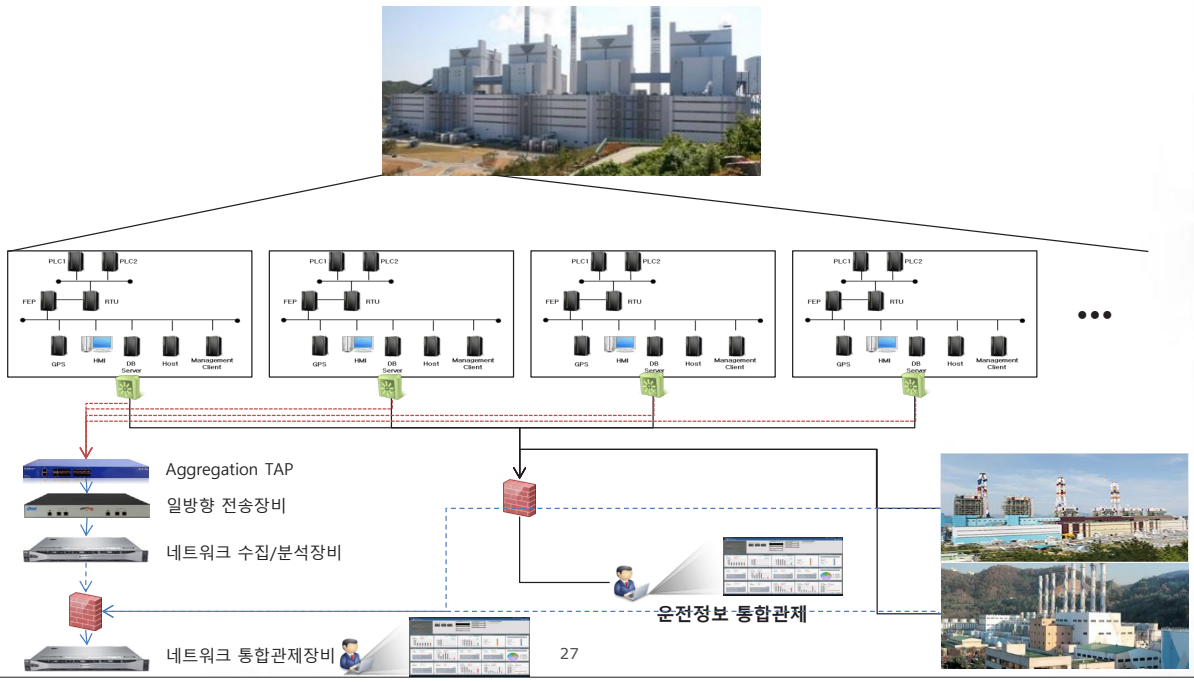
2017년 12월 28일

발전제어시스템 보안체계 기반구축 시스템
본사, 영흥, 삼천포 발전본부 구축 진행 中



# 3. 발전제어시스템 보안관제 구축사례

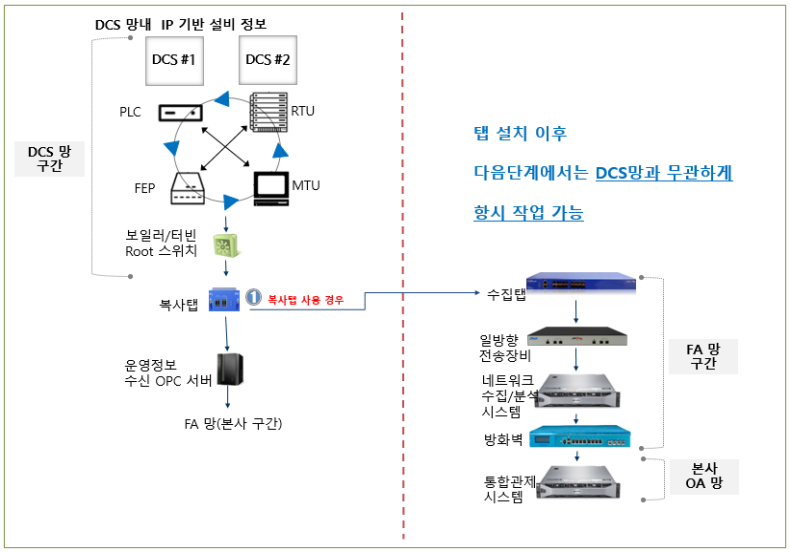
## 발전제어시스템 보안관제 구축사례



# 3. 발전제어시스템 보안관제 구축사례

## 망연결시 고려사항 - 탭

### 네트워크 트래픽 수집 기반 구축(탭)




**장점**

① DCS 망의 스위치 설정 변경 불필요

② Root 스위치와 OPC 서버간의 네트워크 트래픽 정보만 수집 가능

**단점**

① IP 기반 설비들 간의 모든통신 정보 수집 불가능

② 보일러/터빈 Root 스위치 내부의 IP 단말간 트래픽 수집 불가(목적지가 OPC일 경우만 가능)

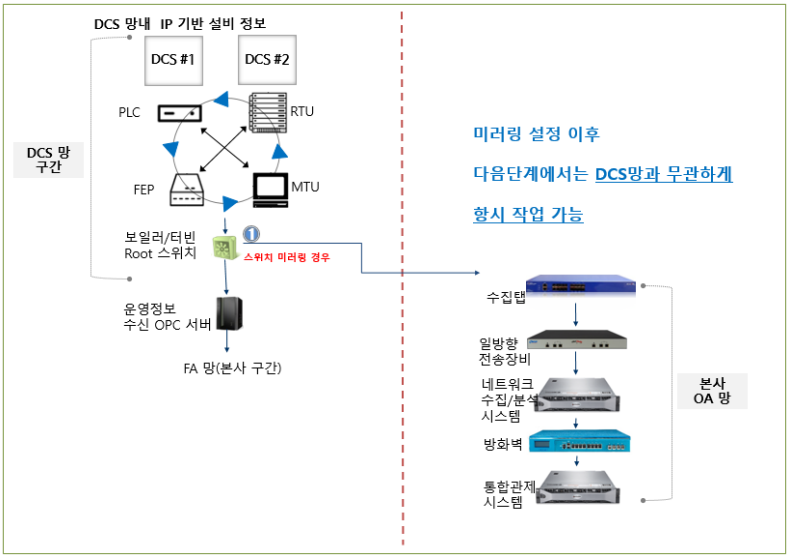
③ 스위치와 OPC 간의 일시적 단절 발생 ->O/H 기간 활용

28

# 3. 발전제어시스템 보안관제 구축사례

## 망연결시 고려사항 – 스위치 미러링

### 네트워크 트래픽 수집 기반 구축(미러링)




**장점**

① Root S/W를 통하는 모든 네트워크 트래픽 수집 가능

② IP 기반 설비 정보에 대한모든 트래픽 대상 상세 분석 가능

③ 패킷 미러링방식(복사)으로 DCS망의 네트워크 영향 無

**단점**

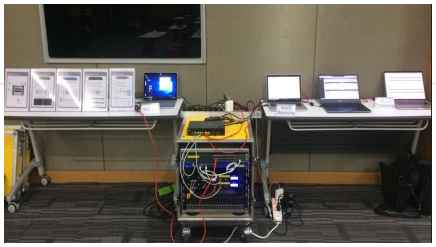
① DCS 망의 스위치 설정 변경 (미러링 기능 설정)

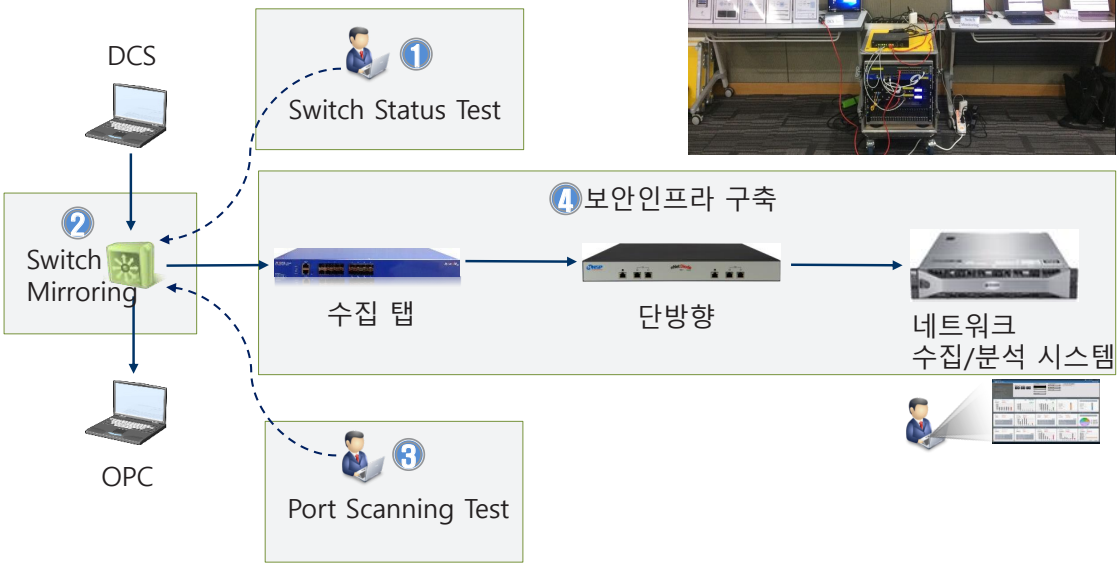
② 스위치 설정 변경에 따른 관리 책임 소재 발생 (예, 스위치 장비 교체 및 설정 변경)

29

## 3. 발전제어시스템 보안관제 구축사례

### 사전 안정성 검증






※ 안정성 검증 및 사전 준비를 통해 충분히 테스트 진행 후 순차적 구축 진행



## 3. 발전제어시스템 보안관제 구축사례

### 안정성 검증 영상 – 스위치 미러링

# 3. 발전제어시스템 보안관제 구축사례

## 안정성 검증 영상 – 포트 스캐닝

32

# 4. 발전제어시스템 보안관제 전략

## 지능형 Hybrid 통합보안관제시스템 구축

- 지능형 Hybrid 통합보안관제시스템은 화이트리스트 방식과 블랙리스트 방식의 장점을 통합
- 제조사별 프로토콜 사용에 따른 보안위협 대응의 한계를 탈피
- 국내 발전사 제어시스템에 최적화된 보안관제 서비스 제공을 목표

33

# Q&A

# 감사합니다.

The 24th Network Security Conference -Korea

# 전력제어 사이버보안 기술 동향

**김진철** 한전KDN 팀장

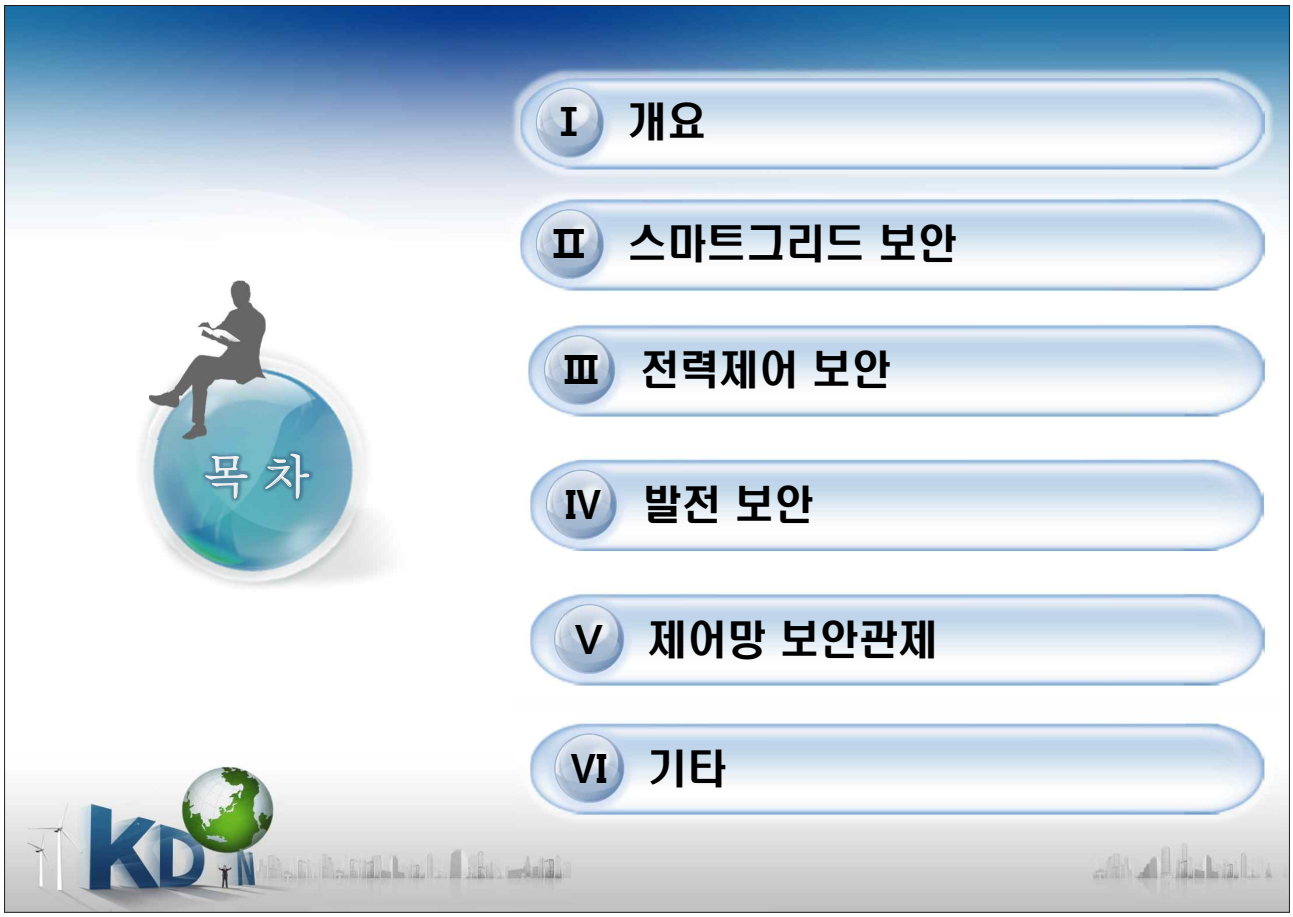
### 학력 및 경력사항

| | |
|---|---|
| 2006.08 | 광운대학교 대학원 전자통신공학과 박사 졸업 |
| 1995.12 ~ 현재 | 한전KDN 전력IT연구원 전력보안연구팀장 근무 |

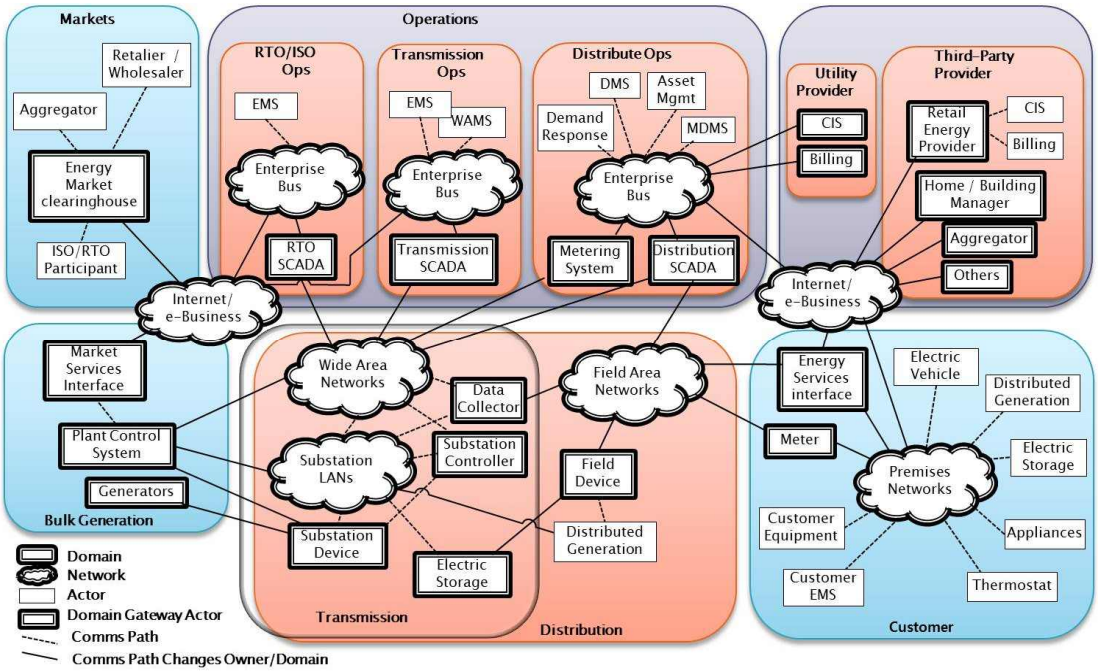
### 강연요약

전력제어시스템 사이버 보안의 중요성과 관심이 높아지고 있다. 본 강연에서는 각 전력계통간의 연계, 전력계통 사이버 보안관련 국제 표준, 전력계통에서 진행되고 있는 보안 솔루션을 살펴보고, 각각의 전력계통별 보안 솔루션 개발 및 적용현황을 소개하고, 향후 전력제어 사이버 보안의 발전방향을 논의함.

전력제어 사이버 보안 기술 동향
2018. 04. 12
Kdn 한전KDN㈜
전력보안연구팀
KDN


목 차
Ⅰ 개요
Ⅱ 스마트그리드 보안
Ⅲ 전력제어 보안
Ⅳ 발전 보안
Ⅴ 제어망 보안관제
Ⅵ 기타
KDN

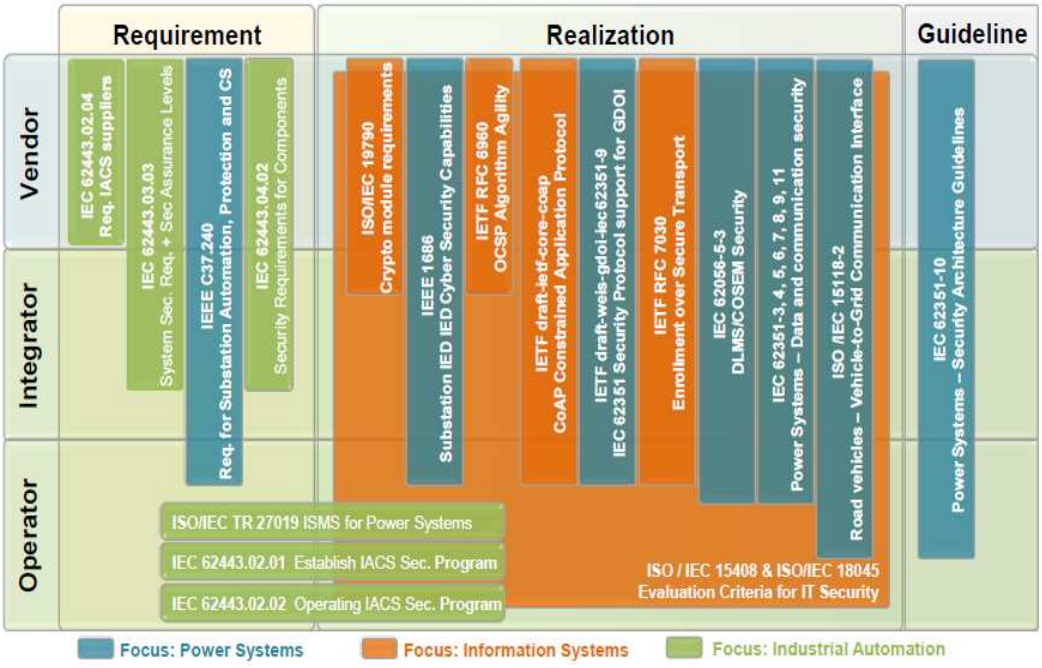
# 1-1 전력계통 다이어그램 개요




[ Smart Grid Reference Diagram, NIST]

3

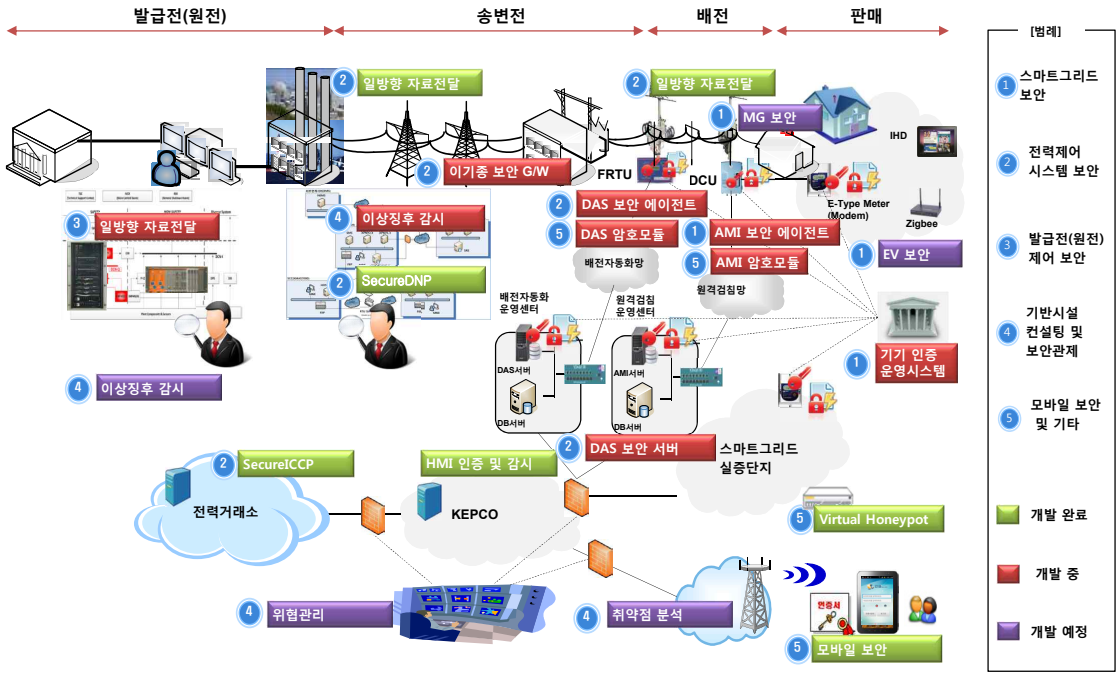
# 1-2 전력제어시스템 보안표준 개요




[ Smart Grid Cyber Security Standards, CERT]

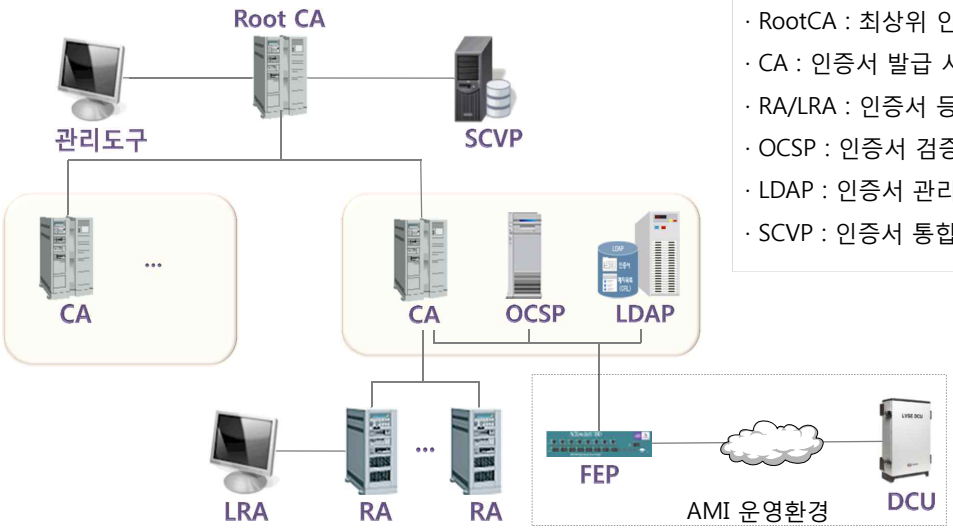
4

# 1-3 전력계통 보안솔루션 개요




5

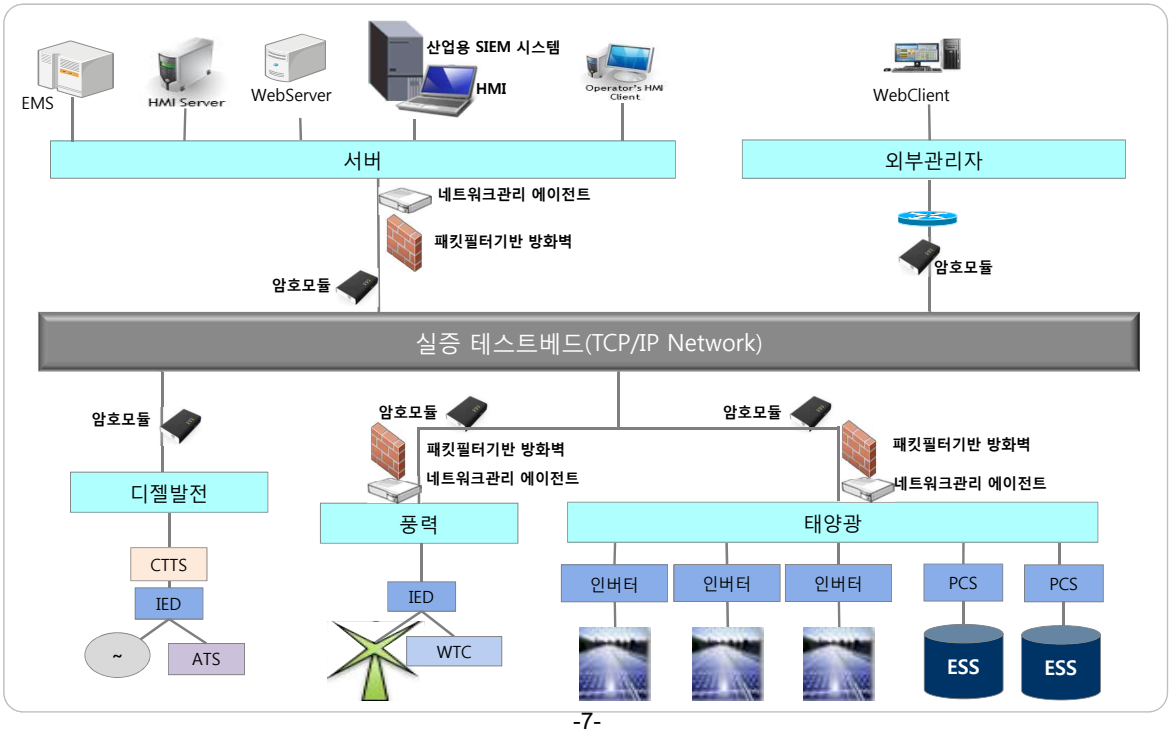
# 2-1 기기인증운영시스템 스마트그리드 보안




· RootCA : 최상위 인증 시스템
· CA : 인증서 발급 시스템
· RA/LRA : 인증서 등록 시스템
· OCSP : 인증서 검증 시스템
· LDAP : 인증서 관리 시스템
· SCVP : 인증서 통합검증 시스템

# 2-2 마이크로그리드 보안

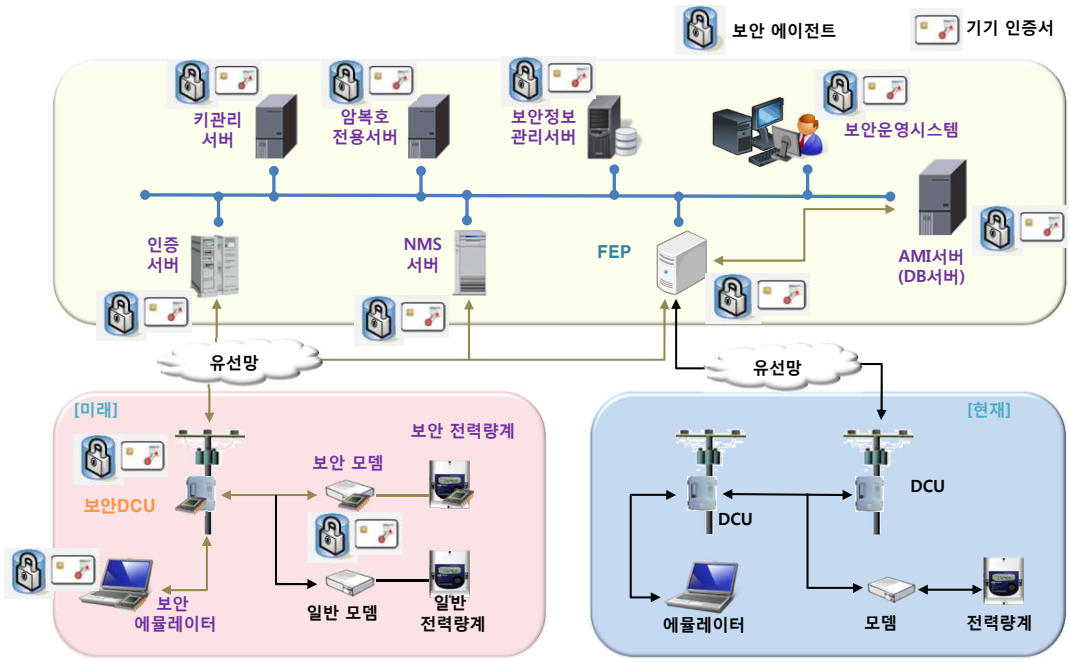
스마트그리드 보안




-7-

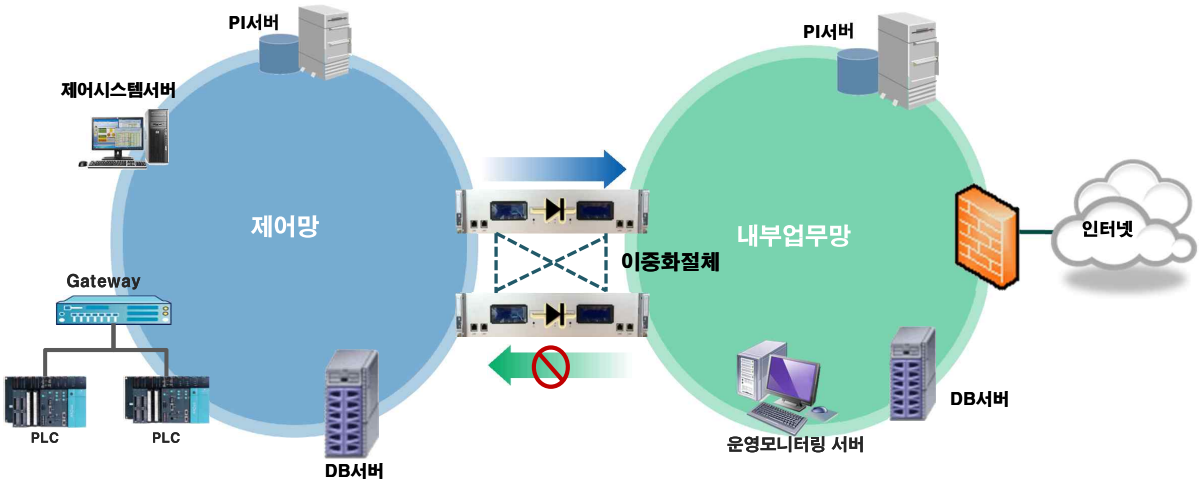
# 2-3 AMI 네트워크 보안

스마트그리드 보안



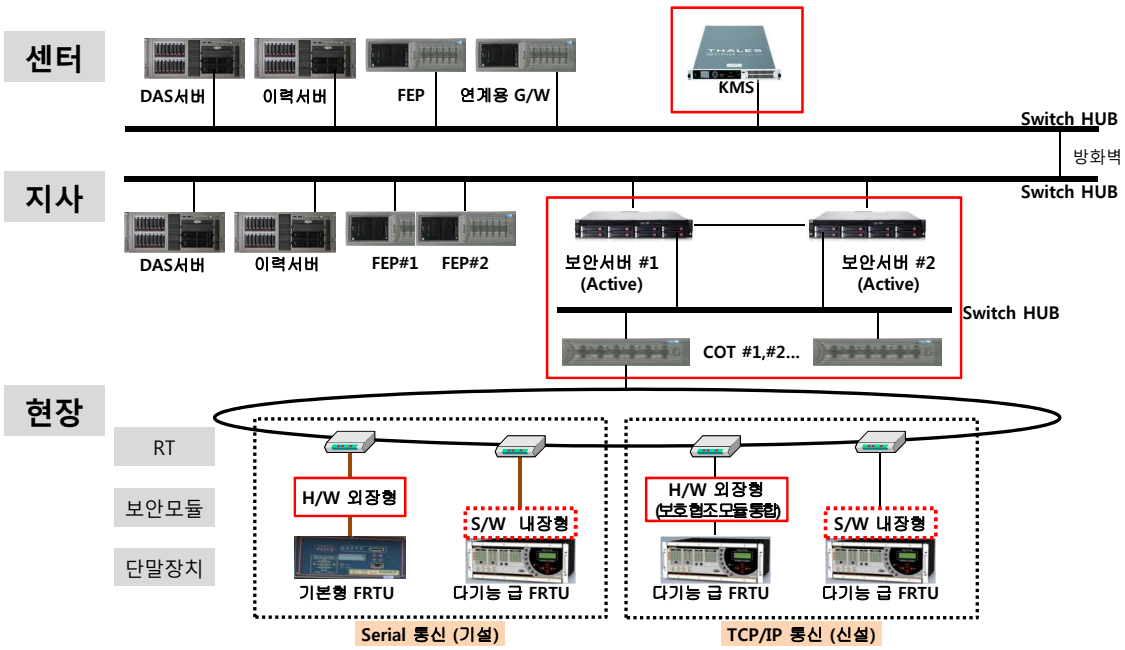

-8-

# 3-1 일방향자료전달시스템 전력제어 보안



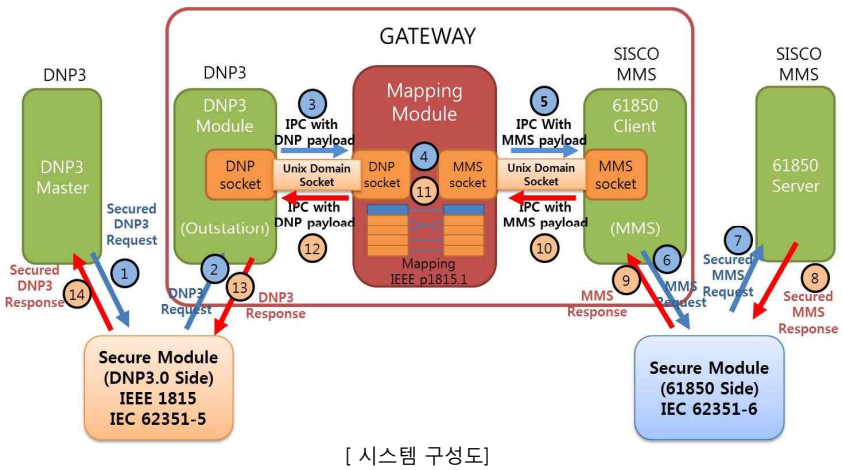

-9-

# 3-2 배전지능화시스템 보안 전력제어 보안

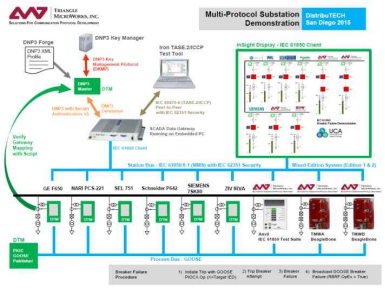



-10-

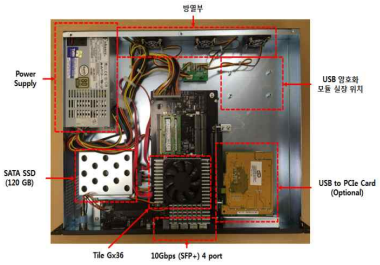
# 3-3 이기종 프로토콜 보안 전력제어 보안




[ 시스템 구성도]



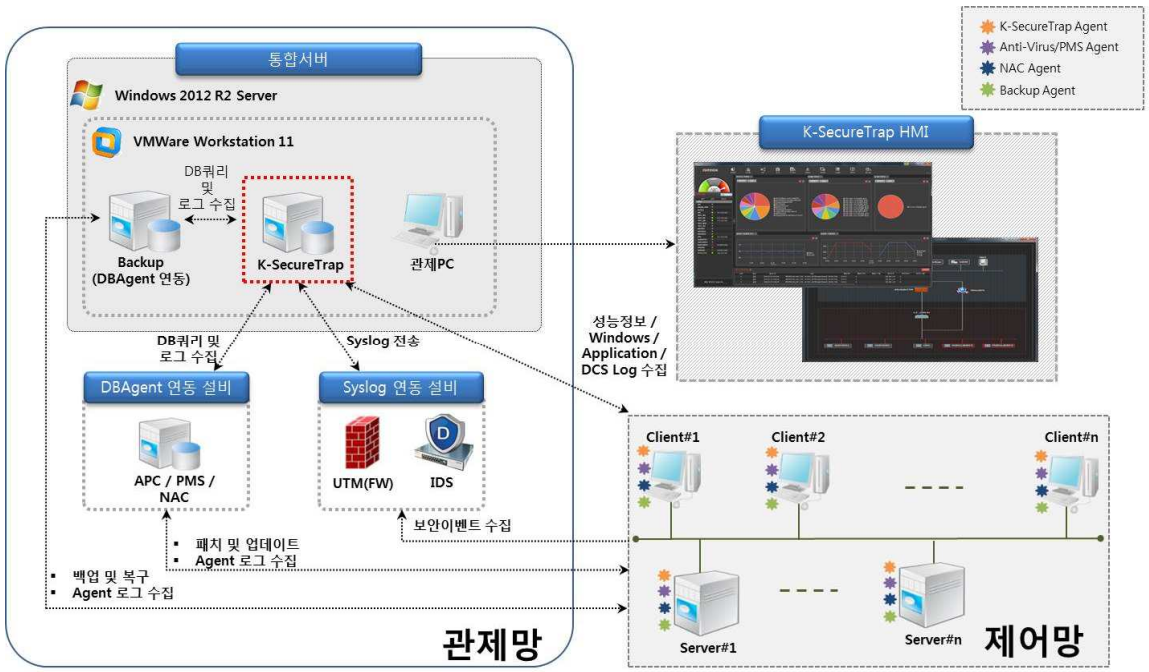

[미국 TM사 솔루션]



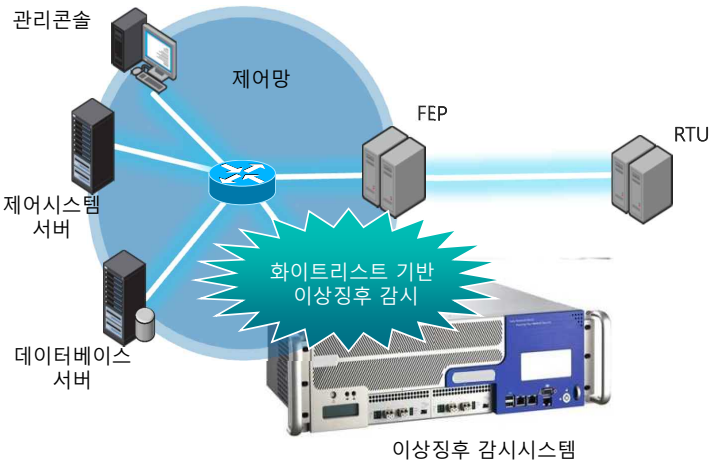

[ 솔루션 사진]

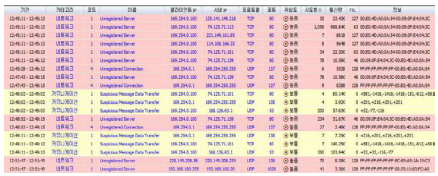


# 4. 발전소제어망 보안솔루션 발전 보안

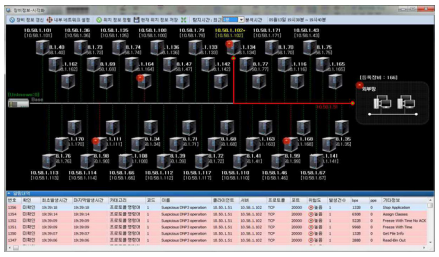


# 5-1. 이상징후감시시스템 제어망 보안관제



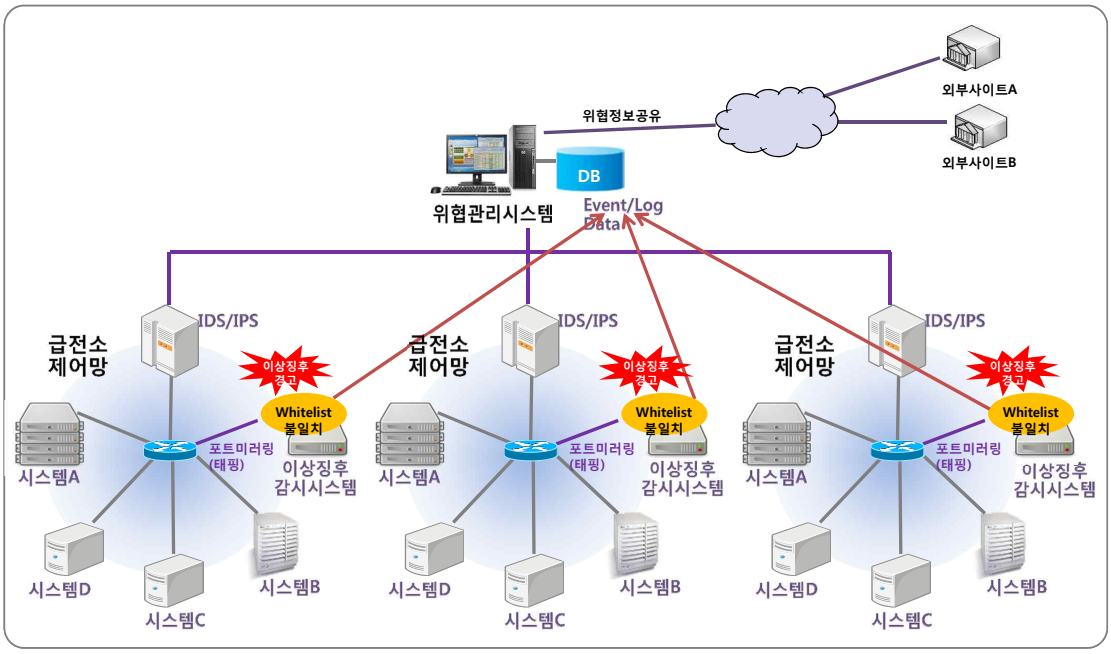
[실시간 이상징후 경보리스트]



[네트워크 구성도에서의 이상징후 시각화]

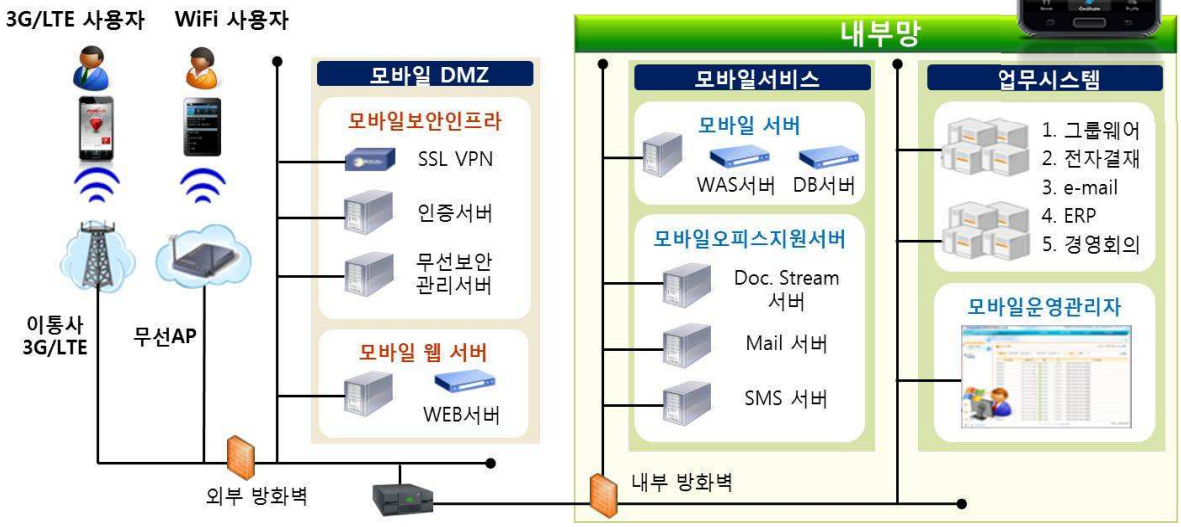


# 5-3. 위협관리시스템 제어망 보안관제



# 6-1. 모바일 보안

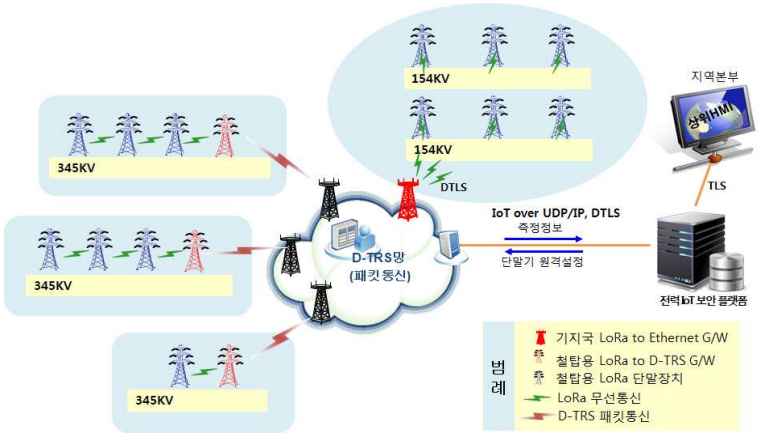
기타



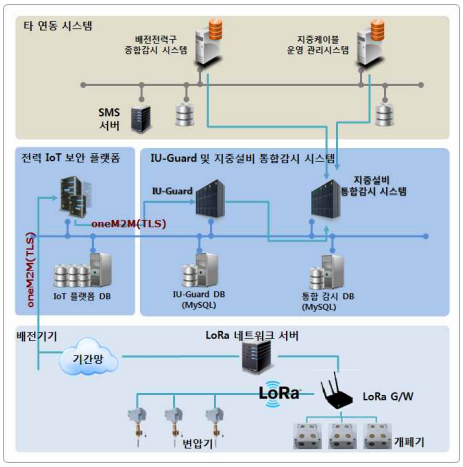



# 6-2. IoT 보안

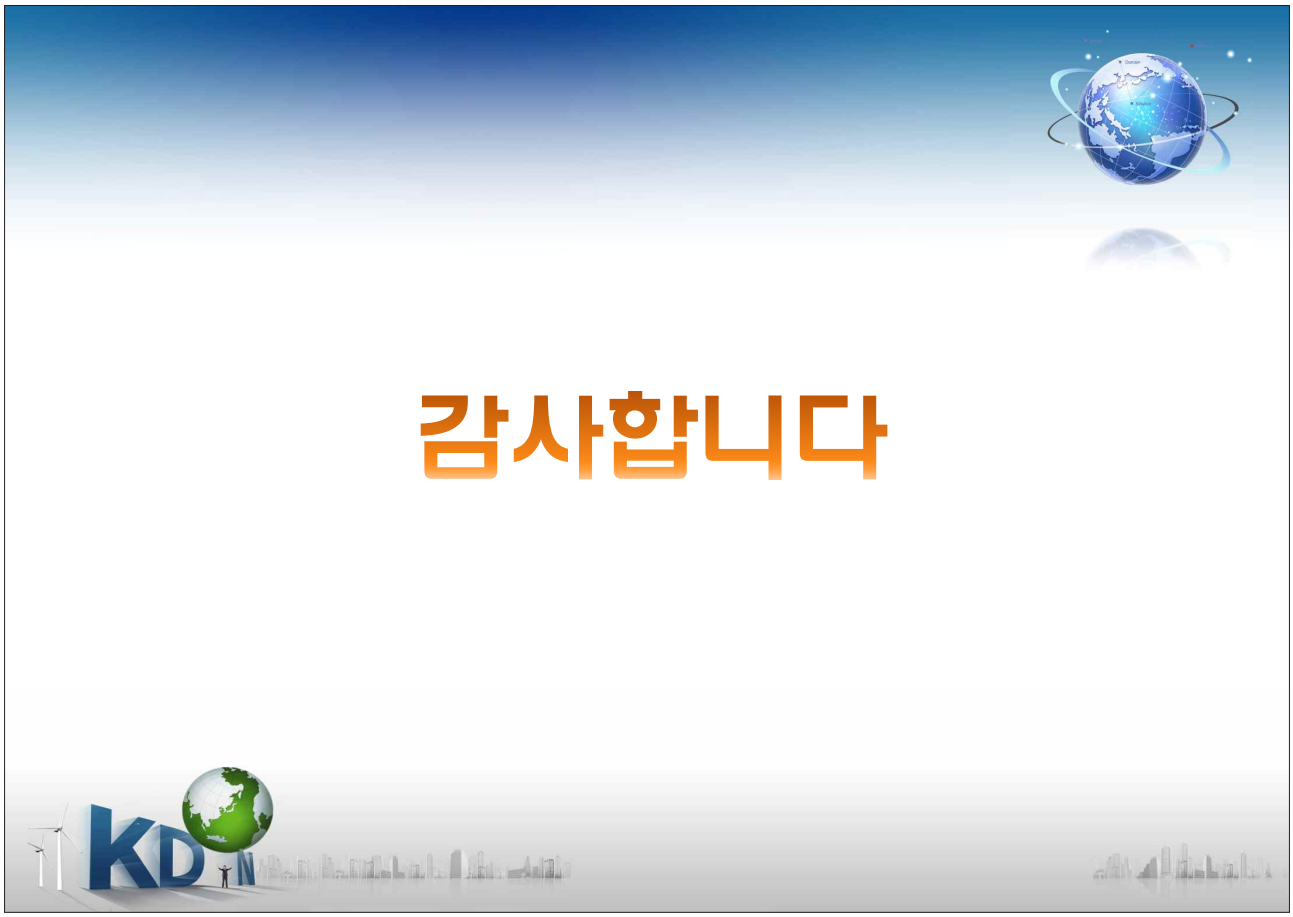
기타




[항공장애등 원격감시시스템 IoT 실증시험




[배전지중설비 통합감시시스템 시범사업]


감사합니다

The 24th Network Security Conference -Korea

# 클라우드 가상화 환경에서의 보안위협: 캐시 기반 은닉 채널

**신영주** 광운대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2014.08 | KAIST 전산학과 (박사) |
| 2008.02 | KAIST 전산학과 (석사) |
| 2006.02 | 고려대학교 컴퓨터학과 |
| 2017.03 ~ | 광운대학교 컴퓨터정보공학부 조교수 |
| 2008.04 ~ 2017.02 | 국가보안기술연구소 선임연구원 |

### 강연요약

클라우드 컴퓨팅의 핵심인 가상화 기술은 물리적으로 단일한 컴퓨팅 시스템을 다수의 논리적 자원으로 분할하여 컴퓨팅 자원을 효율적으로 사용하게 한다. 가상화 기술은 자원의 비용 효율성, 확장성, 가용성 측면에서 장점을 제공하나 메인 메모리, 캐시 등 가상머신 간에 공유되는 하드웨어 자원을 이용하여 상대방의 정보를 불법적으로 획득할 수 있는 침해 위협을 야기한다. 최근 CPU 캐시 메모리를 공유하면서 발생하는 간섭현상을 은닉채널로 활용하여 다른 가상머신의 비밀 정보를 유출하는 캐시 부채널 공격이 많이 연구되고 있다. 본 강연에서는 캐시 부채널 공격에 대한 기본 개념과 현재까지 알려진 기술 동향을 살펴보고 그 파급 효과에 대해 고찰한다.

NetSec-KR 2018

# 클라우드 가상화 환경에서의 보안위협: 캐시 기반 은닉채널

광운대학교 컴퓨터정보공학부
신영주

## 클라우드 컴퓨팅

- 클라우드 컴퓨팅 기술
  - 인공지능, 빅데이터, IoT 기술 실현을 위한 컴퓨팅 플랫폼
  - 클라우드 서비스 시장은 2020년까지 연 25%이상 성장전망 (IDC 2016)
    * IaaS 37.3%, PaaS 35.9%, SaaS 26%

- 클라우드 컴퓨팅 기술 핵심 요소로서의 『서버 가상화』
  - 자원 활용 극대화
  - 장애 고립
  - 새로운 자원 제공의 유연성

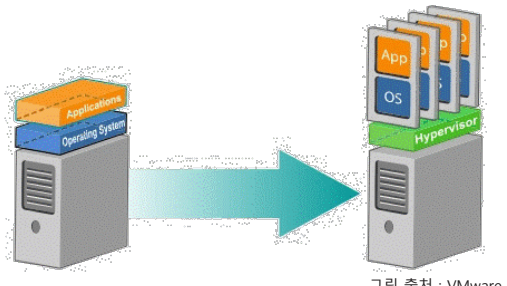


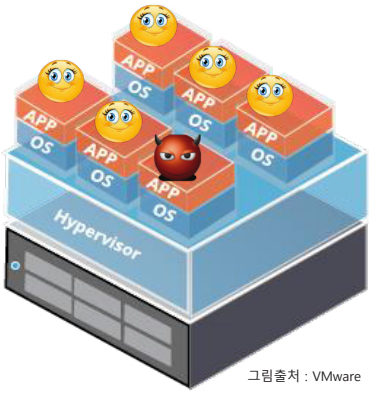

그림 출처 : VMware

서버 가상화 기술

# 서버 가상화 기술의 보안 위협

- 멀티 테넌트Multi-tenant 클라우드 환경
  - 여러 사용자가 단일 서버의 컴퓨팅 자원을 공유
  - CPU, 메모리, 캐시 등
- 가상 머신 간의 완벽한 격리 불가
  - 물리적 분리가 아닌 논리적 분리에 의한 한계
  - 공유 컴퓨팅 자원 활용에 의한 상호 간섭 발생
- 동일 서버 사용자간의 정보 유출 가능성
  - 자원 공유에 의한 간섭을 악용
  - 악의적 사용자는 공유 자원을 사용하는 다른 정상 사용자의 비밀 정보를 획득

캐시 부채널 공격 (Cache side-channel attack)



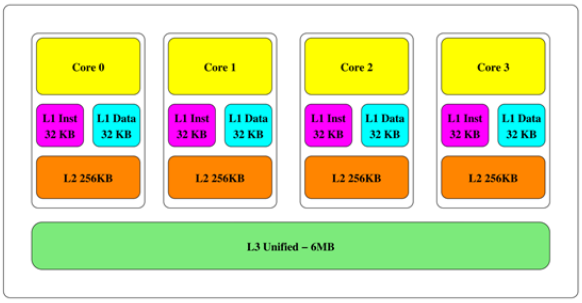
그림출처 : VMware



# 캐시 부채널 공격

- CPU 캐시 구조
  - 자주 사용되는 데이터의 빠른 엑세스를 위한 H/W
    - Temporal/spatial locality
    - 메모리 대비 10~100 배 고속
  - 3단계 캐시 구조
    - L1(64KB), L2(256 KB)
    - L3(6MB ~)
  - CPU 의 데이터 로드 과정
    - 1) 데이터가 캐시에 있는지 확인
    - 2) 캐시에 있을 경우 (hit) 레지스터로 로드
      캐시에 없을 경우 (miss) 메모리 또는 하위레벨 캐시 확인

      * Hit 과 miss 에 따른 시간 차 발생



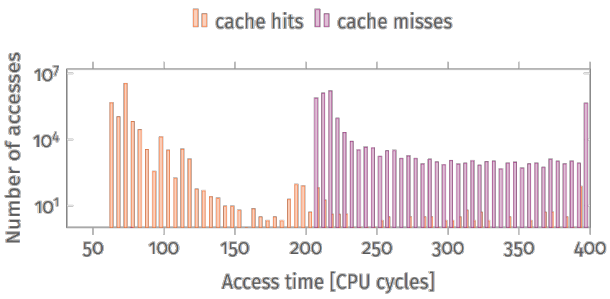



그림 출처: Maurice et al., NDSS'17

# 캐시 부채널 공격

- 가상 머신 간 공유되는 CPU 캐시에서의 간섭 현상을 부채널로 활용하여 비밀 정보를 획득하는 공격

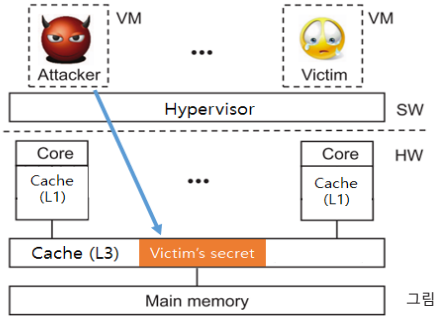



그림 출처: Liu et al., SP'15

클라우드 가상화 환경에서의 캐시 부채널 공격 연구 사례

| 2006 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|
| 캐시부채널 공격가능성 확인/ AES 암호키추출 | VMware ESX 하이퍼바이저 캐시부채널 보안취약점패치 | RSA, ElGamal, ECDSA 등 주요 암호 캐시 부채널 취약점 발표 | Amazon Web Service 불특정 다수 EC2 인스턴스 대상 RSA 키 공격 (남미지역 55% 이상 취약점 노출) | RSA,ElGamal 및 포스트 퀀텀 암호 대상 캐시부채널공격 결과 다수 발표 |



KWANGWOON UNIVERSITY

# 캐시 부채널 공격

KWANGWOON UNIVERSITY

# 주요 캐시 부채널 공격 기법

- Flush+Reload technique
  - 캐시 라인 단위의 간섭 현상을 관측하여 정보 획득
  - 높은 정밀도와 낮은 잡음
  - 공격 선행 조건
    - 프로세스 혹은 가상머신 간 메모리 공유
    - 캐시 제어 명령어 (e.g., clflush in x86)
- Prime+Probe technique
  - 캐시 집합 단위의 간섭 현상을 관측하여 정보 획득
  - Flush+Reload 공격에 비해 상대적으로 높은 잡음 발생
  - 메모리 공유 필요 없음

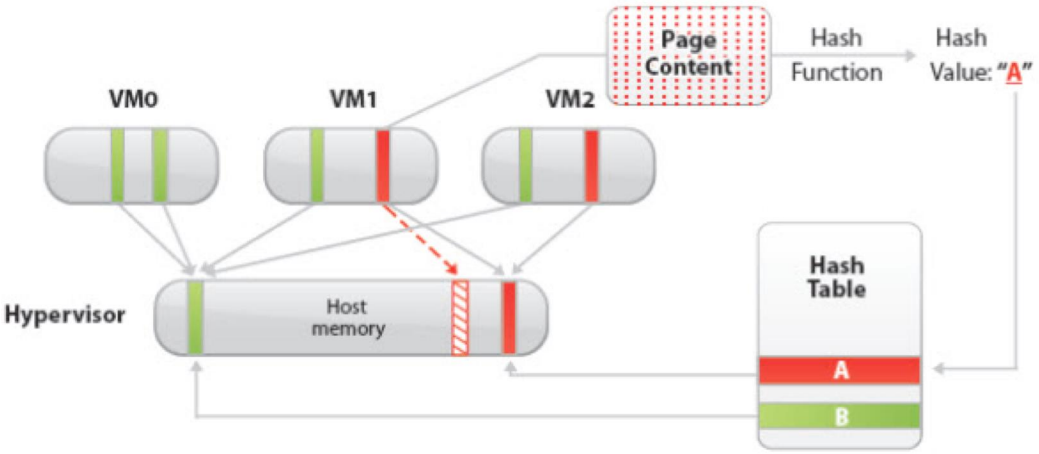


# 메모리 공유 방식

- Content-aware sharing
  - Pages from the same file have identical content
  - Shared program or library code
    - Can also share constant data
  - Shared images in PaaS clouds
- Content-based sharing (a.k.a. memory deduplication)
  - The system identifies and coalesces identical pages
  - Implemented in many hypervisors and in most modern operating systems
  - Linux KVM (KSM), VMware (TPS), Android (Zygote)

# 메모리 공유 방식

- VMware Transparent Page Sharing (TPS)



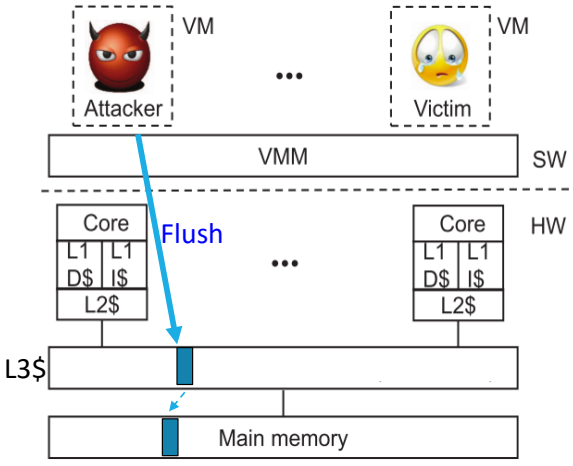

그림출처: VMware



KWANGWOON UNIVERSITY

# Flush+Reload technique

- Phase1 (Flush) : 메모리 라인을 캐시에서 flush

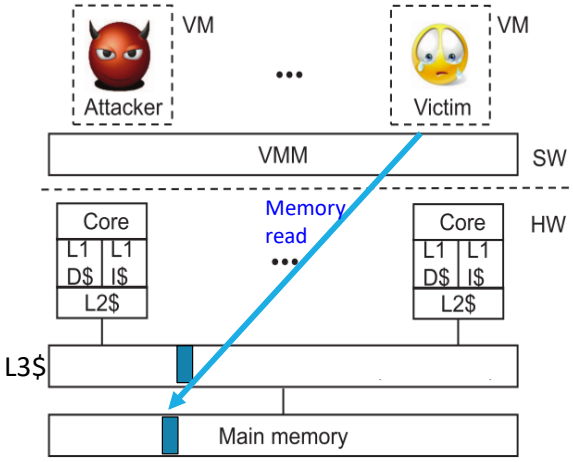





KWANGWOON UNIVERSITY

# Flush+Reload technique

- Phase2 (Wait) : Victim 이 실행할 동안 대기

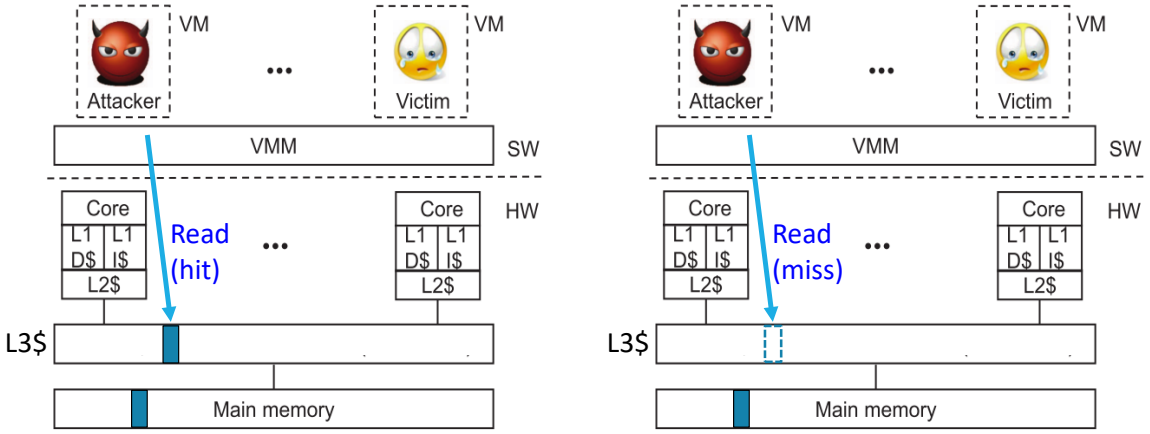





KWANGWOON UNIVERSITY

# Flush+Reload technique

- Phase3 (Reload) : 캐시 상태 확인
  - Victim 이 메모리를 엑세스 했을 경우 (좌측) → Cache hit
  - Victim 이 메모리를 엑세스 하지 않았을 경우 (우측) → Cache miss






KWANGWOON UNIVERSITY

# Variants of Flush+Reload technique

- Evict+Reload
  - Uses cache contention instead of `clflush`
  - ARM processor
- Flush+Flush
  - Measures variations in `clflush` timing between cached and non-cached data
  - Improved temporal resolution
- Invalidate+Transfer
  - Cross-package (CPU) attack
  - Use Flush+Reload on Intel or Evict+Reload on ARM



# Flush+Reload 를 활용한 RSA 복호키 추출 공격

- Square-Multiply Exponentiation (GnuPG 1.4.13)
  - 지수(e) 의 i 번째 bit 값 $e_i$ 에 따라 실행 흐름 결정
    - $e_i$=1 : square → reduce → multiply → reduce
    - $e_i$=0 : square → reduce

```
1  function exponent(b, e, m)
2  begin
3    x ← 1
4    for i ← |e| − 1 downto 0 do
5      x ← x^2                    Square
6      x ← x mod m                Reduce
7      if (e_i = 1) then
8        x ← xb                   Multiply
9        x ← x mod m              Reduce
10     endif
11   done
12   return x
13 end
```

# Flush+Reload 를 활용한 RSA 복호키 추출 공격

- Flush+Reload attack on GnuPG 1.4.13
  - Square-Multiply 알고리즘의 실행 흐름을 probing
  - Probing point
    - Square 연산 : line 5, Multiply 연산 : line 8, Reduce (Modulo) 연산 : line 6, 9

```
1  function exponent(b, e, m)
2  begin
3    x ← 1
4    for i ← |e| − 1 downto 0 do
5      x ← x^2                    Square
6      x ← x mod m                Reduce
7      if (e_i = 1) then
8        x ← xb                   Multiply
9        x ← x mod m              Reduce
10     endif
11   done
12   return x
13 end
```



KWANGWOON UNIVERSITY

# Flush+Reload 를 활용한 RSA 복호키 추출 공격

- Flush+Reload attack on GnuPG 1.4.13

Square in mpih-mul.c

```
0x00000000004931d6 <+838>: mov   %r14,%rdi
0x00000000004931d9 <+841>: callq  0x492d80 <mpih_sqr_n_basecase>
0x00000000004931de <+846>: jmpq   0x493055 <mpih_sqr_n+453>
0x00000000004931e3 <+851>: nopl   0x0(%rax,%rax,1)

334
335                        /* Add/copy Product L (twice).    */
336                        cy += mpihelp_add_n (prodp + hsize, prodp + hsize, tspace, size);   <-- Probing point
0x0000000000493055 <+453>: mov   %ebp,%ecx
0x0000000000493057 <+455>: mov   %r14,%rdx
0x000000000049305a <+458>: mov   %r15,%rsi
0x000000000049305d <+461>: mov   %r15,%rdi
0x0000000000493060 <+464>: callq  0x494240 <mpihelp_add_n>

337                        if( cy )
0x0000000000493065 <+469>: add    0x10(%rsp),%rax
0x000000000049306a <+474>: je     0x4930b0 <mpih_sqr_n+544>

338                          mpihelp_add_1(prodp + hsize + size, prodp + hsize + size,339, hsize, cy);
340
341                        MPN_COPY(prodp, tspace, hsize);
0x00000000004930b0 <+544>: xor    %eax,%eax
0x00000000004930b2 <+546>: test   %r13d,%r13d
0x00000000004930b5 <+549>: jle    0x4930d1 <mpih_sqr_n+577>
```



KWANGWOON UNIVERSITY

# Flush+Reload 를 활용한 RSA 복호키 추출 공격

- Flush+Reload attack on GnuPG 1.4.13

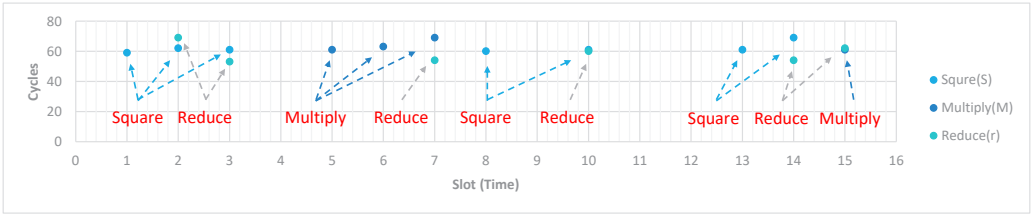
<RSA decryption (Victim VM)>

```
victim@guest1:$ gpg –d ciphertext.gpg
gpg: encrypted with 2048-bit RSA key, ID 7E2BFBC6, created 2016-11-14
```

<Flush+Reload attack (Spy VM)>

```
attacker@guest2:$ spy mygpg.conf
Mapped at 0xf7142000
|S|Sr|Sr||M|M|rM|S||Sr|||S|Sr|rM|||Sr|||rM|||Sr|||Sr|||M||||Sr|||Sr|||rM|||Sr|||Sr|||Sr
...
```

S:Square, M:Multiply, r:Reduce






KWANGWOON UNIVERSITY

# Curve25519 타원곡선 암호 공격

- Flush+Reload attack on ECDH with Curve25519 in Libgcrypt 1.7.6

**Input:** A positive scalar $k$ and an elliptic-curve point P, where $k = \sum_{i=0}^{n-1} 2^i \cdot k_i$ and $k_i \in \{0, 1\}$ for all $i = 0, \cdots, n-1$.
**Output:** $[k]$P.

```
procedure MONTGOMERY_LADDER(k, P)
    R0 ← G1          ▷ G1 represents the order-1 identity element
    R1 ← P
    dif_x ← P.x
    for i ← n − 1 to 0 do
        b ← k_i
        Q0, Q1 ← CONDITIONAL_SWAP(R0, R1, b)
                                ▷ Constant time swap when b = 1
        S0, S1 ← MONTGOMERY_STEP(Q0, Q1, dif_x)
                                ▷ S0 = [2]Q0, S1 = Q0 + Q1
        R0, R1 ← CONDITIONAL_SWAP(S0, S1, b)
                                ▷ Constant time swap when b = 1
    return R0
```

그림 출처: Genkin et al., CCS' 17



KWANGWOON UNIVERSITY

# Curve25519 타원곡선 암호 공격

- Flush+Reload attack on ECDH with Curve25519 in Libgcrypt 1.7.6

Trace (excluding four first bits) of scalar-by-point multiplication of a secret key with an element of order 4.

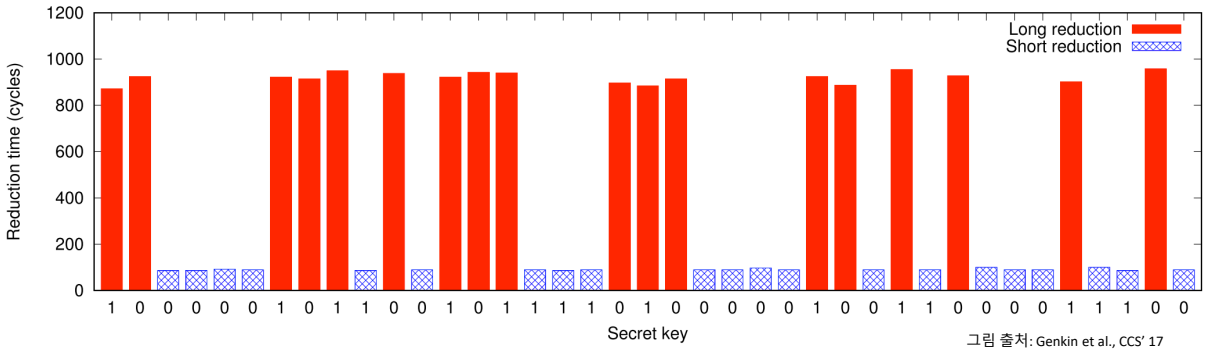



그림 출처: Genkin et al., CCS' 17



KWANGWOON UNIVERSITY

# 기타 암호 알고리즘 대상 최근 공격 기술 연구 결과

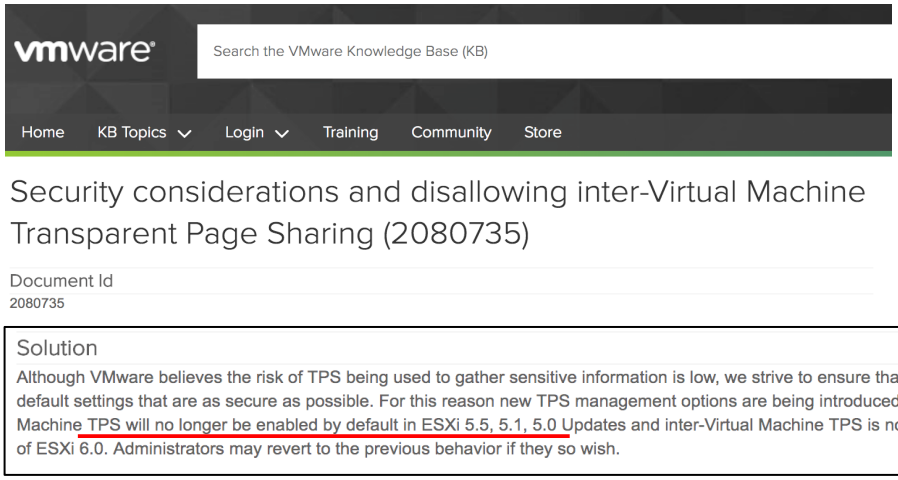
- *To BLISS-B or not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures* (CCS'17)
- *Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing Against strongSwan and Electromagnetic Emanations in Microcontrollers* (CCS'17)
- *Sliding right into disaster: Left-to-right sliding windows leak* (CHES'17)
- *CacheBleed : A Timing Attack on OpenSSL Constant Time RSA* (J. Cryptographic Engineering, 2017)



KWANGWOON UNIVERSITY

# 대응방안: 취약 소프트웨어 패치

- 메모리 중복제거 비활성화 (VMware)




메모리 중복제거를 활용하지 않는 부채널 공격 (Prime+Probe 등) 에 여전히 취약



# 대응방안: 취약 소프트웨어 패치

- 부채널 공격에 안전한 알고리즘 구현

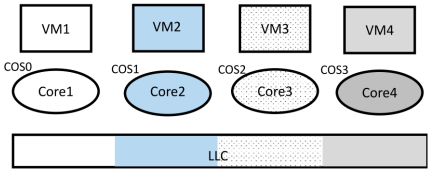
```
1  function modpow (a, b);
   Input  : base b, modulus N, secret
            E = (e_{k-1}, ..., e_1, e_0)
   Output: b^E mod N
2  R_0 = 1; R_1 = b;
3  for i = k − 1 downto 0 do
4      if e_i==0 then
5          R_1 = R_0 * R_1 mod N;
6          R_0 = R_0 * R_0 mod N;
7      end
8      else
9          R_0 = R_0 * R_1 mod N;
10         R_1 = R_1 * R_1 mod N;
11     end
12 end
13 return R_0;
```

```
1  function modpow (a, b);
   Input  : base b, modulus N, secret
            E = (e_{k-1}, ..., e_1, e_0)
   Output: b^E mod N
2  R[0] = 1; R[1] = b;
3  for i = k − 1 downto 0 do
4      R[0] * e_i + R[1] * ê_i = R[0] * R[1] mod N;
5      R[1] * e_i + R[0] * ê_i =
         R[1] * R[1] * e_i + R[0] * R[0] * ê_i mod N;
6  end
7  return R[0];
```

- 구현 복잡성 증가로 인해 여전히 새로운 공격에 노출 (CCS'16, CCS'17)
- 구현에 대한 안전성 검증 방법 부재

# 대응방안: 공유 자원의 격리

- Hardware level isolation
  - Cache partitioning using Intel Cache Allocation Technology (CAT)
    - Provides software control to isolate LLC access between VMs




- System level isolation
  - Allocates a private page with dedicated cache sets
  - Limits memory deduplication by copy-on-access mechanism

- 사용자간 workload 차이를 고려하지 않은 자원 격리로 인한 효율성 저하
- 플랫폼 종속 문제 (CPU, 운영체제, 하이퍼바이저 등)



# 대응방안: 시간 측정 잡음 주입

- On-demand time blurring
  - Add some noise to time source
  - Time stamp counter
    - x86 rdtsc, rtdscp instruction

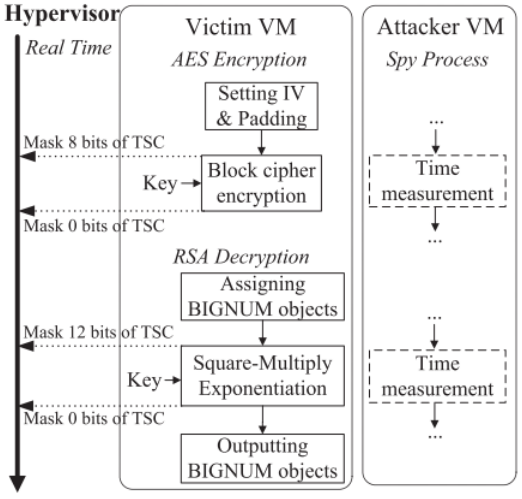



그림 출처: Liu et al., ESORICS'17

TSC 를 대신하여 높은 해상도의 시간 측정 방법 존재 (예: counting instructions)

# 대응방안: 실시간 캐시 부채널 공격 탐지

- Uses hardware performance counters (HPC)
- Detect abnormal behavior by monitoring some performance events (e.g., LLC cache accesses)

```
$ perf stat  make -j

Performance counter stats for 'make -j':

8117.370256  task clock ticks
       678  context switches
       133  CPU migrations
    235724  pagefaults
24821162526  CPU cycles
18687303457  instructions
 172158895  cache references
  27075259  cache misses

Wall-clock time elapsed:   719.554352 msecs
```

Sample output of the perf-stat utility

High cost!

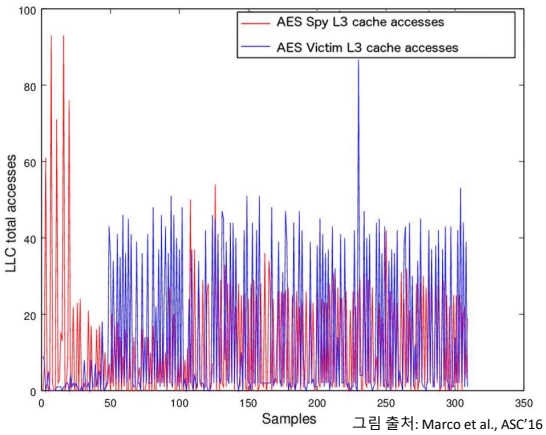



그림 출처: Marco et al., ASC'16

Total L3 accesses of the spy and victim of the attack to AES



KWANGWOON UNIVERSITY

# 마무리

- 클라우드 환경에서의 캐시 부채널 공격 위협
  - 사용자간 공유되는 CPU 캐시 (LLC) 의 상호 간섭에 기인
  - 암호키 복구가 가능한 수준의 높은 정밀도로 인해 심각한 위협이 되고 있음
- 캐시 부채널 보안 위협에 대한 현실성
  - Co-location 에 대한 실현 가능성 논란
  - 불특정 다수에 대한 공격 가능성은 이미 실증됨 (AWS EC2 공격사례, 2016)
- 보안 위협의 근본 원인
  - 단일 사용자를 고려하여 설계된 CPU 가 멀티 테넌트 환경에서 사용
- 근본적 문제 해결을 위해서는 CPU 구조에 대한 재설계 필요



KWANGWOON UNIVERSITY

# 감사합니다



KWANGWOON UNIVERSITY

The 24th Network Security Conference -Korea

# 다양한 클라우드 서비스를 활용한 보안 빅데이터 분석 시스템

**이경용** 국민대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2014 | University of Florida 컴퓨터공학 박사 |
| 2004 | 성균관대학교 전기전자컴퓨터공학부 학사 |
| 2016 ~ 현재 | 국민대학교 소프트웨어학부 조교수 |
| 2014 ~ 2016 | Amazon Web Services 소프트웨어 개발자 |
| 2012 ~ 2014 | HP Labs. 연구 인턴 |
| 2004 ~ 2008 | 삼성전자 디지털미디어 연구소 연구원 |

### 강연요약

나날이 증가하는 보안을 위협하는 공격을 탐지 및 방어하기 위해 다양한 기계학습 알고리즘 방법을 적용한 분석이 이루어지고 있다. 빠르게 증가하는 공격 정보를 저장하고 분석 작업을 수행하기 위해서는 많은 컴퓨팅 자원이 필요하게 되며, 공격 정보의 가변적 특성상 클라우드 컴퓨팅 서비스가 널리 활용된다.

본 발표에서는 클라우드 컴퓨팅 환경에서 보안 공격 빅데이터 시스템을 운용하는 방안에 대한 연구 결과를 경제적, 확장성 측면에서 발표한다. 현재 널리 활용되고 있는 IaaS를 활용한 분석 서비스를 바탕으로, 컨테이너 기술을 활용한 serverless 공격 탐지 시스템 구축을 통한 시스템의 확장성 확보 방안, 유휴 클라우드 컴퓨팅 자원을 활용한 경제적인 탐지 시스템 구축에 관련한 연구 결과를 발표한다. AWS를 활용한 데모 시스템 구축을 통해서 다양한 종류의 클라우드 컴퓨팅 서비스의 활용 방안에 대해서 선보인다.

# OPPORTUNITIES OF USING CLOUD SERVICES TO ANALYZE SECURITY BIG-DATA

KYUNGYONG LEE
COLLEGE OF COMPUTER SCIENCE
KOOKMIN UNIVERSITY

## DIVERSE CLOUD SERVICES

### Compute

- Over 70s of EC2 instances

### Storage

### Event processing

### Messaging

### Data analysis

### Development

**Compute**
EC2
Lightsail
Elastic Container Service
Lambda
Batch
Elastic Beanstalk

**Storage**
S3
EFS
Glacier
Storage Gateway

**Database**
RDS
DynamoDB
ElastiCache
Amazon Redshift

**Migration**
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
Snowball

**Networking & Content Delivery**
VPC
CloudFront
Route 53
API Gateway
Direct Connect

**Developer Tools**
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

**Management Tools**
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services

**Media Services**
Elastic Transcoder
Kinesis Video Streams
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor

**Machine Learning**
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate

**Analytics**
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue

**Security, Identity & Compliance**
IAM
Cognito
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
CloudHSM
Directory Service
WAF & Shield
Artifact

**Mobile Services**
Mobile Hub
AWS AppSync
Device Farm
Mobile Analytics

**AR & VR**
Amazon Sumerian

**Application Integration**
Step Functions
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

**Customer Engagement**
Amazon Connect
Pinpoint
Simple Email Service

**Business Productivity**
Alexa for Business
Amazon Chime
WorkDocs
WorkMail

**Desktop & App Streaming**
WorkSpaces
AppStream 2.0

**Internet Of Things**
IoT Core
IoT Device Management
IoT Analytics
Greengrass
Amazon FreeRTOS

**Game Development**
Amazon GameLift

# OPPORTUNISTIC RESOURCES IN CLOUD

## Major cloud service providers generally have a huge volume of infrastructures

### 2 Million Servers

Amazon has 11 cloud regions across the world, said James Hamilton, an Amazon distinguished engineer, during a presentation at re:Invent. Each region has multiple sets of data centers, and there are 28 total sets across the world. Each of those has one or more data centers, with a typical facility containing 50,000 to 80,000 servers. A conservative estimate puts Amazon over 1.5 million servers globally. Lydia Leong, an analyst at research firm Gartner, puts it at 2 million or more.

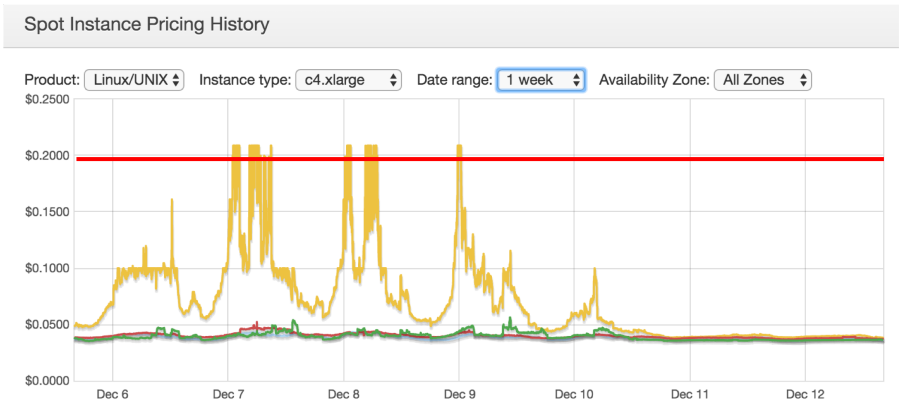
**AWS as of 2014**

## As of April. 2018, there are 36 availability zones

# OPPORTUNISTIC CLOUD COMPUTING RESOURCES

## Spot instance

- Providing surplus of cloud computing resources (compute) resources at a cheaper price (10 ~ 20% of on-demand instance price)




Spot instance price history of c4.xlarge
On-demand instance price: $0.21/hour

# CHALLENGES IN USING CLOUD SERVICES

## Difficult to find proper services to meet needs

- Might end up doing from scratch

## Difficult to find a cheaper solution

- Spot instance can be up to 90% cheaper

## How to improve monetary and time efficiency

- Using diverse cloud services (EC2, Batch, Lambda, …)
- Using spot instances
- Case study of running security analysis workloads

# DEEP LEARNING ON CLOUD

## DeepLearning

- Wide range of applications in speech recognition, image processing, autonomous driving, malware analysis, …

## Monetary limitation

- Hardware purchase and compute cluster build
- Cloud computing service is not cheap
- AWS GPU instance (g2.2xlarge) – $0.65/hour

## GPU spot instance for economical computation

## How much cost gain can we get?

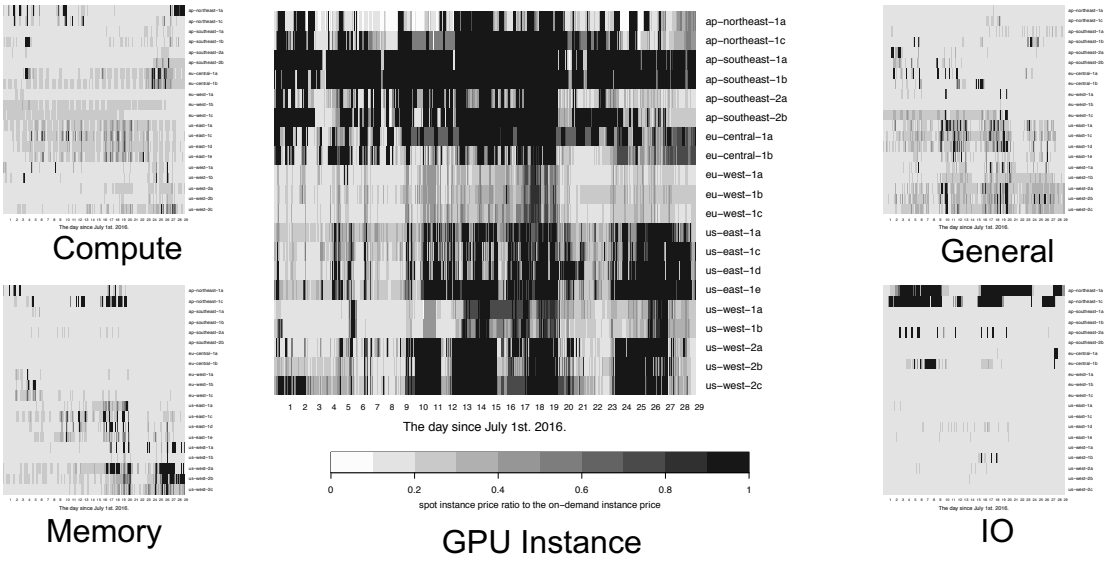
- In general, people expect using GPU spot instance results in the similar degree of cost gains with other types of instances, such as Compute, Memory, IO, etc.

IEEE Cloud 2017

# GPU SPOT INSTANCE PRICE DIVERSITY

## Spot instance price analysis

- Normalized spot instance price to that of on-demand instance
- Heatmap: darker region indicates the spot price is closer to on-demand instance price - temporal (x-axis) and spatial(y-axis)




# UNIQUENESS OF GPU SPOT INSTANCE

## Temporal price diversity

- Price fluctuation in the same region and different time
- About 35% of time, GPU spot instance presents higher price than on-demand instance. Other instance types show less than 5% of time.

## Spatial price diversity

- Price fluctuation in the same time and different AZs
- Standard deviation of spot instance price – GPU spot instance more than twice times of s.d.

## Hardware configurations

- GPU instance should be equipped with GPU devices
- Users might have different usage pattern (interactive or batch)

# IMPROVING COST GAIN IN USING GPU SPOT INSTANCES

## DeepSpotCloud

- Using GPU spot instances across regions in a global-scale to run DeepLearning tasks

## Challenges

- Handling unexpected service interruption
- Deploying existing deep learning systems on cloud

## Real-time task migration in a global-scale

- **How** to make task migration
- **Where** to migrate/start a instance
- **When** to make task migration

# HOW TO MAKE TASK MIGRATION IN A GLOBAL SCALE

## Handling unexpected instance termination during task execution

- Hadoop: automatic re-execution of failed task, speculative execution
- Spark: RDD lineage
- Deep learning platforms (e.g., TensorFlow): check-pointing

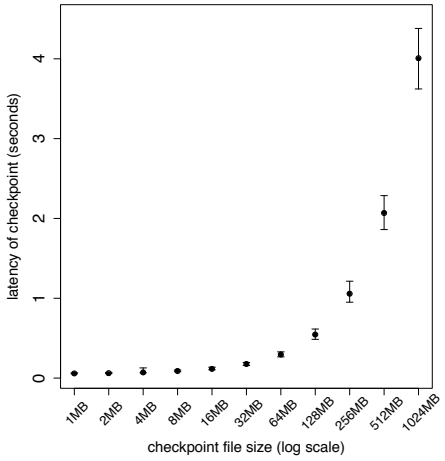
## Two minutes of grace period before forced shutdown

- Preparation for task migration
- Live task migration within two minutes in global scale is infeasible
- Store only intermediate weight vectors to a permanent storage (check-pointing)

# FEASIBILITY OF CHECK-POINTING IN A GLOBAL SCALE

## Use checkpointing feature of existing deep learning platforms

- In TensorFlow – tf.train.Saver class save() and restore()




Latency to complete checkpointing

| | | Destination | | | |
|---|---|---|---|---|---|
| | | US West | US East | Europe | Asia |
| Source | US West | 11.9(22.5) | 20.4(37.7) | 16.4(21.3) | 13.3(15.5) |
| | US East | 14.4(24.7) | 14.8(31.4) | 12.9(14.4) | 16.6(20.8) |
| | Europe | 18.1(24.7) | 24.1(37.9) | 10.0(10.8) | 22.3(24.8) |
| | Asia | 13.8(16.2) | 27.5(47.0) | 21.0(10.8) | 10.2(11.7) |

Latency to upload 1GB of checkpoint file in seconds – mean(maximum)

## Feasible to complete migration of 1GB checkpoint file

- Note the device memory size of g2.2xlarge (4GB)

# WHERE TO MAKE TASK MIGRATION

## Predicting an availability zone that is more likely to be cheaper and more stable

- Currently, it references the current price only

## Price of opportunistic resources becomes rather static

- AWS EC2 spot instance
- Google Pre-emptible VM
- Microsoft Azure low priority VM

# WHEN TO MAKE TASK MIGRATION

## Forced task migration

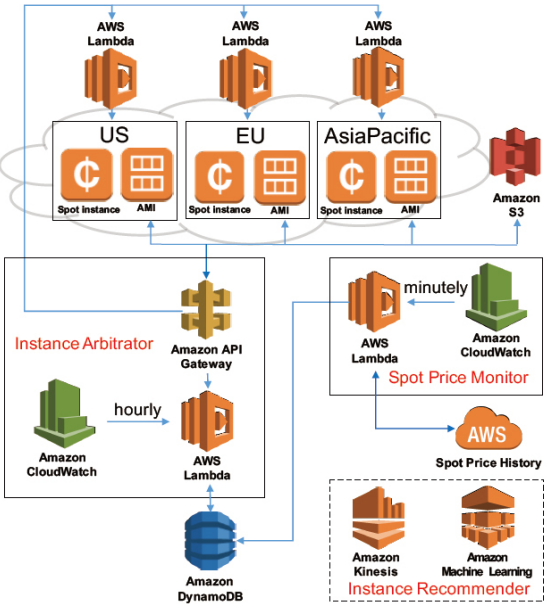
- In case of service interruption

## Voluntary task migration

- Look for a cheaper availability zone
- An active research topic

# DEEP SPOT CLOUD IMPLEMENTATION

## Implementation of DeepSpotCloud on AWS



# SERVERLESS SERVICE IMPLEMENTATION

## CloudWatch and Lambda

- Periodic price checker (cron job)

## API Gateway and Lambda

- HTTP server to get interrupt notification
- Invoke a new instance initiation

## S3

- Share file storage across continents

## DynamoDB

- A database

# PARALLEL BATCH PROCESSING OF INDEPENDENT TASKS

# USING BATCH CLOUD SERVICE FOR INDEPENDENT TASKS EXECUTION

# CLOUD BATCH SERVICE FOR MALWARE ANALYSIS

# THANKS!

## Contact me via


- leeky@kookmin.ac.kr
- http://leeky.me

The 24th Network Security Conference -Korea

# I'm listening to your location inferring user location with acoustic side channel

**윤지원** 고려대 교수

### 학력 및 경력사항

University of Cambridge 전자공학 박사 (통계신호처리전공)
University of Edinburgh 정보학 석사 (인공지능 및 생명통계)
성균관대학교 정보공학 학사
고려대학교 정보보호대학원/사이버국방학과 부교수
고려대학교 정보보호대학원 사이버보안학과 주임교수
IBM Research lab 정규 연구원
Trinity College Dublin 통계학과 강사 및 Research Fellow
University of Oxford, 로봇연구소 박사후연구원 (기계학습)

### 강연요약

Electrical network frequency (ENF) signals have common patterns that can be used as signatures for identifying recorded time and location of videos and sound. To enable cost–efficient, reliable and scalable location inference, we created a reference map of ENF signals representing hundreds of locations world wide — extracting real–world ENF signals from online multimedia streaming services (e.g., YouTube and Explore). Based on this reference map of ENF signals, we propose a novel side–channel attack that can identify the physical location of where a target video or sound was recorded or streamed from. Our attack does not require any expensive ENF signal receiver nor any software to be installed on a victim's device — all we need is the recorded video or sound files to perform the attack and they are collected from world wide web. The evaluation results show that our attack can infer the intra–grid location of the recorded audio files with an accuracy of 76% when those files are 5 minutes or longer. We also showed that our proposed attack works well even when video and audio data are processed within a certain distortion range with audio codecs used in real VoIP applications.

# I'm Listening to your Location! Inferring user location with acoustic side channel.

**교수 윤지원**
**(Email : jiwon_yoon@korea.ac.kr)**
고려대학교 사이버국방학과, 정보보호대학원
http://signal.korea.ac.kr

고려대학교 KOREA UNIVERSITY

## Source from Today's topic (1)

CIKM 2017 SINGAPORE

### Construction of a National Scale ENF Map using Online Multimedia Data

Hyunsoo Kim, Youngbae Jeon, and Ji Won Yoon
Center for Information Security Technologies (CIST)
Korea University
Republic of Korea
{aitch25,jyb9443,jiwon_yoon}@korea.ac.kr

**ABSTRACT**

The frequency of power distribution networks in a power grid is called electrical network frequency (ENF). Because it provides the spatio-temporal changes of the power grid in a particular location, ENF is used in many application domains including the prediction of grid instability and blackouts, detection of system breakup, and even digital forensics. In order to build high performing applications and systems, it is necessary to capture a large-scale nationwide or worldwide ENF map. Consequently, many studies have been conducted on the distribution of specialized physical devices that capture the ENF signals. However, this approach is not practical because it requires significant effort from design to setup, moreover, it has a limitation in its efficiency to monitor and stably retain the collection equipment distributed throughout the world. Furthermore, this approach requires a significant budget.

In this paper, we proposed a novel approach to constructing the worldwide ENF map by analyzing streaming data obtained by online multimedia services, such as "Youtube", "Earthcam", and "Ustream" instead of expensive specialized hardware. However, extracting

**ACM Reference format:**
Hyunsoo Kim, Youngbae Jeon, and Ji Won Yoon. 2017. Construction of a National Scale ENF Map using Online Multimedia Data. In *Proceedings of CIKM'17, November 6–10, 2017, Singapore.*, , 10 pages.
DOI: https://doi.org/10.1145/3132847.3132982

**1 INTRODUCTION**

The supply frequency of electrical power in distribution networks is called electrical network frequency (ENF). The signal is captured in a particular frequency, either $50Hz$ or $60Hz$, depending on the geographic location. This ENF has temporal fluctuation as the load in the power grid can vary in a time series. Therefore, ENF signals are often used as a spatio-temporal pattern for identifying both location and time.

This electrical pattern would be an important factor in the analysis of power system. ENF is oscillated by the influence of societal events, disaster, and electrical disturbances. With regard to this phenomenon, [5] deals with impacts of societal events on the power system. They explained how the electrical signal oscillates when


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Source from Today's topic (2)

UNIVERSITÉ DE LYON THE WEB CONFERENCE

WWW 2018

**I'm Listening to your Location!**
**Inferring User Location with Acoustic Side Channels***

Anonymous Author(s)

ABSTRACT

Electrical network frequency (ENF) signals have common patterns that can be used as signatures for identifying recorded time and location of videos and sound. To enable cost-efficient, reliable and scalable location inference, we created a reference map of ENF signals representing hundreds of locations world wide – extracting real-world ENF signals from online multimedia streaming services (e.g., YouTube and Explore). Based on this reference map of ENF signals, we propose a novel side-channel attack that can identify the physical location of where a target video or sound was recorded or streamed from. Our attack does not require any expensive ENF signal receiver nor any software to be installed on a victim's device – all we need is the recorded video or sound files to perform the attack and they are collected from world wide web. The evaluation results show that our attack can infer the intra-grid location of the recorded audio files with an accuracy of 76% when those files are 5

Such VoIP applications or streaming services, however, may raise privacy concerns. As for VoIP applications, some users, e.g., those engaged in secretive meetings, anonymous reporting or those doing a secret chat in general, have to not only anonymize their identities but also their locations even when they do not perceive the location privacy threat because they are not intentionally sharing their locations. Several previous studies [3, 17] demonstrated that location information can reveal sensitive information about users. Therefore, some services already tried to anonymize or obfuscate a user's actual location. For example, Skype, which is one of the most widely used VoIP applications, recently updated its default application settings to use a proxy server to hide users' IP addresses [32].

Location privacy issues are also prevalent in streaming services. The safety of those broadcasting and hosting live shows at homes may be threatened because stalkers or potentially inappropriate fans could locate their victims, and make physical visits to the vic-

e, most streaming services might conceal
' (or broadcasters') IP addresses but also
information about them. Popular stream-
lready use an anonymity policy to hide
for their privacy [47].

ave presented various ways of compro-
owerSpy [38], for instance, is a technique
ne's location with the only measurement
onsumption of the phone. Furthermore,
oid mobile phone [39], it can also be in-
sors like gyroscope, accelerometer and
quiring any permission.

e a novel side-channel attack for compro-
on a "*Location Inference using SignaTures*
*et work frequencies*" (LISTEN) technique.
, 39, 53] that requires the installation of
cation on a victim's device, the LISTEN
vith popular VoIP applications or online
re already being used. In fact, the only
he attack is a target multimedia file.
EN attack, an attacker collects electrical

▼ I'm Listening to your Location! Inferring User Location with Acoustic Side Channel

**Authors**: Youngbae Jeon, Minchul Kim, Hyunsoo Kim, Hyoungshick Kim, Jun Ho Huh and Ji Won Yoon

**Keywords**: Electrical network frequency, Location tracking, Side channel analysis

**Abstract**:

Electrical network frequency (ENF) signals have common patterns that can be used as signatures for identifying recorded time and location of videos and sound. To enable cost-efficient, reliable and scalable location inference, we created a reference map of ENF signals representing hundreds of locations world wide — extracting real-world ENF signals from online multimedia streaming services (e.g., YouTube and Explore). Based on this reference map of ENF signals, we propose a novel side-channel attack that can identify the physical location of where a target video or sound was recorded or streamed from. Our attack does not require any expensive ENF signal receiver nor any software to be installed on a victim's device — all we need is the recorded video or sound files to perform the attack and they are collected from world wide web. The evaluation results show that our attack can infer the intra-grid location of the

고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Blackout

출처: http://www.pbs.org/wgbh/americanexperience/films/blackout/

고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Monitoring the abnormity on power grid

- **Rapid Attack Detection, Isolation and Characterization Systems (RADICS)**

**DARPA fortifies early warning system for power-grid cyber assault**

DARPA taps BAE Systems to speed network development that will help restore grid after a malicious cyber attack

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# FNET/GridEye (경쟁기술)

고려대학교
정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

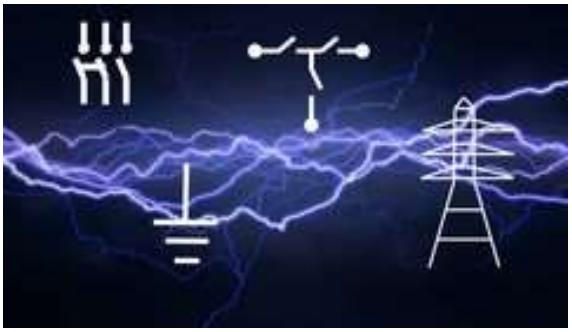
# Introduction - Background

- What is **Electrical Network Frequency** (ENF)?
  - ENF is an unique pattern of electricity from power grid
  - Electrical energy has an unique pattern in accordance with time and location, by the influence of demand-supply
  - We can capture these patterns by measuring the electricity
  - A simple way to capture these signals is monitoring electricity of the power plug

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Monitoring the abnormity on power grid



고려대학교
정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Installing physical FDRs

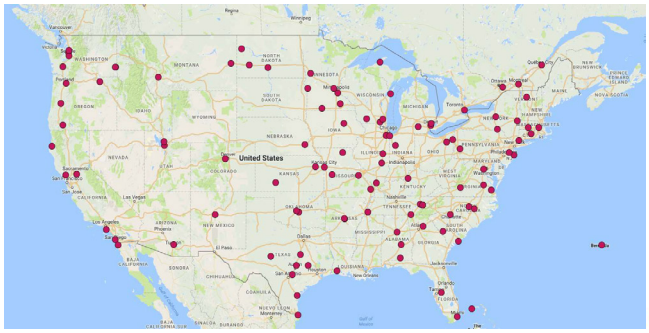
- Problem of previous collection method
  - Traditional method for collecting world-wide signals is difficult and expensive
    (for manufacture, installation, and maintenance)
  - Below device is FDR for collection of ENF (over $2,000 per device)
  - Fig ref: "Frequency Disturbance Recorder Design and Developments"

Fig. 5a. Second generation Frequency Disturbance Recorder

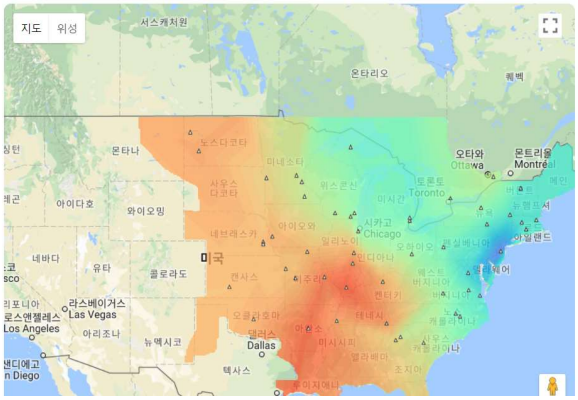

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# FNET/GridEye




출처: http://fnetpublic.utk.edu/

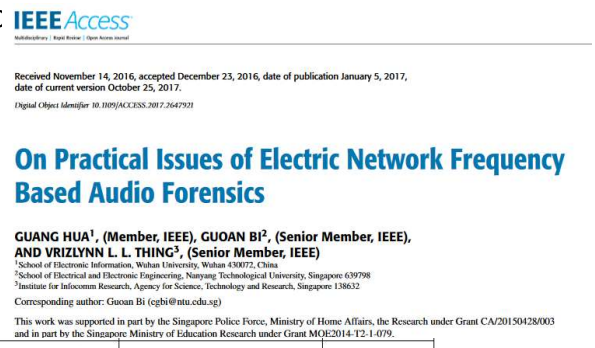



고려대학교
정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Introduction – Application of ENF

- Why are the ENF signals important?
  - ENF can be used in many application domains..
    - The prediction of grid instability and blackouts
    - Detection of system breakup
    - Societal events detection
    - Digital forensics
    - etc..


IEEE Access

Received November 14, 2016, accepted December 23, 2016, date of publication January 5, 2017, date of current version October 25, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2647921

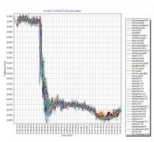
On Practical Issues of Electric Network Frequency Based Audio Forensics

GUANG HUA[1], (Member, IEEE), GUOAN BI[2], (Senior Member, IEEE), AND VRIZLYNN L. L. THING[3], (Senior Member, IEEE)

[1]School of Electronic Information, Wuhan University, Wuhan 430072, China
[2]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798
[3]Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore 138632

Corresponding author: Guoan Bi (egbi@ntu.edu.sg)

This work was supported in part by the Singapore Police Force, Ministry of Home Affairs, the Research under Grant CA/20150428/003 and in part by the Singapore Ministry of Education Research under Grant MOE2014-T2-1-079.

| | | | | |
|---|---|---|---|---|
| 4/27/2011 | Tornado Outbreak in Southeastern U.S. |  | | Movie |

quency (ENF), has become
wing much attention from
properties of ENF enable
ng detection. In this paper,
cal problems and facts that

THE UNIVERSITY of TENNESSEE UT
OAK RIDGE National Laboratory

고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Problems in FNET/GridEye

Frequency Color Scheme (Deviation from nominal value, Hz)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| [-0.09, -0.07) | [-0.07, -0.05) | [-0.05, -0.03) | [-0.03, -0.01) | [-0.01, 0.01) | [0.01, 0.03) | [0.03, 0.05) | [0.05, 0.07) | [0.07, 0.09) | [0.09, |

** The frequency values displayed here on the public website are fed from a set of sample data and do not represent the current system frequency.

| Eastern Interconnection | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| UTC Time | 07:35:20 | 07:35:16 | 07:35:12 | 07:35:08 | 07:35:04 | 07:35:00 | 07:34:56 | 07:34:52 | 07:34:48 | 07:34:44 |
| Unit #601 | 60.0215 | 60.0231 | 60.0243 | 60.0171 | 60.0250 | 60.0206 | 60.0249 | 60.0192 | 60.0279 | 60.0260 |
| Unit #620 | 60.0230 | 60.0212 | 60.0232 | 60.0254 | 60.0296 | 60.0231 | 60.0227 | 60.0187 | 60.0225 | 60.0238 |
| Unit #621 | 60.0229 | 60.0192 | 60.0258 | 60.0255 | 60.0164 | 60.0212 | 60.0188 | 60.0239 | 60.0248 | 60.0258 |
| Unit #623 | 60.0189 | 60.0195 | 60.0262 | 60.0141 | 60.0179 | 60.0243 | 60.0272 | 60.0260 | 60.0286 | 60.0252 |
| Unit #634 | 60.0267 | 60.0225 | 60.0216 | 60.0276 | 60.0234 | 60.0260 | 60.0233 | 60.0218 | 60.0222 | 60.0219 |
| Unit #640 | 60.0215 | 60.0192 | 60.0203 | 60.0165 | 60.0231 | 60.0263 | 60.0239 | 60.0238 | 60.0255 | 60.0251 |
| Unit #647 | 60.0196 | 60.0173 | 60.0246 | 60.0252 | 60.0250 | 60.0239 | 60.0175 | 60.0233 | 60.0203 | 60.0274 |
| Unit #664 | 60.0165 | 60.0243 | 60.0181 | 60.0196 | 60.0208 | 60.0267 | 60.0240 | 60.0272 | 60.0237 | 60.0257 |
| Unit #670 | 60.0244 | 60.0195 | 60.0241 | 60.0249 | 60.0254 | 60.0170 | 60.0204 | 60.0215 | 60.0233 | 60.0253 |
| Unit #671 | No Data | No Data | 60.0249 | No Data | 60.0238 | 60.0237 | 60.0210 | 60.0272 | No Data | 60.0306 |
| Unit #673 | 60.0233 | No Data | No Data | No Data | 60.0211 | No Data | No Data | No Data | 60.0248 | 60.0253 |
| Unit #674 | No Data | 60.0229 | No Data | No Data | No Data | No Data | 60.0255 | No Data | No Data | 60.0251 |
| Unit #682 | 60.0237 | 60.0253 | 60.0175 | 60.0240 | 60.0218 | 60.0268 | 60.0225 | 60.0247 | 60.0192 | 60.0256 |
| Unit #684 | 60.0241 | 60.0231 | 60.0260 | 60.0251 | 60.0237 | 60.0216 | 60.0268 | 60.0173 | 60.0192 | 60.0245 |

설치 비용, 고장난 센서들에 대한 지속적 관리 비용

고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

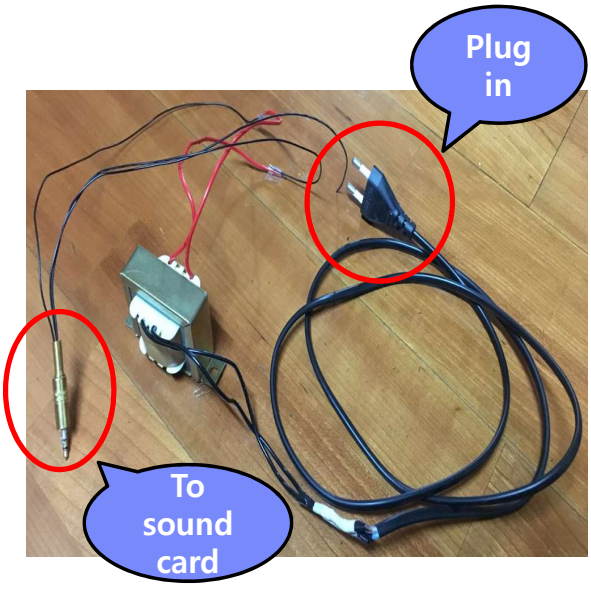
# 제안기술


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

## Introduction - Background

- Is there any other way to obtain **Electrical Network Frequency** (ENF)?

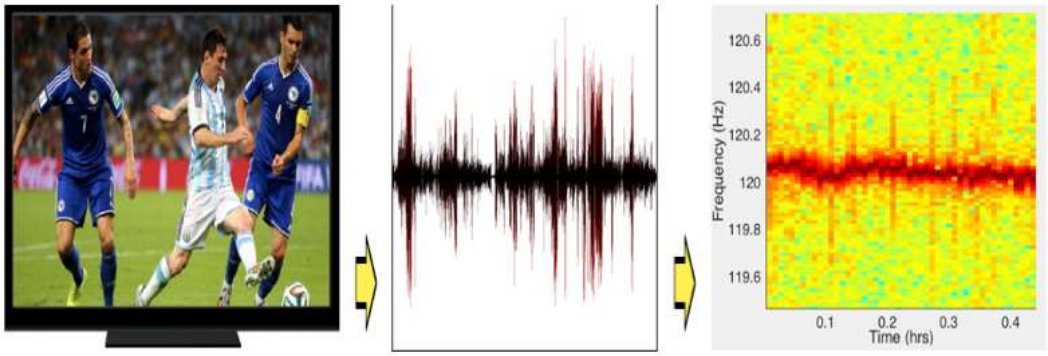



고려대학교 정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Introduction - Background

- ENF signals can be extracted from audio/video
  - When audio/video are being recorded, ENF signals are also being recorded together because of the electromagnetic influences from power line (wireless devices are not applicable)
  - ENF signals appear around 50Hz or 60Hz and its harmonics bands

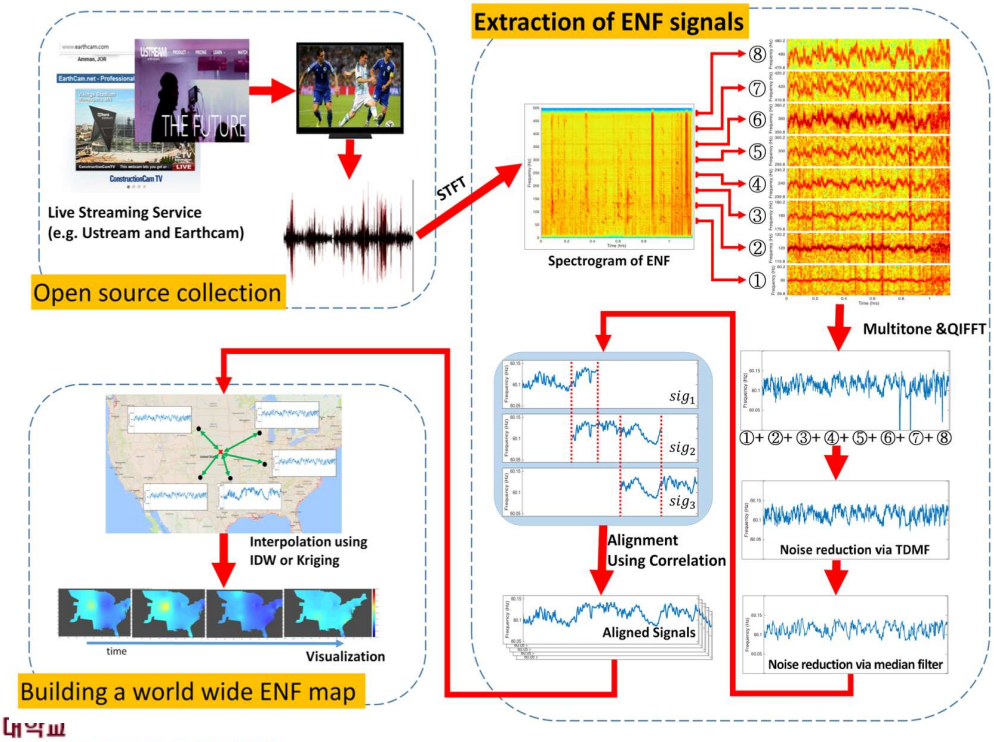



(a) Multimedia data (b) Extracted audio signals (c) ENF patterns in spectrogram


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# ENF Construction - Overview



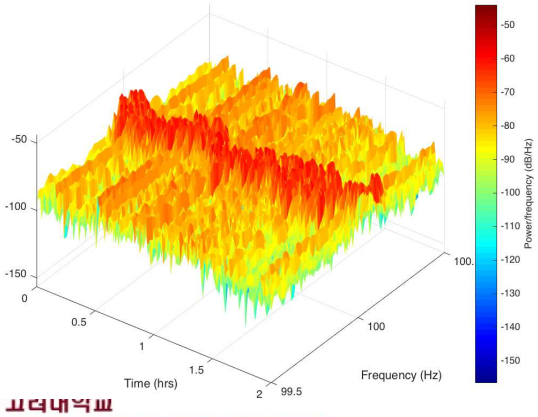


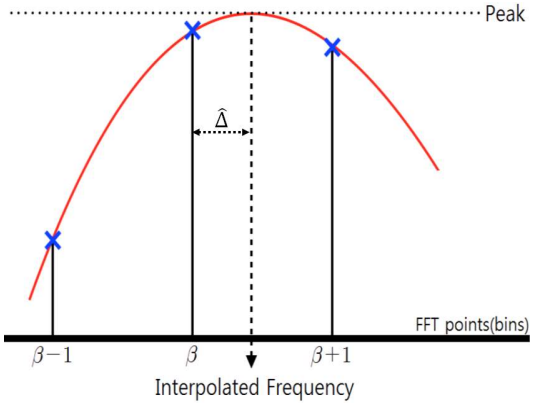
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# ENF Construction – Signal extraction

- Extraction of ENF signals from multimedia with QIFFT
  - QIFFT is one of the non-parametric methods for extracting signals from consecutive peaks of frequency domain data
  - Basic concept is similar to STFT, but it works more rapidly than STFT
  - It does not require large window size and overlap length for high resolution since it uses interpolated peak instead of calculation of accurate position of frequency peak



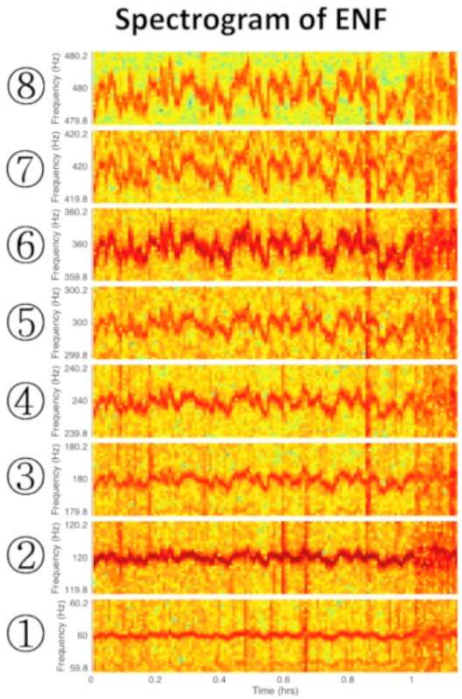


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# ENF Construction – Signal extraction

- Using harmonics information?
  - A harmonic is a signal or wave whose frequency is an integral (whole-number) multiple of the frequency of some reference signal or wave
  - For a signal whose fundamental frequency is f, the second harmonic has a frequency 2 f, the third harmonic has a frequency of 3 f, and so on
  - If the wave is not sinusoidal, it must include harmonics as shown in figure
  - We used these harmonics signals for noise removal and signal intensification



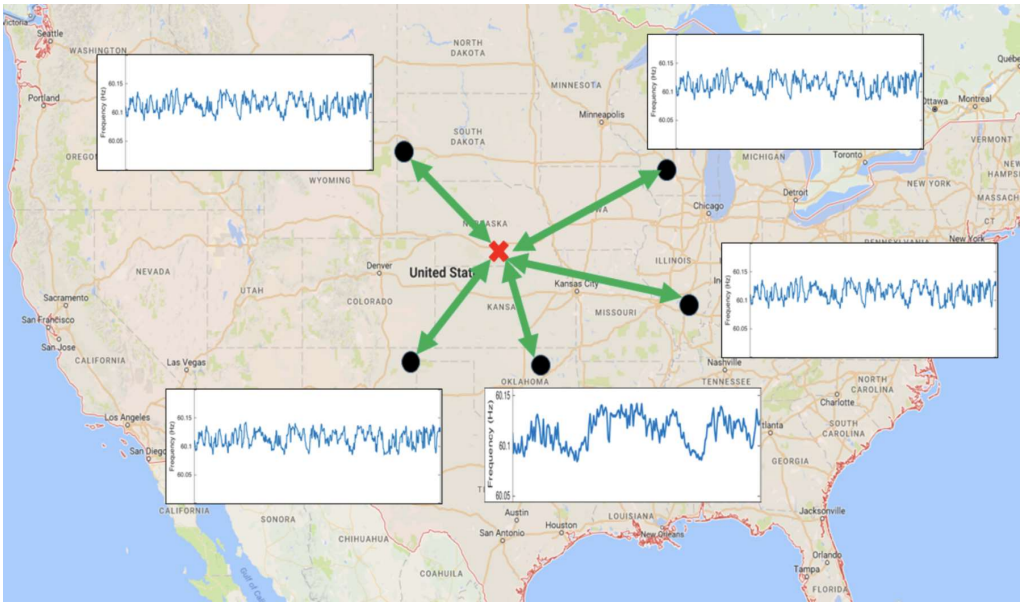


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# ENF Construction – Building ENF map…

- By calculating IDW for all ENF signals collected from same grid,



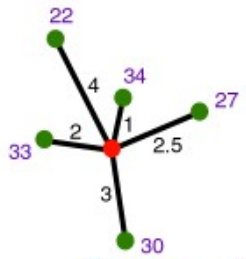


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

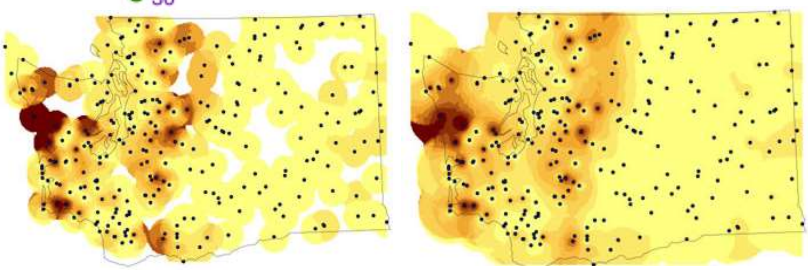
고려대학교 KOREA UNIVERSITY

# ENF Construction – Building ENF map…

- Then, we constructed large-scale ENF map using IDW interpolation
  - IDW (Inverse Distance Weighted) interpolation is a geometrical method
  - It is used for interpolation two-dimensional data to obtain signals from where we could not download multimedia




$$Z(x) = \frac{\sum w_i z_i}{\sum w_i} = \frac{\frac{34}{1^2} + \frac{33}{2^2} + \frac{27}{2.5^2} + \frac{30}{3^2} + \frac{22}{4^2}}{\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{2.5^2} + \frac{1}{3^2} + \frac{1}{4^2}} = 32.38$$

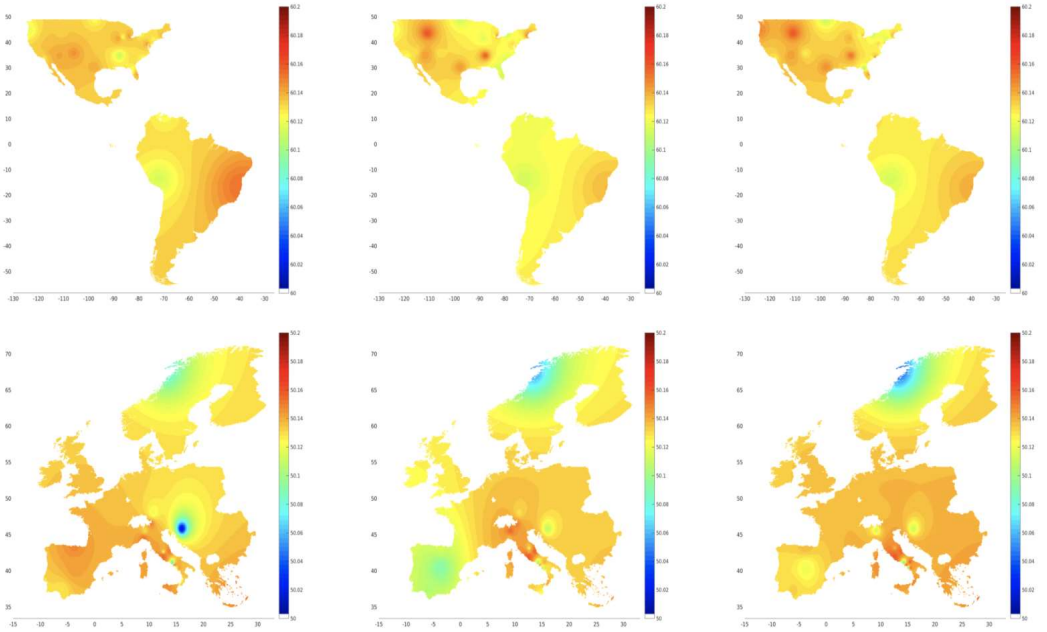


고려대학교
정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# ENF Construction – Building ENF map…

- We, finally, could obtain these world ENF map for geometry analysis




ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Application


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Introduction - Traditional Forensics

오사마 빈 라덴 (자료사진)

Location tracking using Image analysis

고려대학교
정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Introduction - Traditional Forensics

Location tracking using audio signals

https://www.youtube.com/watch?v=eBqEpGk_HGY

고려대학교
정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Introduction - Difficulty in traditional Forensics

오사마 빈 라덴 (자료사진)

Voice Phishing Attack Targeting Numerous Financial Institutions

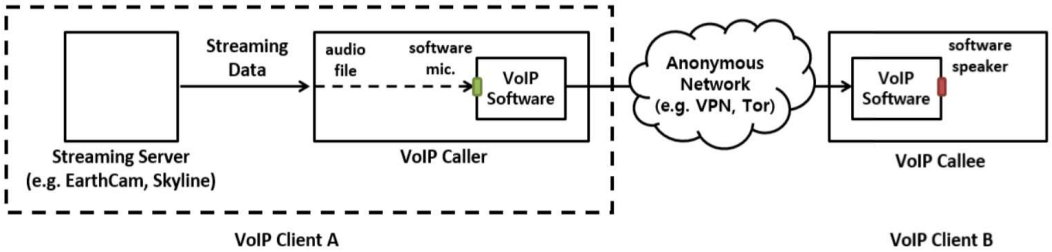
고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Inferring User Location – Estimation

- **Experimental setup:** To emulate VoIP client A (Caller) from a remote host,we first obtained the audio data from streaming servers and inputted the audio file directly to VoIP software.




- and speaker operations were processed with virtualization technique. By splitting the experiment into two parts - gathering audio files and actually running VoIP S/W, we can increase the re-producibility without losing details.

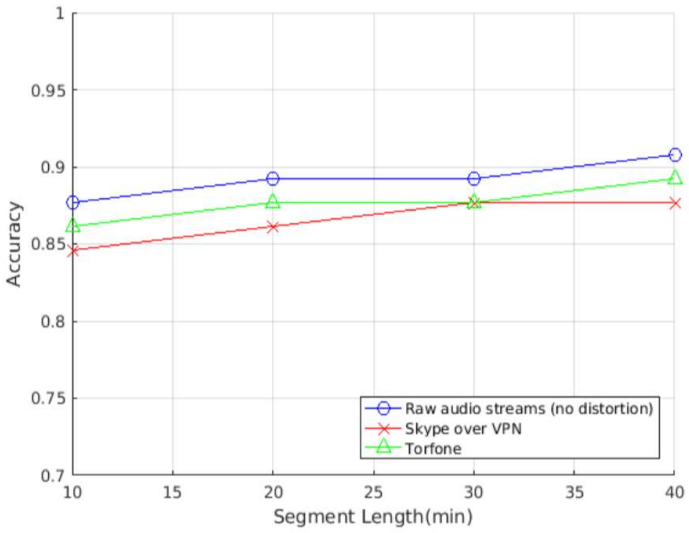
고려대학교 정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Inferring User Location – Estimation

- **Inter-grid Estimation**: Accuracy vs Segment length (min) for inter-grid estimation with 40-minutes segment length.





ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Inferring User Location – Estimation

- **Intra-grid Estimation**: Accuracy vs Segment length (min) for intra-grid estimation.

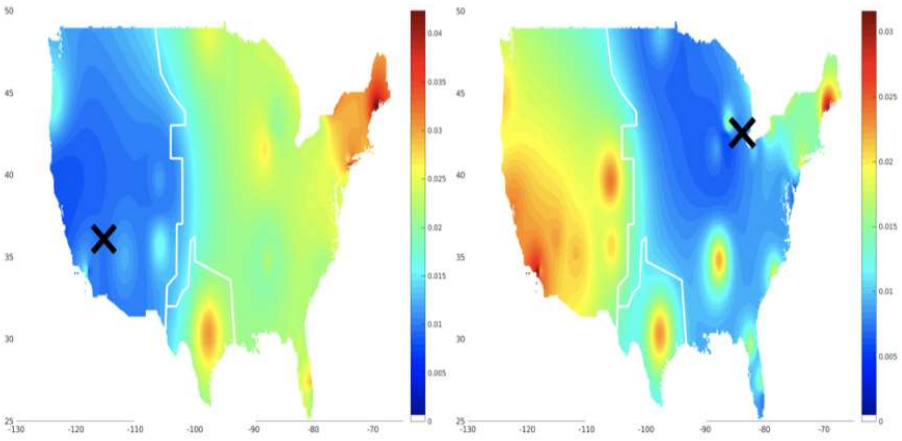
| Segment length (min) | Accuracy (%) | | |
|---|---|---|---|
| | Raw data | Torfone | Skype + VPN |
| 5 | 76.4 | 76.4 | 70.5 |
| 10 | 76.4 | 76.4 | 70.5 |
| 15 | 76.4 | 76.4 | 70.5 |
| 20 | 70.5 | 76.4 | 70.5 |
| 25 | 76.4 | 76.4 | 76.4 |
| 30 | 76.4 | 76.4 | 76.4 |
| 35 | 82.3 | 82.3 | 82.3 |
| 40 | 82.3 | 82.3 | 82.3 |

고려대학교 정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Applications

- With the collected data, we tried to check several applications are properly working
  - First application is estimating the time and the location using ENF signals
  - Through this examination, we could confirm that discovering the source location of multimedia is available

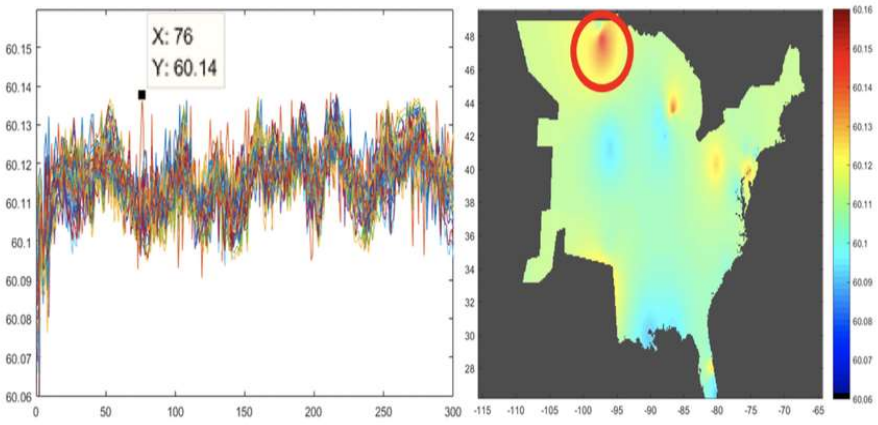



ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Applications

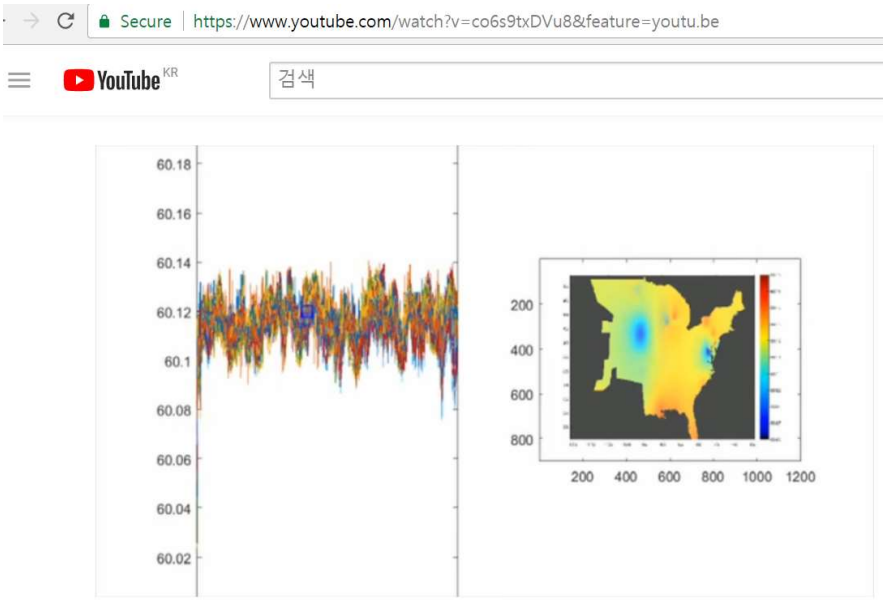
- With the collected data, we tried to check several applications are properly working
  - Second application is detection and prediction of abnormal events using a worldwide ENF map
  - It is not complete yet, but we checked the possibility of event detection




고려대학교
정보보호학부 · 정보보호대학원
ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Additional link




Demo video for CIKM 2017
미등록

https://youtu.be/co6s9txDVu8


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Conclusion

- ENF is a good signature to identify the location and time.
- This can be used to tackle the privacy.
- The ENF can be obtained from multimedia.


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# 해당 연구진행자들

김현수

전영배

김*철


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

# Center for Future Intelligence Studies (CFIS)

- 고려대학교 정보보호대학원/사이버국방학과에서 곧 "글로벌정보분석센터"를 개소할 예정입니다.
- 영문명: Center for Global Intelligence Studies (CGIS, "씨지스")

- 주제:
  - 국제정세를 파악
  - 테러나 마약거래 등의 국내외 범죄에 대한 분석
  - 사이버전 관련 동향 및 첩보 수집 및 분석
  - 해킹 등의 사이버범죄에 대한 정보분석 연구 및 공유

- 기술적인 부분에서부터 국제관계에 이르기까지 다양한 연구를 포함
- 학계 + 법집행기관(Law Enforcement Agency, LEA)와의 협력 모색

- 세부부서 (총 4개 부서)
  - Section 1: Open Source Intelligence
  - Section 2: Signal Intelligence
  - Section 3: Cyber Threat Intelligence
  - Section 4: Intelligence Analysis


ⓒ 2013 Center for Information Security Technology (CIST), Korea University

고려대학교 KOREA UNIVERSITY

고려대학교
정보보호학부 · 정보보호대학원

ⓒ 2013 Center for Information Security Technology (CIST), Korea University

The 24th Network Security Conference -Korea

# 이더넷 기반의 커넥티드 자동차 보안

**권혁찬** ETRI 책임

### 학력 및 경력사항

2001 충남대학교 컴퓨터과학과 이학박사

2001 ~ 한국전자통신연구원 정보보호연구본부 책임연구원/PL

### 강연요약

자동차, 교통 환경이 점차 자율주행, 지능형 교통시스템으로 발전하면서, 자동차는 점점 복잡화, 지능화되고 자동차 내/외부 연결성도 대폭 확대되고 있다.

이러한 자동차의 지능화 및 연결성 확대는 다양하고 보다 정밀한 자율주행 등의 서비스가 가능한 면이 있지만, 사이버 공격을 위한 벡터가 증가하여 보안 위협 역시 확대되는 문제가 있다.

본 발표에서는 오토모티브 이더넷을 포함하여 커넥티드 자동차의 특성 및 최신 트랜드를 살펴보고, 관련 보안 위협, 대응 기술 현황, 보안 이슈 등을 소개한다.

Netsec-KR 2018

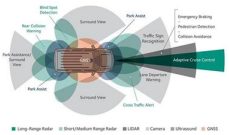
2018.4.13

# 이더넷 기반 커넥티드 자동차 보안

한국전자통신연구원 권혁찬 (hckwon@etri.re.kr)

## 개요

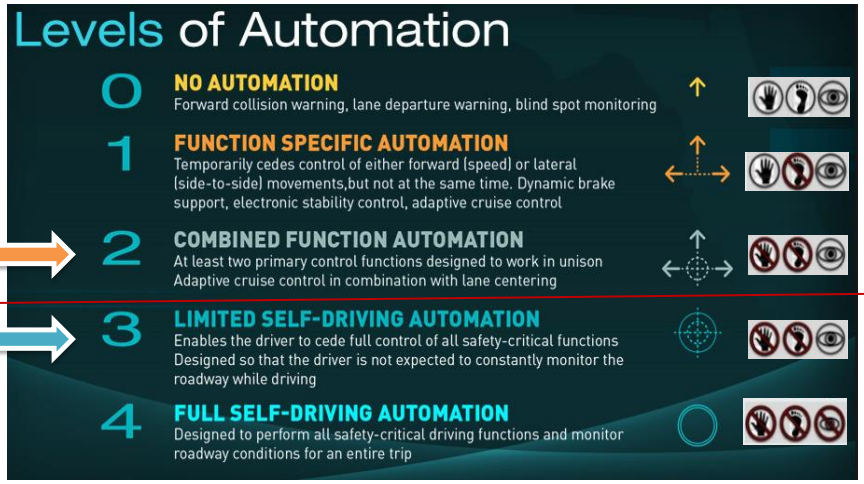
### NHTSA의 Levels of Automation



**Automated Driving**
Vision
Perception
Navigation

+

**Cooperative Driving**
V2V communication
V2I communication
Smart Environment




운전자 보조
자동차 기술 중심

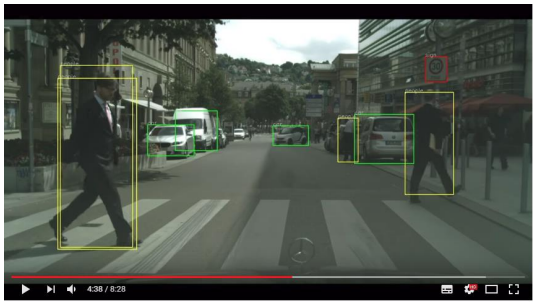
자동운전
자동차/인프라 연계
(자동차/ICT/ITS 융합)

ETRI

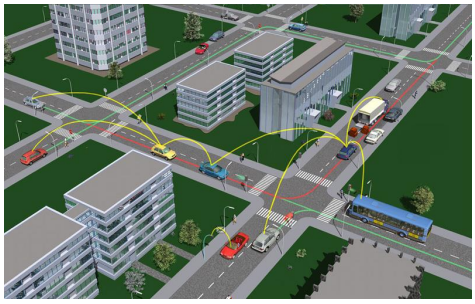
# 개요

## 자율주행을 위한 Core technology

| | |
|---|---|
| AI / SW | Sensor |
| Big Data / Cloud | V2X / IoT |




CES 2016: NVIDIA DRIVENet Demo - Visualizing a Self-Driving Future (part 5)



ETRI



# 개요

## 주요 표준화 기구

*International*

ISO International Organization for Standardization — TC22 WG (Road, Vehicle) → IVN, diagnostics, functional safety, extended vehicle
TC204 WG (Intelligent Transport Systems)

IEEE — WAVE 기반 V2X 통신 규격, 보안 (1609.x, 802.11p…)

3GPP A GLOBAL INITIATIVE — Cellular V2X (rel. 14 ~ )

ETSI World Class Standards — C-ITS (EU)

ITU International Telecommunication Union — Security framework, SOTA/FOTA…

*De-facto*

CAMP *Vehicle Safety Communications 3* — Mercedes-Benz, GM, TOYOTA, HONDA Honda R&D Americas, Ford, NISSAN, HYUNDAI-KIA MOTORS, VOLKSWAGEN — *Intelligent Transportation Systems*
Vehicular PKI, V2X 규격, 실증

GENIVI — Infotainment platform

AUTOMOTIVE GRADE LINUX

CAR 2 CAR COMMUNICATION CONSORTIUM — C-ITS, V2X, security

AUTOSAR — ECU middleware platform

*ETC*

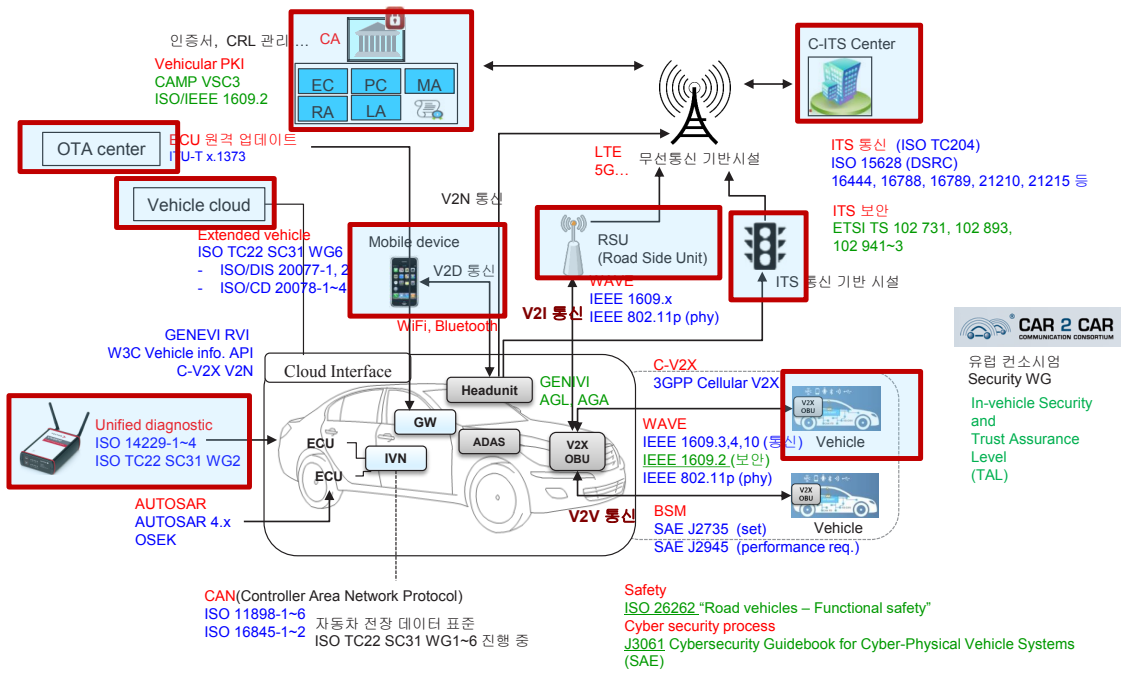
NHTSA NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

SAE INTERNATIONAL

ETRI

# 개요 - Trend

## 연결성의 확대






# 개요 - Trend

## 연결성의 확대 – V2X

### V2X (WAVE)

OBU

RSU

ITS 5.9 GHz

**WAVE 기반 V2X 통신 표준**

| 표준 | 용도 | 개요 |
|---|---|---|
| IEEE 802.11p | WAVE PHY, MAC | WAVE 물리계층과 MAC 계층을 정의 |
| IEEE 1609.2 | Security | WAVE 관리 및 메시지 보안 규격 |
| IEEE 1609.3 | Networking | WAVE 네트워크 및 전송 계층 규격 |
| IEEE 1609.4 | Multi-chan. Operation | WAVE MAC 계층의 멀티채널 오퍼레이션 규격 |
| IEEE 1609.12 | ID allocation | WAVE 서비스를 위한 ID 할당 규격 |
| SAE J2735 | DRSC message set | DSRC로 전송하는 메시지 set 정의 |
| SAE J2945 | DSRC performance requirement | DSRC 전송 메시지 성능 요구사항 |

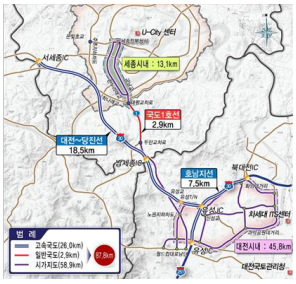
### V2X (Cellular)

3GPP release 14 ~

# 개요 - Trend

## 연결성의 확대 – 실증 테스트베드

**국내 – C-ITS, K-city…**

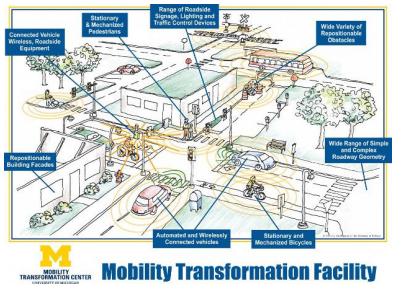



C-ITS 시범 도로(대전-세종 80km)
시범사업('14~16), 본 사업 ('17~ )

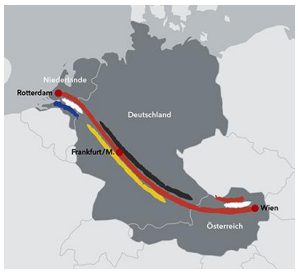
K-City (자율주행 시범도시, 화성)

**미국 – Mcity**

Ann Arbor, Mich.




**EU – C-ITS corridor**




**일본 – J-Town**

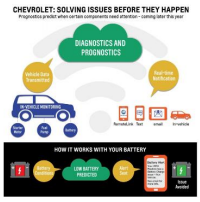
**중국 – Nice city**



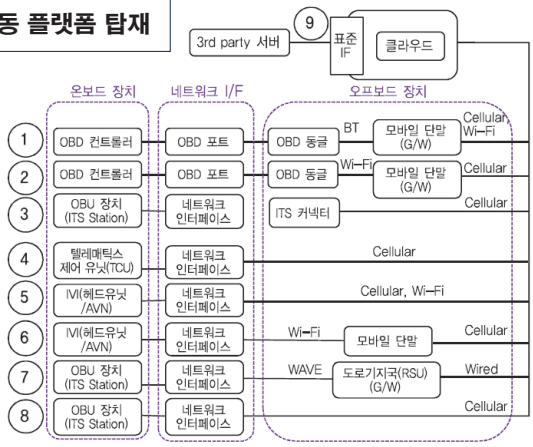
# 개요 - Trend

## 연결성의 확대 – 클라우드 연계

**Continental** → 클라우드 기반 차량 정보 분석/진단
**Bosch** → eCall을 차량 클라우드로 확장
**GM** → 클라우드 기반의 차량 부품 관리 서비스 (Prognostics)
**Benz** → 클라우드 기반 커넥티트카 서비스 me
**Toyota** → MS와 공동으로 도요다 커넥티드 플랫폼 발표
**Jaguar Land Rover** → 컨셉 EV카에 클라우드 연동 플랫폼 탑재




| 표준 | 개요 |
|---|---|
| ISO TC22 Extended vehicle | 원격진단 및 차량 클라우드 서비스 지원을 위한 인터페이스 표준 (SC31) |
| 3GPP V2N | 이동통신 기반 차량-클라우드간 통신 (V2Network) 서비스 표준 |
| GENEVI RVI | 클라우드 등 차량 외부 서비스에서 차량의 데이터에 접근하고 통신하기 위한 규격 (GENEVI alliance) *RVI: Remote Vehicle Interaction* |
| W3C vehicle information API | 외부에서 차량의 신호 및 데이터 속성에 접근하기 위한 Web API 표준화 |



# 개요 - Trend

## IVN 효율화 – automotive Ethernet

**OPEN**(One-pair Ethernet) Alliance → BroadR-Reach PHY, 100baseT, 1000baseT

IEEE, **AVB** (Audio Video Bridging) → IEEE 802.1AS, 802.Qat, 802.1Qav, 1722, 1722.1

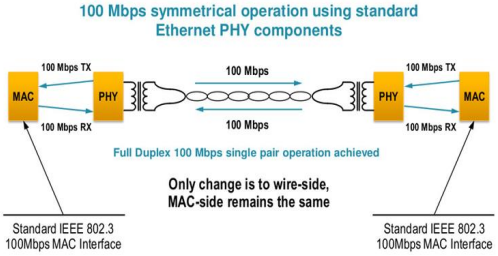
: 네트워크 기반의 Digital Audio 분배, 시간동기, 스트림 예약, 스케줄링

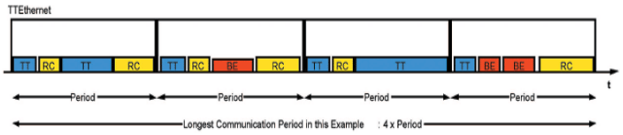
SAE, **TTEthernet** (Time-Triggered Ethernet) → SAE AS6802

: 사이클 기반의 TDMA 방식, 혼합 송신 (Time-triggered traffic, Rate-Controlled traffic, Best-Effort traffic)

IEEE 802.1 WG, **TSN** (Time Sensitive Networking)

→ IEEE TSN task group, 802.1as-REV, 802.1Qcc, 802.1Qbu, 802.1Qbv, 802.1cb, 802.1Qch, 802.1Qci



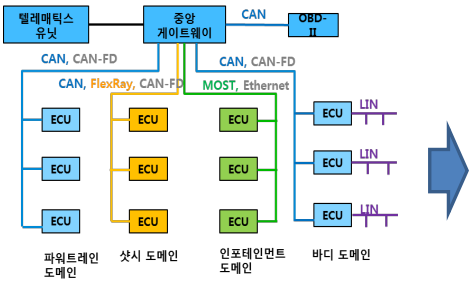



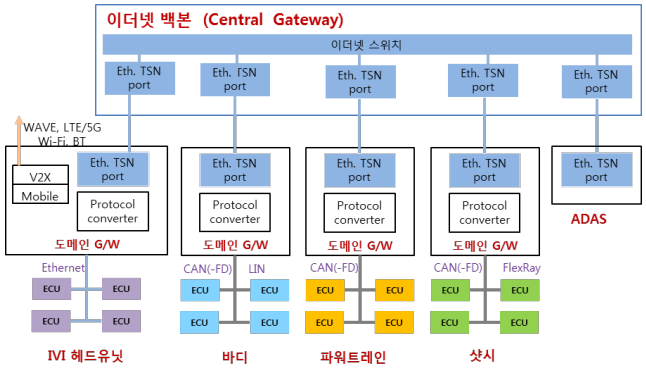

ETRI

16.10.13 | 9

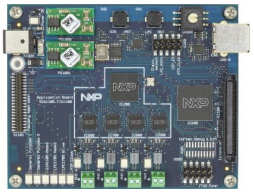
# 개요 – Trend

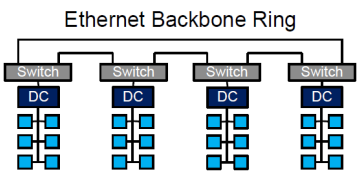
## IVN 효율화 – automotive Ethernet 도입

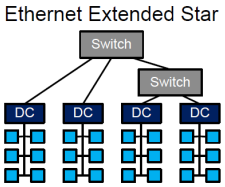



Some/IP, SD
DoIP






ETRI

16.10.13 | 10

# 보안 위협

## 사례

**Jeep Cherokee hack (2015)**
**C.Miller, C.Valasek**

**Mitsubishi outlander PHEV hack (2016)**
**Pen test partners**

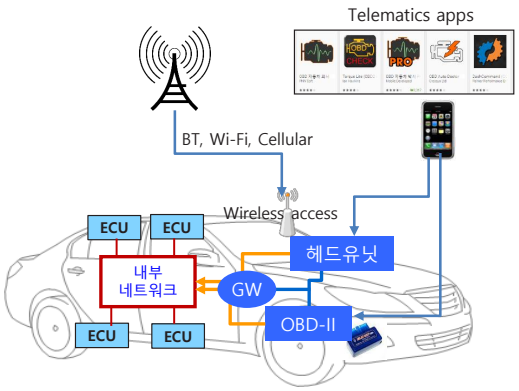
**Tesla Model S hack (2016, 2017)**
**Keen Security Lab. (Tencent)**

# 보안 위협

| 분류 | 보안 위협 |
|---|---|
| 전장 플랫폼 | - ECU 소프트웨어 결함, ECU 리버스 엔지니어링<br>- ECU 펌웨어 해킹 및 위/변조<br>- 위장 ECU 장착<br>- IVI(in-Vehicle Infotainment) 해킹, 악성 감염<br>- 스마트 센서 물리 공격 (블라인딩, 스푸핑, 재밍) |
| 내부 네트워크 | - 차량 내부네트워크에 악의적인 제어 메시지 주입<br>- 정상적인 내부네트워크 방해 (패킷 삽입, 삭제, 임의조작, 지연 등)<br>- 도청, DoS, 리플레이, 스푸핑, 패킷 폐기 공격 |
| 외부 네트워크 | - 무선 통신망 해킹, DoS 공격<br>- 위장 OBU(Onboard Unit), RSU(Road Side Unit)<br>- 악의적인 차량(Misbehavior Vehicle)<br>- 거짓 정보 (Fake message) 제공<br>- 차량 접속 기기 해킹 |
| 관리, 진단 | - 프라이버시 침해, OBD-II 해킹<br>- 원격 업데이트 및 진단 프로토콜 해킹<br>- 해킹에 의한 사고원인 분석/증거 보존의 어려움 |

# 보안 위협

- **Types of Attack**
  - **Injection of malicious control commands**
  - **Prevention of correct system function (insertion, deletion, manipulation, replay and delay of messages)**
- **Points of attack**
  - **Additional nodes (e.g. via OBD connector or wireless access)**
  - **Corrupted and misused existing nodes (e.g. root access to infotainment system via cellular network)**
  - **Nodes replaces by manipulated ones**




**출처** : Secure Ethernet communication for Autonomous Driving, Elektrobit, 2015



# 보안 위협

## V2X security threats

# 보안 기술 현황

## 주요 자동차 보안 기술

| 분류 | 보안 기술 |
|---|---|
| 전장 플랫폼 보안 | 시큐어 부트, 시큐어 플래싱, 접근제어<br>애플리케이션 샌드박스, 플랫폼 가상화<br>HSM(hardware security module)<br>부채널 방지<br>Autosar CSM(Cryptographic Security Manager), SecOC(Secure Onboard Communication) |
| 내부 네트워크 보안 | 침입 탐지 시스템 (IDS), 차량용 방화벽(F/W)<br>침입 방지 시스템(IPS)<br>ECU 인증, 키관리, 암호화<br>위협탐지 (rule-based, machine learning-based) |
| 외부 네트워크 보안 | V2X 메시지 인증, 암호화<br>차량 PKI, V2X 메시지 서명 (고속) 검증<br>IEEE 1609.2, CAMP VSC3 |
| 보안 관리, 진단 | 보안 모니터링, 보안 취약성 분석<br>차량 이상징후, 비정상 행위 분석<br>원격 SW/FW 보안 업데이트<br>J2735 기반 보안성 평가<br>포렌식 및 사고 원인 분석 기술 |

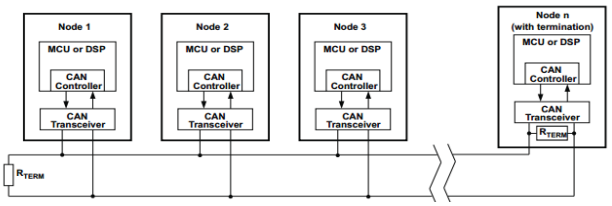


# 보안 기술 현황

## 주요 기술

### Intrusion Detection

- Location sensor
- Range sensor
- Frequency sensor
- Correlation sensor
- Protocol sensor
- Plausibility sensor
- Consistency sensor

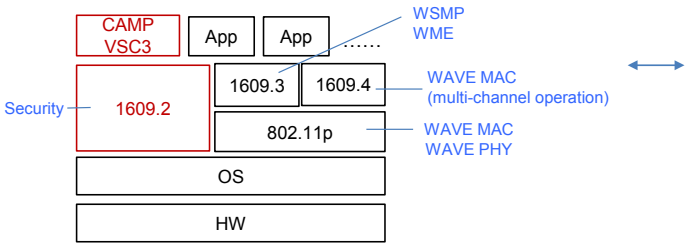



- Broadcast
- No Encryption/Authentication
- Weal Access control
- 8byte packet

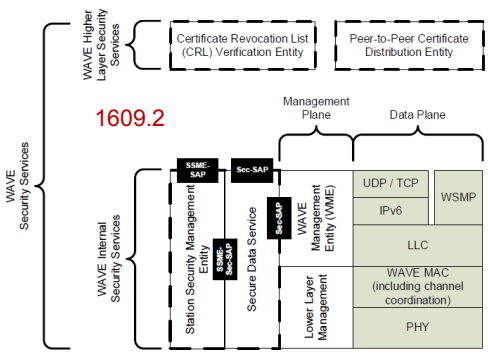
# 보안 기술 현황

## V2X 보안 – IEEE1609.2, CAMP

기타: IEEE 1609.1(resource management), 1609.12
SAE J2735(BSM set), J2945



A Security Credential Management System for Vehicle-to-Vehicle Communications



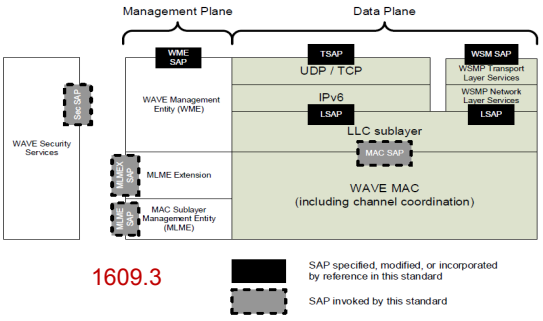
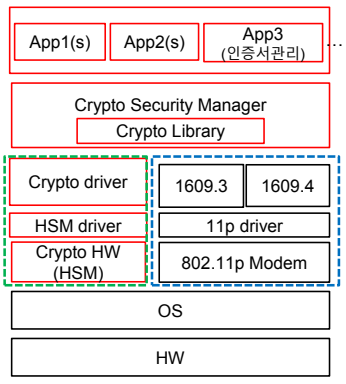




Figure 13—Service access points

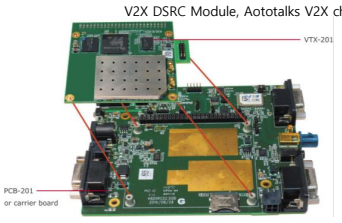


# 보안 기술 현황

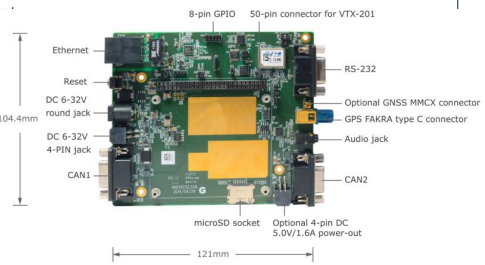
## V2X 보안 – IEEE1609.2, CAMP



OBU (On-board unit)




GNSS and HSM carrier board



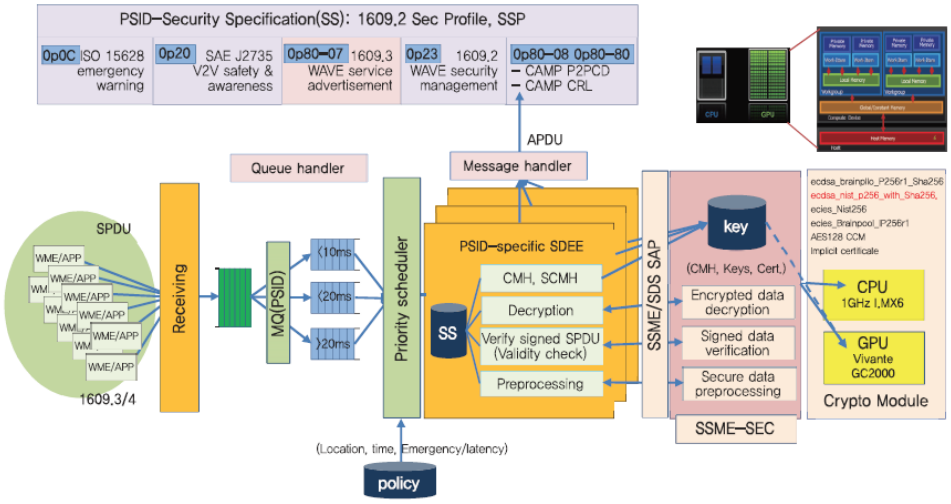

| | | | | | |
|---|---|---|---|---|---|
| | RMII_TXEN | 36 | 35 | PPS | GNSS PPS signal |
| VSS | GND | 38 | 37 | GPIO30 | GPIO30: default for microSD CS pin |
| Default for HSM(Infineon's SLE97xx) | GPIO26/SPI2_SCLK | 40 | 39 | UART_0_TXD | Console |
| | GPIO27/SPI2_Frame | 42 | 41 | UART_0_RXD | |
| | GPIO25/SPI2_TXD | 44 | 43 | UART_1_TXD | To GNSS module(Telit's SL869) |
| | GPIO24/SPI2_RXD | 46 | 45 | UART_1_RXD | |
| GPIO22/I2S_DATA | GPIO22/I2S_DATA | 48 | 47 | GPS_ON_GPIO16 | default: GPIO to |

| | |
|---|---|
| Chipset | • Telit SL869 GNSS module<br>• Infineon SLE97 Hardware Security Module (HSM) |

# 보안 기술 현황

## V2X 보안 – IEEE1609.2, CAMP -- 고속화 이슈

### 1609.2 고속 처리 스케줄러 (ETRI)

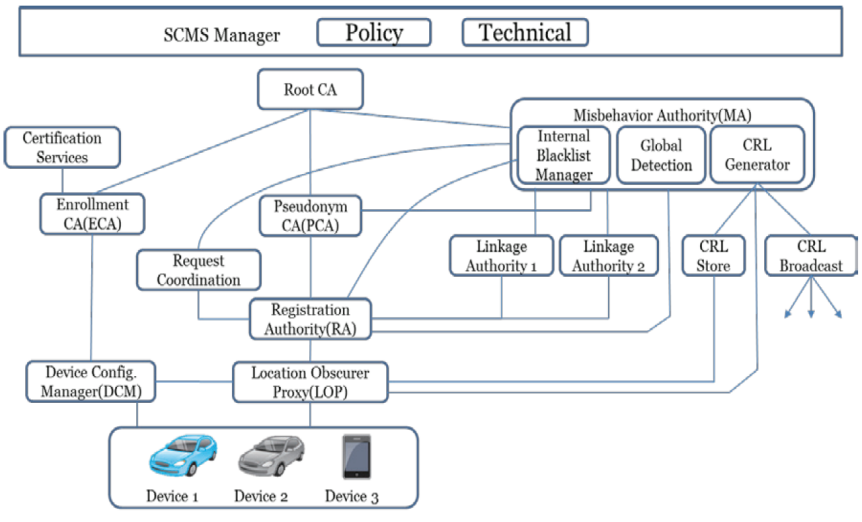





# 보안 기술 현황

## V2X 보안 – 차량 PKI

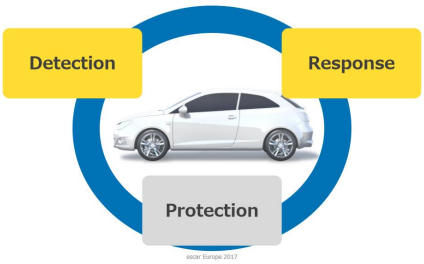
### Vehicular PKI (1609.2, CAMP)

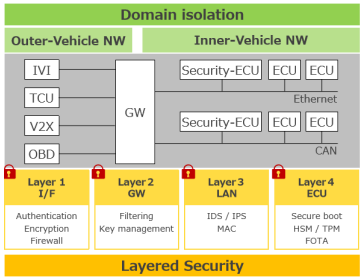


# 보안 이슈

## Analytics

### Build-up an Automotive Security Life-cycle, Panasonic




| | ECU | Cloud |
|---|---|---|
| | Rule-based detection | Machine learning based detection |
| method | Detect outlier from the predefined rule | Detect outlier from the statistical model |
| Accountability | Very Good | |
| Detect unknown and new threat | | Very Good |
| Apply for new vehicle model | | Very Good |
| CPU Spec | Low | High |

### Intel

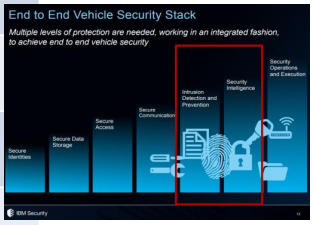
- Secure the platform
- Secure the communication
- Secure the backend
- Secure analytics

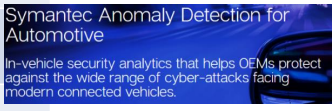


# 보안 기술 동향/이슈

## Analytics – cloud

| 업체 | 특 징 |
|---|---|
| ESCRYPT | Intrusion protection and prevention system (CycurGATE + CycurIDS + CycurGUARD)<br>3단계(Firewall, Intrusion Detection, Monitoring & Analysis) 방어 기법 적용 |
| Harman | ECUshield, TCUshield<br>탐지된 위협을 클라우드로 전송 → 경고 및 보고서 자동화, 소프트웨어 업데이트 |
| IBM | Cloud-based Intrusion Detection System(IDS)<br>IQRadar Security Intelligence Platform에서 지능형 분석을 통해 위협 탐지 |
| ARGUS cyber security | Cloud IDS<br>클라우드 기반의 통신데이터 분석 및 위협탐지 |
| Cisco | Cloud-Assited Vehicle Security<br>클라우드 기반의 악성코드 검사/제거 및 비정상 행위 차량을 탐지 |
| Symantec | Anomaly detection for automotive<br>DPI(Deep packet inspection)과 딥러닝을 통해 차량의 이상징후를 탐지<br>메시지 패턴, 페이로드 값, 트래픽 주기, 다른 디바이스들의 행위 들을 종합 분석 |
| Panasonic | 자동차의 이상징후 탐지를 위해 머신러닝 기반의 Sand Sprinkled iForest (Isolation Forest) 기법을 개발 |

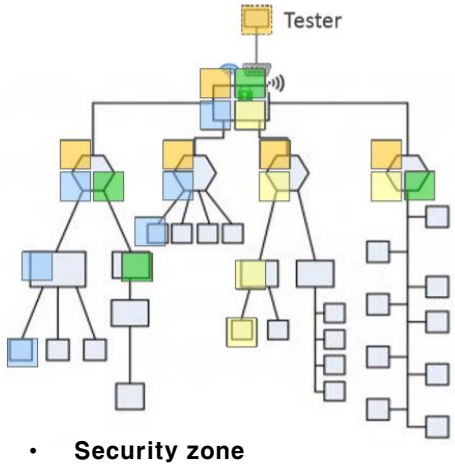


# 보안 기술 동향/이슈

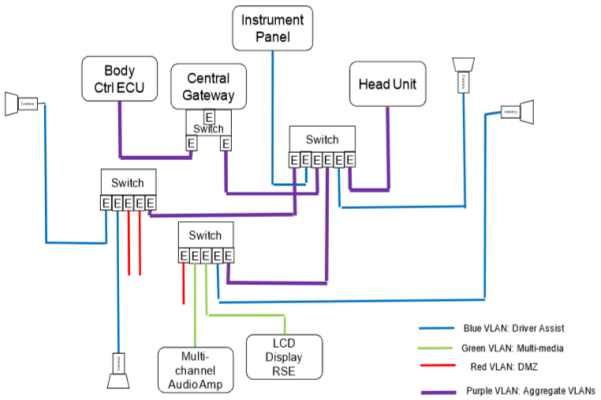
## 차세대 IVN 보안 – 이더넷

### Restrict access to the network




- Security zone
- Restrict traffic between zones
- VLAN tagging
- IEEE 802.1q (VLAN)

출처: Automotive Ethernet Congress 2016, Elektrobit, Pallierer / Ziehensack




- New devices initially connect by default to DMZ LAN
- Switches limit bandwidth to combat DoS attacks
- Connection to target VLAN only if authenticated

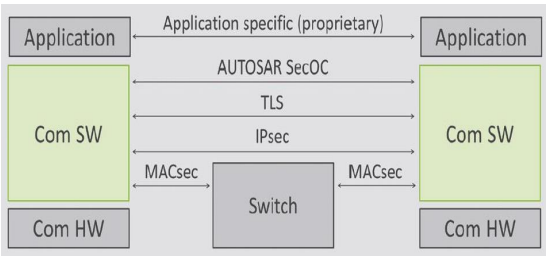
출처: "Requirements for automotive AVB system profiles", whitepaper, Avnu Alliance, Jinichi Takeuchi, 2011



# 보안 기술 동향/이슈

## 차세대 IVN 보안 – 이더넷

### Secure onboard communication




- IEEE 802.1x (port-based network access control, authentication, key management)
- IEEE 802.1AE (MACsec)
- IETF RFC 4302(AH), 4303(ESP) – IPsec
- IETF RFC 5246(TLS)
- AUTOSAR SecOC

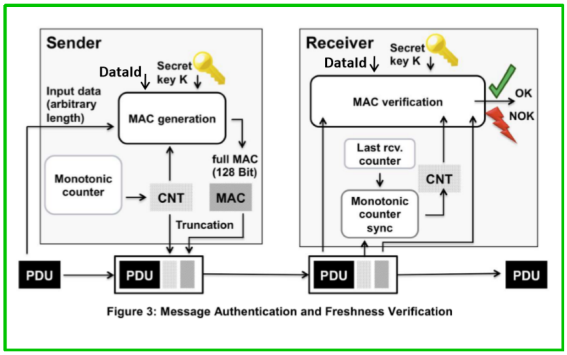



Figure 3: Message Authentication and Freshness Verification

Source: AUTOSAR 4.2 SecOC SWS

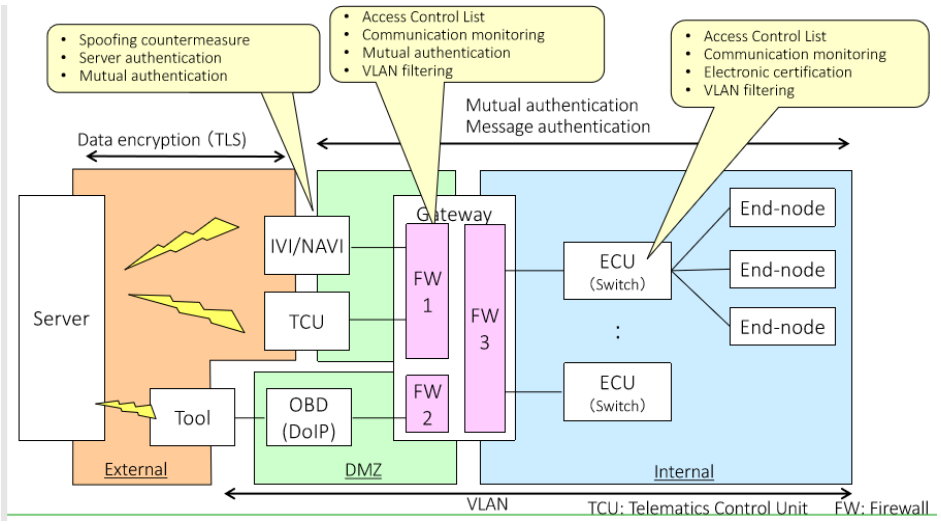
### Detect anomalies & defend

출처: Automotive Ethernet Congress 2016, Elektrobit, Pallierer / Ziehensack

# 보안 기술 동향/이슈

## 차세대 IVN 보안 – 이더넷

### Jasper: Japan automotive software platform and architecture




출처: Cyber Security Study for Automotive Ethernet in Japan Automotive Industry, JASPAR Next Generation High-Speed Network WG, 7th IEEE-SA Ethernet&IP Automotive Technology Day, Nov. 2017



# 보안 기술 동향/이슈

## 차세대 IVN 보안 – 이더넷

| Category | Applied layer L2 | L3 | L4 or above | Target |
|---|---|---|---|---|
| Filter | Port based VLAN | | | Input Port |
| | Tagged VLAN | | | VLAN Tag |
| | Private VLAN | | | Input Port |
| | | Sub network based VLAN | | IP Address |
| | MAC filtering<br>Port security<br>IEEE802.1X<br>MAC Authentication bypass | | | Mac Address |
| | Static MAC Table | | | MAC Address |
| | Dynamic ARP Inspection | | | ARP |
| | | IP Source Guard | | IP Address |
| | | IP filtering | | IP Address |
| | | VLAN ACL | | VLAN ID |
| | | NAT(Network Address Translation) | | IP Address |
| | | NAPT(Network Address Port Translation) | | IP Address+PortNo. |
| | | DDoS Open Threat Signaling (dots) | | Traffic |
| | | | OCSP (Online Certificate Status Protocol) | Certification |
| Intrusion Detection | | | DPI(IPS/IDS)<br>DPI : Deep Packet Inspection<br>IPS: Intrusion Prevention System<br>IDS:Intrusion Detection System) | payload |
| | | | WAF(Web Application Firewall) | http/https |
| | | | MAC(Message Authentication Code) | Payload |
| Cipher | MACsec | | | Ethernet Frame |
| | | IPSec | | IP |
| | | | DTLS | UDP/IP |
| | | | SSL/TLS | TCP/IP |
| Authentication | | | Kerberos Authentication | ID/PASSWORD |
| | | | RADIUS (Remote Authentication Dial In User Service) | Identification Information (ID/PASSWORD, Cerfication) |

출처: Cyber Security Study for Automotive Ethernet in Japan Automotive Industry, JASPAR Next Generation High-Speed Network WG, 7th IEEE-SA Ethernet&IP Automotive Technology Day, Nov. 2017

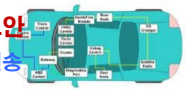
# 보안 기술 동향/이슈

## 보안 트랜드

**AS-IS**

**V2X 통신보안**
1609.2

**IVN(레거시) 보안**
ECU 인증/보안 전송
OBU-II 접근제어
PUF



**차량 PKI 인프라**
CAMP
차량 인증서 관리
CA, RA, LA, MA

**취약성 분석**
자율주행차량
보안취약성 분석

**To-be**

**Analytics (AI)**
→ Anomaly/misbehavior detection
**SOTA/FOTA**
**Automotive Ethernet Security**
**Functional security analysis (J3061)**
**Cellular V2X (4G/5G)**
**Forensic Blackbox**
**Root cause analysis (detect attack ECU)**

ETRI

16.10.13 | 27

# 감사합니다!

ETRI

16.10.13 | 28

The 24th Network Security Conference -Korea

# 자동차 해킹사례와 방어기법

**이유식** ESCRYPT 부장

### 학력 및 경력사항

ESCRYPT GmbH Security Consultant
박사수료 (고려대학교)
2013 소방방재청장 표창
2014 LEA 개발경진대회 우수상
한국암호포럼 산업표준화분과 위원
C-ITS 포럼 집행위원

### 강연요약

현재의 자동차는 다양한 정보통신기술과 빠른 속도로 융합하여 거대한 IT 시스템으로 진화하고 있다. x-by-wire, 커넥티드카, 자율주행차 등으로 대표되는 IT와의 융합은 혁신적인 기술과 편의 및 안전 기능을 제공하고 있지만, attack surface를 증가시켜 다양한 사이버 공격의 표적이 되고 있다. 또한 전통적인 IT 환경에서 활동하던 해커들이 전문적인 mechanic의 영역이었던 자동차로 자연스럽게 이동할 수 있는 계기가 되었다. 본 강연에서는 자동차에 대한 주요 해킹 사례를 분석하여 소개하고, 해당 공격을 방어하기 위한 기법들을 설명한다.

escrypt
Embedded Security by ETAS

# Plans for Car Hacking training

NetSec-KR 2018
Yousik Lee @ESCRYPT

## Autonomous Driving
Status Quo

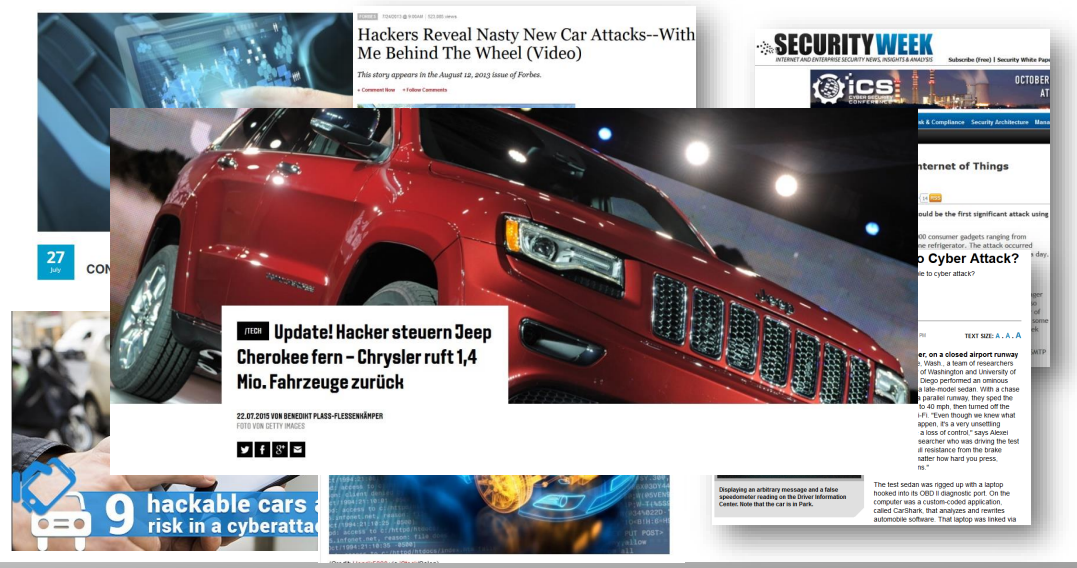
escrypt
Embedded Security by ETAS

CES 2017 Bosch Concept Car (https://www.youtube.com/watch?v=m6JfAnQuoGs)
© Google Self-Driving Car Project (https://www.google.com/selfdrivingcar/)
Night Rider 2015 (www.youtube.com)

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Challenges
Real threats

escrypt Embedded Security by ETAS

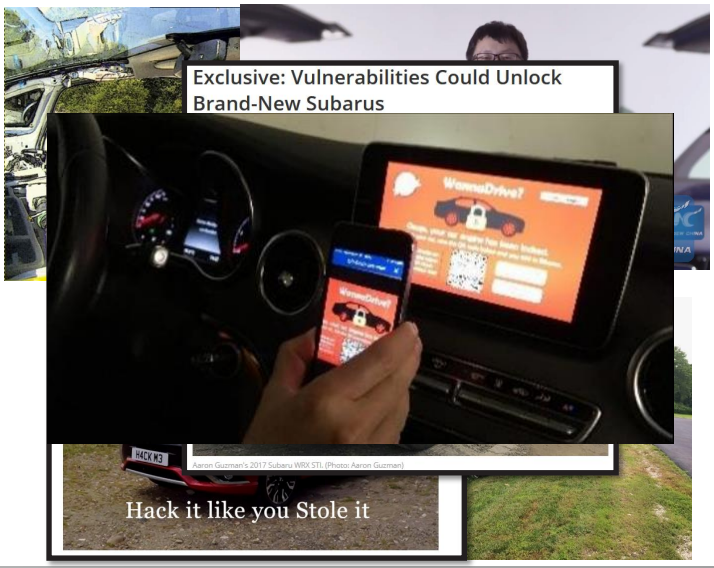



NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Challenges
Real threats

escrypt Embedded Security by ETAS

- 2017.11 WannaDrive?
- 2017.08 App. Repackaging attack
- 2017.06 SUBARU Starlink
- 2017.04, HMC Bluelink
- 2016.09, Tesla Model S
- 2016.03, Key relay attack on 19 OEM, 24 Cars
- 2016.01, Mitsubishi Outlander
- 2015.10, Jeep Cherokee
- 2013.07 Toyota Prius
- 2010~2011, Washington & California Univ.
- …




NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

# Vulnerabilities of the past

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
info@escrypt.com

## Vulnerabilities of the past

Charlie Miller & Chris Valasek

escrypt
Embedded Security by ETAS

- 2013: Advantures In Automotive Networks and Control Units – Prius Hack
- 2014: A Surbey of Remote Automotive Attack Surfaces
- 2015: Remote Exploitation of an Unaltered Passenger Vehicle – Jeep Hack

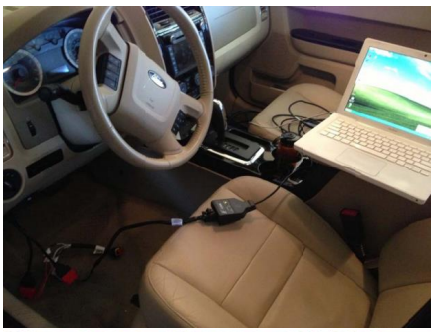
NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past

Charlie Miller & Chris Valasek - 2013: Advantures In Automotive Networks and Control Units

escrypt Embedded Security by ETAS

- Target: Ford Escape, Toyota Prius
- Analyze CAN packet and hack vehicles with wired environment
- Develop EcomCat – CAN packet monitoring tool (read/write)
- https://www.youtube.com/watch?v=oqe6S6m73Zw



NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Vulnerabilities of the past

Charlie Miller & Chris Valasek - 2014: A Surbey of Remote Automotive Attack Surfaces

escrypt Embedded Security by ETAS

| Car | Attack Surface | Network Architecture | Cyber Physical |
|---|---|---|---|
| 2014 Audi A8 | ++ | -- | + |
| 2014 Honda Accord LX | - | + | + |
| 2014Infiniti Q50 | ++ | + | + |
| 2010 Infiniti G37 | - | ++ | ++ |
| 2014 Jeep Cherokee | ++ | ++ | ++ |
| 2014 Dodge Ram 3500 | ++ | ++ | -- |
| 2014 Chrysler 300 | ++ | - | ++ |
| 2014 Dodge Viper | ++ | - | -- |
| 2015 Cadillac Escalade | ++ | + | + |
| 2006 Ford Fusion | -- | -- | -- |

| Car | Attack Surface | Network Architecture | Cyber Physical |
|---|---|---|---|
| 2014 Ford Fusion | ++ | - | ++ |
| 214 BMW 3 Series | ++ | -- | + |
| 2014 BMW X3 | ++ | -- | ++ |
| 2014 BMW I12 | ++ | -- | + |
| 2014 Range Rover Evoque | ++ | - | ++ |
| 2010 Range Rover Sport | - | -- | - |
| 2006 Range Rover Sport | - | -- | - |
| 2014 Toyota Prius | + | + | ++ |
| 2010 Toyota Prius | + | + | ++ |
| 2006 Toyota Prius | - | -- | -- |

Most Hackable

2014 Jeep Cherokee

2015 Cadillac Escalade

2014 Infiniti Q50

2014 Audi A8

2014 Honda Accord

2014 Dodge Viper

Least Hackable

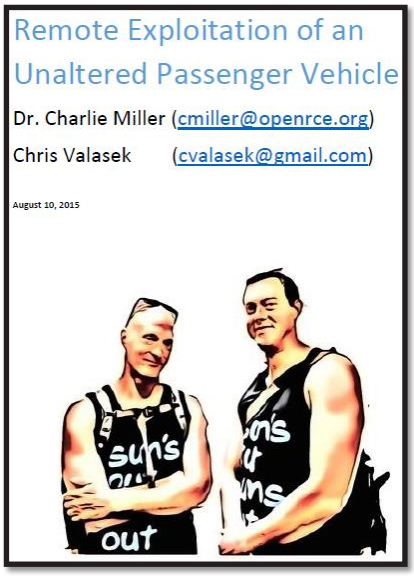
NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past

Charllie Miller & Chris Valasek - 2015: Remote Exploitation of an Unaltered Passenger Vehicle

escrypt Embedded Security by ETAS

- Everybody heard of it!!
- The biggest issue of automotive cyber security.
- No special hardware required, only common notebook/PC
- Car's IP address is the only information needed
- https://www.youtube.com/watch?v=MK0SrxBC1xs
- http://illmatics.com/Remote%20Car%20Hacking.pdf

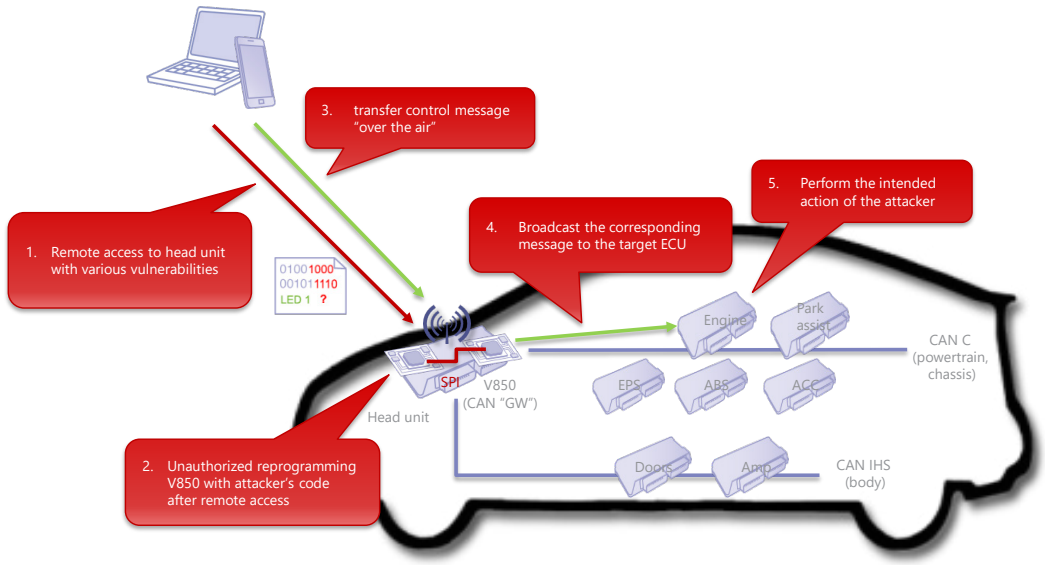



NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
info@escrypt.com

## Vulnerabilities of the past

Charllie Miller & Chris Valasek - 2015: Remote Exploitation of an Unaltered Passenger Vehicle

escrypt Embedded Security by ETAS




NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
info@escrypt.com

## Vulnerabilities of the past

Charllie Miller & Chris Valasek - 2015: Remote Exploitation of an Unaltered Passenger Vehicle

escrypt Embedded Security by ETAS

- **Impact**
  - Full control over comfort features
    - Heating, infotainment…
  - Full control over the car's steering behavior
    - disable brakes, lights…
    - control acceleration and in some special cases even the wheel
  - Full surveillance
    - Track GPS route, speed etc.
- **Consequences**
  - Affects all FCA cars with the Uconnect unit built btw. late 2013 and early 2015
  - Led to recall of 1.4m vehicles
  - Extensive press coverage and negative publicity for FCA
  - **Note:** Attack was found by researchers and reported to FCA months before publication

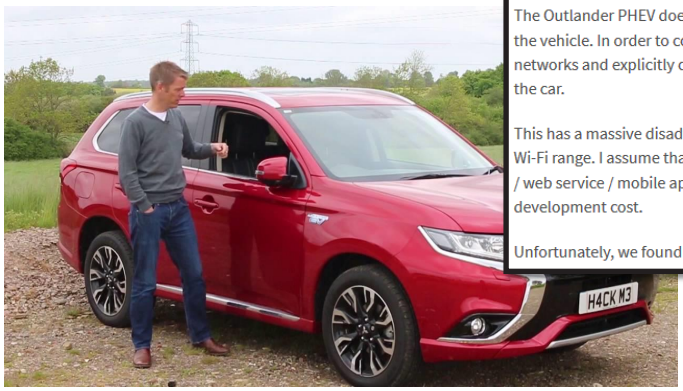
NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
info@escrypt.com

## Vulnerabilities of the past

Mitsubishi Outlander

escrypt Embedded Security by ETAS

- https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/




**Different, but not better**

The Outlander PHEV does it differently. Instead of a GSM module, there is a Wi-Fi access point on the vehicle. In order to connect to the car functions, we have to disconnect from any other Wi-Fi networks and explicitly connect to the car AP. From there, we have control over various functions of the car.

This has a massive disadvantage to the user in that we can only communicate with the car when in Wi-Fi range. I assume that it's been designed like this to be much cheaper for Mitsubishi than a GSM / web service / mobile app based solution. There's no GSM contract fees, no hosting fees, minimal development cost.

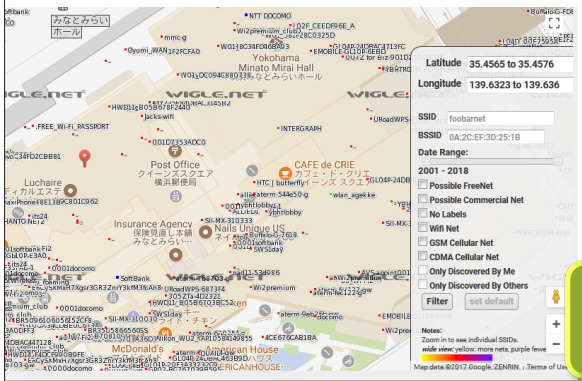
Unfortunately, we found that this system had not been implemented securely.

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past
Mitsubishi Outlander

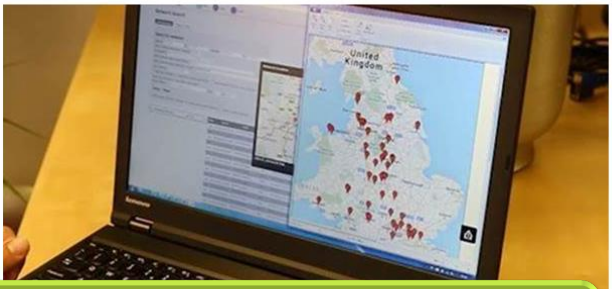
escrypt Embedded Security by ETAS

- Each car has a different SSID
- … which mean you can track cars online




The access point has a unique SSID fortunately. It is of the format: [REMOTEnnaaaa] where 'n' are numbers and 'a' are lower case letters.

This means that you can search wigle.net and easily geolocate Outlander PHEVs. Here are a few in the UK, including some spotted whilst driving and others parked at the owner's house:



Identify data that is accessible and give out private data (even indirectly)

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Vulnerabilities of the past
Mitsubishi Outlander

escrypt Embedded Security by ETAS

- … Wi-Fi password was too short

The Wi-Fi pre shared key is written on a piece of paper included in the owners' manual. The format is too simple and too short. We cracked it on a 4 x GPU cracking rig at less than 4 days. A much faster crack could be achieved with a cloud hosted service, or by buying more GPUs.

Know how passwords are generated and know how long it would take to actually bruteforce them once you know the pattern.

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past
Mitsubishi Outlander

escrypt Embedded Security by ETAS

- WPA security was the only security count ermeasure
- No software obfuscation of application

**The hack**

First, we replayed various messages from the mobile app. After figuring out the binary protocol used for messaging, we could successfully turn the lights on and off.

Next, we messed around with the charging programme, from which we could force the car to charge up on premium rate electricity.

We could also turn the air conditioning or heating on/off to order, draining the battery. This is remarkably similar to the Nissan Leaf hack, though the next part is far worse than that.

**Finally, we disabled the theft alarm. Yes, seriously**

This took a bit of proving, as we didn't want to have to break a window to make the point.

```
...
>>> def sendit(payload):
...   c=crc(payload)
...   s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
...   s.connect(("192.168.8.46",8080))
...   s.send(payload+c)
...   s.close()
...   time.sleep(10)
...
>>>
>>> alarmoff()
```

Identify weak countermeasures. Report software that is not obfuscated.

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Vulnerabilities of the past
Tesla Hack 2016

escrypt Embedded Security by ETAS

**2016** : TESLA remote control

**How to** : set-up a fake access-point, distribute pages that exploit browser's vulnerabilities to gain control execution. Use kernel vulnerabilities to gain root privilege on the IVI, reprogram the gateway to send your own messages.
**Root causes** : Old versions of web browser and kernel, weak authentication, absence of code signature.

http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past
Hyundai Bluelink 2017

escrypt Embedded Security by ETAS

**2017/04** : Hyundai Blue Link Application Vulnerabilities
**How :** They used HTTP traffic, encrypted with a static fixed key

**Why :** Attackers could retrieve they key from the smartphone app and attack any car

**Ref** : https://community.rapid7.com/community/infosec/blog/2017/04/25/r7-2017-02-hyundai-blue-link-potential-info-disclosure-fixed

Focus on non-standard implementations.

> Affected versions of Hyundai Blue Link mobile application upload application logs to a static IP address over HTTP on port 8080. The log is encrypted using a symmetrical key, "1986I12Ov09e", which is defined in the Blue Link application (specifically, C1951e.java), and cannot be modified by the user.
>
> Once decoded, the logs contain personal information, including the user's username, password, PIN, and historical GPS data about the vehicle's location. This information can be used to remotely locate, unlock and start the associated vehicle.

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Vulnerabilities of the past
App. Repackaging Attack

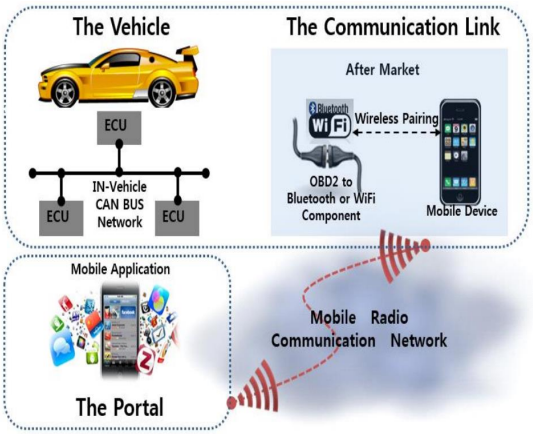
escrypt Embedded Security by ETAS

- Car's IP address is the only information needed
- https://youtu.be/siDwpyIIpnE
- https://youtu.be/Esus6GMOZoU

**2017** : Attack through ELM327 with App. repackaging

**How to** : Modify and insert attack code into commercial automotive apps and control the vehicle to which ELM327 is connected.

**Root causes** : No access control for both vehicles and dongles



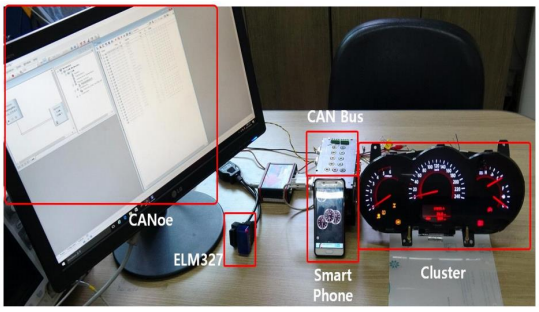

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

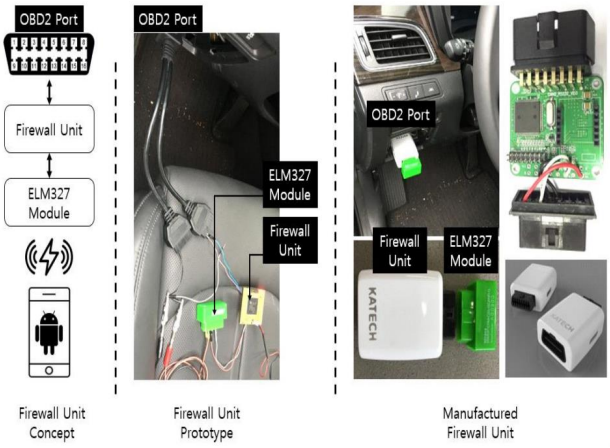
## Vulnerabilities of the past
App. Repackaging Attack

escrypt Embedded Security by ETAS

Table 5. App Analysis Results Using Automatic Vulnerability Analysis Tool

| | Number of apps | Possible to attack (%) | Impossible to attack (%) |
|---|---|---|---|
| Total | 213 | 166 (78) | 47 (22) |
| Paid apps | 66 | 58 (88) | 8 (12) |
| Free apps | 147 | 108 (73) | 39 (27) |



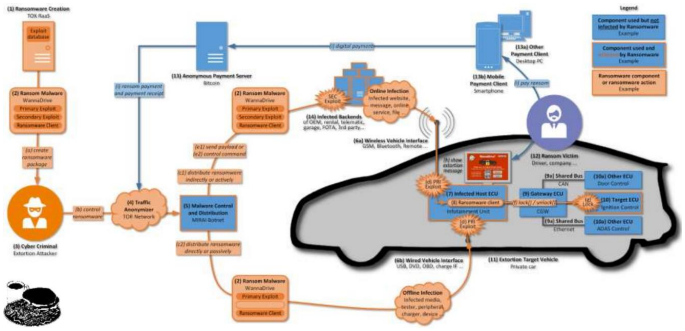



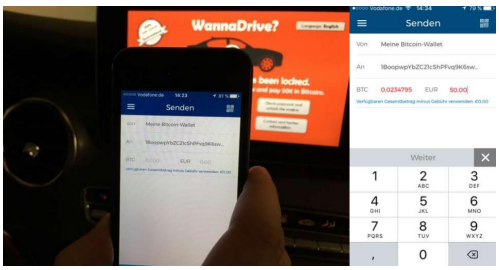

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Vulnerabilities of the past
WannaDrive?

escrypt Embedded Security by ETAS

- Feasible attack paths and effective protection against ransomeware in modern vehicles - Marko Wolf el al
- https://www.escar.info/images/Datastore/2017_escar_EU/2017_escar_EU_Marko_Wolf_ESCRYPT_GmbH.pdf





NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Vulnerabilities of the past
WannaDrive?

escrypt
Embedded Security by ETAS

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

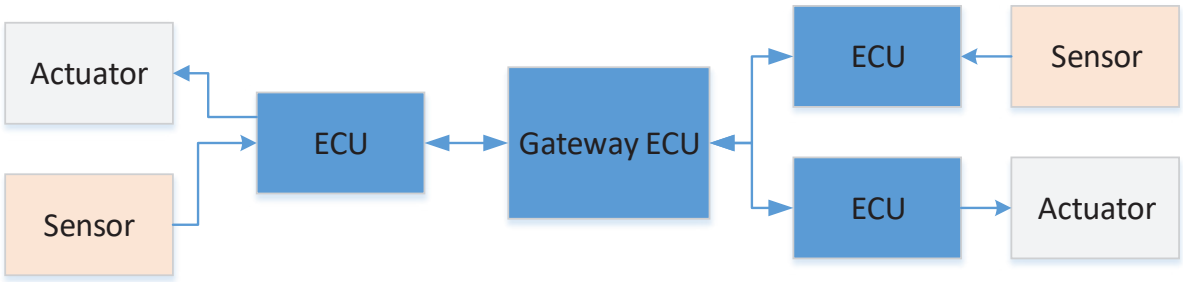

## Effective Protections

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Effective Protection
Overview

escrypt Embedded Security by ETAS

- Q: What is a car?
- A: a network of ECUs → System




NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Effective Protection
Vulnerabilities

escrypt Embedded Security by ETAS

- Maybe the system is already vulnerable by design
- Maybe the system is correct, but the protocol is flawed
- Maybe the protocol is correct, but the software is flawed
- Maybe the software is correct, but the hardware is flawed
- Maybe everything is perfect within your model, but physics say otherwise

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Effective Protection
Vulnerabilities

escrypt Embedded Security by ETAS

- Vulnerabilities are present
  - At ALL levels
    - Design
    - System
    - Software
    - Hardware
  - And of ALL kinds
    - Some require that you read fine prints
    - … and some are obvious and yet ended-up in industry standards

Never let your guard down

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Effective Protection
Vulnerabilities

escrypt Embedded Security by ETAS

A wild vulnerability appears !

It's not like this

…

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

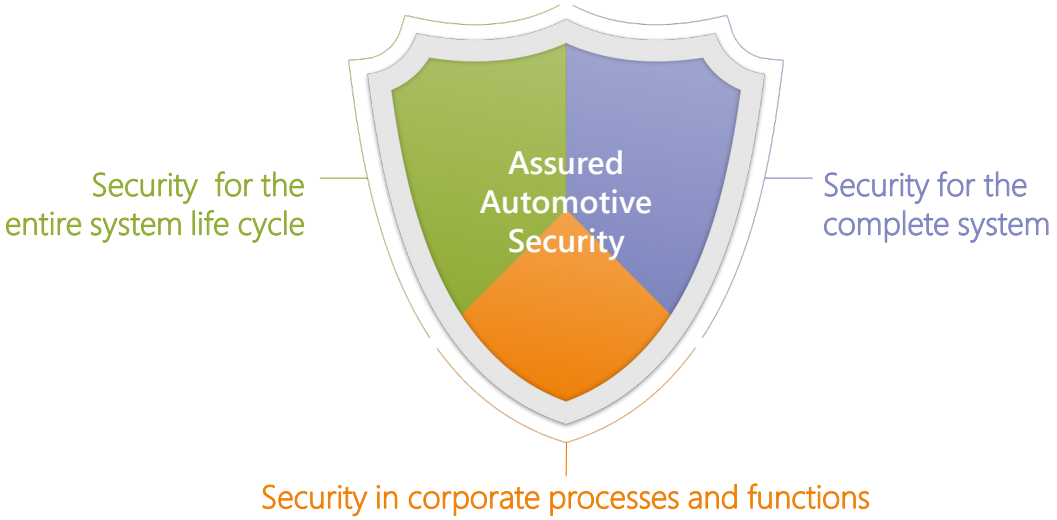
## Effective Protection
Vulnerabilities

escrypt Embedded Security by ETAS

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Effective Protection
A Holistic Approach

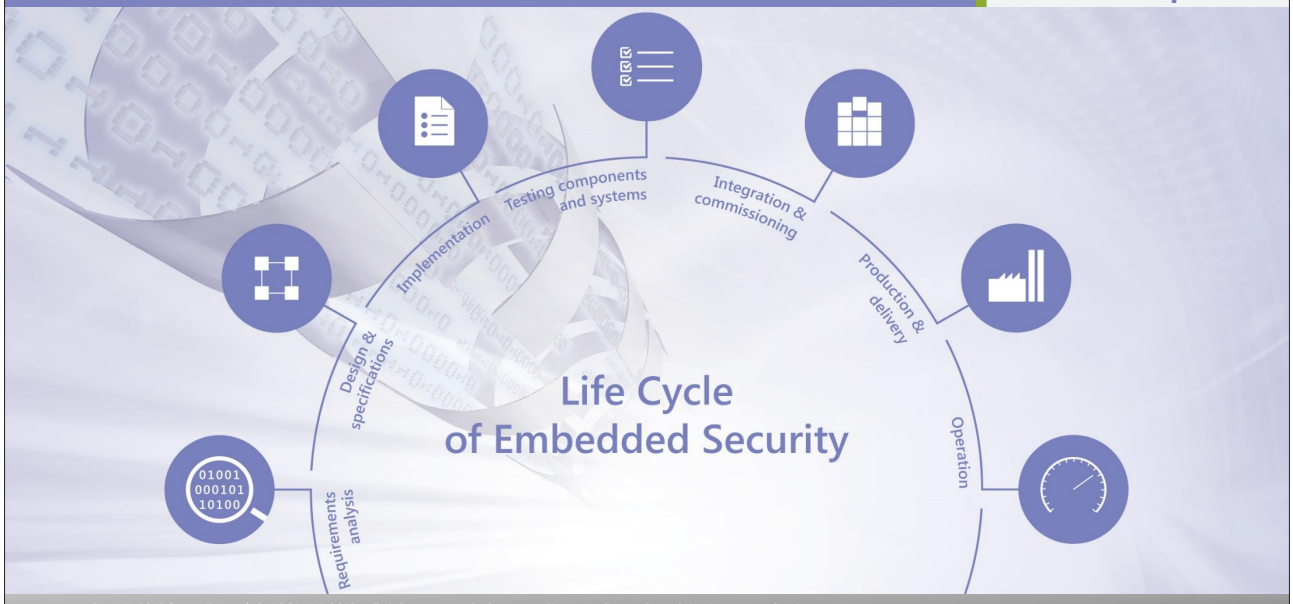
escrypt Embedded Security by ETAS




NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Effective Protection
Security for the entire system life cycle

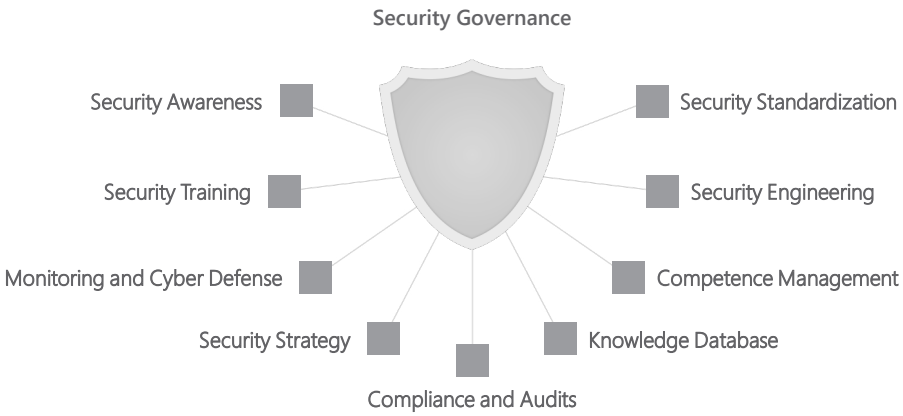
escrypt Embedded Security by ETAS




NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Effective Protection
Security in corporate processes and functions

escrypt Embedded Security by ETAS

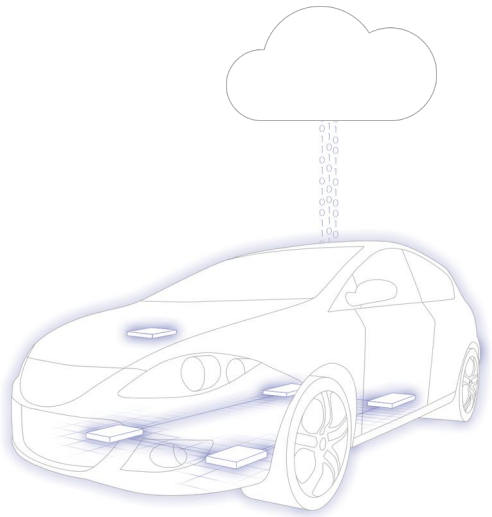



NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Effective Protection
Security for the complete system

escrypt
Embedded Security by ETAS

- **Secure** ECU
- **Secure** Onboard Network
- **Secure** E/E-Architecture
- **Secure** connected vehicle



NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.


## Conclusion

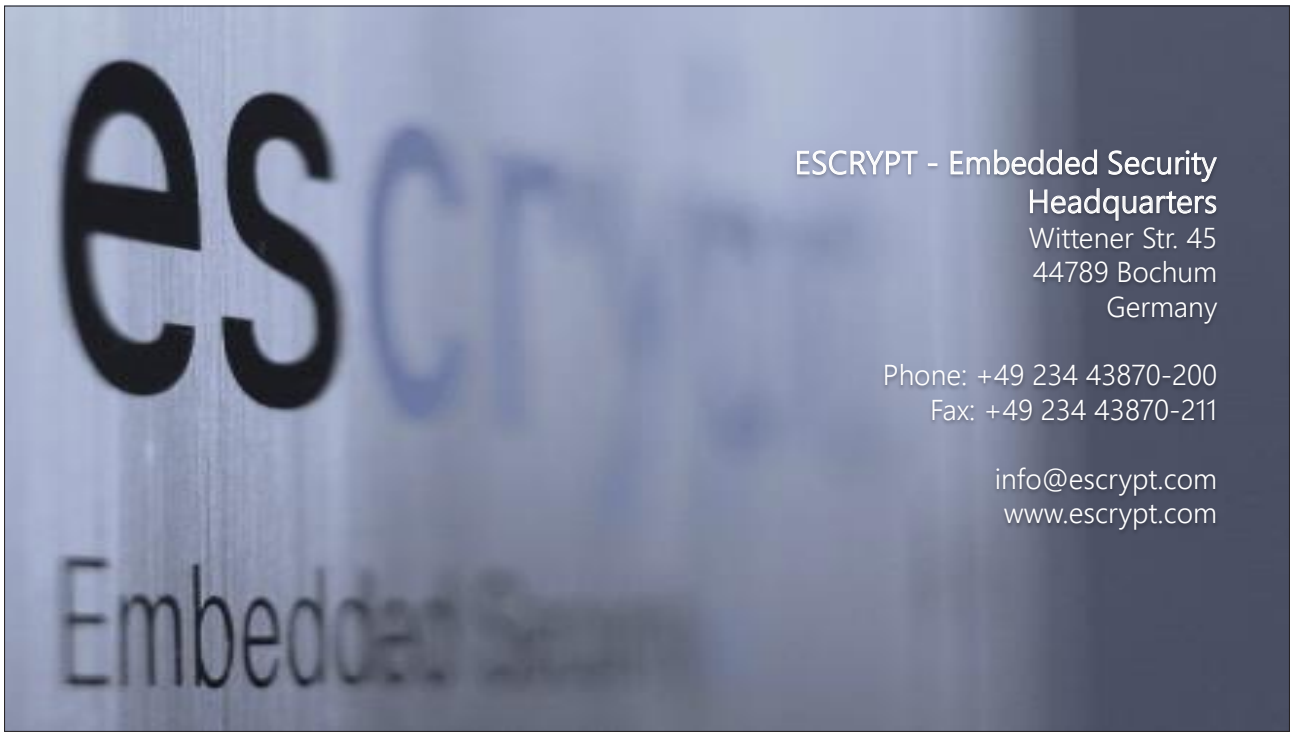
NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

## Conclusion

escrypt
Embedded Security by ETAS

- **Threats** for data security and privacy protection of modern cars **are already real** and continuously increasing.
- The more SW is adopted to vehicles, the more cyber attacks might be conducted.
- **A Holistic approach** is the only solution against past/current/future cyber attack on vehicles.
- Protections like **SOTA, IDS** will be essential counter measure to follow not only regulations but also practical needs.
- **Security should not be a competitive feature** ⇨ Go for a world-wide **minimum automotive security standard** and mandatory **third party security evaluation** similar to safety.

NetSec-KR 2018 | Yousik Lee | © ESCRYPT 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

The 24th Network Security Conference -Korea

# 자동차 보안 표준화 동향

**박승욱** 현대자동차 파트장

### 학력 및 경력사항

2000 고려대학교 전자공학과 학사
2004 서울대학교 전기컴퓨터공학부 석사
2004 ~ 2015 LG전자 차세대 표준화 연구소
– ISO/IEC JTC1 MPEG 표준화활동 (H.264/SVC/MVC, HEVC)
– 안드로이드 기반 적응형 스트리밍 (MPEG–DASH) 클라이언트 개발
– 안드로이드 네이티브 프레임웍용 비디오/오디오 S/W 코덱 개발
– 스마트 TV용 HEVC S/W 코덱 최적화
2015 ~ 현재 현대자동차 표준전략파트 파트장
– ITU–T SG17 Question 13 (ITS 보안 분과) 부라포쳐

### 강연요약

자동차와 ICT 기술의 융합에 따라 자동차는 해커들의 새로운 타깃이 되어가고 있으며, 자동차의 안전은 사람의 생명과 직관되어 있기에 자동차 보안은 더욱 중요하다 할 수 있다.
본 강연에서는 근래에 발생하고 있는 자동차 보안 문제에 대해서 몇 가지 사례를 공유하고, 이를 방지하기 위한 국제적인 활동에 대해 자동차 보안 국제 표준화 및 법제화 활동에 대해 소개하려고 한다.

# 자동차 보안 위협 및 대응

beyond THE CAR

2018. 4. 13

현대자동차
박승욱 책임

HYUNDAI MOTOR GROUP

## ■ 목차

Ⅰ. 자동차 보안 위협

Ⅱ. 글로벌 대응

# I. 자동차 보안 위협

**차량보안 정책**
(북미 중심 → 글로벌 대응)

- 3 차량 사이버 보안 UN Task Force 구성
- 5 스마트카/교통 보안 표준 제정
- 8 美 연방 자율주행차 법안 발의
- 10 차량보안 정부 권고 및 법안 동향

**차량해킹 확대**
(해킹사례 공개 및 언론보도 지속)

- 2 자동차 해킹 공격/테스트
- 4 위키리스크, CIA 차량해킹 기술 개발 폭로
- 6 $22 리모트키 공격 도구로 차량 탈취

**차량보안 동향**
(컨퍼런스 및 동향보고서 정착)

- 1 차량보안 CES 2017
- 7 차량보안 컨퍼런스 ESCAR 북미 개최
- 9 ESCAR Asia/Europe 2017

Together We can!

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

Together We can!

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

대상 범위 선정 → 정보 수집 취약점 분석 공격 시도 → 악용



# I. 자동차 보안 위협 – 차량 해킹 증가

**Fig. Jeep Cherokee 원격 해킹** (2015, 찰리밀러 / 크리스 발라섹)

**<ICT 기술>**
1. 인포테인먼트 시스템
2. 적응형 순항 제어 장치
3. 전방 충돌 경고 +
4. 주차 보조 시스템

→

**<취약점>**
1. 인포테인먼트 wi-fi 접속 패스워드 생성 룰의 단순함
2. 포트 스캐닝 허용
3. 인증 없이 내부 버스 접속 가능
4. 디지털 서명 확인 없이 시스템 업데이트 허용

→

# I. 자동차 보안 위협 – 차량 해킹 증가

**우버 저율주행차, 보행자 사망사고** ('18.3.19,10pm,아리조나)

- 자율주행차 시험운행 관련 첫 보행자 사망사고
- 센서 인식 문제, 또는 차량 내 센서간 정보 처리 솔루션에 오류
- 우버 자율주행 테스트 전면 중단

**테슬라 모델 X, 자율주행 중 사고, 운전자 사망**

('18.3.30,캘리포니아 101 고속도로)

- 오토파일럿 + 적응형 크루즈컨트롤 사용
- 중앙분리대를 인식하지 못하고 충돌 (센서 문제?)
- 2016년, 모델 S차량의 사고 (센서 문제) 이후 두 번째
- 신뢰 하락

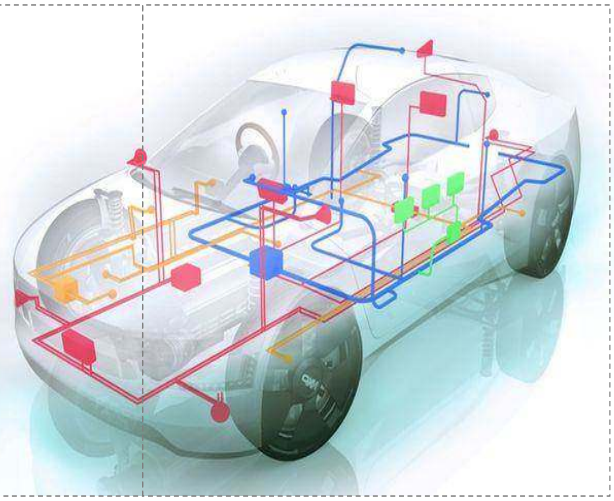
**자율주행차 + 해킹 ⇨ 재앙**

Together We can!

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

▣ 영역별 보안 위협

| | 차량외부 | 접점 | 차량내부 (IVN/ECUs) |
|---|---|---|---|
| 분류 | scanner, external storage — Wired connection<br>3G/4G, WiFi, BT, smart key, V2X, sensors — Wireless connection |  | |
| 관련 시스템 | • Vehicle Diagnosis System<br>• Telematics center<br>• Wired / Wireless network<br>• Road side unit | • PKES<br>• Infotainment System<br>• OBD-II port<br>• Sensors | • Central gateway<br>• In-vehicle network<br>- CAN, Ethernet, Lin FlexRay, MOST …<br>• ECUs<br>- Engine, Transmission , Brake, Airbag… |

Together We can!

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – PKES (Passive Keyless Entry System)

### ► Automotive security system

- Operating automatically when the user is in proximity to the vehicle
  - Unlocking the door by just pushing door open button
  - Locking it when the user walks away
- Starting/stop engine by just pushing start/stop button

### ► Essential components in a key and a vehicle

- Key : RF signal transmitter and LF signal receiver
- Car : LF signal transmitter and RF signal receiver
- Common : Message encoder/decoder

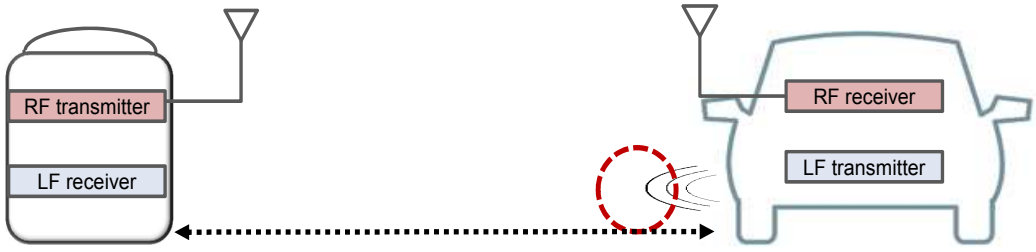
### ► Operation process

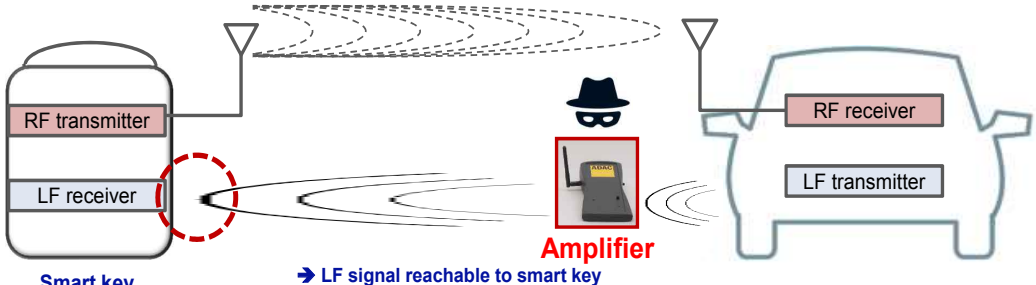
Together We cc ➔ *It works only when the driver is near the vehicle*

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – PKES (Passive Keyless Entry System)




Together We can!

HYUNDAI MOTOR GROUP

# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – PKES (Passive Keyless Entry System)

**Vulnerability test results** (from ADAC, German Auto Club)

| Fahrzeug-hersteller | Modell | Erst-zulas-sung | Reichweite der Keyless-Verlängerung in Testhalle | Illegales Öffnen möglich? | Illegaler Motorstart möglich? |
|---|---|---|---|---|---|
| Audi | A3 | 10/2015 | Max. | Ja | Ja |
| | A4 | 9/2015 | Max. | Ja | Ja |
| | A6 | 9/2014 | Max. | Ja | Ja |
| BMW | 730d | 8/2015 | Max. | Ja | Ja |
| Citroen | DS4 CrossBack | 11/2015 | Max. | Ja | Ja |
| Ford | Galaxy | 5/2014 | Max. | Ja | Ja |
| | Eco-Sport | 10/2015 | Max. | Ja | Ja |
| Honda | HR-V | 6/2015 | Max. | Ja | Ja |
| Hyundai | Santa Fee | 8/2015 | Max. | Ja | Ja |
| KIA | Optima | 11/2015 | Max. | Ja | Ja |
| Lexus | RX 450h | 12/2015 | Max. | Ja | ja |
| RangeRover | Evoque | 9/2015 | Max. | Ja | ja |
| Renault | Traffic | 11/2015 | Max | Ja | Ja |
| Mazda | CX-5 | 3/2015 | Max. | Ja | Ja |
| MINI | Clubman | 8/2015 | Max. | Ja | Ja |
| Mitsubishi | Outlander | 12/2013 | Max. | Ja | Ja |
| Nissan | Qashqai+2 | 11/2013 | Max. | Ja | Ja |
| | Leaf | 05/2012 | Max. | Ja | Ja |
| Opel | Ampera | 03/2012 | Max. | Ja | Ja |
| SsangYong | Tivoli XDi | 09/2015 | Max. | Ja | Ja |
| Subaru | Levorg | 8/2015 | Max | Ja | Ja |
| Toyota | RAV4 | 12/2015 | Max. | Ja | Ja |
| VW | Golf 7 GTD | 10/2013 | Max. | Ja | Ja |
| | Touran 5T | 12/2015 | Max. | Ja | Ja |

► Tested **24 production cars** sold in Europe
- All car's door open w/o a key
- All car's engine started w/o a key

➔ *Critical vulnerable point*



# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – OBD-II port

**< Usages >**

► **Diagnosis** of various vehicle sub-systems
:: **Engine, Transmission, Steering, Body stabilization, Brake, Air-bag and etc.**

► **S/W updating** in ECUs to fix problems

**< Vulnerable points >**

► No authentication process for accessing to this port
➔ diagnostic tools and various wireless devices

► **Remote attack is possible if wireless device is attached**

➔ ***WiFi, BT, 3G*** **ODB-II dongle is only 10$ in AliExpress**

**ex) After market HUD, For collecting information by insurance company …**

1. Plug Kiwi 3 into the OBD2 Port
2. Launch your favorite app

# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – OBD-II port

**< Attack scenario >**

① Intentionally, **Bluetooth OBD-II dongle attached to OBD-II port** by owner

→ **Insurance fee discount, private vehicle diagnosis, convenient service (e.g. HUD) and etc.**

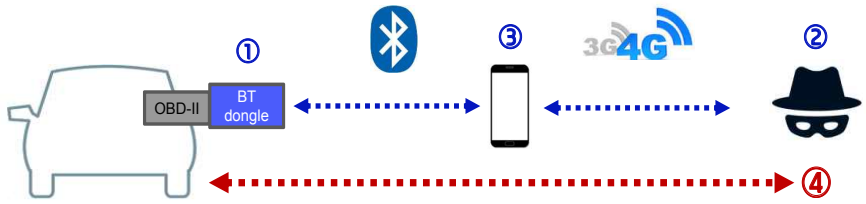
② **App including malware distributed**

→ **Enabling send/receive CAN message w/o owner's permission**

③ **Owner using the app**

→ **Malware working**

④ **Sending CAN messages to control the vehicle / Eavesdropping private information** (routing information, banking accounts and etc.)






# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – OBD-II port

| No. | Date | Hacker | Target vehicle | A way to access to OBD-II port | Contents |
|---|---|---|---|---|---|
| 1 | '10.05 | Washington Univ./ Sandiego Univ (US) | Unknown | Laptop → OBD-II port | Instrument cluster control, Radio channel/volume control, door control, wiper control, engine stop, steering wheel control, light control and etc. |
| 2 | '12.08 | Korea Univ. (Kor) | Accent (Hyundai) | Smart phone with a hacked app → Bluetooth dongle → OBD-II port | Instrument cluster control, engine stop, automatic parking system control and etc. |
| 3 | '13.04 | Kristoffer Smith (US) | Grand Cherokee (Jeep) | Tablet → OBD-II port | Instrument cluster control, radio control and etc. |
| 4 | '13.08 | Charlie Miller, Chris Valasek (US) | Prious (Toyota) Escapte (Ford) | Laptop → OBD-II port | Instrument cluster control, radio control, brake system/steering wheel/transmission control when over 80 km/h |
| 5 | '15.05 | NHTSA (US) | Prious (Toyota) Fusion (Ford) | Laptop → OBD-II port | Instrument cluster control, window open/close, brake system control, engine stop and etc. |
| 6 | '15.08 | Sandiego Univ (US) | Corvette13MY (Chevrolet) | Sending SMS → 3G dongle (provided by insurance company) → OBD-II port | Instrument cluster control, radio control, brake system/steering wheel/transmission control and etc. |
| 7 | '15.12 | Hirosima Univ (Jap) | Corolla (Toyota) | Smart phone with a hacked app → WiFi dongle → OBD-II port | Instrument cluster control, window open/close and etc. |

# I. 자동차 보안 위협 – 차량 해킹 증가

## ▣ 영역별 보안 위협 – Infotainment system

| No. | Date | Hacker | Target vehicle | How to hack | Contents |
|---|---|---|---|---|---|
| 1 | '15.07 | Charlie Miller / Chris Valasek | Cherokee (Chrysler) | Attacker ↔ Mobile network ↔ Infotainment system ↔ CAN bus in a vehicle | Engine stop, Steering wheel control, Brake control and etc. |
| 2 | '15.07 | Samy Kamkar | On-Star telematics system (GM) | Attacker ↔ Spoofed WiFi ↔ App in a vehicle | Stealing private information, remote controlling window/air conditioner and etc. |
| 3 | '15.08 | Mark Roger / Kevin Mahaffy | Model S (Tesla) | Acquisition root permission through Ethernet ↔ Tesla Network ↔ App in a vehicle | Remote door open/close, Engine start/stop and etc. |
| 4 | '16.02 | Troy Hunt | Leaf (Nissan) | Attacker ↔ Proxy server ↔ App in a vehicle | Used vulnerability of using VIN for authentication<br>➔ Attacker in Australia controlling air-conditioner of a vehicle in UK |
| 5 | '16.06 | Pen Test Partners (UK) | Outlander PHEV (Mitsubishi) | Attacker ↔ Wi-Fi eavesdropping ↔ App in a vehicle | Acquisition of secret key used in communication with app in a vehicle<br>➔ Attacker controlling light, air-conditioner, tracking vehicle position and etc. |



# II. 글로벌 대응

## ▣ 북미

**언론의 관심**

2015.2.6

CAR HACKED ON 60 MINUTES

*No real security on the Internet – even the military is under daily assault - says the man the Defense Department hired to make the web more secure*

"60 minutes", 원격 차량 해킹 공개

2015.2.2

BMW ConnectedDrive hack sees 2.2 million cars exposed to remote unlocking

BMW, 원격도어잠금해제 보안 결함 발견

2015.3.11

Ford, GM and Toyota sued for 'dangerous defects' in hackable cars

A class action lawsuit against GM, Ford, and Toyota claims the automakers know their vehicles are vulnerable to remote hacking, but failed to alert consumers about the 'dangerous defects.'

Ford/GM/Toyota, 해킹 가능성 방치 이유로 소송

**정부의 대응**

"차량 제조사가 사이버보안 위협 정보를 타제조사와 정부기관에 공유하도록 촉구"

법규 제정시, 1) 사이버보안 시스템 평가,
2) 원격 접속 보안성 강화,
3) 차량 침투 시험
을 포함시킬 것

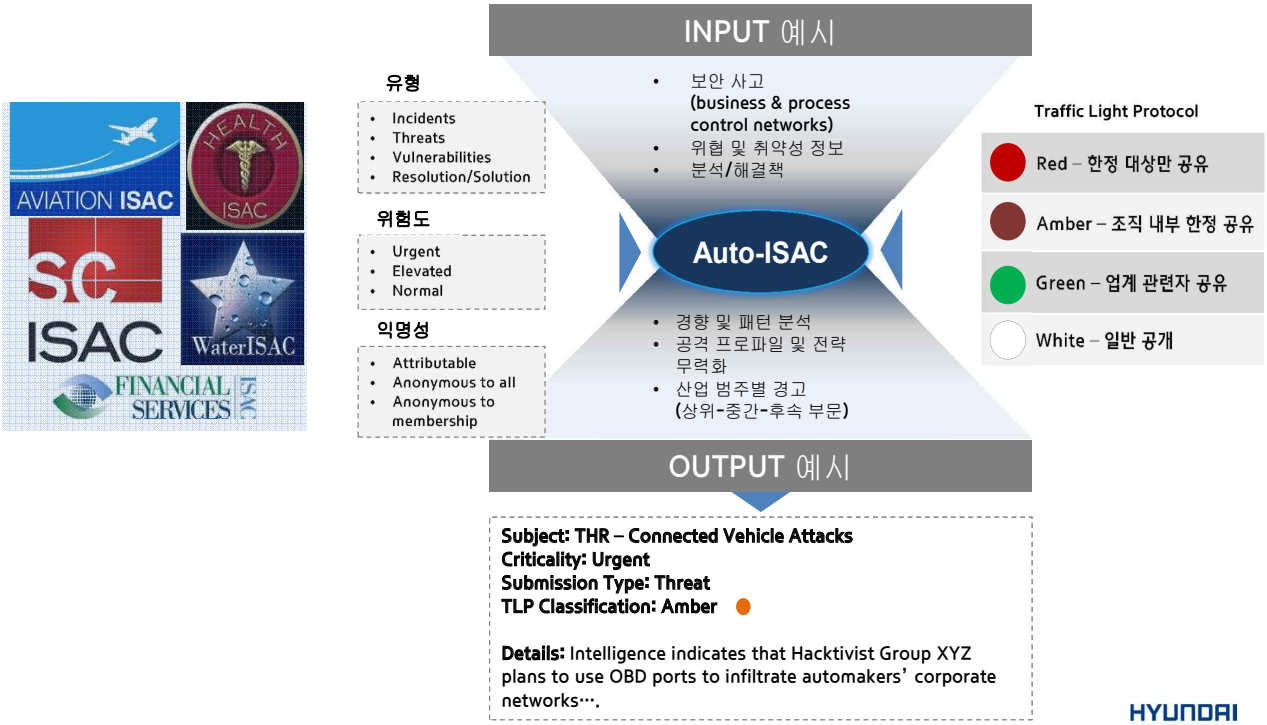
NHTSA

보안 관련 정보를 공유할 수 있는 조직을 구성할 것을 자동차 제조사에게 요구

➔ AUTO-ISAC 설립

# II. 글로벌 대응

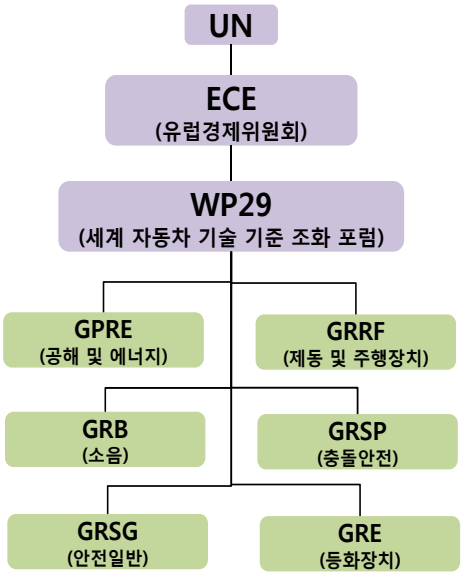
## ▣ 북미 – AUTO ISAC (Information Sharing & Analysis Center)




HYUNDAI MOTOR GROUP

# II. 글로벌 대응

## ▣ 북미 ➔ 글로벌 (UN/ECE WP29 TF/CS)




- 국제연합 유럽경제위원회 산하 기관
- 세계자동차 기술 기준의 조화 수행하는 실무위원회

**UN/ECE WP29 ITS/AD IWG 조성** (2015.3)

1) 자율주행기술 관련 법적인 이슈사항 발굴
2) 안전기준 항목 도출
3) 관련된 법규의 제개정을 지원하기 위한 '인포멀 워킹 그룹' 발족 (2015.3월)

**<세부내용>**
- 자율주행기술의 정의
- 법적 한계 및 이슈
- 국제조화기준 논의 아이템
- eSafety
- **eSecurity**

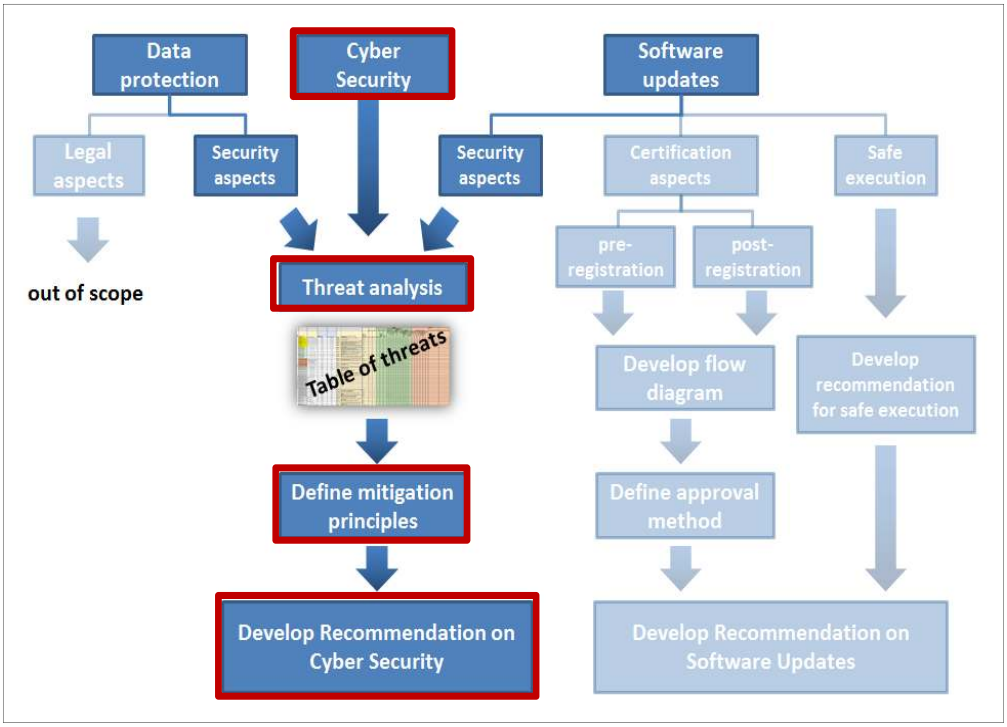
**UN/ECE WP29 TF/CS (Task Force / Cyber Security) 조성** (2016.12, 2018.4 완료 예정)

1) 차량 사이버보안
2) 차량 데이터보호
3) 차량 OTA (원격업데이트)

**참여: 글로벌 차량 제조사, 세계자동차 제작사 협회 (OICA), 각국 교통부 등**

# II. 글로벌 대응

## ▣ UN/ECE WP29 TF/CS 활동




# II. 글로벌 대응

## ▣ UN/ECE WP29 TF/CS 활동 – 사이버 보안 권고안

Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD

Document status: v0.5 - revised following TFCS11 date: 01/03/2018

Contents

1. Introduction ..... 2
1.1. Preamble ..... 2
1.2. Scope ..... 3
1.3. Approach ..... 3
2. Definitions (and abbreviations) ..... 3
3. Reference Model ..... 5
4. Cyber security principles ..... 11
5. Threats to vehicle systems and ecosystem ..... 12
6. Mitigations ..... 13
7. Requirements for cyber security processes and how to evidence their application ..... 15
8. Conclusion and Recommendation for further proceedings ..... 17
Annex A List of threats and corresponding principles and mitigations ..... 18
Annex B List of Security Controls related to mitigations incl. examples ..... 49
~~Annex C Alternate reference model~~ ..... 58
Annex D Draft proposal to introduce a regulation on cyber security ..... 62
Annex E List of reference documents ..... 72

- 25 mitigations
- 사이버 보안 프로세스를 위한 요구 사항 제시

| Category of threat | Sub Category |
|---|---|
| Compromise of **back-end server** | Server used to attack vehicle |
| | Services from back-end server disrupted |
| | Data held lost "data leakage" / compromised |
| **Communication channels** used to attack a vehicle | Spoofing |
| | Communication permits tampering with vehicle held cod e/data |
| | Attack on Integrity / Data Trust |
| | Information Disclosure (including eavesdropping) |
| | Denial of service |
| | Elevation of privileges |
| | Virus infection |
| | Message injection / tampering |
| **Update process** used to attack a vehicle | Misuse of updates |
| | Denying updates |
| **Human factor and social engineering** | Misconfiguration |
| | Unintended actions |
| Compromise of **external connectivity** | Vehicle functions using connectivity |
| | Hosted 3rd party software e.g. entertainment apps |
| | External interfaces |
| Target of an attack on a **vehicle** | Extract Data/Code |
| | Manipulate Vehicle Data |
| | Erase Data/Code |
| | Introduce malware |
| | Introduce new software or overwrite existing software |
| | Disrupt systems or operations |
| | Manipulate Vehicle Parameters |
| **System design** exploits (inadequate design a nd planning or lack of adaption) | Encryption |
| | Early stage attack |
| | Software and hardware development |
| | Network design |
| **Data loss / "data leakage"** from vehicle | Physical loss of data |
| | Unintended transfer of data |
| **Physical manipulation** of systems to enable an attack | Physical manipulation of systems to enable an attack |
| **Communication loss** to/from vehicle (potent ially out of scope as not cyber security) | Communication jamming |
| | Environmental effect |
| Non-cyber security vehicle threats (potentiall y out of scope) | Vehicle - failure |
| | Manipulate Data/Code |
| | Sensor spoofing |

# II. 글로벌 대응

## ▣ ITU-T SG17 Q13 표준화 활동

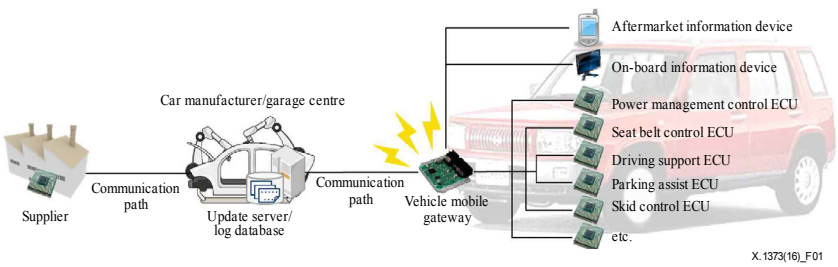
ITU-T ITU-R ITU-D

- SG2 : Operational Aspect
  ...
- SG17: Security
  ...
- SG20: IoT and app, smart cities
  - Q1 : ICT security coordination
    ...
  - Q6 : Security aspect of ubiquitous telecom services
    ...
  - Q12: Formal language for S/W
  - Q13: ITS security

- **ITU-T**
  - 국제전기통신연합 통신 부문 국제 표준화 기구
  - 1865년 5월 UN 산하에 신설
  - 산하에 11개의 Study Group 활동
- **Study Group 17**
  - 정보보호 표준화 담당 (ex: **X.509**)
  - 산하에 13개의 Question (세부 표준화 기술) 활동
  - 총 33개국 160여명의 전문가가 참석
- **Question 13**
  - ITS 보안 관련 표준화 ('17.3월 신설)

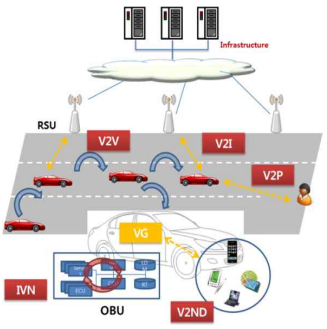
# II. 글로벌 대응

## ▣ ITU-T SG17 Q13 표준화 활동

| | |
|---|---|
| 타이틀 | Secure software update capability for intelligent transportation system communication devices (X.1373) |
| 표준화 단계 | International Standard ('17.3) |
| 표준화 범위 | In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer in order to prevent threats such as tampering of and malicious intrusion to communication devices on vehicles. This includes a basic model of software update, security controls for software update and a specification of abstract data format of update software module.<br>The procedure related to in-vehicle communication is the out of scope of this Recommendation. For reference, the procedure used in-vehicle in this Recommendation is informative.<br>The procedure is intended to be applied to communication devices on ITS vehicles under vehicle-to-infrastructure (V2I) communication by means of the Internet and/or ITS dedicated networks. The procedure can be practically utilized by car manufactures and ITS-related industries as a set of standard secure procedures and security controls. |
| 내용 |  |

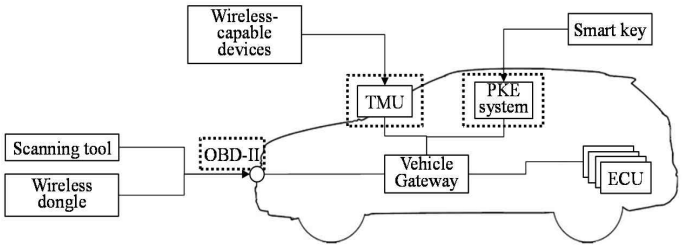
# II. 글로벌 대응

## ▣ ITU-T SG17 Q13 표준화 활동

| 타이틀 | Security Guidelines for V2X Communication Systems (X.itssec-2) |
|---|---|
| 표준화 단계 | '18.10 determine 예정 |
| 표준화 범위 | This Recommendation provides security guidelines for V2X communication systems. V2X is a generic term for communication modes of V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) and V2ND (Vehicle-to-Nomadic Devices) and V2P (Vehicle-to-Pedestrian) in this Recommendation. This Recommendation identifies threats in V2X communications environment based on the results of UNECE WP29/TFCS and specifiesy security requirements for V2X communication systems based on the threats.<br>In-Vehicle Network/Communication is out of scope of this Recommendation. |
| 내용 |  <br>• **Identified threats**<br>• **Security requirements**<br>• **Examples for V2X security system** |

# II. 글로벌 대응

## ▣ ITU-T SG17 Q13 표준화 활동

| 타이틀 | Security requirements for vehicle accessible external devices (X.itssec-3) |
|---|---|
| 표준화 단계 | '19.10 determine 예정 |
| 표준화 범위 | In the context of using external devices accessible to internal sub-systems of the vehicle, this draft Recommendation aims to provide possible threats and vulnerabilities tampering with and intruding to internal sub-systems of the vehicle and security requirements in order to prevent and mitigate threats.<br>This draft Recommendation can be practically utilized by car manufacturers, suppliers, 3rd party external device manufacturers and ITS-related industries as a security requirement standard for manufacturing and maintaining external devices accessible to the vehicle.<br>This draft Recommendation:<br>- describes and identifies security threats when external devices access to internal sub-systems of the vehicle<br>- defines security requirements for vehicle accessible external devices<br>Security requirements of V2X system are in the scope of X.itssec-2. |
| 내용 |  |

# Q/A

The 24th Network Security Conference -Korea

# IoT 디바이스 하드웨어 취약성 및 보안기술

**김호원** 부산대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1999.02 | POSTECH 전자전기공학과 공학박사 |
| 1998.12 ~ 2008.02 | ETRI 선임연구원/팀장 |
| 2003.07 ~ 2004.06 | 독일 University of Bochum, Post–Doctorial |
| 2008.03 ~ 현재 | 부산대 전기컴퓨터공학과 교수 |
| 2014.06 ~ 현재 | 부산대 사물인터넷 연구센터 센터장 |

정보보호학회 상임이사

정보처리학회, 멀티미디어학회 이사

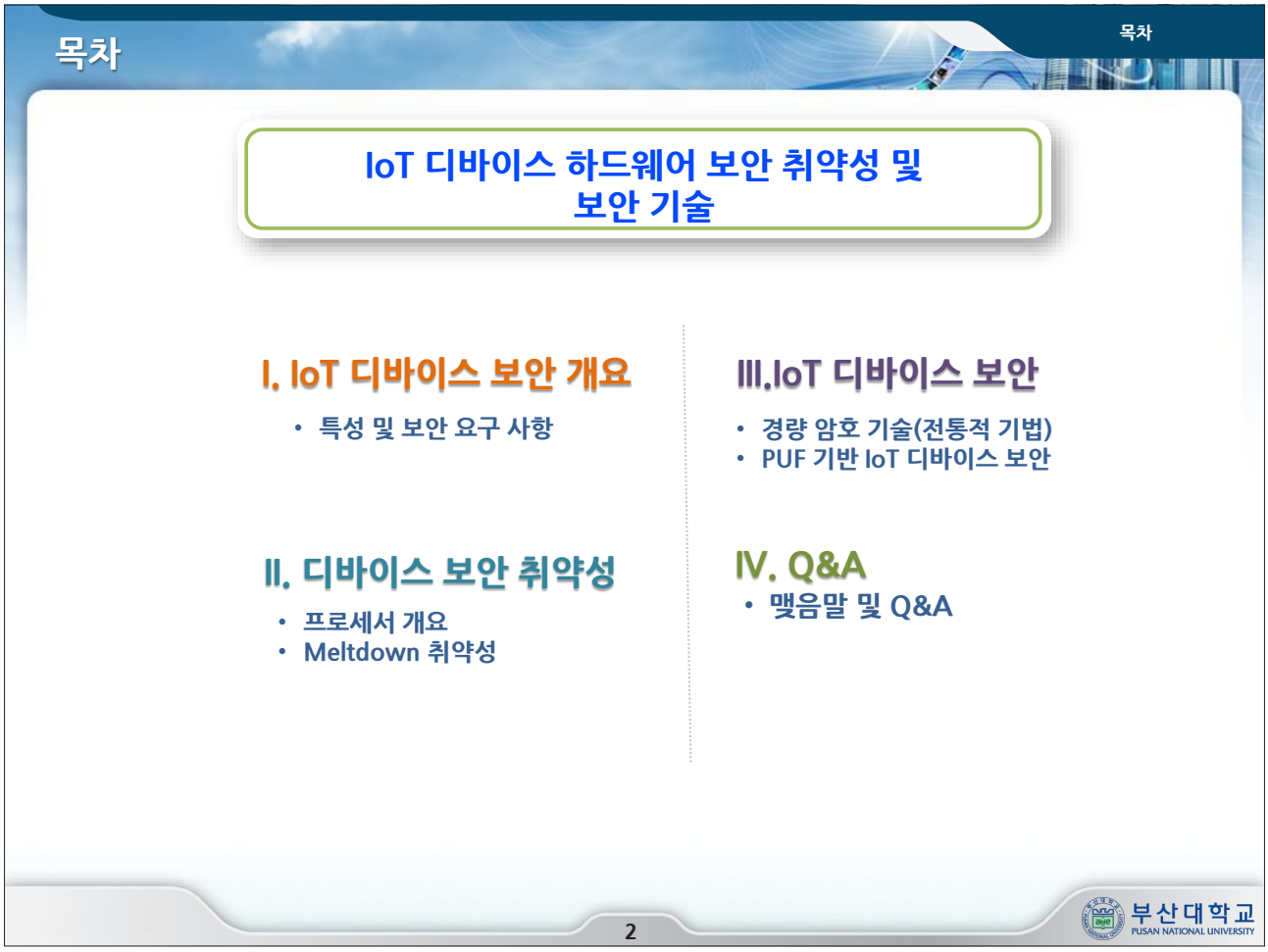
IEEE Member, IACR Member, ACM Member

### 강연요약

로봇, 드론, 자율주행자동차, 블록체인 등, 지능형 시스템과 서비스에서의 보안과 프라이버시 보호의 중요성은 더욱 높아지고 있다. 이러한 응용 분야 보안을 위해 필요로 하는 암호 기술과 Security Anchor는 궁극적으로 하드웨어의 보안성에 토대를 두고 있다.

본 발표에서는 기밀성과 무결성, 인증/인가, 프라이버시 보호, 키 관리, 전자지갑 등, 최근 다양한 응용 분야 보안의 근간이 되는 하드웨어 보안 기술의 구조와 원리, 구현 방법, 취약성 사례를 살펴본다. 즉, HSM(Hardware Security Module), TPM(Trusted Platform Module), PUF(Physically Unclonable Function)의 구조와 특성, 그리고 최근 공개된 하드웨어 보안 취약성(Meltdown 취약성) 등을 자세히 살펴본다.

IoT 디바이스 하드웨어 보안 취약성 및 보안 기술
- Meltdown 취약성 및 디바이스 보안 기술 -
부산대학교
김호원 교수
2018.4.13
부산대학교 PUSAN NATIONAL UNIVERSITY


목차
목차
IoT 디바이스 하드웨어 보안 취약성 및 보안 기술
I. IoT 디바이스 보안 개요
• 특성 및 보안 요구 사항
II. 디바이스 보안 취약성
• 프로세서 개요
• Meltdown 취약성
III.IoT 디바이스 보안
• 경량 암호 기술(전통적 기법)
• PUF 기반 IoT 디바이스 보안
IV. Q&A
• 맺음말 및 Q&A
2
부산대학교 PUSAN NATIONAL UNIVERSITY

# I. IoT 디바이스 보안 개요

1. IoT 디바이스 특성 및 보안 요구 사항





## 1. IoT 디바이스 주요 특성 및 보안 요구 사항

### IoT 주요 특성

- 기본적으로 정보 센싱, 가공, 분석, 공유에 기반을 두고 있음
  - 정보를 센싱하는 디바이스와 수집된 정보를 가공/분석/활용하는 플랫폼/서비스로 구성됨
  - 외부 노출이 쉬워 물리적 공격, 네트워크 공격이 용이하며, 프라이버시 침해 가능성 높음
- 다양하고 복잡한 요소로 구성됨
  - 디바이스, 통신/네트워크, 플랫폼, API, 서비스,LOD, API, 오픈소스 SW/패키지 활용 등
  - 다양한 보안 취약성 존재
- 환경에 대한 물리적인 제어 수행
  - 사용자 생명에도 영향을 주는 보안 취약성

### IoT 발전으로 인해 더욱 중요해지는 보안 이슈

- 사물의 지능화 및 대상 사물 확대
  - 지능화된 사물에 의한 자율적 상황 학습 및 제어(Sensor & Actuator :Autonomous Control) → 디바이스 보안 취약성 해결, embedded system 보안, 프라이버시 침해 문제, 인증/인가, 권한제어/접근제어 중요성 증대
- LOD, SNS 데이터와의 통합(서비스 Mashup, Horizontal 서비스)
  - 다양한 주체의 데이터/정보 활용 신규 서비스 개발. 외부 LOD/SNS 데이터 활용 확대 → API보안, Mashup 보안, 인증/인가, 권한제어/접근제어, 프라이버시 보호 중요성 증대
- 사람/사물/서비스의 초연결 특성(Hyperconnectivity)
  - 다양한 이기종 프로토콜/네트워킹/데이터 공유 기술 사용으로 인한 보안정합/보안 취약성 유발, Data Analytics를 통한 지식 추출/활용 → 프라이버시 보호(자기정보통제권), 통신/네트워크 프로토콜 보안/정합 중요성 증대

참고) Securing the Internet of Things by Paul Fremantle, Paul Madsen

## 1. IoT 디바이스 주요 특성 및 보안 요구 사항

### IoT 디바이스 보안성 유지의 어려움

- 공격자에게 노출되기 쉬운 환경에 deploy 됨
  - 공격자에게 노출되기 쉬운 센서 디바이스 (환경센서, 스마트미터 등)
  - 낮은 visibility (사용자 interface가 좋지 않음. No UI, it's a thing !)
  - Reversing을 통한 취약성 파악, Side channel 공격이 용이함
  - Chip Cloning, Chip Reversing, ROM Code 추출, key/password 값 추출 용이함
- 높은 자원 제약성 및 Low cost 요구로 인한 높은 보안성 제공 어려움
  - 제한적 연산 능력 보유(resource constraints: 기존 보안기술/crypto/SSL 적용의 어려움)
  - Secure OS 적용 및 HSM(Hardware Security Module), PUF 등 적용의 어려움
- Firmware 보안 유지의 어려움
  - SW 업데이트 및 관리의 어려움 (터널내 센서, 교량 설치 센서 등)
  - 불안정한 통신/네트워크 환경으로 인한 최신 보안성 제공의 어려움 등

참고) Securing the Internet of Things by Paul Fremantle, Paul Madsen





## 1. IoT 디바이스 주요 특성 및 보안 요구 사항

### 사물인터넷 디바이스 보안 요구 사항

- 하드웨어 구조적인 보안성 제공 필요
  - Meltdown 공격은 칩 동작 성능 고속화에서 사용하는 기법(superscalar, speculative execution의 취약성을 활용함)
- Tamper resistance 기술/Tamper Evidence 필요
  - Clone detection (PUF 기술 등)
  - Key zeroisation 기술 등
- Side channel attack countermeasure 필요
  - SPA/DPA/CPA attack countermeasure (Random Masking 기법 등)
- 인증/인가 기술 필요
  - Secret credential, Certificate (X.509 기반 등) 사용 등
- 접근 제어 기술 필요
  - Access Control (ACL, RBAC, etc.)
  - Memory protection, Secure OS 등
- Code Integrity 보장 기술 필요
  - Hash value, MIC(Message Integrity Code) 등

# II. 디바이스 보안 취약성

## 1. Meltdown 보안 취약성

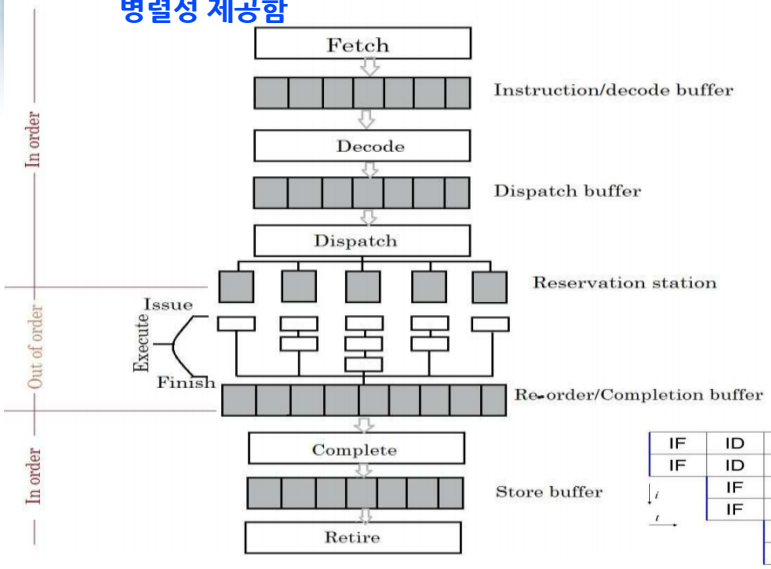


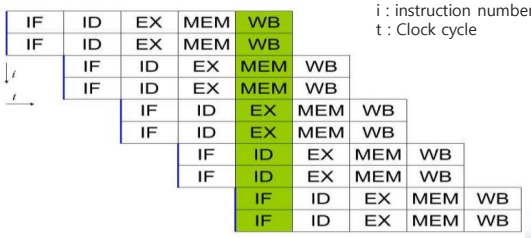


## 2.1 프로세서 개요

### 수퍼스칼라 프로세서(Superscalar Processor)

- Instruction level parallelism을 활용하여 프로세서를 고성능화하는 기법
- 실행 유닛(정수연산, 실수연산, 메모리 접근 등)을 복수개를 사용하여 명령어 수준의 병렬성 제공함



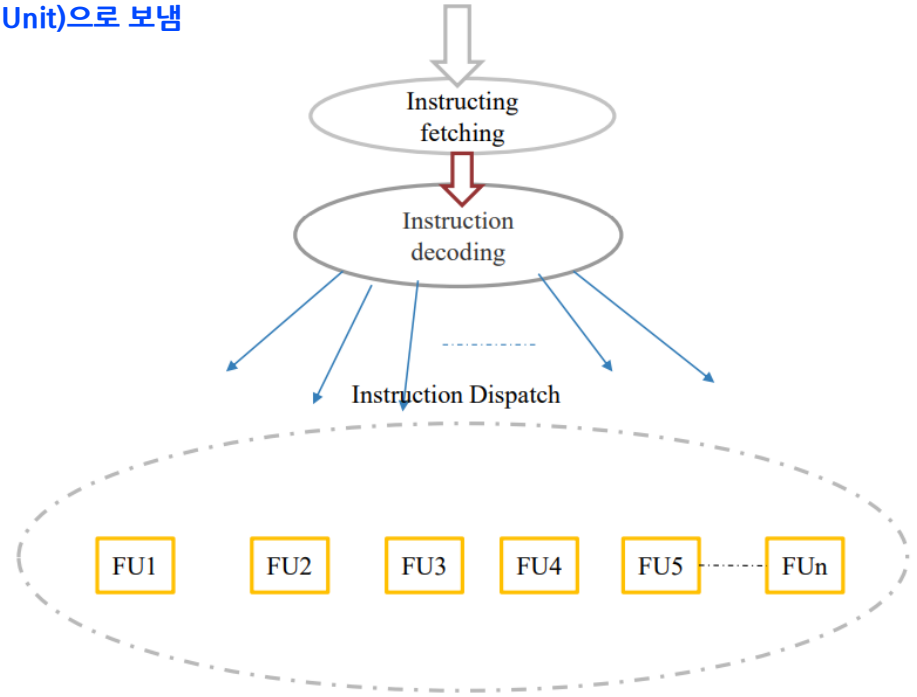



## 2.1 프로세서 개요



### Instruction Dispatch

- Super Scalar 프로세서에서는 디코딩된 명령어를 적절한 실행 유닛(Functional Unit)으로 보냄



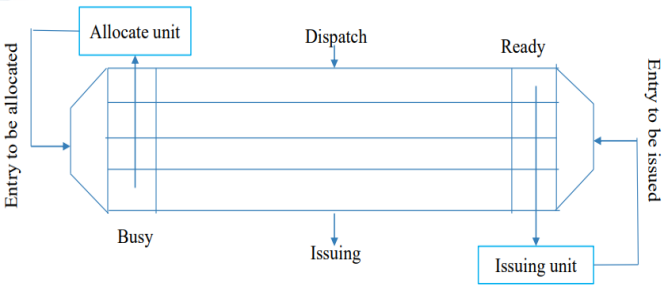


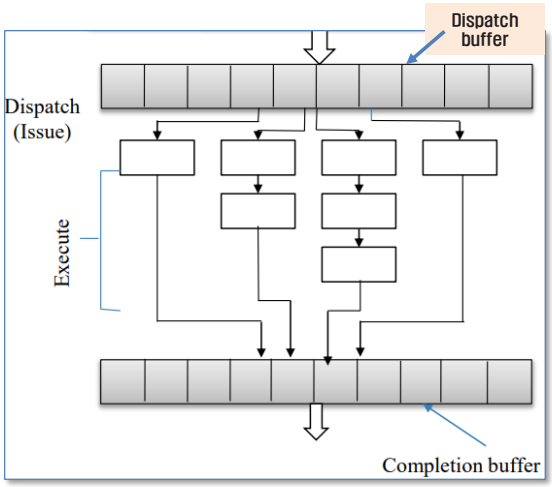

## 2.1 프로세서 개요



### Reservation Station

- 고성능화를 위해 명령어의 fetch/decoding 순서와 실제 실행 순서는 다르게 할 수 있음(in-order vs. out-of-order execution)
- Reservation station에선 instruction decoding과 instruction execution이 decouple됨

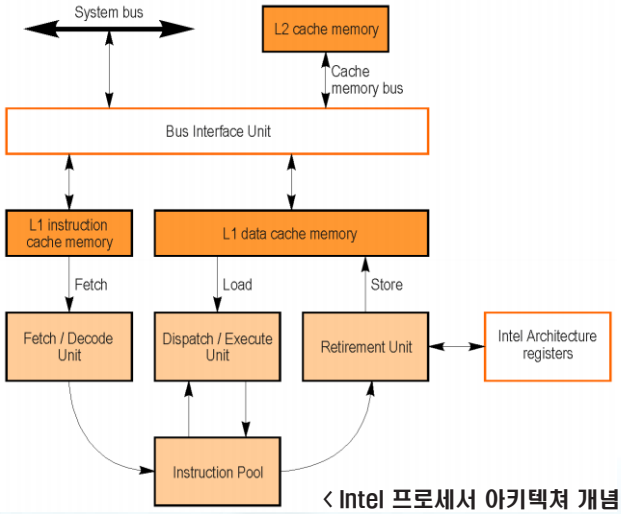


## 2.1 프로세서 개요

### Instruction completion & Retire

- Completion
  - Execution이 완료되어 machine state를 update하는 것
  - Interrupt가 발생하면, completion 결과는 더 이상 유효하지 않음
- Retire:
  - Speculatively 실행된 microoperation 결과를 user-visible한 registe에 쓴 후, reorder buffer상의 microoperation을 제거




< Intel 프로세서 아키텍쳐 개념도 >





## 2.1 프로세서 개요

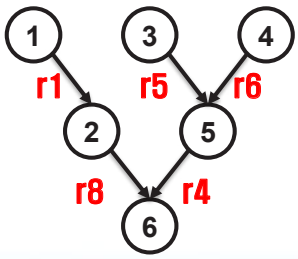
### OOO(Out of order) Execution

- 비순차적 명령어 처리는 고성능 마이크로프로세서가 특정한 종류의 지연으로 인해 낭비될 수 있는 명령 사이클을 이용하는 방법이다.

**Example Instruction**

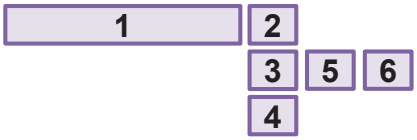
1) r1 ← r4 / r7
2) r8 ← r1 + r2
3) r5 ← r5 + 1
4) r6 ← r6 − r3
5) r4 ← r5 + r6
6) r7 ← r8 * r4

**Data Flow Graph**

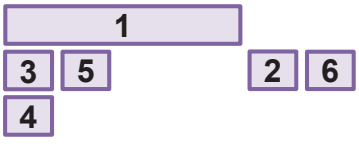



**In-order execution**

**In-order execution (superscalar 3)**



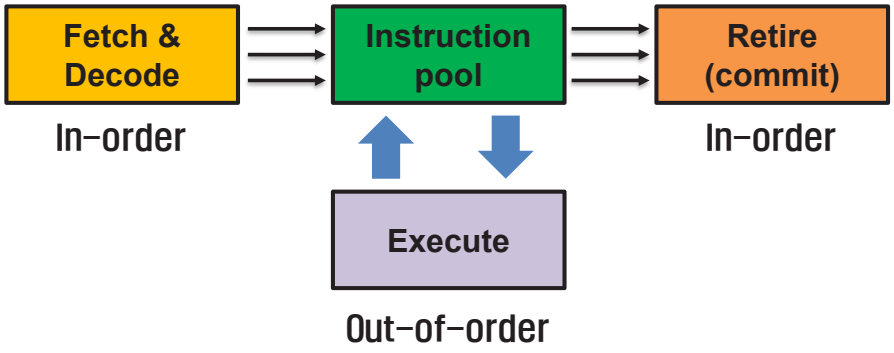

**Out-of-order execution**



## 2.1 프로세서 개요

### OOO(Out of order) Execution

- 기본 개념도




참고) Securing the Internet of Things by Paul Fremantle, Paul Madsen





## 2.1 프로세서 개요

### Speculative Execution

- 조건 분기 예측 및 예측된 path를 사전에 실행함
- 1. Each entry is extended to include a speculative status field
  - indicating whether the corresponding instruction has been executed speculatively
- 2. speculatively executed instruction are not allow to retire
  - before the related condition is resolved
- 3. After the related condition is resolved,
  - if the guess turn out to be right, the instruction can retire in order.
  - if the guess is wrong, the speculative instructions are marked to be cancelled.
    Then, instruction execution continue with the correct instructions.

## 2.2. Meltdown



### CVE-2017-5754 : Meltdown

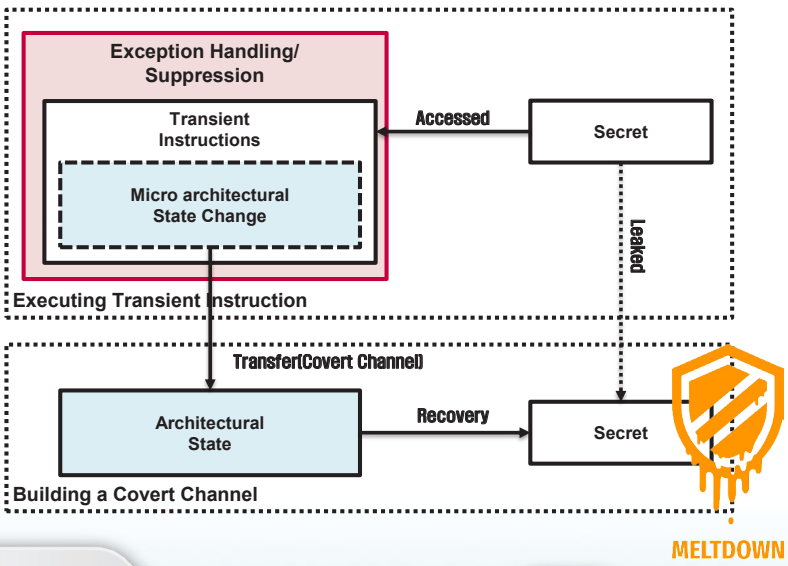
- 비 순차적 명령어 처리(OoOE) 기술을 악용한 보안 취약점.
- 사용자 응용프로그램과 운영 체제간의 기본적인 격리 구조를 파괴함에 따라, 프로그램이 다른 프로그램과 운영체제의 메모리, 비밀정보에 엑세스 할 수 있게함.
- 마이크로 프로세서의 취약성을 이용함에 따라, 가상화를 통해 보호되던 클라우드 컴퓨팅 환경에서도 이런 보안을 부수고 다른 프로그램에 접근이 가능해짐.
- Intel 뿐 아니라 POWER CPU, ARM Processor 까지 영향을 줌.
- 하드웨어 구조의 문제로 소프트웨어 패치로는 근원적인 해결이 될 수 없음.

## 2.2 Meltdown



### Basic Concept

- 비 순차적 명령어 처리(OoOE) 기술을 악용한 보안 취약점.



## 2.2 Meltdown

### Exploit

- Meltdown Attack Code

Exception 발생

```
1.  ; rcx = kernel address
2.  ; rbx = probe array
3.  retry:
4.      mov al, byte [rcx]          // move a byte to %al (%rcx)
5.      shl rax, 0xc                // multiply by 4096 ( << 12)
6.      jz retry                    // retry if byte was 0**
7.      mov rbx, qword [rbx + rax]          // access probe_array[%al * 4096]
```

speculative

Pagesize





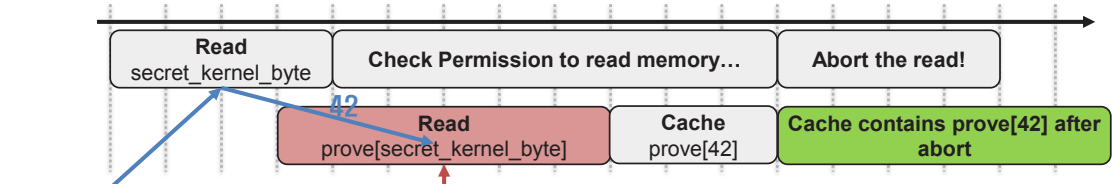
## 2.2 Meltdown

### Exploit

- Meltdown Attack Code

If the probe array access wins the race, a cache line is loaded from memory. The line to load is determined by the value of the illegal load (byte %al) and uses %rax before it is zeroed by the exception

```
1.  ; rcx = kernel address
2.  ; rbx = probe array
3.  retry:
4.      mov al, byte [rcx]          // Exception 발생
5.      shl rax, 0xc                // 하지만 5-7번 코드는 실행이 됨.
6.      jz retry                    // speculatively
7.      mov rbx, qword [rbx + rax]          // Races with Exception
```

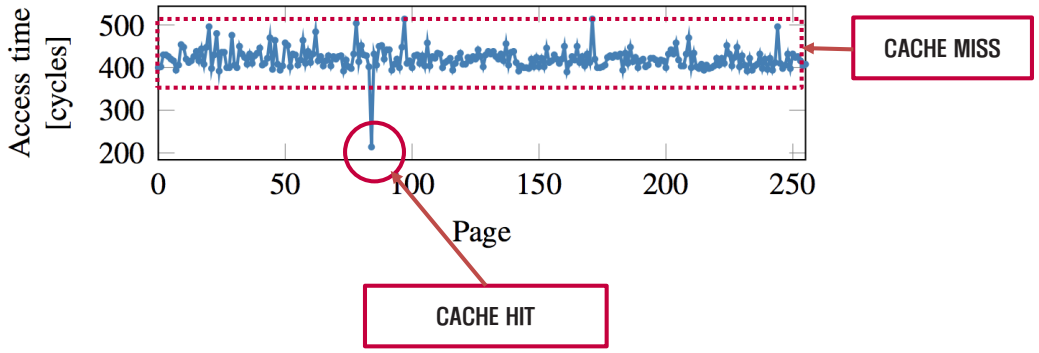



Assume 42

Meltdown 공격의 핵심 부분
It is possible to Speculatively read memory without permission

## 2.2 Meltdown

- Exploit
  - Meltdown Recovery
  - Probe array에서 데이터를 읽으며 Access Time 측정
  - CACHE HIT된 부분의 주소 값 = Kernel에서 읽어온 데이터 값







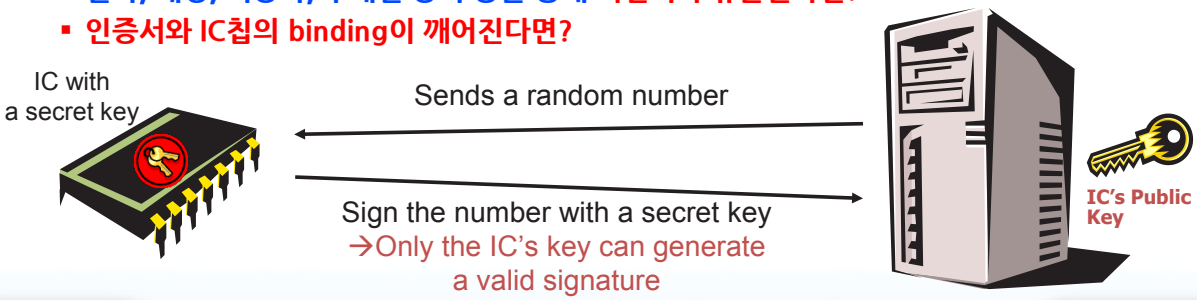

# III. IoT 디바이스 보안

1. 경량 암호 기술 (전통적인 기법)
2. PUF 기반 IoT 디바이스 보안

## 3.1 전통적인 인증 방법



- 각 IC칩은 유일성(uniqueness)를 제공할 필요가 있음
  - 일반적으로 non-volatile memory에 비밀키 정보를 가짐으로써 이를 제공함
- 기존에는 IC 칩에 대한 인증을 위해 일반적으로 암호 알고리즘을 사용함
  - 서명에 대한 검증(공개키 암호), 비밀키 기반의 Challenge-Response를 통해, 디바이스에 대한 인증을 수행함
    - A verifier sends a randomly chosen number
    - An IC signs the number using its secret key so that the verifier can ensure that the IC possesses the secret key
- 이러한 암호 알고리즘 기반 인증 및 유일성 제공을 위해선 비밀키 정보(Secret key) 혹은 인증서 등이 필요함
  - 만약, 해킹, 역공학, 부채널 공격 등을 통해 비밀키가 유출된다면?
  - 인증서와 IC칩의 binding이 깨어진다면?






## 3.2 IoT 디바이스 보안 - PUF

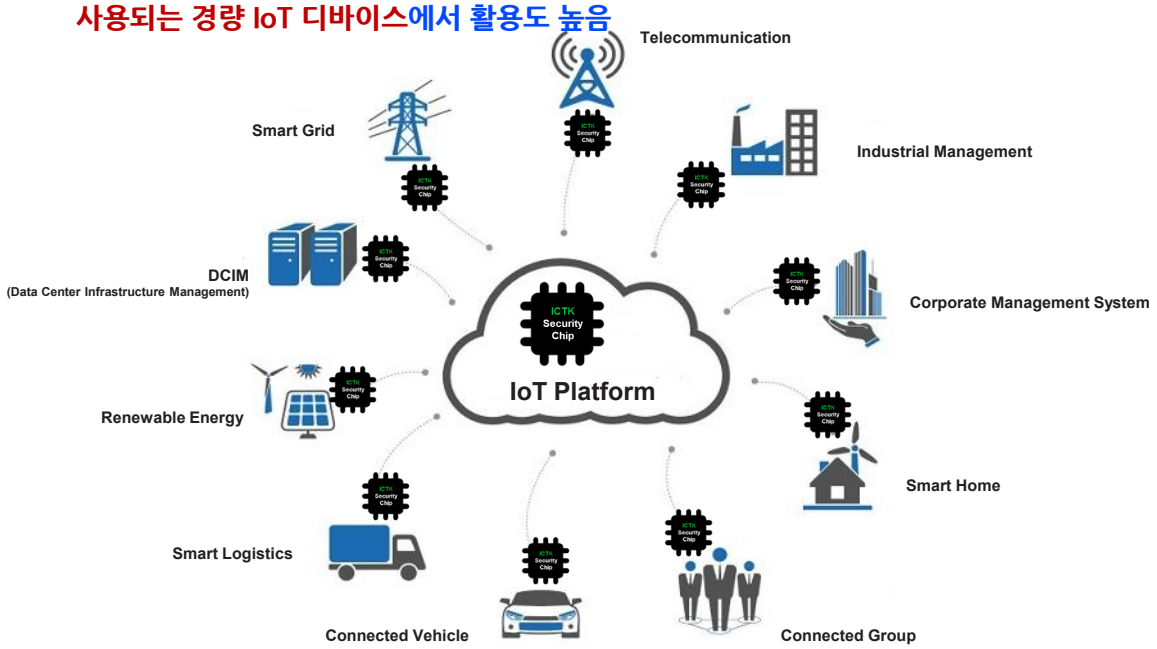


- 전통적인 암호학적 기법의 안전성은 비밀키 안전성에 의존
  - 비밀키 유출, 복제(cloning) 등에 대해서는 제한적인 기능을 가짐 → PUF 기술 출현
- PUF (Physically Unclonable Function) 기술
  - 디지털 시스템에 대한 cloning 공격과 같은 physical 공격을 방지하기 위한 기술로서 physical random function으로 불리기도 함
    - 디바이스에 유일한 난수성을 이용하므로 복제가 매우 어려운 Master key(secret key)를 가짐
    - Chip 해킹을 통한 Key 탈취가 매우 어려움
    - PUF 키와 암호 알고리즘을 결합하여 안전한 Root of Trust 역할
    - 디바이스에 대한 유일성 제공(fingerprint) 역할(폐기/갱신 가능한 지문)
- PUF의 특성
  - Physical system의 특성에 의존함
    - wire delay, gate delay, quantum mechanical fluctuations, electro-migration, etc.
  - Evaluation이 용이하고 reliable해야 함
  - 출력값은 Random 특성을 가져야 함
    - Unpredictability
    - Difficulty of modeling
  - Physical access 공격에도 안전해야 함
    - Tamper resistance

## 3.2 IoT 디바이스 보안 - PUF

### PUF 응용 분야: 경량 IoT 디바이스 보안

- 스마트그리드 보안, 드론 보안, 물류 디바이스, 자동차 부품 등 해커에 노출된 환경에서 사용되는 경량 IoT 디바이스에서 활용도 높음




참고) ㈜ICTK 발표자료, 김동현 대표





## 3.2 IoT 디바이스 보안 - PUF

### Weak vs Strong PUFs

**Weak PUFs**

- Use cases
  - New form of key storage

- No challenge, just response
- Responses remain internal
  - Perfect internal error correction
- Attacks
  - Cloning and invasive reading of responses

**Strong PUFs**

- Use cases
  - New cryptographic primitive

- Many challenge-response pairs
- Public CRP interface
  - Error correction outside PUF is possible
- Attacks
  - Modeling attacks and protocol attacks

## 3.2 IoT 디바이스 보안 - Arbiter 기반 PUF

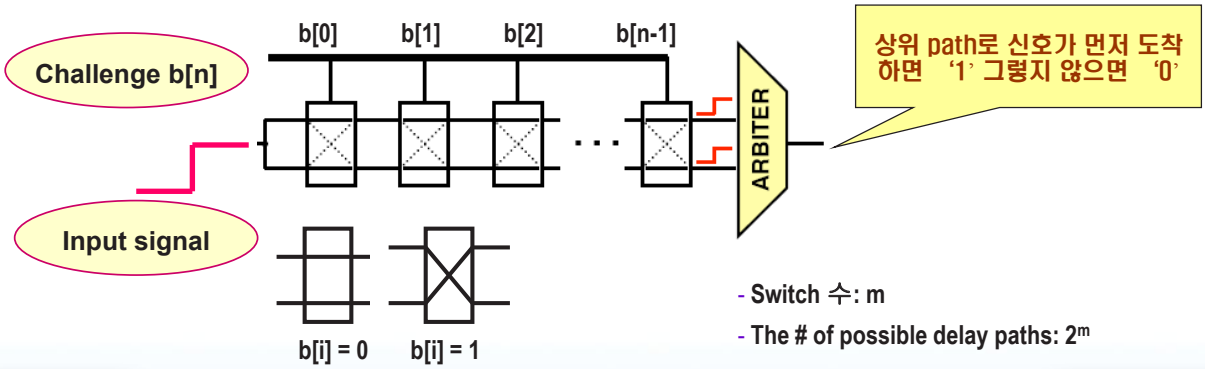


### 실리콘 공정 기술을 사용한 PUF 기술

- 공정상의 특성으로 인해 완벽히 동일한 회로가 존재하지 않는 특성 응용

### 실리콘 PUF 기술 (예: Arbiter based PUF)

- 각 challenge 값은 각 스위칭 회로의 path를 결정함
- 동일한 "input signal"은 각 path를 따라 racing 수행(path 설정에 따라 delay 변화 생김)
- Arbiter 입력 부분에 먼저 도착하는 신호의 path에 따라 출력값 결정

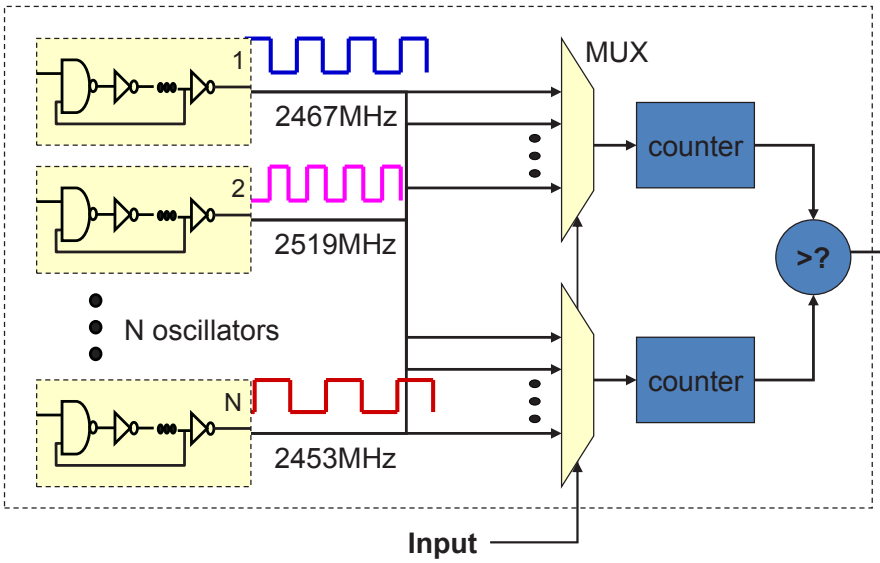





## 3.2 IoT 디바이스 보안 - Ring Oscillator 기반 PUF



### Ring Oscillator 기반의 PUF 사례




| Top | Bot. | Out |
|---|---|---|
| 1 | 2 | |
| | | |
| | | |

*Compare frequencies of two oscillators → The faster oscillator is randomly determined by manufacturing variations*

## 3.2 IoT 디바이스 보안 - PUF

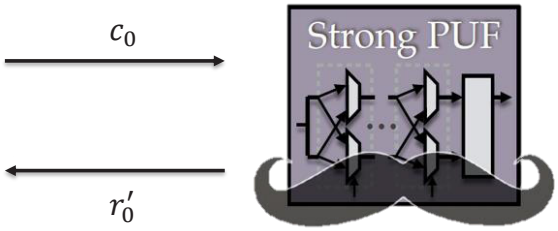
### Authentication using Strong PUF

Enroll PUF

- Choose random challenges
- Apply and store private CRPs

Authenticate

$r_0 \approx r_0' ?$




*Responses can be public if PUF resists modeling*



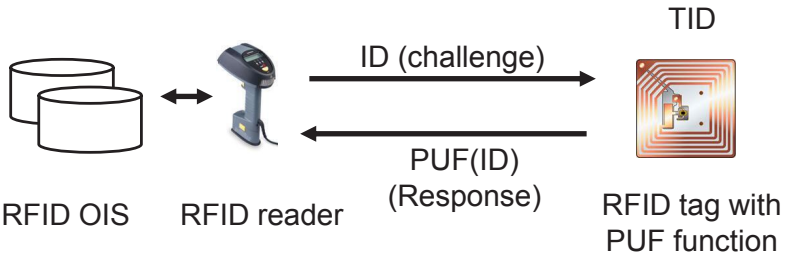


## 3.2 IoT 디바이스 보안 - PUF

### Challenge-Response를 통한 cloning 여부 확인

- 특정 태그(TID 혹은 code 값으로 구분)의 PUF 함수에 대한 challenge/response 값을 RFID back-end system에 미리 저장
- 안전하게 저장된 challenge 값을 tag에 query하여, 저장된 response 값과 비교하여 cloning 여부 확인
- PUF의 안전성에 의존함
  - reliability, no loops in PUF chains, no identical PUF outputs, tamper resistance
  - Eavesdropping, replay attack 등을 방지하기 위해 cloning 확인 protocol 변형 가능

| EPC | Challenge/Response list |
|---|---|
| 00E1 | 5423/6895 4235/6566 ... |
| 00E3 | 8553/7045 6784/9033 ... |
| 00FA | 9443/4555 3224/1247 ... |
| 00EE | 4455/8629 3557/3894 ... |



## 3.2 IoT 디바이스 보안 - PUF

### Power-up State PUF as Secret Key

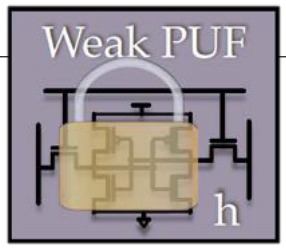
**Enroll PUF at Manufacture**

- Learn response r
- Choose key k and derive public helper data h:
  $h = \mathrm{Encode}(k) \oplus r$
- Store h with PUF
- Disable access to response r

**Generate Key in Field**

- Measure $r' \oplus h$
- Key k : Decode$(r' \oplus h)$

K is reliable key




*Reliable unclonable key for crypto*
*Assumes that r cannot be read in field*

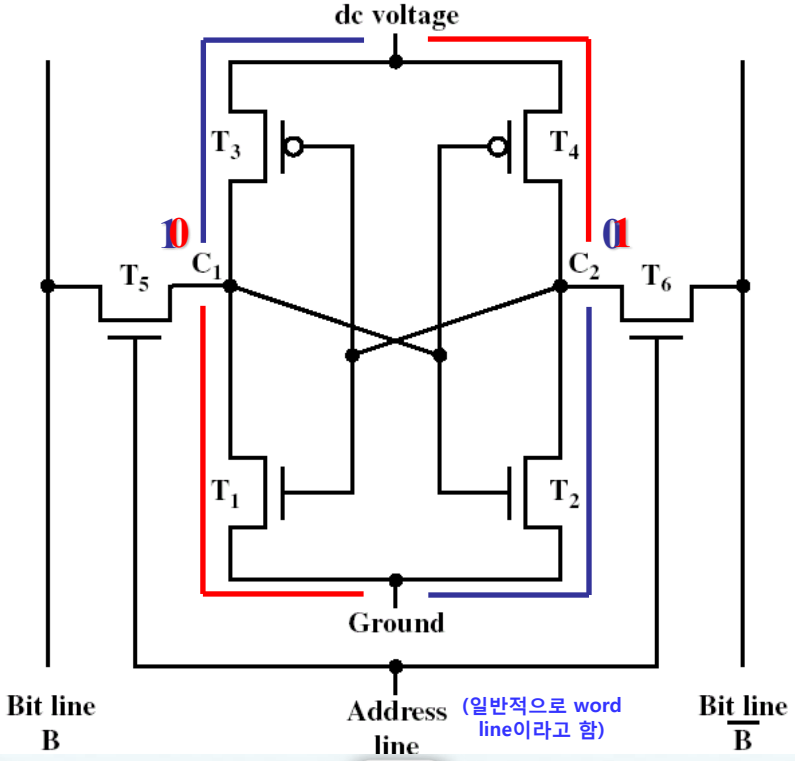
Code offset construction
[Dodis et al. '08]





## 3.2 IoT 디바이스 보안 - SRAM 기반 PUF

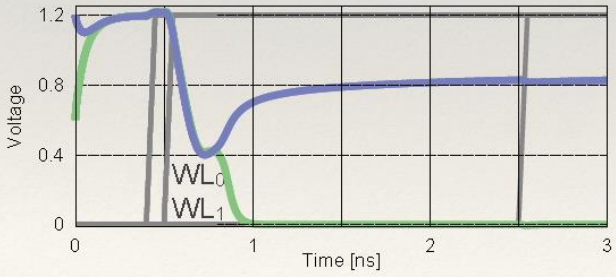
### SRAM의 bistable한 상태를 이용한 PUF

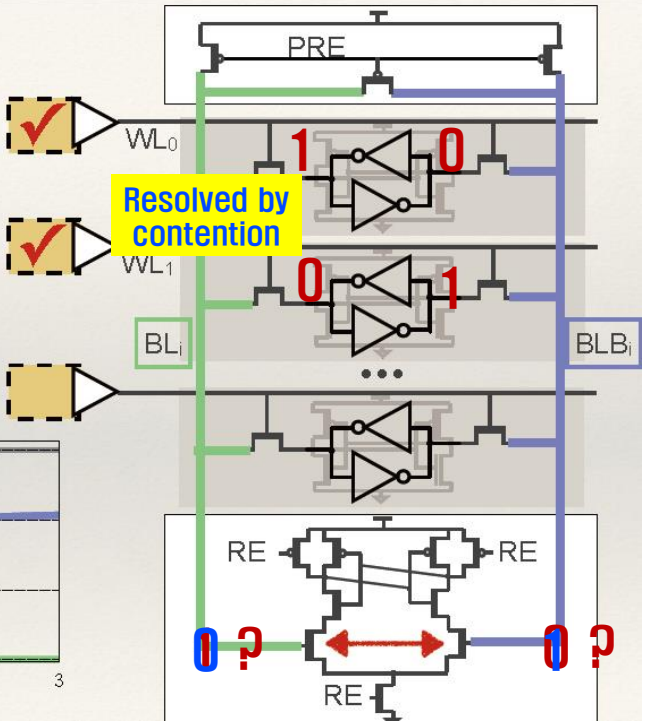


## 3.2 IoT 디바이스 보안 - SRAM 기반 PUF



- Read with contention
- Contention resolves according to variation
- Largely consistent over time for given column



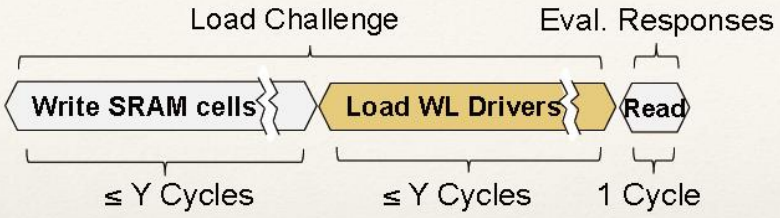



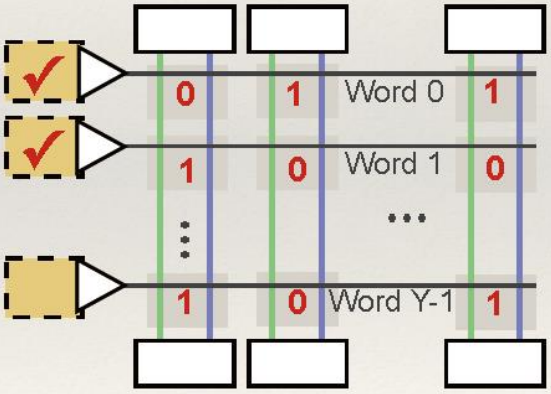



## 3.2 IoT 디바이스 보안 - SRAM 기반 PUF



■ SRAM 기반 PUF는 **기존 SRAM 활용** 가능하며, 셀에 **특정 값 설정이 가능**하여 응용 가능성 높음



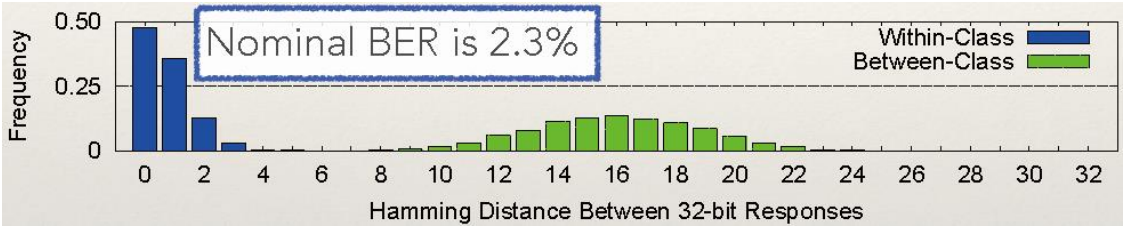



## 3.2 IoT 디바이스 보안 - SRAM 기반 PUF



### PUF의 보안 특성

- Uniqueness(유일성)
  - Between-class difference는 표현 비트수의 ½만큼 출력 비트 차이를 가지면 좋음
  - 디바이스 사이 의존성 없음. 디바이스간 높은 독립성 가짐
- Reliability(신뢰성)
  - Within-class difference는 0에 가까울 수록 좋음
  - 즉, 동일한 PUF는 안정적인 challenge-response 값을 가짐






## 3.2 IoT 디바이스 보안 - PUF 응용



### 물리적으로 공격당해도 비밀키 노출이 되면 안되는 응용 분야에 적합

- 드론, 전력 시스템 부품, 군용 장비, 원전 시스템 주요 장비 등, 국가 주요 인프라에 활용
- 가전 제품, 의료 용품 등, 불법 복제 유혹이 많은 분야에 적합

### PUF 자체에 대한 공격 기법

- Machine Learning을 이용한 모델링 공격
- Fuzzy Extractor에 대한 부채널 분석 공격
- EM 공격을 통한 RO PUF 모델링 공격 등 Strong PUF에 대한 다양한 공격 가능함(Weak PUF로 활용하는 것이 좋음)

# IV. 맺음말 및 Q&A

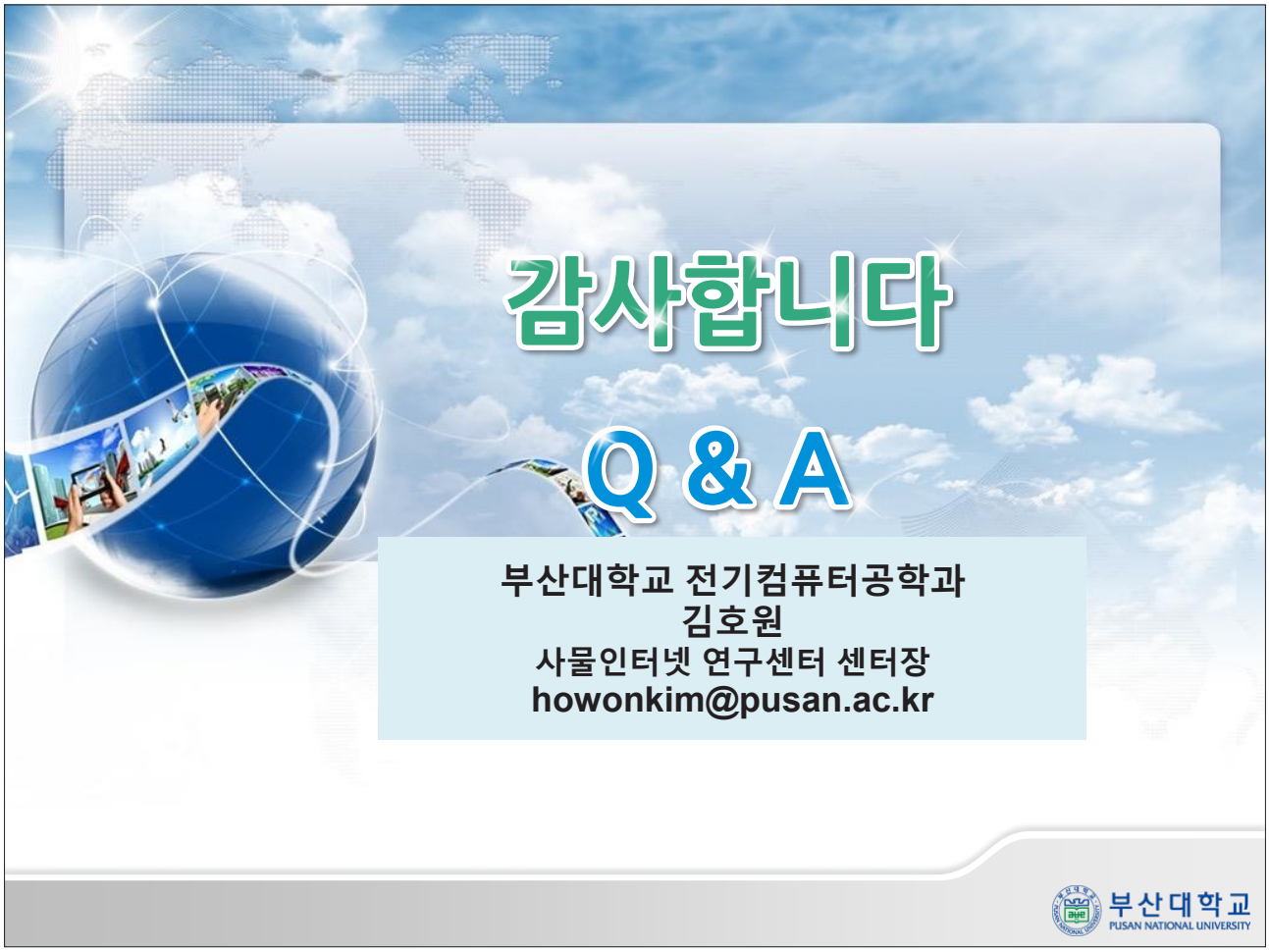
1. 맺음말 및 Q&A





## 4.1 맺음말 및 Q&A

- IoT 디바이스는 다양한 공격 취약성을 가짐
  - 공격자에게 노출되기 쉬운 환경에 설치되고 높은 자원 제약성, 그리고 Firmware 업데이트 등, 다양한 취약성을 가짐
    - 특히 최근에는 하드웨어적인 특성(speculative execution, super-scalar architecture)에 기인한 원천적인 보안 취약성도 존재
    - 또한, 낮은 가시성과 Reversing 및 Side channel 공격, Code 추출, key/password 추출은 IoT 디바이스의 근본적인 보안 취약성임
  - 이에, 하드웨어 구조 자체에 대한 보안성 강화, Secure HW를 통한 Security Anchor 기능 제공, OS 보안성 강화, 물리적 복제 탐지/방지, Tamper Resistance/Evidence는 안전하고 신뢰할 수 있는 IoT를 위해 필요한 요소임




## 참고 문헌

[1] SRAM-based Physical Unclonable Functions by Daniel E. Holcomb, 2015
[2] TS0003, Security in oneM2M
[3] PUF 보안 칩과 활용 사례, ㈜ICTK, 2016.8
[4] Superscalar Processor by Manash Kumar Mondal, M.Tech, CSE
[5] Meltdown by Moritz Lipp, et.al, http://arxiv.org/pdf/

The 24th Network Security Conference -Korea

# IoT용 디바이스를 위한 보안 SoC의 활용 방안

**김동규** 한양대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1986 ~ 1992 | 서울대학교 컴퓨터공학부 학사 졸업 |
| 1992 ~ 1994 | 서울대학교 컴퓨터공학부 석사 졸업 |
| 1994 ~ 1999 | 서울대학교 컴퓨터공학부 박사 졸업 |
| 1999 ~ 2006 | 부산대학교 정보컴퓨터공학부 조교수 |
| 2006 ~ 현재 | 한양대학교 융합전자공학부 정교수 |

### 강연요약

IoT의 디바이스들은 낮은 단가, 저전력 등의 요구조건을 만족해야 하므로, 보안시스템을 구축하기 위해서는 기존 서버/클라이언트 환경과는 다른 개념의 적용이 필요하다. IoT용 디바이스 상에서 MCU core가 내장된 프로세서에서 software로 보안시스템을 구축할 경우, 앞서 언급한 여러 요구조건을 만족하기 힘든 상황이다.

이를 위하여 SoC 형태의 전용 하드웨어 칩으로 보안 시스템을 구축하는 것이 매우 효율적이다. 보안 전용칩에서는 인증에 필요한 암호 key의 안전한 사용과 저장이 보장되어야 하는데, 이를 위한 단순한 형태의 모듈로 활용되는 기술이 PUF(Physical Unclonable Function) 기술이다.

본 강연에서는 IoT용 디바이스들의 보안을 강화하기 위한 보안 하드웨어 칩의 활용 방안과 현황에 대하여 설명하고자 한다. 먼저 PUF 기술이 내장된 SoC 형태의 칩과 응용분야를 설명하고, 현재 중국등의 IoT업체들이 어떤 응용시스템에 적용하고 있는지의 현황을 설명하고자 한다.

# IoT용 디바이스를 위한 보안 SoC의 활용방안

NETSEC-KR (2018)

Dong Kyue Kim
(DQKIM@hanyang.ac.kr)
Dept. of Electronic Eng., Hanyang Univ.
2018. 4. 13

EMBEDDED SECURITY SYSTEM LABORATORY
HANYANG UNIVERSITY

## Contents

EMBEDDED SECURITY SYSTEM LABORATORY

[TOPIC 1] IoT 보안의 필요성 및 요구사항
- IoT 보안의 필요성
- IoT 보안 요구사항

[TOPIC 2] 보안 SoC(System on Chip)를 위한 PUF 기술
- PUF 기반 키 관리
- PUF 응용 시스템

[TOPIC 3] IoT 용 보안 SoC 사업화 현황
- 제품 군
- 적용 사례

EMBEDDED SECURITY SYSTEM LABORATORY

# IoT 보안의 필요성 및 요구사항



EMBEDDED SECURITY SYSTEM LABORATORY

## IoT 보안의 필요성

- IoT 시장의 폭발적인 성장
  - 2017년 84억개, 2020년 204억개의 IoT Device 예측 – 가트너/2017년
  - 70% 이상의 IoT Device는 암호화 되지 않은 상태로 사용됨 – HP/2015년
- 보안 문제
  - 기하 급수적인 Device의 증가로 인해 예측할 수 없는 보안 문제 초래 예상
  - IoT 보안 문제가 기기 구입에 장벽 (47% 응답) – Accenture 설문(2015년)

*"Internet of Insecure Things"*

*"IoT could be a "Plug & Pray" case*

EMBEDDED SECURITY SYSTEM LABORATORY

## IoT Trend

### 시장 현황

- H/W↔S/W를 아우르는 IoT Platform 경쟁 심화
  - H/W, S/W 지배력을 기반으로 플랫폼 경쟁

〈구글〉 〈애플〉 〈Microsoft〉 〈삼성〉

  - 계층별 Open Platform 체계화

〈H/W Platform〉

- IoT End-Point 보안 기술
  - IP 카메라 해킹 등 보안 사고 다수 발생
  - H/W 보안성 강조
    - IoT 보안 IC : STmicro, Infineon 등
    - H/W 기반 기기 인증, S/W 보호
  - 키 관리, 인증, 보안 관리 등 Turn-key 보안 솔루션

〈IP 카메라 해킹 사고〉

- IoT SoC 통합화 가속
  - 제어, 통신, 보안 통합 SoC
  - 글로벌 대형 업체 위주
  - 외산 SoC 의존도 매우 높음

〈리얼텍,대만〉 〈퀄컴,미국〉 〈TI,미국〉

### 발전 방향

기기별 ID를 기반으로 하는 사물인터넷 플랫폼

- Open 플랫폼 연동
  - 표준 연동
- 계층별 보안성 확보 (보안 SoC, 디바이스, 서버)
  - H/W 보안 기술
  - 서버 인프라 보안 기능 개발
  - Root-of Trust 기능
- 기술 내재화
  - 해외 기술 의존도 최소화
  - 국산 암호 알고리즘 적용



EMBEDDED SECURITY SYSTEM LABORATORY

## IOT 보안 문제 사례 (1)

- SmartThings Zigbee 표준 보안문제 (2015년 8월)
  - 보안업체 Cognosec의 T.Zillner가 Black Hat 2015에서 발표
  - Zigbee 통신 표준이 갖는 취약점을 이용하여 Key 탈취
    - 대부분의 Zigbee Device가 Default Key를 사용하거나 F/W로부터 쉽게 Key를 알아낼 수 있음.
    - Key 교환 과정을 Sniffing 하여 Key 탈취
  - 사용자가 알지 못하게 Doorlock 해제가 가능

EMBEDDED SECURITY SYSTEM LABORATORY

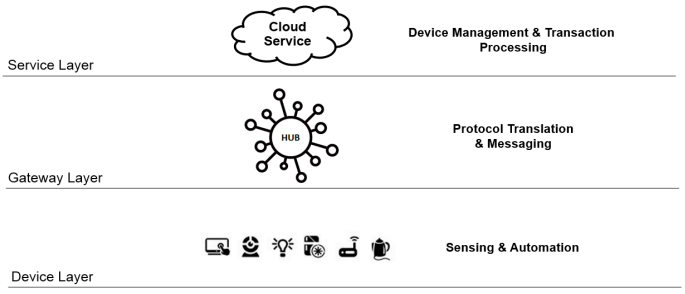
## 보안 문제 사례 (2)

- IP Camera 해킹
  - 중국 성인 사이트 Upload (JTBC, 2017.4월)
    - 한국 가정에서 사용하는 IP Camera를 해킹 & 영상 Upload

EMBEDDED SECURITY SYSTEM LABORATORY

## 해킹 사례로 분석한 보안 문제

- 사용성, 상호 연동성만을 강조하는 것은 전체 보안 수준을 크게 저하시킴
- 표준을 준수하는 것이 모든 보안을 보장하지 않음
- IoT 보안은 단일 계층의 보안 강화로 달성할 수 없음
  - 디바이스, 통신 네트워크, 플랫폼/서비스 등 모든 계층이 공격 대상
  - 상대적으로 보안이 취약한 Embedded 디바이스에 대한 공격 연구 활발



EMBEDDED SECURITY SYSTEM LABORATORY

## IoT 보안 요구사항

- IoT 센서/노드 단에서의 데이터를 토대로 빅 데이터로 분석 되는데,
  - 과연 IoT 센서/노드단에서의 보안은 ?
  - 과연 콘트롤의 주체는 ?

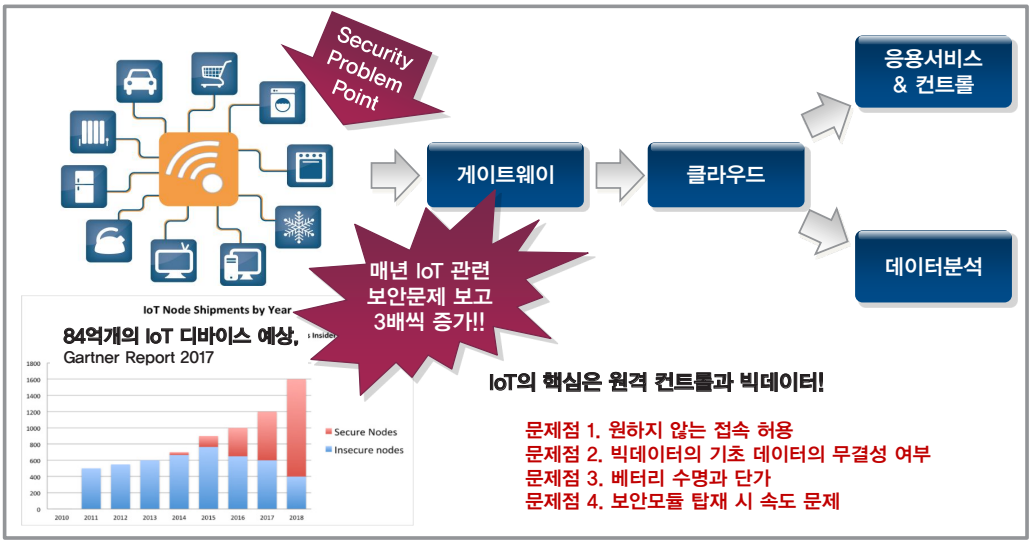


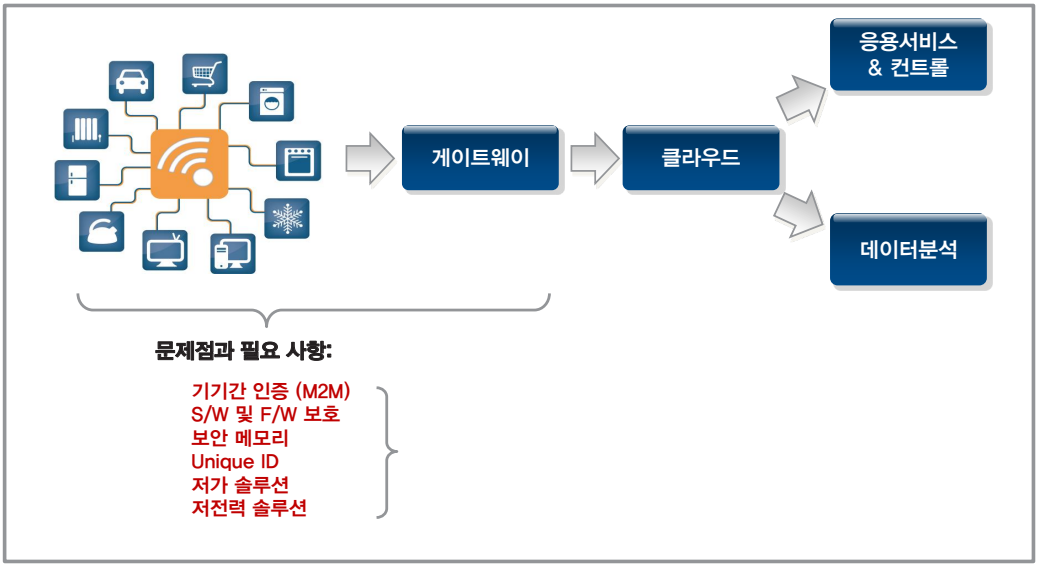

Image source: Citrix



EMBEDDED SECURITY SYSTEM LABORATORY

## IoT 보안 해결방안

- ICTK의 PUF 기반의 보안 솔루션은 IoT에 필요한 요소인 저가, 저전력에 알맞은 가볍고 간단하나 보안성이 높은 구조임



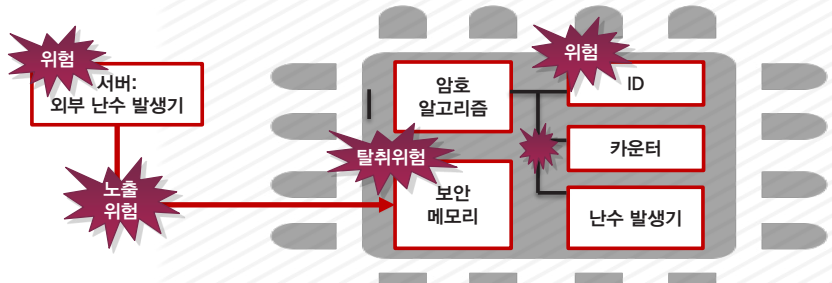
# IoT 보안을 위한 SoC(System on Chip)

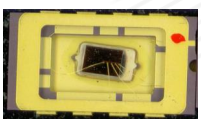




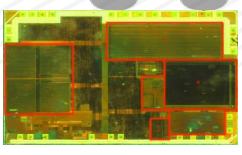
## H/W Chip 해킹 기술 진화

- 인증의 시작인 Seed Key 생성이 외부에서부터, 보관은 복제 가능한 S/W 형태로 있어 해킹에 취약함

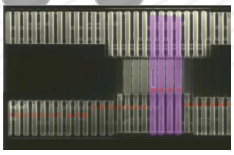


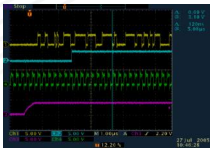
Chip Decapsulation Attack



Chip Architecture Analysis



Core & Bus Search & Analysis



Probing to Data Collection & Analysis

EMBEDDED SECURITY SYSTEM LABORATORY

## 보안 트렌드의 변화: ID 및 키 관리 기술

- 하지만 기존의 H/W 보안 역시 Private Key 관리 위험이 존재하며, 새로운 해결방안이 필요함

"S/W Key에서 H/W Key로"

* Source : Globalplatform

| Only Software | Software and Hardware | Software and Tamper resistant HW |
|---|---|---|
| Rich OS | TEE (Trusted Execution Environment) | SE (Secure Element) |
| *Pros*<br>• 다양한 운용 체제 | *Pros*<br>• 중간 수준의 보안 단계 | *Pros*<br>• 높은 수준의 보안<br>• 복잡한 보안 프로그램 불필요<br>• 효율적인 전력 소비<br>• 빠른 처리 속도 |
| *Cons*<br>• 낮은 수준의 보안 단계<br>• 암호화 개인 키 관리 위험 존재 | *Cons*<br>• 보안 알고리즘 복잡성<br>• 높은 전력 소비<br>• 느린 처리 속도<br>• 암호화 개인 키 관리 위험 존재 | *Cons*<br>• 암호화 개인 키 관리 위험 존재 |

WHAT'S NEXT?

Solution → PUF
Physical Unclonable Function



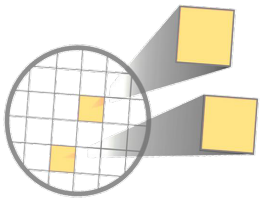
EMBEDDED SECURITY SYSTEM LABORATORY

## 해결점: 디바이스를 위한 생체(같은) ID PUF

사람은 생체 정보 등 복제 불가능한 ID를 가지고 태어나지만,

디바이스는 ID를 주입 받거나 메모리를 사용하여 복제가 가능한 현재의 문제점...

복제 불가능한 기기용 지문 필요!!



특성 1. 각 개체별 unique한 ID

특성 2. 복제가 불가능하여, 중복 제품 방지

특성 3. 안정적인 기술로, 환경에 바뀌지 않는 ID

PUF는 2001년 공식 명칭 부여 후 차세대 반도체 응용 보안 기술로 다양한 개발이 시도되며 시장이 형성됨

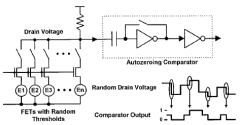
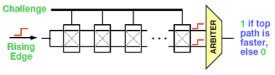
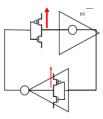
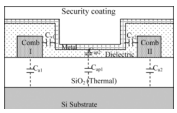
EMBEDDED SECURITY SYSTEM LABORATORY

# PUF(Physical Unclonable Functions)



EMBEDDED SECURITY SYSTEM LABORATORY

## The Previous PUFs and Commercialization

| Published year | Implementation method | Author Organization | Circuit layout | Reference (paper link) | Commercialization company |
|---|---|---|---|---|---|
| 2000 | Random drain voltage of CMOS | SiidTech, Portland State University |  | IEEE International Solid-State Circuits Conference | SiidTech → Hitachi ULSI |
| 2005 | Random difference of two delay path | MIT |  | IEEE Trans. On VLSI Systems | Verayo |
| 2007 | Random bit from unstable state of SRAM | Philips |  | international workshop on Cryptographic Hardware and Embedded Systems | Philips → Intrinsic ID |
| 2009 | Random capacitance value due to the coating layer | NXP semiconductors |  | IEEE Trans. on Semiconductor Manufacturing | NXP semiconductors |

- Problems of the PUFs
  - Non-permanent values, need for error correction → The root drawback
  - ECC(Error Correction Codes): Additional processes or complicated circuits

EMBEDDED SECURITY SYSTEM LABORATORY

## Requirements to commercialize PUF

The basic property of PUF

Each device has **different PUF value** from the same design layout

The format of the PUF circuit determine this property

PUF value is hard to predict and **true random number**

PUF value maintain **permanently** after manufacturing

The main drawback of the existing PUF circuits due to noises, TR characteristics, etc.

PUF circuit guarantees high **semiconductor yield** at low cost

This property should be considered for commercialization



EMBEDDED SECURITY SYSTEM LABORATORY

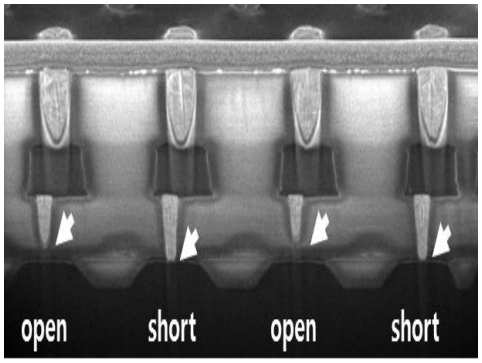
## New PUF Technology : Process-based PUF

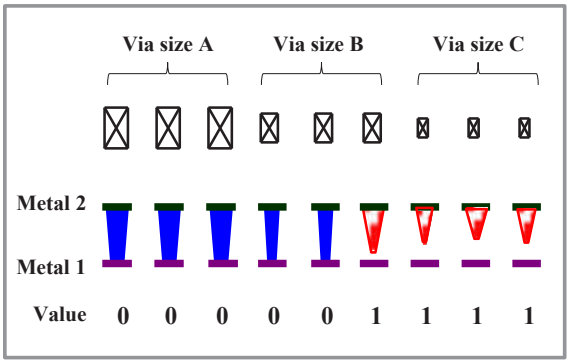
- Circuit-based PUF
  - Every previous PUF devices generate random values using the differences of electric characteristics of semiconductor devices (e.g., TR, capacitance, etc.)
  - The electric characteristics of semiconductor devices can change from environmental effects (e.g., noise, leakage current, time, temperature, etc.)
  - Circuit-based PUF can not maintain the PUF value permanently.
  - This is main barrier to commercialize.
- Process-based PUF
  - No comparator, no device → a rise in semiconductor yield
  - We proposed a process-based PUF
  - After manufacturing this type PUF as the real chip in 2009, the PUF values are still fixed

EMBEDDED SECURITY SYSTEM LABORATORY

## VIA PUF 기술

- 2009년부터 ㈜아이씨티케이와 한양대학교 공동 개발
- 순수 국내 기술로 PUF 기술 개발 및 양산 적용
- JDEC 기준의 반도체 신뢰성 Test 결과 PUF 값 불변






EMBEDDED SECURITY SYSTEM LABORATORY

## PUF 기술의 경쟁 현황

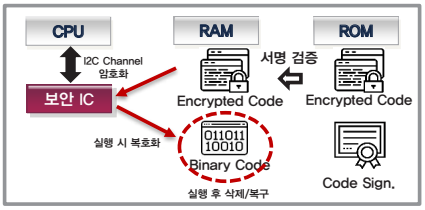
- 10여년 째 일어나고 있는 글로벌 업체들의 PUF 구현 각축장, Active vs Passive 소자
  - S/W Key 구조의 한계를 벗어나기 위한 H/W Key PUF 개발

→ Active (능동) 소자의 응용에는 환경 변화에 따른 ID의 안정화 문제가 있어 추가적인 ECC (error correction code) 의 필요 문제가 있어 생산성에 큰 문제를 주고 있음

EMBEDDED SECURITY SYSTEM LABORATORY

## PUF 기술로 Root-of Trust 확보

- 양산성 검증된 PUF 기술 적용
  - Randomness 및 Repeatability 확보
  - PUF 기반의 Key Management로 Key 해킹 원천 차단
- 자체 개발한 보안 알고리즘 적용
  - H/W logic 기반의 대칭 암호 연산 구현
  - S/W 보안 알고리즘 대비 저 전력/고속 암호 연산 모듈 구현
- PUF 기반 S/W 보호 Solution 적용
  - Code 난독화 기법 적용
  - Critical F/W 암호화

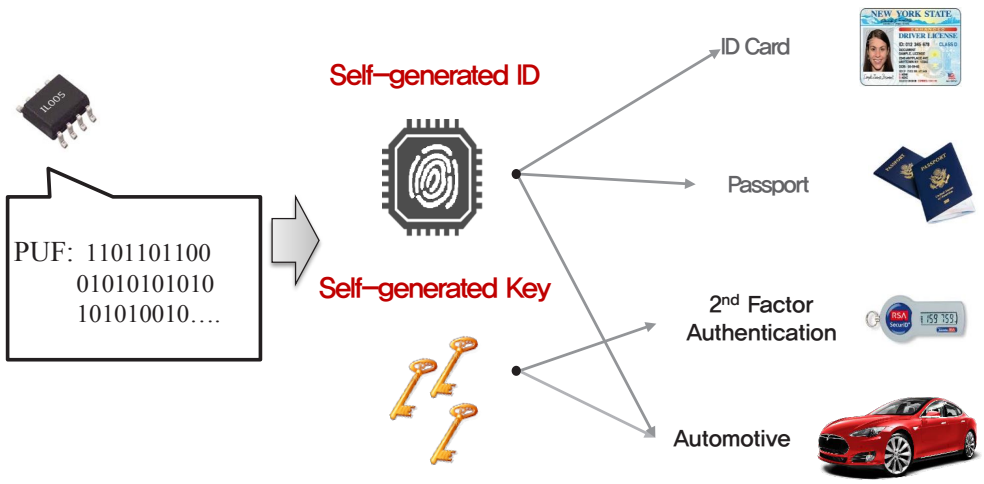





EMBEDDED SECURITY SYSTEM LABORATORY

## PUF 활용

- PUF Key를 이용하여 데이터 암호화 및 기기 인증 수행
- PUF Key로 암호화 된 데이터는 PUF IC 없이 복호화 불가능
- PUF를 고유의 ID 및 Key로 활용



EMBEDDED SECURITY SYSTEM LABORATORY

## PUF 기술 해외 적용 현황

### 국방사례

- 미 국방부 H/W 보안 방향
  - Secure Microprocessor 적용
  - 전자기기 보호 (동작중)
  - PUF/RNG 적용 필수
- 전자기기 보호
  - Reverse Engineering 방어
  - S/W 방어
  - Supply Chain 방어

### Smartphone

- 네덜란드 Cyber Security 음성/영상 보호
- 적용 예
  - Smartphone 음성/영상보호
  - Second Factor 인증

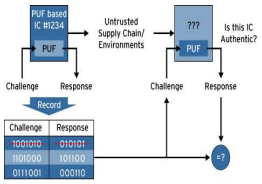
INTRINSIC ID

Rijksdienst voor Ondernemend Nederland

### 정품 인증, 위조 방지

- 복제 불가능한 ID
- Challenge-Response 인증
- 적용 예
  - Drone용 Battery 인증
  - Printer Cartridge
  - Verayo PUF RFID

VERAYO






EMBEDDED SECURITY SYSTEM LABORATORY

## PUF 기술 해외 적용 현황

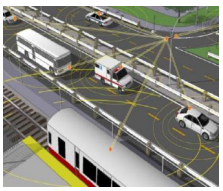
### FPGA IP 보호

- FPGA IP bit stream 암호화
- 적용 예
  - SmartFusion2
  - Altera Stratix 10

### V2X 보안

- PUF 키를 유출되지 않는 PKI 개인키로 활용
- PKI: Public Key Infrastructure
- 적용 예
  - EU Preserve Project
  - Home IoT용 가전제품
    - 에어컨, TV, 냉장고

PRESERVE
preparing secure v2x communication systems



EMBEDDED SECURITY SYSTEM LABORATORY

# IoT용 보안 SoC와 사업화사례

HANYANG UNIVERSITY

EMBEDDED SECURITY SYSTEM LABORATORY

## ICTK Security Chip List

- ㈜아이씨티케이 보안 칩 주요 사양
  - 현재 양산중인 제품 : 3종 (Giant-1/2/3, 5월/’17년~)
  - 주요 응용 분야
    - Dron (J社/중국 ), Wifi Hub/AP (L社/국내), HomeIoT (H社/중국)

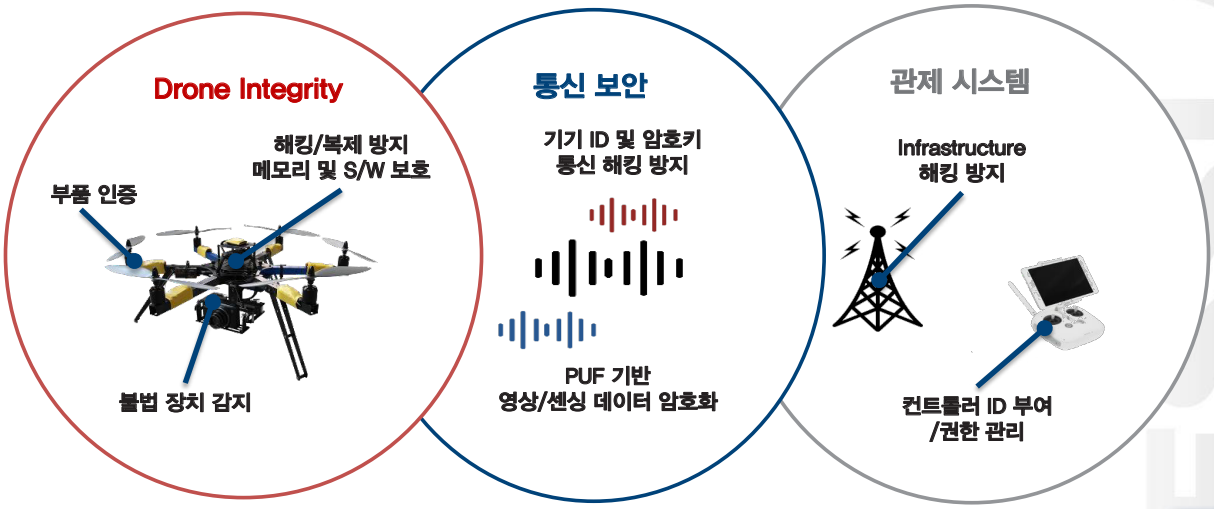
| 구분 | Giant-1 | Giant-2 | Giant-3 |
|---|---|---|---|
| 용도 | 기기인증, 정품인증 | 정품인증 (NFC) | 軍/Home IoT |
| 응용분야 | IoT, Printer Cartridge, Door Lock, S/w Copy Protection | 보안물류, 화장품, 명품 인증 | Wifi 모듈 (통신보안, 에어컨, 냉장고, TV 등) |
| 보안 알고리즘 | 대칭형 보안 알고리즘 (SHA-256) | 대칭형 보안 알고리즘 (SHA-256) | 대칭형 + 비 대칭형 알고리즘 (ECC+AES+ARIA) |
| I/F | I2C | 무선 NFC | SPI/I2C |
| 소비전력 | 매우 낮음 (5mA) | 극도로 낮음 (1mA) | 매우 낮음 (5mA 전, 후) |
| CPU | X | X | O (32-bit, 40MHz) |
| 공정 | 130nm | 130nm | 65nm |

HANYANG UNIVERSITY

EMBEDDED SECURITY SYSTEM LABORATORY

## 사업화 사례 1 – Drone

- Drone 보안 Chip 사용 예
  - 4개/드론 Giant-1 사용 (J社/중국, 7월/' 17년)
    - 통신용 – 1개, Battery 인증용 – 2개, 리모콘용 – 1개

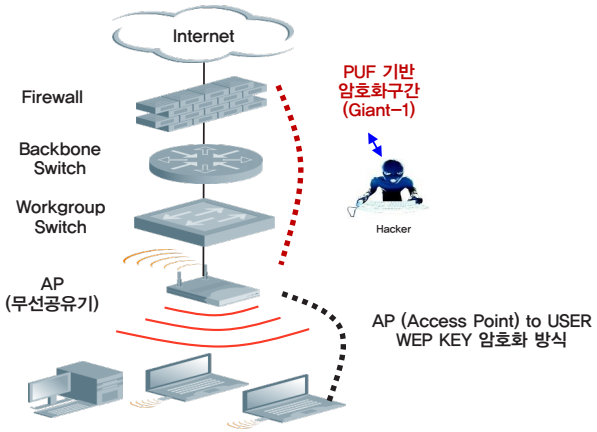





EMBEDDED SECURITY SYSTEM LABORATORY

## 사업화 사례 2 – 무선 공유기

- Wifi용 Access Point 사용 예
  - Giant-1 적용 제품 개발 중 (L社/국내, 12월/'17년 양산)
    - 인증 및 F/W 보호용, 초기 High-end 제품 적용 후 '18년 전 제품 횡 전개 예정



EMBEDDED SECURITY SYSTEM LABORATORY

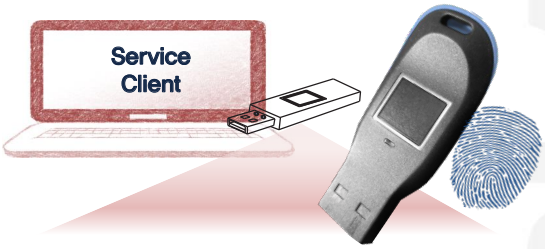
## 사업화 사례 3 – Home IoT

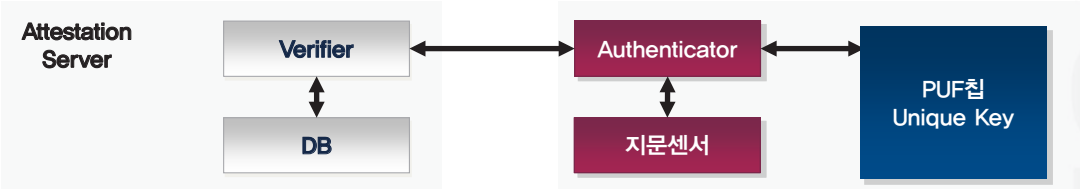
- Home IoT 보안 Chip 사용 예
  - 국내 가전 L社 Giant-3 적용 예정 (4월/'18년)

EMBEDDED SECURITY SYSTEM LABORATORY

## 사업화 사례 4 – ID

- PUF 칩과 지문 인증을 활용한 기기 인증 및 복제방지
  - 고유한 복제 불가능한 키
    - PUF의 고유키 값을 기기 인증을 위한
    - Root of Trust 로 활용
  - 개인 키의 자체 생성을 통한 위험 분산
    - 발급 과정에서 개인키가 노출되지 않아 키 유출에 대한 위험성 감소
  - 지문을 통한 중요 리소스 접근제어 및 사용자 인증 제어

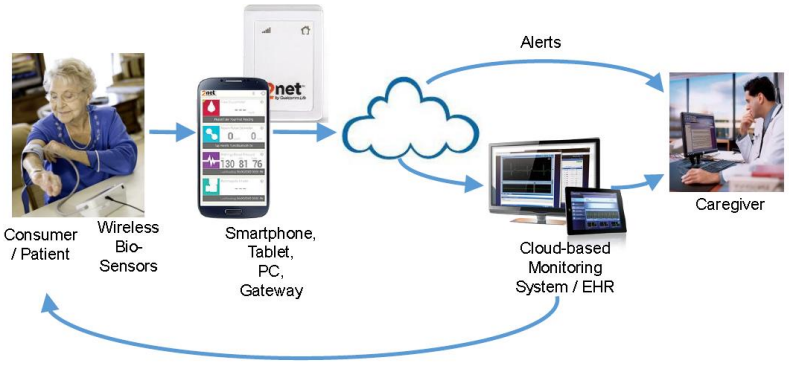


EMBEDDED SECURITY SYSTEM LABORATORY

## 사업화 사례 5 – 헬스케어

- 헬스케어 보안 Chip 사용 예
  - 제세동기 Giant-1/3 적용 (R社/국내, 5월/'17년~)
    - Auto ID, 기기인증, S/W Copy Protection, Data 암호화 용

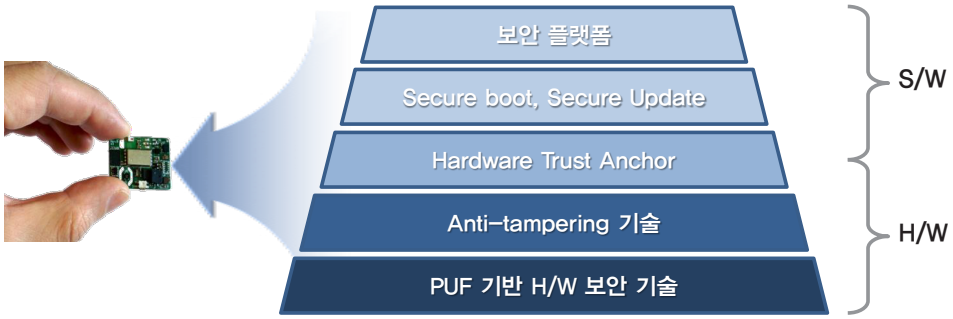





EMBEDDED SECURITY SYSTEM LABORATORY

## 맺음말

- IoT 보안
  - H/W Chip 기반 End-point Security 가 가장 중요
- Key Management
  - Key 생성, 저장, 갱신, 폐기는 PUF 기반 필수
- H/W Trust Anchor 기술
  - 높은 보안성과 가격 경쟁력을 갖는 보안 SoC



EMBEDDED SECURITY SYSTEM
LABORATORY
감사합니다!
ESSLAB
HANYANG UNIVERSITY

The 24th Network Security Conference -Korea

# IoT환경에 적합한 자율형 보안기술

**최두호** ETRI 실장

### 학력 및 경력사항

| | |
|---|---|
| 1990.03 ~ 1004.02 | 성균관대학교 학사 |
| 1994.03 ~ 2002.02 | KAIST 수학과 석/박사 |
| 2002.01 ~ 현재 | ETRI, 정보보호연구본부 책임연구원 |
| 2005.03 ~ 현재 | 과학기술연합대학원대학교(UST) 교수 |

### 강연요약

IoT 서비스 환경은 기존의 서비스별 개별 환경에서, 보다 통합적이고 표준적인 개방형 환경으로 진화하고 있음. 이에 따라, IoT환경에 적합한 보안기술도 IoT 환경의 특성에 맞게 진화하고 있음.

본 발표에서는 IoT 환경(주로, 자원 제약성)을 고려한 보안기술 특히, 암호 엔지니어링 기술들에 대해 소개하고, IoT환경의 진화 특성 즈, 디바이스 대규모성, 네트워크 다양성 및 관리 범위의 대규모성 등에 적합한 자율형 IoT 보안기술(디바이스 측면, 네트워크 측면, 보안관리 측면)에 대해 살펴보고자 함.

ETRI Electronics and Telecommunications Research Institute

NetSec-KR 2018 제24회 정보통신망 정보보호 컨퍼런스

# IoT환경에 적합한 자율형 보안기술

## - 암호엔지니어링 중심 현황과 전망 -

2018. 04. 13.

ETRI/정보보호연구본부

최두호

## 목 차

1 들어가기 전에…
- 암호엔지니어링?
- 연구결과(탭 수준) → 실제 범죄 활용 실제 간극?
- IoT 관련 주요 이슈는?

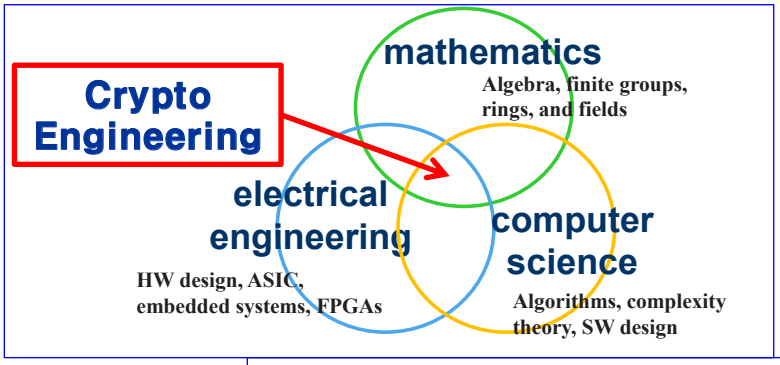
2 IoT 고려 Crypt. Engineering
- Lightweight – 우겨 넣기
- Side Channel Analysis & Countermeasure – 키누출
- Key Hiding – 숨기기, 그때 그때 만들기, 인프라에 보관
- Quantum-Safe

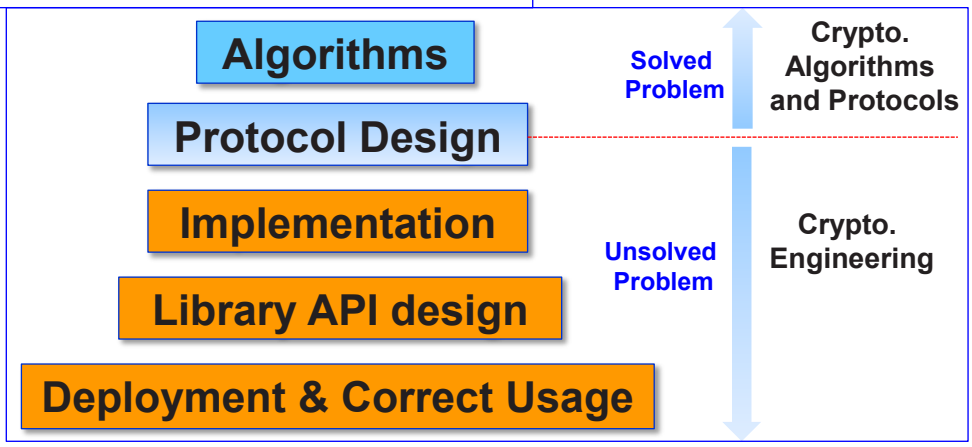
3 IoT환경 변화 방향

4 IoT환경 적합 보안 전망 – 자율보안

5 맺음말

# 암호 엔지니어링?



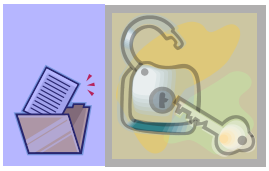

* Modified from CHES2015 invited talk, "Secure Protocols in a Hostile World", Mathew Green



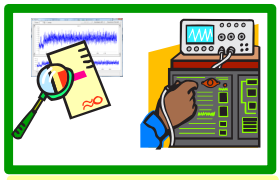
# 암호엔지니어링 - 트렌드

**Enc./Sign/Hash**

Symm: DES, SEED, AES, ARIA, etc.
Asymm: RSA, ECC, etc.
Hash: MD5, SHA1,2, etc.



**Efficient Implementation**



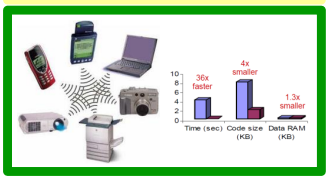
**Side Channel Attack(SCA)**

SPA, DPA, CPA, etc.
Fault Attack

**Quantum-Safe**

Homomorphic Encryption, Neural Crypt,
**PQCrypt. Q-Complexity Analysis & Implementation**

**Lightweight Implementation**




PRESENT, HIGHT, LEA, Simon and Speck etc.
Lightweight AES implementation

**Secure Implementation**

SCA Countermeasures
Fault Response

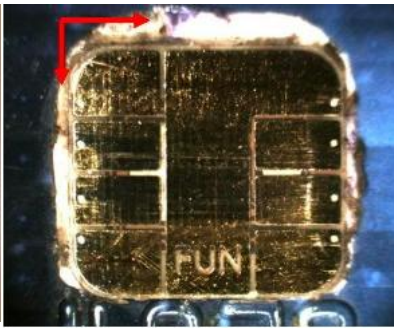
**Key Hiding**

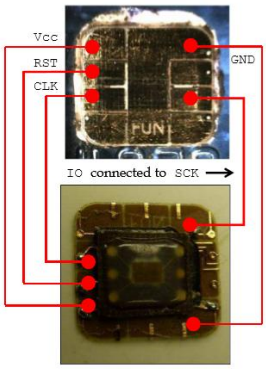
PUF(Physically Unclonabl Function), WBC(White-Box Cryptography), Key Generation

# 랩수준 연구결과의 사이버범죄 적용 간극?

## When Organized Crime Applies Academic Results...('15)

- 2011년 5월 프랑스에서 발생한 신용카드 도난 사건에서 유출된 신용카드 이용해 상품을 대량 구입하는 피해가 발생했음 → PIN 코드는 유출 X
  - 신용카드 40장으로 7,000회에 달하는 결제를 통해 60만 유로 피해가 발생
  - 범인 중 한명 검거 → 도난 신용카드(IC카드) 압수



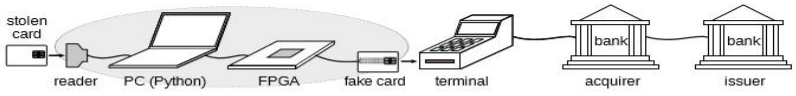






# 랩수준 연구결과의 사이버범죄 적용 간극? – 1년

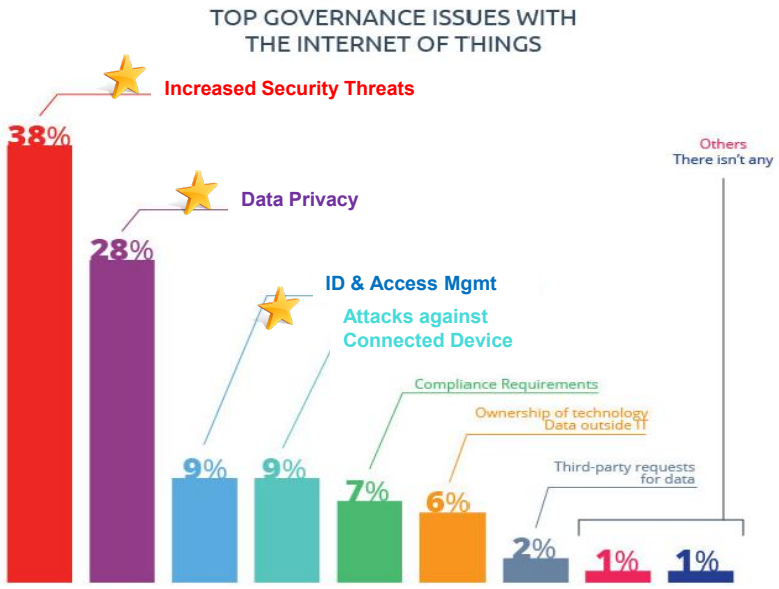
## When Organized Crime Applies Academic Results...('15)

- 2010년 IEEE Symposium on Security and Privacy, Chip and PIN is Broken 논문에서
  - IC카드와 POS 시스템 사이의 Man-in-the-Middle 공격을 통해,
  - EMV 프로토콜의 PIN 입력 우회 가능함을 입증 → FPGA 형태 시험



◎ 이제, 단지 학계 연구결과이고, 실제로는 악용은 어려울 거라는 생각 제고 필요..

# Internet of Things 주요 이슈는?




* Source: ISACA's Risks and Rewards of the Internet of Things

- **IoT관련 주요이슈의 대부분은 보안관련 이슈임 – 증가하는 보안위협 38%, 데이터 프라이버시 28%**



2 IoT 고려 Crypt. Engineering
- Lightweight – 우겨 넣기
- Side Channel Analysis & Countermeasure – 키누출
- Key Hiding – 숨기기, 그때 그때 만들기, 인프라에 보관
- Quantum-Safe

3 IoT환경 변화 방향

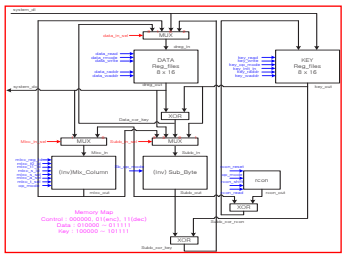
4 IoT환경 적합 보안 전망 – 자율보안

5 맺음말

# IoT 고려 Crypt. Engineering – Lightweight(우겨넣기)

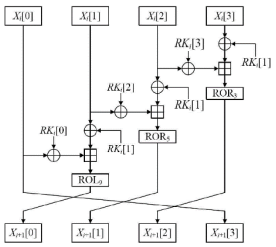
## 경량(저전력/저면적) AES 암호모듈(ETRI)

- Power Consumption : 13uW(@100kHz)
- Encryption : 216 cycles
- Decryption : 256 cycles
- Encryption module size : 4k gates
- Encryption/Decryption module size : 5k gates



## 경량(SW) 대칭키 암호 LEA(NSR)

- 128비트 블록 암호
- 키길이: 128비트(24라운드)/192비트(28)/256비트(32)
- ARX(Addition, Rotation, XOR) 구조(S-box 사용X)
- 32비트 프로세서 SW 구현 적합한 구조

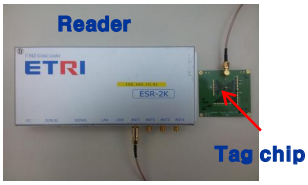




# IoT 고려 Crypt. Engineering – Lightweight(우겨넣기)

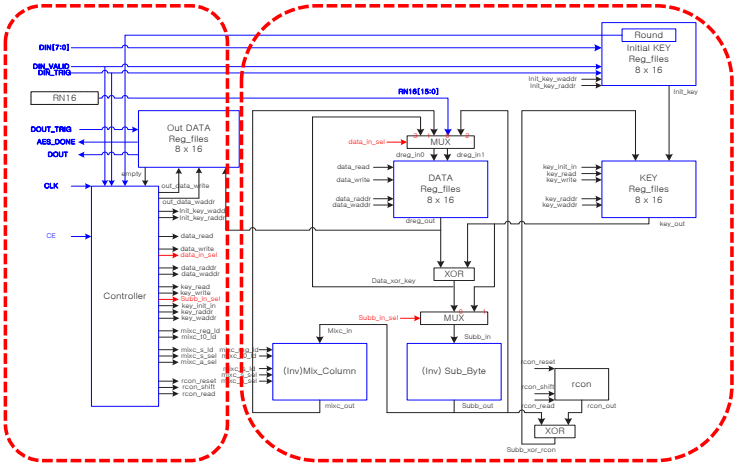
## Security protocol for Low-cost RFID tag

- Compatible with ISO 18000-6 Type C(Gen2) Tag
- Security Memory Bank for AES key
- Modes of Operation : AES-OFB mode
- ISO/IEC 29167-14 ( '15 표준 완료)

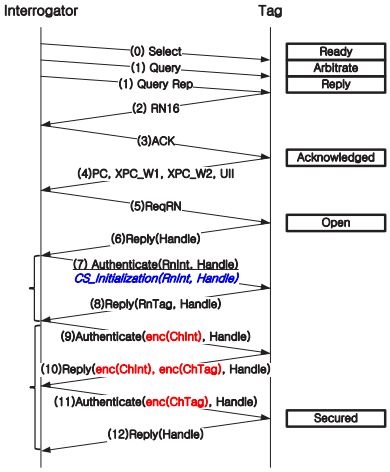



수동형 RFID 태그
digital part interface

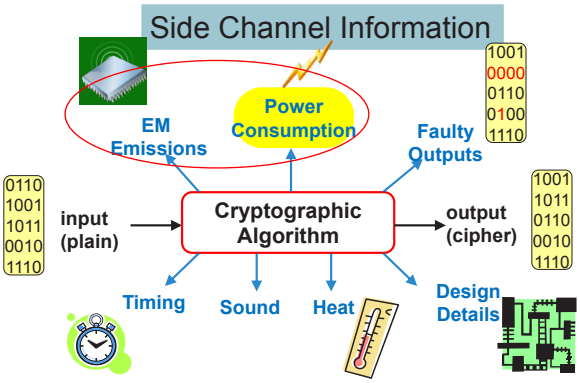
AES 암호 연산 모듈




Mutual Authentication



# IoT 고려 Crypt. Engineering – SCA(키누출)



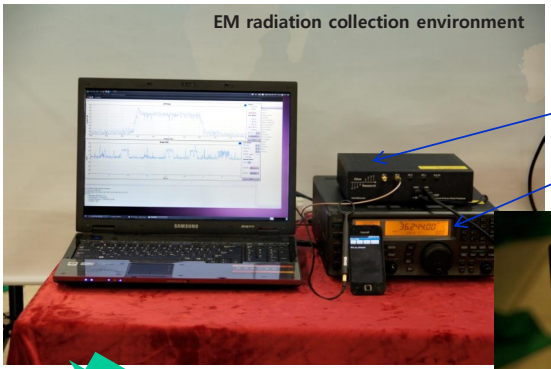

**Algorithm 1** Left-to-Right Exponentiation Algorithm

**Input:** $a$, $b = [b_{n-1}b_{n-2}b_1b_0]$ with binary expression
**Output:** $c = a^b \bmod m$ ← Secret key
$c \leftarrow 1$
**for** $k = n-1$ down to 0 **do**
  $c \leftarrow c \cdot c \bmod m$
  **if** $b[k] = 1$ **then** ← Conditional clause
    $c \leftarrow c \cdot a \bmod m$
  **end if**
**end for**
**return** $c$

M S M S S S M S M S S S
1 1 0 0 1 1 0 0



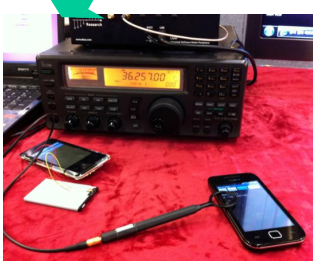
# IoT 고려 Crypt. Engineering – SCA(키누출)




USRP(Universal Software Radio Peripheral)

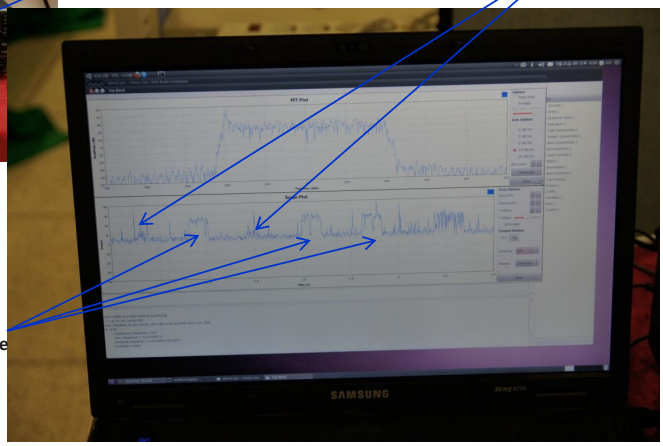
HAM

Multiplication



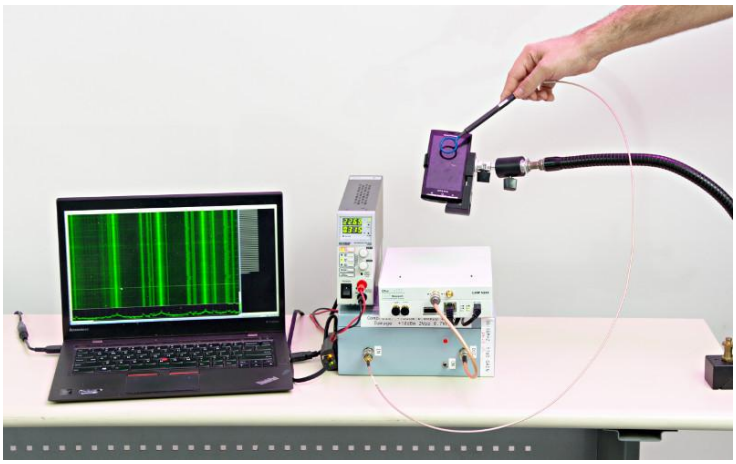
RSA computation on the smartphone

Square

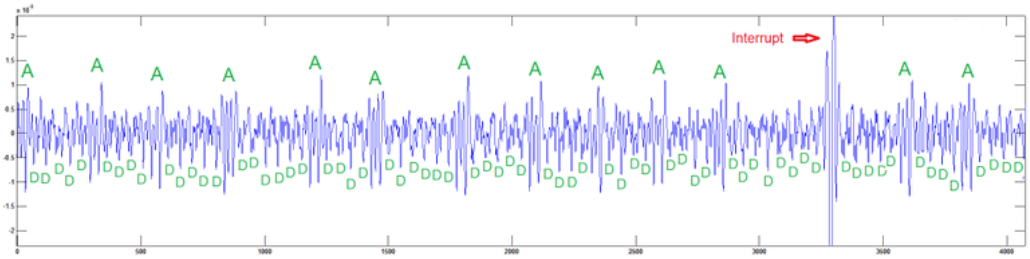


Smartphone RSA secret leakage(SEMA)

# IoT 고려 Crypt. Engineering – SCA(키누출)



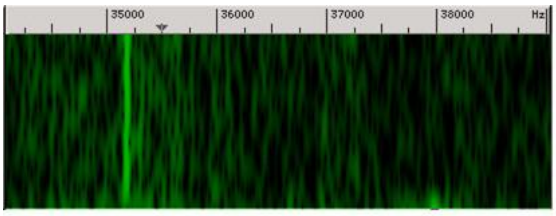
- 스마트폰 전자파 부채널 분석을 통한 ECDSA 키 공격
  - OpenSSL 1.0.x, 1.1.x,
  - iOS 7.1.2-8.3 CommonCrypto
  - Android’ s BouncyCastle



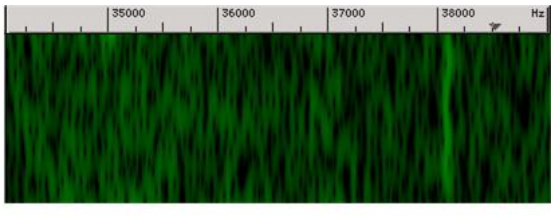



# IoT 고려 Crypt. Engineering – SCA(키누출)

- Acoustic side channel attack – RSA 키 full break



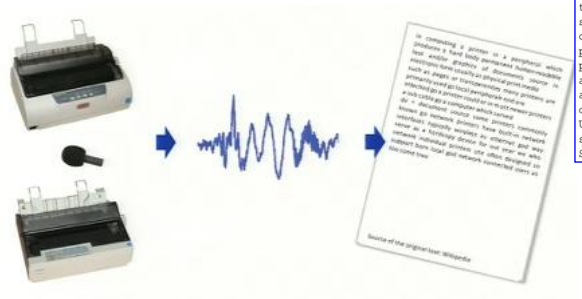

Attacked bit is 0




Attacked bit is 1

# IoT 고려 Crypt. Engineering – SCA(키누출)

- Acoustic Side-Channel Attack
  - 도트 프린터 근처에 마이크로폰을 설치하여 소리를 수집 이를 분석(기계학습)하여 프린트된 텍스트 복원(72%)

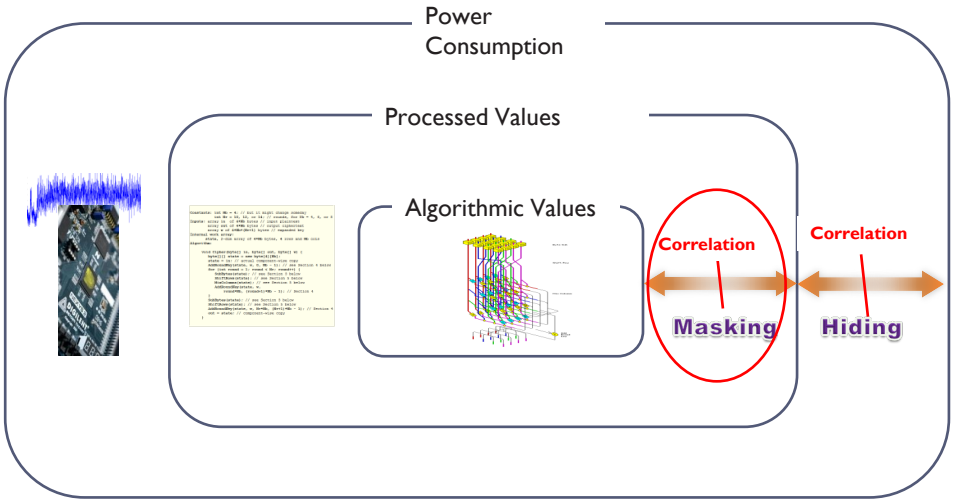


In computing, a printer is a peripheral which produces a hard copy (permanent human-readable text and/or graphics) of documents stored in electronic form, usually on physical print me... paper or transparenc... printers are primari... as local peripherals ... attached by a printe... or, in most newer pr... USB cable to a comput... serves as a document ... Some printers, commo...

in computing a printer in a peripheral which produces a hard body permanent human-readable text and/or graphics of documents source in electronic form usually as physical print media such as pages or transparencies many printers are primarily used go local peripherals end are attached go a printer could or in most newer printers a usb cable go a computer which served de = document source some printers commonly known go network printers



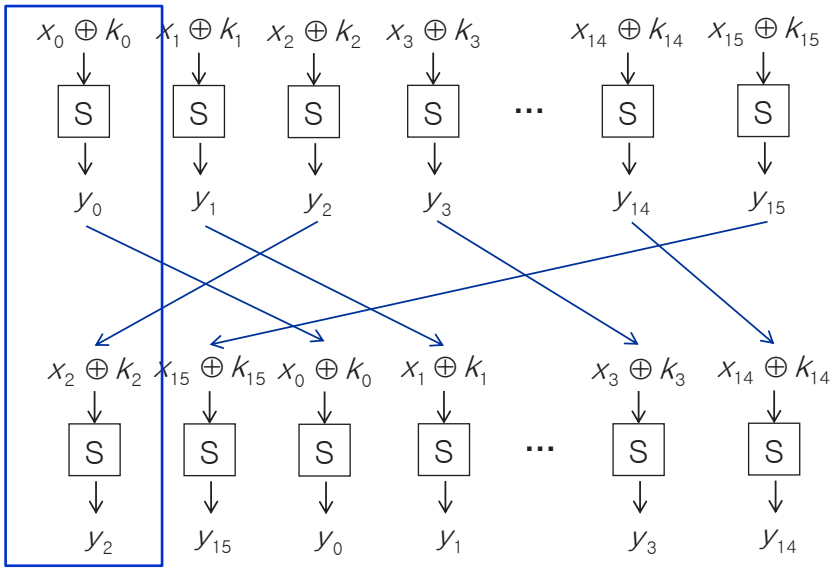
# IoT 고려 Crypt. Engineering – SCA 대응 안전 구현



# IoT 고려 Crypt. Engineering – SCA 대응 안전 구현

## Shuffling : The order of S-box computation is shuffled

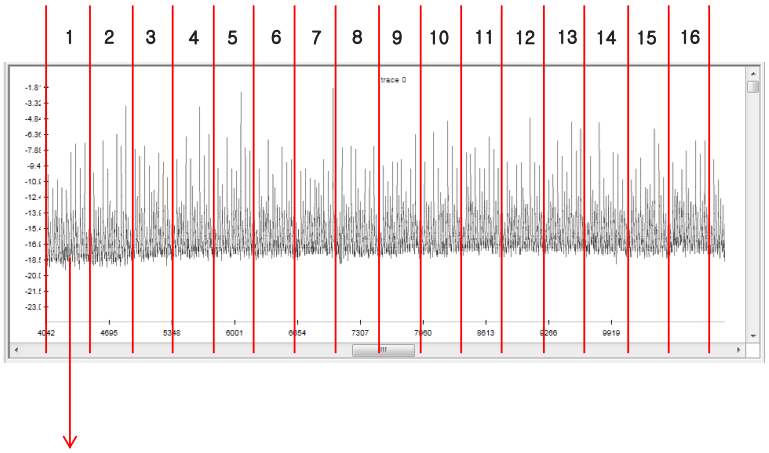
At every encryption, apply random permutation






# IoT 고려 Crypt. Engineering – SCA 대응 안전 구현

## Shuffling : The order of S-box computation is shuffled

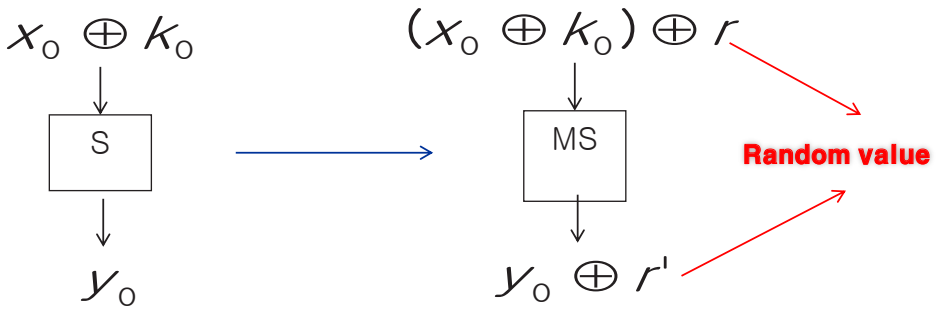



**Is this 1st S-box computation ????**

# IoT 고려 Crypt. Engineering – SCA 대응 안전 구현

**Masking : The input/output of S-box computation are randomized**

At every encryption, change these random r and r'




**Can Not Guess this output!!**

$$S(x \oplus r) \neq S(x) \oplus S(r)$$

**Non-linear**

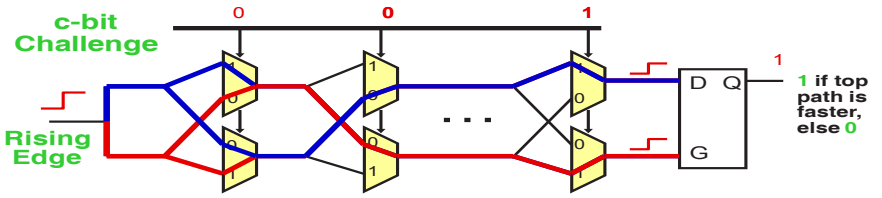


# IoT 고려 Crypt. Engineering – Key Hiding(PUF)

**PUF, Physically Unclonable Function**

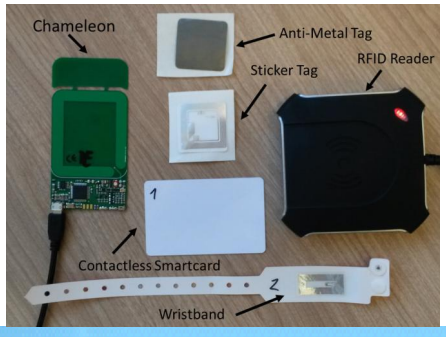
- 다양한 물리적 특성을 이용하여 복제 불가능하도록 만드는 기술
- 주요 응용: (초기) 디바이스 식별/인증(Anti-counterfeit), (요즘) 암호키 동적 생성(Key Hiding)

**주요 PUF 소스**



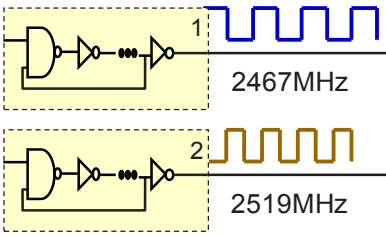

- Arbitor-PUF
- Verayo社, Toppan

→ **CHES 2015,** The Gap Between Promise and Reality: On the Insecurity of XOR Arbiter PUFs,
**Arbitor-PUF ML기반 Modeling 공격기반으로 Arbitor-PUF 장착 RFID 태그 복제 성공**



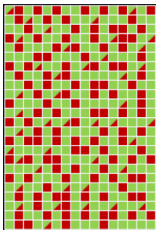
# IoT 고려 Crypt. Engineering – Key Hiding(PUF)

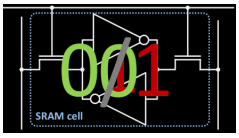
## 주요 PUF 소스




- RO(Ring Oscillator)-PUF
- → Modeling Attack

SRAM cells






- SRAM-PUF
- Intrisic-ID, NXP
- → Side Channel Attack(Fault Attack)

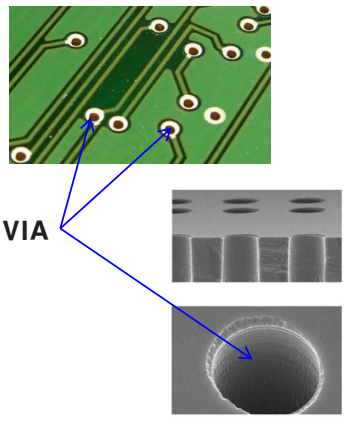
→SRAM(Static Random Access Memory), the SRAM cells are initialized with a pattern randomly made of zero and one

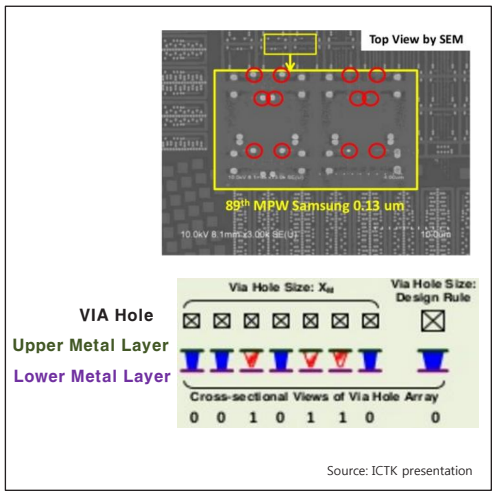
→This startup behavior (i.e., each specific bit in SRAM cells getting zero or one as an initial value) is different for every individual chip



# IoT 고려 Crypt. Engineering – Key Hiding(PUF)

## 주요 PUF 소스



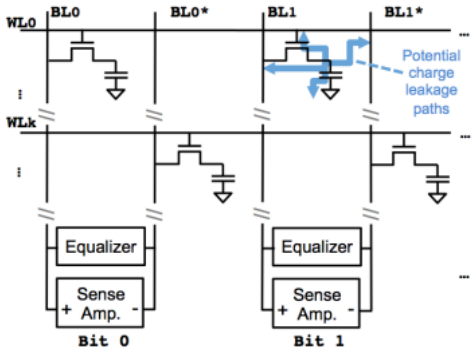




- VIA-PUF
- ICTK

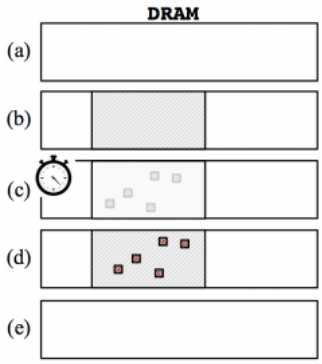
→메탈 층 사이를 연결하는 Path, 공정에서 VIA 홀의 연결 상태의 불확정성을 이용한 방법

# IoT 고려 Crypt. Engineering – Key Hiding(PUF)

## 주요 PUF 소스




DRAM




idea

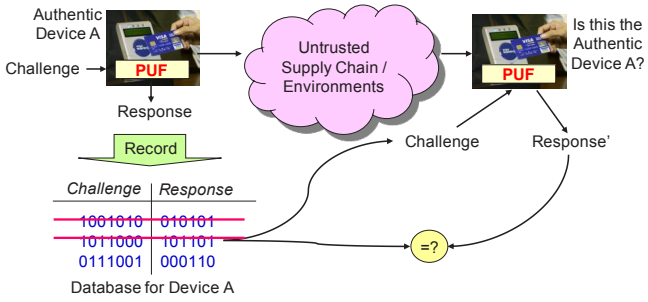
- DRAM-PUF
- Yale Univ.

→DRAM reflesh 기능 중지시키면, 적당한 decay time 후에, 전기가 빠져나가기 때문에
→0으로 읽힐지 1로 읽힐지 애매한(random) 상태가 생기고 이때의 값을 읽어서 PUF값으로 사용
→장점: commodity device에서 PUF를 구성할 수 있음



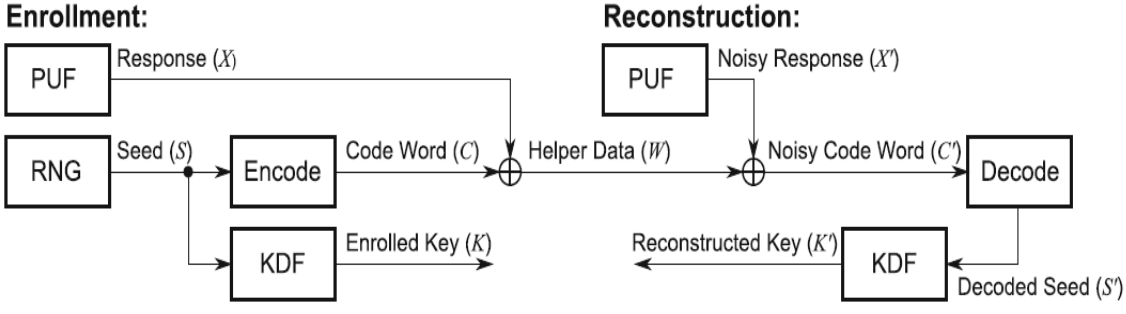
# IoT 고려 Crypt. Engineering – Key Hiding(키생성)

## PUF 기반 디바이스 인증




- PUF뿐 아니라, 디바이스 내외부의 다양한 노이지 소스를 결합하여 암호키를 은닉하거나, 생성하는 기술로 발전하고 있음

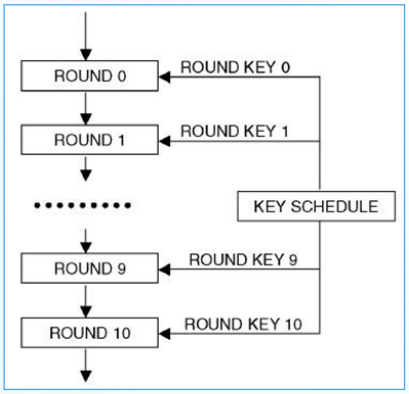
## PUF 기반 키은닉/키생성 기법

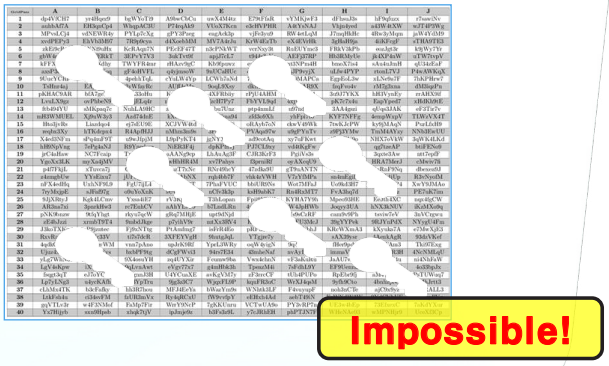


# IoT 고려 Crypt. Engineering – Key Hiding(WBC)

## Basic Concept

- Remove Key Storage/Injection, Hide the Key into the Crypto Algorithm



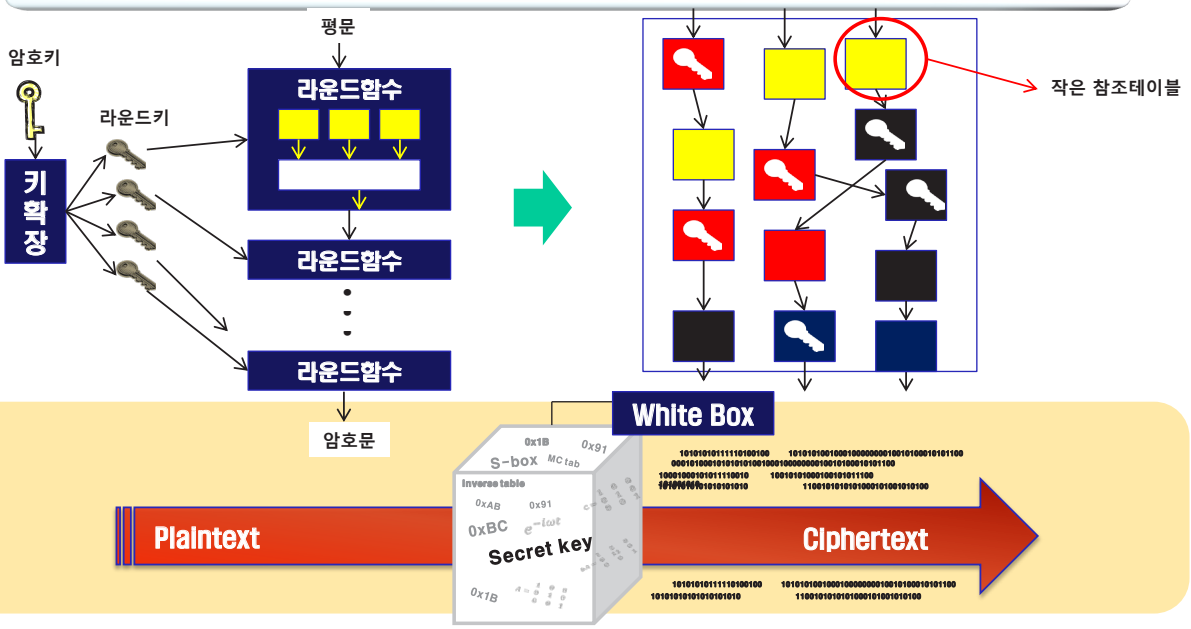






# IoT 고려 Crypt. Engineering – Key Hiding(WBC)

## Basic Concept

- 화이트박스 공격 모델 하에서 키누출이 없도록 SW적으로 암호를 설계/구현하는 암호



# IoT 고려 Crypt. Engineering – Key Hiding(WBC)

## 한계

- 표준적으로 구현된 암호대비 성능이 떨어짐 : 대략 12배 정도 느림
- 많은 메모리 필요: 508KB ~ 770KB
- 신규 공격들이 나오고 있음 : 대수적 공격, 최근 DCA(Differential Computation Analysis) 공격(CHES2016)
  → IoT 환경에 적합할지는 약간 미지수임

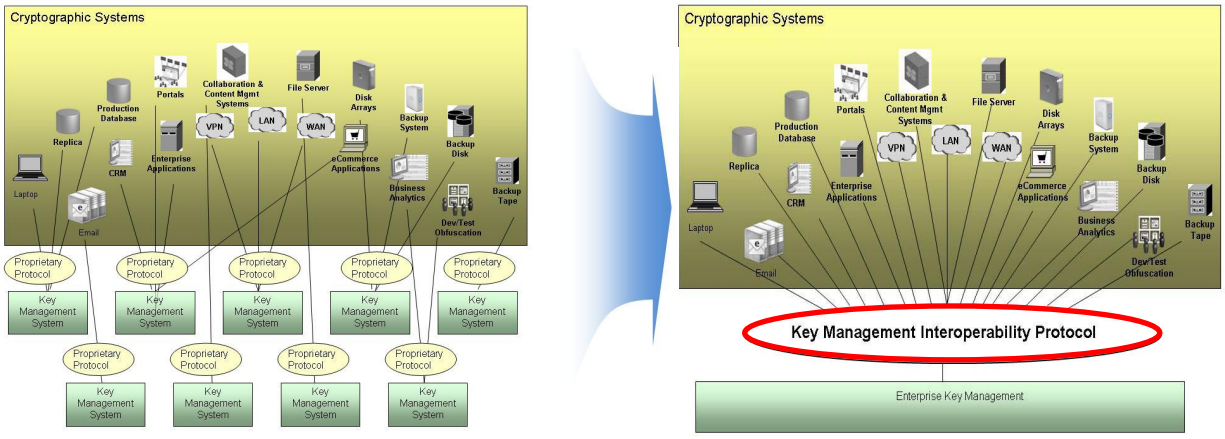


# IoT 고려 Crypt. Engineering – Key Mgmt

## 표준기반의 키관리 인프라

- KMIP : Key Management Interoperability Protocol, OASIS 표준, 2009 ~
  - v1.2 was published 11. Nov. 2014
- Objective of KMIP
  - A single, comprehensive protocol for communication between enterprise key management servers and cryptographic clients

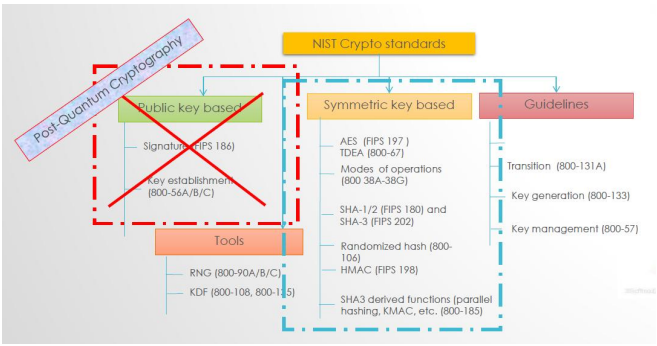
Before KMIP | KMIP : Key Management Interoperability Protocol | After KMIP




Source: OASIS KMIP White Paper (http://xml.coverpages.org/KMIP/KMIP-WhitePaper.pdf)

# IoT 고려 Crypt. Engineering – Quantum-Safe

- Quantum Computing
  - 1988 – 2 qubits
  - 2000 – 4, 5, 7-qubits
  - 2006 – 12 qubits
  - 2011 – 14 qubits
  - 2017 – 49 qubits
  - 2018 – 72 qubits




- RSA – X
- ECC – X
- Symm. Key(AES) – larger key size
- Hash – longer output



# IoT 고려 Crypt. Engineering – Quantum-Safe

## Quantum Computation

Complex value

$$|\psi>=a|0>+b|1> \qquad |a|^2+|b|^2=1$$

$$|x>=\begin{pmatrix}a\\b\end{pmatrix} \qquad <y|=(c \quad d)$$

vector　　covector

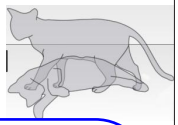
$a=1 \Rightarrow$ : Classical 0 bit

$a=0 \Rightarrow$ : Classical 1 bit

$a\neq 0 \Rightarrow$ : 중첩(Superposition) 상태

$$\frac{1}{\sqrt{2}}|0>+\frac{1}{\sqrt{2}}|1>$$

제곱은 |0>이 관측될 확률



## Quantum 계산 전략

$|0\rangle$

$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

- Classical bits $|0\ldots0\rangle$ → (Hadamard)동일 amplitude(확률) 중첩상태로 변환 $\sum_{i=0}^{2^n-1}\alpha_i|i\rangle$
- Unitary Operation들을 통해, 답이 되는 값의 amplitude(확률)가 커지도록 control
- 이를 관측(measurement)하면, 높은 확률로 답을 맞출 수 있음

# IoT 고려 Crypt. Engineering – Quantum-Safe

Peter Shor

## Shor's Algorithm

소인수 분해 문제: Classical Complexity ~ $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$

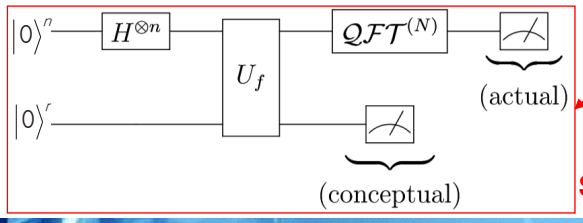
RSA 암호의 secret value(key)  Shor' s Algorithm ~ $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$

- N = p·q, find p or q

Classical Algorithms
1. Pick a random number g < N
2. Compute gcd(g, N) (만약 1이면, g가 p 또는 q)
3. Find the period r of $f:[0,2^n-1]\to Z_N, f(x)=g^x \bmod N$

$g^r = 1 \bmod N$

Classical Algorithms
4. r : odd → go back to step 1 and r : even, $g^{r/2} = -1 \bmod N$ → go back to step 1
5. Otherwise, $(g^{r/2}-1),(g^{r/2}+1)$ : nontrivial factors of N




$(\because)(g^{r/2}-1)(g^{r/2}+1) = g^r - 1 = 0 \bmod N$

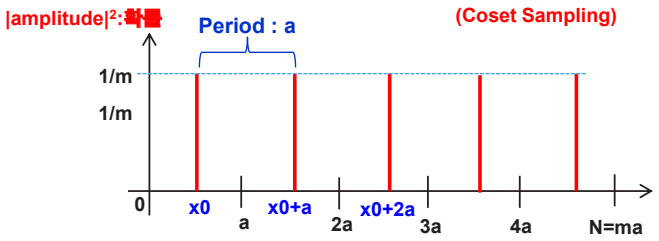
(Quantum Algorithm)
Shor's Order Finding Algorithm



# IoT 고려 Crypt. Engineering – Quantum-Safe

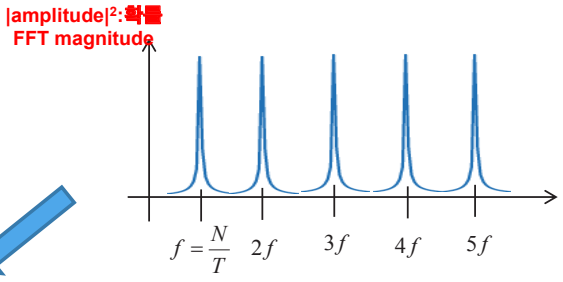
## Shor's Order Finding Algorithm - Idea

*



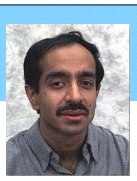

Period
Frequency
$T := a$
$T \cdot f = N$

QFT (FFT)




이제, 관측하면,
Freq.(Harmonic) 근처가
관측될 것이고, 이로부터 Period를 찾을 수 있음

# IoT 고려 Crypt. Engineering – Quantum-Safe


Lov Grover

## Grover's Algorithm

**검색 문제: Square-root speed-up** $O(\sqrt{N})$

**For** $N = 2^n$ **and given an** $d \in \{0,1\}^N$**, find an index** $i$ **such that** $d_i = 1$

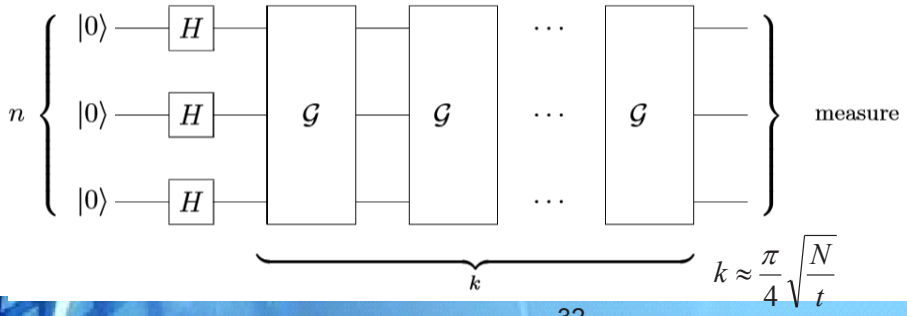
**Solution Complexity :** $O(\sqrt{N})$ **queries, and** $O(\sqrt{N}\log N)$ **gates**

**Let** $S_{d,\pm}|i\rangle = (-1)^{d_i}|i\rangle$ **and** $S_0|i\rangle = \begin{cases} -|i\rangle & \text{, if } i \neq 0 \\ |i\rangle & \text{, } i = 0 \end{cases}$

**비밀키 암호의 키 사이즈가 기본적으로 두 배 증가시켜해만 현재와 수준의 동일한 보안강도를 유지할 수 있음**

$\text{AES-128}: N = 2^{128} \Rightarrow \sqrt{N} = 2^{64}$

**Consider** $G := \left(H^{\otimes n} S_0 H^{\otimes n}\right) S_{d,\pm}$**, called *Grover iterate***




$k \approx \frac{\pi}{4}\sqrt{\frac{N}{t}}$



# IoT 고려 Crypt. Engineering – Quantum-Safe

## Grover's Algorithm - Idea

$|G\rangle = \frac{1}{\sqrt{t}} \sum_{i:d_i=1} |i\rangle$ and $|B\rangle = \frac{1}{\sqrt{N-t}} \sum_{i:d_i=0} |i\rangle$

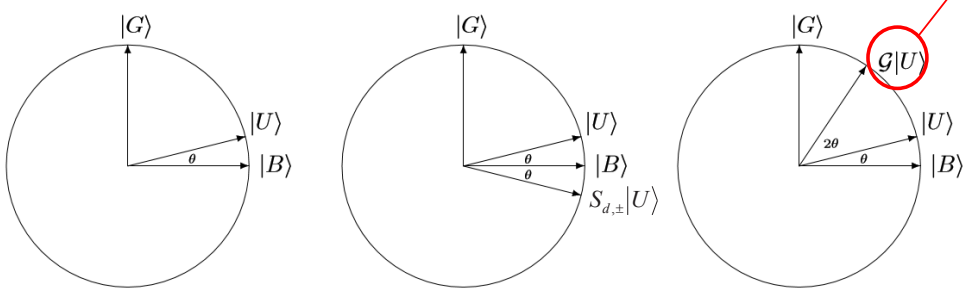
**Let** $|U\rangle := H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$ **And consider "good" and "bad" states:**

**Fact 1)** $S_{d,\pm}$ **: a reflection through** $|B\rangle$

**Fact 2)** $\left(H^{\otimes n} S_0 H^{\otimes n}\right)$**: a reflection through** $|U\rangle$

$|U\rangle = \sin\theta|G\rangle + \cos\theta|B\rangle, \qquad \theta = \arcsin\left(\frac{\sqrt{t}}{\sqrt{N}}\right)$

Grover iterate 한번 시행 결과, Good state쪽으로 3theta 이동




$G|U\rangle$ **increase the angle from** $\theta$ **to** $3\theta$ **moving to the good state**

$G^k|U\rangle = \sin(2k+1)\theta|G\rangle + \cos(2k+1)\theta|B\rangle$

3 IoT환경 변화 방향

4 IoT환경 적합 보안 전망 - 자율보안

5 맺음말



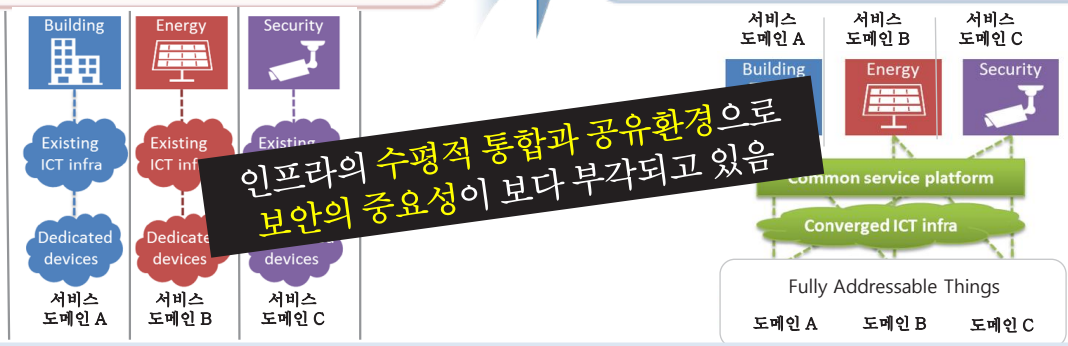
# IoT환경 변화

**초기 IoT : Vertical (Silo)**

- (서비스방식) 서비스별 단말, 플랫폼, 어플리케이션 구축
- (특징) 폐쇄형, 수직구조, 호환성없음, 센서/액츄에이터/데이터 중심
- (규모) 근거리/이통망 서비스 규모 (수만 규모)
- (생태계) 도메인 중심의 생태계로 개발, 구축, 운영, 유지비용 과다

**미래 IoT : Horizontal (Common & Generic)**

- (서비스방식) 개방형 사물인터넷 인프라 상에서 **멀티 도메인 디바이스 및 서비스 공유**
- (특징) **개방형 인프라구조, 수평적 통합, 플랫폼간 호환성**, 데이터/프로세스/지능 중심
- (규모) 인터넷기반 글로벌 규모 (수백억 규모)
- (생태계) **제품 및 서비스 중심의 생태계**로 개발, 구축비용 최소화 (규모의 경제)




**IoT 디바이스, 네트워크, 서비스들이 안전하게 운영되기 위해서 대규모의 다양한 IoT 환경에 적용할 수 있는 보안 기술 필요!**

# IoT환경 변화

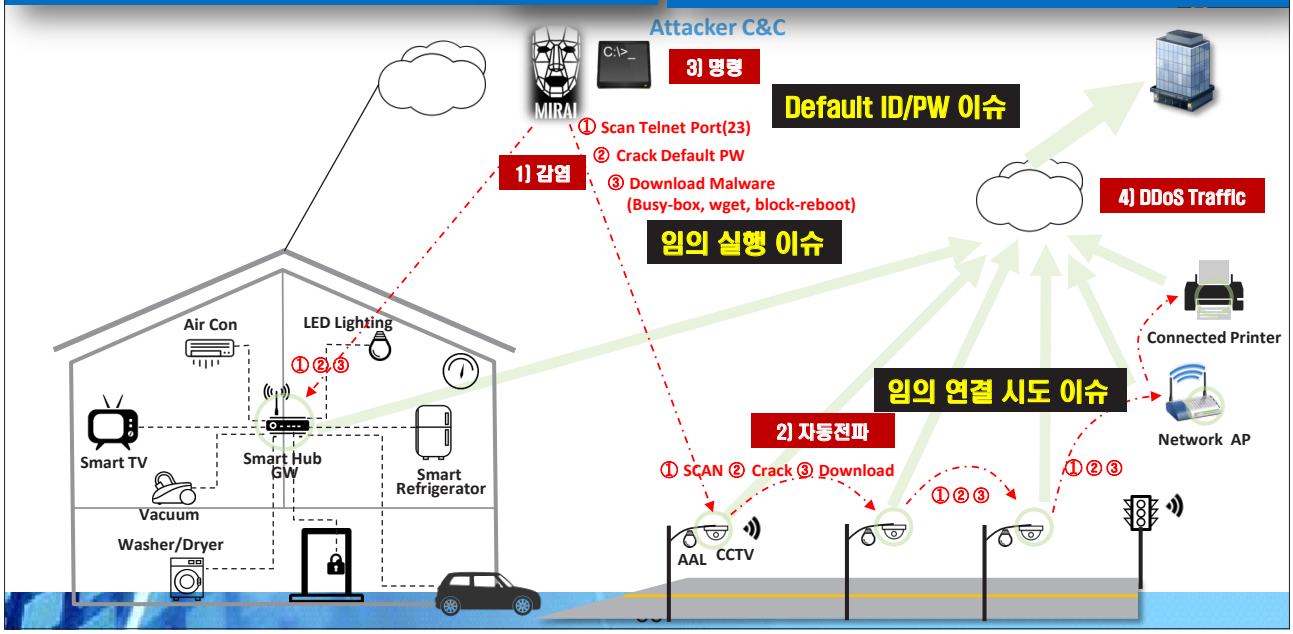
## IoT 환경은 사람이 관리할 수 있는 볼륨과 다양성의 범위를 넘어, 위협이 지속적으로 발생 중

**The Mirai Botnet**

In October of 2016, the largest Distributed Denial-of-Service (DDoS) attack ever was launched on service provider Dyn using an IoT botnet. This led to many websites going down, including Twitter, Netflix, Reddit, and CNN.

**BrickerBot**

In April 2017, a hacker released multiple versions of BrickerBot, a program that disabled thousands of insecure IoT devices, saying he wanted to raise awareness of inadequate IoT security.




# IoT환경 변화 – Lessons Learned

## 1. Device Security

**현황**
- ID, PW, KEY의 쉬운 노출
- 관리 가능 디바이스 수량의 한계 초과
- 임의 코드 실행

**대응**
- 사람의 개입 없는 단말 자율 인증
- 원격 디바이스 자율 검증
- 신뢰 실행 환경 강화

자율 인증 및 신뢰 실행기술 필요

## 2. Secure Network Management

**현황**
- 비인가 접속 시도, 위장서버 연결 (Scan, 임의 접속 등)
- 전송 트래픽 도청 위/변조
- 이종망 연결 접점 보안 취약점 미지원

**대응**
- 상호인증 기반 연결 기기 원격 검증 강화
- 신뢰연결 관리 및 제어
- 이종망 간 신뢰 연결 관리 및 제어

기기 간 연결 보증 기반 신뢰 관리 및 제어 필요

**Autonomous (자율성)**

## 3. Security Response

**현황**
- 위/변조 및 감염기기 비인가 접속
- 악성코드 자동 전파로 인한 디바이스 좀비화
- IoT 서비스 보안 위협 사전 인지 및 대응 미비

**대응**
- 비 허가 트래픽 차단 /정책 기반 디바이스 자동 복구 (Secure Patch)
- 상황 인지 기반 보안 위협 전파 격리
- 서비스 특화 자율적 보안 통제

상황 인지형 자율 보안통제 기술 필요

## 4. Situation Analysis

**현황**
- IoT 인프라 보안 상황 모니터링 부재
- IoT환경의 신종 위협의 이상 디바이스/트래픽 분석 기술 부재
- 서비스 도메인 별 보안상황 전파 부재

**대응**
- 전지적 관점의 보안상황 분석
- 기기 상태 기반 지능형 이상징후 /트래픽 분석 강화
- 다중 IoT서비스 도메인 상황 전파 공유 분석

IoT 인프라 전지적 자율 분석 기술 필요

# IoT환경 적합 보안 기술 – IoT 자율 보안

- IoT Security, what is different from security for legacy IT systems ?

❖ (Scalability, 확장성) **단일 도메인에서의 관리되어야 하는 IoT 디바이스 볼륨이 사람의 관리 한계를 벗어나고 있음**

※ 의료, 공공 서비스, 스마트 홈/빌딩 등 스마트시티 분야 IoT 디바이스 설치 현황 : `15년 12억대, `18년 30억대 규모 예상 (`15년 가트너 통계)

➢ **증가하는 IoT 디바이스에 대해 실시간 관리가 어려워 디바이스의 급속한 확장에 대하여 유연한 대응이 가능한 자율적 대응기술 필요**

❖ (Mobility, 이동성) **BAN(Body), WAN, NAN(Neighborhood), HAN(Home) 등에 사용되는 다양한 접속환경에서 네트워크 이동성이 강화**

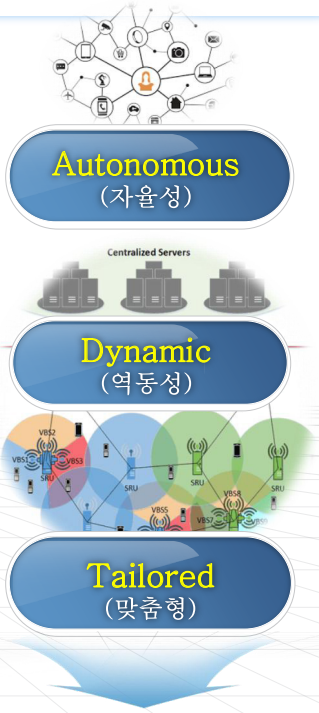
※ BAN(Zigbee, Thread, WiFi, Z-Wave, Wemo, Bluetooth), WAN(Fiber, Ethernet, Cellular GSM, LTE, 5G), NAN(PLC, LPWAN, Sigfox, LoRa) 등 다양한 접속환경

➢ **다양한 네트워크 및 서비스 이동성에서도 보안 상황에 맞게 서비스 분리/차단을 통한 위협 확산 방지 기술이 필요**

❖ (Heterogamous, 다양성) **Sensor, Actuator, 미터기, AP 등 디바이스 종류, 자원 등급별로 다양한 OS, CPU로 구성**

※ 국내외 표준기구에서 정의하는 IoT 디바이스 등급은 4개 등급으로 구성

➢ **자원제약 상황의 이질적인 디바이스 환경에서도 양질의 보안 상태(Level of Security)가 유지될 수 있도록 보안기술 적용 필요**






# IoT환경 적합 보안 기술 – IoT 자율 보안

**사람의 개입 없이 모든 사물들이 자율적으로 안전해지는 보안기술**

**IoT 디바이스 자율보안 기술**

**IoT 디바이스 자율 보안**

IoT 디바이스가 자동으로 ID를 생성하여 인증하고, 신뢰 실행 환경에서 스스로 진단/치유하는 기술

**IoT네트워크 공격 확산 방지**

**적응형 보안 자율 제어**

IoT 네트워크 환경에서 원격 기기를 검증하고 신뢰연결을 보장하며 감염 및 피해 확산을 통제하는 기술

**IoT 적응형 사이버위협 탐지/분석**

**적응형 보안위협 관리**

전역적 관점에서 IoT 디바이스, 네트워크 이상징후 및 신종 악성행위 연관성 분석하여 전지적으로 위협을 관리하는 기술

# 맺음말

- IoT 환경에서 고려해야 하는 암호엔지니링 기술들은
  - 암호 경량 구현 기술 → 기존 legacy system과 동일 레벨 보안 수준을 유지
  - IoT디바이스는 부채널 분석 등 공격에 더 취약 → 암호 안전 구현
  - 키 유출 가능성도 현저하게 증가됨으로 → 키 안전 저장, 키은닉, 키관리 기술
  - IoT기기의 장기간 사용(10~20년)으로 인해, 양자컴퓨팅 대응도 고려해야 함

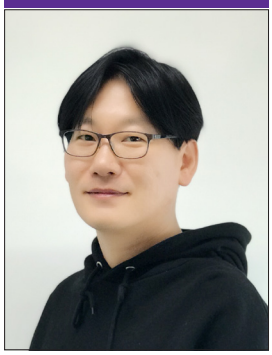
- IoT 환경은 디바이스 규모 증가, 네트워크 연결성 확대, 관리 스케일 폭발로 인해,
  → 사람의 관리 한계를 넘어서고 있기 때문에,
  → 사람의 개입 없이, 사물들이 자율적으로 안전해지는 보안 기술이 대두되고 있음
  ( 디바이스 자율보안, 네트워크 공격 확산 방지, 적응형 IoT 위협 분석/탐지 )



# 감사합니다!

ETRI

The 24th Network Security Conference -Korea



# 악성코드 분석 오픈 플랫폼

**최원혁** 누리랩 대표

### 학력 및 경력사항

2001.02 동국대학교 국제정보대학원 정보보호학 석사 졸업
2015.02 동국대학교 정보통신공학과 컴퓨터공학 박사 수료
공개용 백신 (키콤백신) 개발
前 (주)하우리 연구소장 (창업멤버, 백신 개발 총괄)
前 (주)잉카인터넷 보안기술 CSO 이사
現 (주)누리랩 대표이사

### 강연요약

악성코드가 기하급수적으로 늘어나고 있지만 악성코드 분석가의 수는 그렇지 못하다. 하지만 다행스럽게도 악성코드가 새롭게 만들어지는 비율보다 기존 악성코드를 변형하거나 소스코드를 재사용하는 비율이 훨씬 높다. 그래서 바이너리 유사도를 계산하여 악성코드 그룹을 결정할 수 있다.

하지만, 기존의 바이너리 유사도만으로는 한계가 있다. 악성코드는 다양한 압축 기법을 이용하여 숨겨져 있기 때문에 숨겨진 악성코드를 추출하지 못한다면 바이너리 유사도는 잘못된 결과를 초래하게 된다.

이 강연에서는 숨겨진 악성코드를 추출하여 기존 악성코드와의 유사도를 측정하여 악성코드 여부를 보여주는 오픈 플랫폼을 소개한다. 또한 이 정보를 바탕으로 오픈 소스 백신에 DB를 추가하여 악성코드를 치료하는 일련의 과정을 보여준다.

강연자의 요청으로
발표자료를 공개해 드리지 못한 점
양해 부탁드립니다.

The 24th Network Security Conference -Korea

# 오픈소스 보안 글로벌 동향 및 보안 인텔리전스 관리 방안

**기태현** 영남이공대 교수

### 학력 및 경력사항

1998 숭실대학교 정보통신공학 전공(학사)
2001 숭실대학교 산업공학 전공(석사)
2007 숭실대학교 산업공학 전공(박사 휴학)
2018 現 영남이공대학교 사이버보안학과 교수(오픈소스, 블록체인, 보안 연구)
2017 現 블랙덕소프트웨어코리아 보안 자문위원
2017 現 레피드7 PSO그룹 보안 자문위원
2017 現 신한 미래위협실무협의회 자문위원
2017 現 한국인프라사이버보안포럼 사무국장
2015 現 인포에스아이 부사장
2017 前 한화그룹사 31개사 외부 전문가 자문 PM
2017 前 신한금융그룹 12개사 외부전문가 자문 PM
2015 前 과기정통부 정보보호 실무 협의회 회장 역임
2015 前 성균관대 LINK 사업단 기업 대표
2015 前 정보보호 산업협회(KISIA) 이사 역임
2011 前 대중소 상생위원회 패널 활동

### 강연요약

오픈소스의 글로벌 활용으로 인한 역기능으로 오픈소스의 보안 이슈를 살펴보고 해당 이슈에 대한 보안 사례 및 보안 관리 현황을 통한 기업의 오픈소스 관리 사례와 현명한 보안 이슈 대응을 위한 보안인텔리전스 활용 방안을 통해 활용도가 높아지는 오픈소스의 최적화된 보안 관리 방안 연구 및 오픈된 퍼블릭 블록체인관련 보안 이슈 처리 방안을 소개합니다.

Blockchain Security SECURITY 블록체인시큐리티

# 오픈소스 글로벌 동향 및 보안 인텔리전스 관리방안

## 4차 산업 오픈 소스 플랫폼화와 다방면의 활용, 보안 위험, 관리 방안

## Contents

I 개요
II 오픈소스 글로벌 동향
III 블록체인 분야 이슈
IV 보안 위협
V 대응방안
VI 보안 인텔리전스

Blockchain Security SECURITY 블록체인시큐리티

# Contents

# Ⅰ. 개요



## 1.1 연구소 소개

서울대학교 전기정보공학부 보안최적화 연구실

### 보안최적화 연구실 (Security Optimization Research Lab.)

백윤흥 교수
서울대학교 공과대학 전기정보공학부

약력

- B.S., M.S. Computer Science, SNU
- Ph.D. Computer Science, UIUC
- Assistant Prof., Dept. of Computer Science, NJIT (1995~97)
- Assistant Prof.(1997~99), Associate Prof. (2002), Dept. of Electrical Engineering, KAIST
- Associate Prof. (03~06), Prof. (07~present), Dept. of Electrical and Computer Engineering, SNU

연구분야

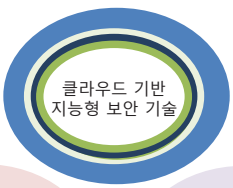
- SoC architectures to efficiently ensure the security of smart computing devices
- Coprocessor-based Security Systems for Mobile devices
- Security enhancement for system software
- Applying deep learning to enhance security

연구원 18명

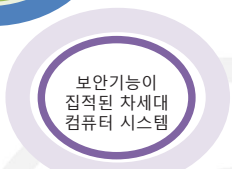
- 박사 과정 9명
- 석사 과정 9명

### 연구 분야

ETRI(한국전자통신연구원) 주관
국내 유수의 기업들 및 학교들과 연계하여
맞춤형 지능 보안 서비스 연구



SK 인포섹 보안 관제 서비스 Secudium과 연동될
딥러닝 기반의 보안 기술 산학협력 연구




IoT 시대의 중심인
차세대 smart computing device에 알맞은
하드웨어/소프트웨어 보안 기술의 연구

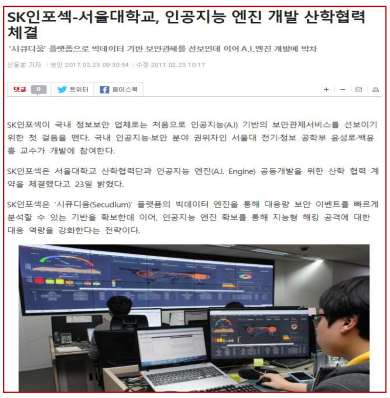
## 1.2 연구분야

1 개요

서울대학교 전기정보공학부 보안최적화 연구실

인공지능, 딥러닝, 사물인터넷(IoT)에 발맞추어 **클라우드 지능형 보안 서비스, 딥러닝 기반의 보안, 하드웨어/소프트웨어 보안 기술** 총 세 가지 분야에 대해 연구를 진행한다

### 보안 관제를 위한 딥러닝 기반 보안 연구


SK인포섹-서울대학교, 인공지능 엔진 개발 산학협력 체결

'시큐디움' 플랫폼으로 빅데이터 기반 보안관제를 선보인데 이어 A.I.엔진 개발에 박차

SK인포섹이 국내 정보보안 업계로는 처음으로 인공지능(A.I) 기반의 보안관제서비스를 선보이기 위한 첫 결음을 뗐다. 국내 인공지능·보안 분야 권위자인 서울대 전기정보 공학부 윤성로 책임 교수가 개발에 참여한다.

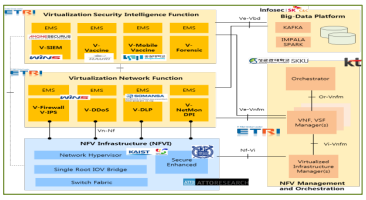
SK인포섹은 서울대학교 산학협력단과 인공지능 엔진(A.I. Engine) 공동개발을 위한 산학 협력 계약을 체결했다고 23일 밝혔다.

SK인포섹은 '시큐디움(Secudium)' 플랫폼의 빅데이터 엔진을 통해 대용량 보안 이벤트를 빠르게 분석할 수 있는 기반을 확보한데 이어, 인공지능 엔진 확보를 통해 지능형 해킹 공격에 대한 대응 역량을 강화한다는 전략이다.

### 클라우드 기반 지능형 보안 기술 연구

맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발

본 연구에서 서울대학교 팀은 해당 시스템 내의 클라우드 기반 지능형 보안 위협 분석 기술 및 고성능 서버/스위치 기반 Dynamic Enforcement 기술과 연동될 수 있는 고성능 동적 정보 추출 기술의 개발을 맡고 있음




### 보안 기능이 집적된 차세대 컴퓨터 시스템 연구

차세대 smart computing device의 설계 단계부터 보안을 고려

본 연구에서 보안 솔루션의 성능과 보안 측면의 구조적 문제 해결을 위해, 보안을 고려한 기능을 시스템 내부에 집적함으로써 실시간으로 악성 행위 탐지 가능성을 높이고자 함

연구성과 로 인한 특허 보유

Snoop-Based Kernel Integrity Monitoring Apparatus And Method Thereof

- 2017-01-10, 미국
- 삼성 스마트 TV에 해당 기술 기반의 보안 모듈 탑재

Blockchain Security SECURITY



## 1.3 블록체인 시큐리티

1 개요

**블록체인 생태계의 보안, 오픈소스 보안**, 컴플라이언스 및 거버넌스 솔루션을 공급하고, **오픈소스 컨설팅을 수행**, 악성코드들을 넘버링/관리할 수 있는 **CVE** 코드를 발급하는 **CAN(CVE Numbering Authority)** 권한이 있고, 해외 여러 보안 업체 및 소프트웨어 제조사들과 협업하여 취약점을 찾아내는 일을 적극적으로 진행하는 **취약점 관리**에 특화된 보안 연구 협의체

### 오픈 소스 (블랙덕소프트웨어)

**Code Center™**

- ✓ 오픈소스 자동화 프로그램
- ✓ 오픈소스 협력업체코드 및 내부 커스텀 코드 결합

**Black Duck® Protex**

- ✓ 오픈소스 컴플라이언스 관리 프로그램
- ✓ 라이선스 법적책임 및 저작권 분쟁의 리스크 감소

- ✓ 사용자 코드내 모든 오픈소스 탐지
- ✓ 기존에 파악된 보안취약점 맵핑
- ✓ 라이선스 및 컴포넌트 퀄리티 리스크 식별
- ✓ 오픈소스 정책 설정 및 시행
- ✓ 데브옵스 환경과의 오픈소스 관리 통합
- ✓ 새로운 보안취약점이 리포팅 될 경우, 지속적인 모니터링 및 공지

### 보안 컨설팅(RAPID7)

취약점 진단 관리 | 모의 침투 테스트 | 사용자 위험 관리

**nexpose appspider**

- ✓ 네트워크,OS,DB,어플리케이션,모바일등 모든IT인프라 취약점 진단
- ✓ 제로데이 취약점, 기존 취약점, 보안 설정의 즉각적 전수조사
- ✓ 에이전트 설치 없는 원격 진단
- ✓ 이론적 점수가 아닌 실제 위험을 반영하여 정교하게 우선순위화
- ✓ 각종 컴플라이언스 대응 리포팅

**metasploit**

- ✓ 세계최고의 자동화된 모의 침투 테스트 솔루션
- ✓ 세계적으로 검증된 안전한 공격 모듈 DB 업데이트 제공
- ✓ 파싱 테스트 기능으로 직원들의 보안의식 재교육
- ✓ 다양한 고급 공격 기술 제공
- ✓ 취약점 검증 후 Nexpose에 업데이트 하여 우선 조치 경고

**insightIDR**

- ✓ 네트워크 경계, 모바일, 클라우드로 접근하는 비정상 행위의 위험을 실시간으로 진단 후 경고
- ✓ 이미 침해당한 상태를 즉시 인지하여 경고
- ✓ 중요한 자산 접근 모니터링
- ✓ 보안 이벤트에 즉각적인 응답
- ✓ 모바일 위협 관리

Blockchain Security SECURITY

## 1.3 블록체인 시큐리티

1 개요

| 구성요소 | 보안사고 탐지 및 공격 자동화 | 최고의 전문가에 의한 공격/방어 보안 컨설팅 | Online app + AI를 활용한 맞춤형 보안 교육 및 감사 서비스 |
|---|---|---|---|
| 연구팀 | • 서울대학교 전기정보공학부<br>• Black Duck HUB<br>• Rapid7 Metasploit | • BlackDuck Soft.<br>• 마이트<br>• 영남이공대학교<br>• 서울대학교<br>• 중앙대학교<br>• RAPID7 | • 보안 프로젝트<br>• 서울대 해킹동아리<br>• 중앙대 해킹동아리<br>• 영남이공대 해킹 동아리 |
| 내용 | • **세계 최초 하드웨어 기반 악성코드 (APT, 멀웨어,랜섬웨어 등) 탐지 분석**<br>• **사이버킬체인방법론**을 적용하여 효과적인 사이버 공격/방어 분석 결과 제공<br>• 서버환경 모의해킹(서버 및 OS환경, 웹 어플리케이션, DB서버 공격 대응)<br>• 중요 정보시스템에 대한 **기술보안 아키텍처 및 권장 가이드라인 제시** | • ISMS, PIMS, ISO27001 등 인증 및 고객사 정보보호 목표 모델을 분석<br>• 이행과제를 정의, 마스터플랜 수립<br>• 구축방안, 소요자원, 기대효과 분석<br>• 통합 추진 로드맵 수립<br>• **AI + ICBM 보안 인텔리전스**<br>• **최적의 보안시스템 구축 및 운영지원을 위한 취약성 진단 및 솔루션 공급 제안** | • 웹 해킹, 악성코드 분석, 모바일 보안 등 최신 해킹 및 방어 기술에 대한 실무 위주 교육 서비스<br>• 최신 보안 취약점, 해킹기술 등 보안기술연구팀에서 순수 연구하고 발표하는 최신 정보 습득 및 보안기술 자문 |

Blockchain Security SECURITY 블록체인 시큐리티



## Contents

# Ⅱ. 오픈소스 글로벌 동향

Blockchain Security SECURITY 블록체인 시큐리티

## 2.1 오픈소스의 위상

2 오픈소스 글로벌 동향

### 개요

- 오픈소스는 제작자의 권리를 지키면서 누구나 새로운 가치를 쉽게 창조할 수 있는 공개된 자원으로, 제 4차 산업혁명을 이끄는 기술동력
- 최근 데이터, 소프트웨어, 하드웨어를 아우르는 산업 전 분야에서 다양한 오픈소스 사례가 확장 중

### 관련 기사

최근 오픈소스 기술을 소개하는 컨퍼런스가 활발히 진행 중이며 다양한 산업에서 오픈소스를 활용하고 있음

### 1 오픈소스 이점

- 오픈소스 활용의 경쟁 우위

### 2 산업별 오픈소스 현황

- 하드웨어 플랫폼, OS, 인공위성, 인공지능, 은행권 공동 오픈플랫폼

### 3 오픈소스 취약점 및 대응방안

- Apache Sturcts2
- Open SSL
- 워드프레스



## 2.2 오픈소스 공개 사례

2 오픈소스 글로벌 동향

### 오픈소스 사례

- 제 4차 산업혁명의 원동력이 혁신, 지능화, 연결을 위해서는 '공개'와 '참여'가 중요
- 오픈소스를 통해 제 4차 산업혁명에 다가갈 수 있음

우리나라 정보의 정보공개(www.data.go.kr)

미국 NASA의 오픈데이터(open.nasa.gov)

리눅스(컴퓨터운영체제)

안드로이드(스마트폰운영체제)

큐브셋(오픈소스 인공위성)

3D Warehouse(3D디자인 커뮤니티)

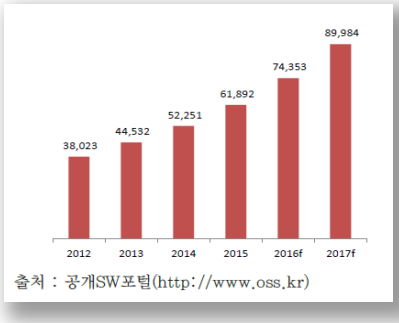
## 2.3 오픈소스 글로벌 현황



### 글로벌 오픈소스 현황

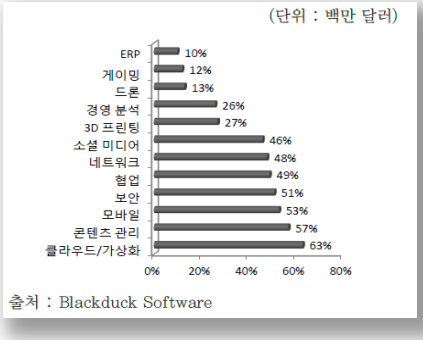
- 클라우드, 문서관리, 모바일 보안 등 다양한 신산업분야로 확대되면서 세계 오픈소스 시장규모는 연평균 1838%로 급성장하여 2015년 기준 619억 달러로 추정

#### 세계 오픈소스 시장 성장 추이




출처 : 공개SW포털(http://www.oss.kr)

#### 부문별 오픈소스 활용 바일




출처 : Blackduck Software



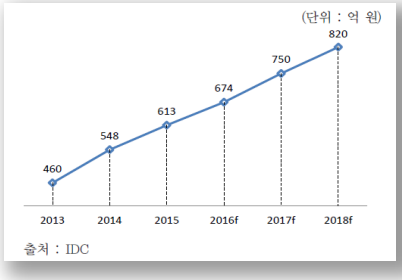
## 2.4 국내 오픈소스 시장



### 국내 오픈소스 현황

- 국내 오픈소스 시장은 연평균 12.3%로 성장 중
- 2015년 613억 원의 규모

#### 국내 오픈소스 시장 성장 추이




출처 : IDC

#### 국내 오픈소스 활성화 정책

| 연도 | 사업명 | | 주요내용 |
|---|---|---|---|
| 2010 ~2012 | 공개 SW 신시장 창출 지원사업 | 분야 | 클라우드, 빅데이터, 핀테크, 모바일 등 |
| | | 주요내용 | SW 기업의 오픈소스 개발을 지원하고 상용화 추진 및 오픈소스 신시장 창출 유도 |
| | | 지원금액 | 과제당 최대 2억 |
| 2013 | 공개 SW 전환 지원사업 | 분야 | 비공개 SW |
| | | 주요내용 | 기업 및 연구소에서 개발한 사유 SW를 오픈소스로 전환 |
| | | 지원금액 | 과제당 최대 0.3억 원 |
| 2014 ~2016 | 공개 SW 개발 지원사업 | 분야 | 클라우드, 빅데이터, 모바일 등 |
| | | 주요내용 | 오픈소스 커뮤니티 및 기업의 최신 오픈소스 개발 지원 |
| | | 지원금액 | 심의를 통한 지원금 결정 |
| | | 분야 | 기반 SW 컴퓨팅, 빅데이터, 드론 등 |
| | | 주요내용 | SW 기업의 글로벌 시장 주도를 위한 오픈소스 개발 지원 |
| | | 지원금액 | 과제당 최대 1.5억 원 |

## 2.5 오픈소스 활용의 이점



### 이점

- 오픈소스 활용은 개발 시간 단축, 비용 절감, 기술・인력 내재화를 실현하여 기업 경쟁력 향상에 기여
- 중소 SW기업의 시장진출 가능성 향상 및 SW 창업 환경 조성
- 집단지성의 창의력과 협동력을 활용해 품질・성능 강화 가능
- 해외 진출에 유리

### 오픈소스 활용의 경쟁우위

| 기술적 측면 | 경제적 측면 | 사업적 측면 | 기타 |
|---|---|---|---|
| • 개발 시간 단축<br>• 집단지성을 활용한 안정성 향상<br>• 시장 독점적 사유 SW와의 기술격차 완화<br>• 외부 우수개발자 내재화 | • 개발 비용 절감<br>• 도입 비용 절감<br>• 세부적 고객화(Customization)<br>• 우수 오픈소스 코드 재사용 증가 | • 자사의 부족한 제품군 보완<br>• 다양한 소비자의 니즈 충족<br>• 브랜드 가치 향상 | • 에너지 절감<br>• 직무만족도 향상 |



## 2.6 산업별 오픈소스 활용(1/5)



### 하드웨어 플랫폼

누구나 제작, 수정, 배포하고 사용할 수 있는 물리적 인공물

- 대표적으로 아두이노, 라즈베리파이, 비글본 블랙이 있음
- 마이크로컨트롤러 보드, 소형 단일보드 컴퓨터 등으로 불리며, 센서 등 입력장치, 외부장치 컨트롤 기능, 무선통신 모듈과 쉽게 연결 등 장점이 있음

| | 아두이노 | 라즈베리파이 | 비글본 블랙 | 갈릴레오 보드 |
|---|---|---|---|---|
| 사진 | | | | |
| 특징 | '05년 이탈리아에서 시작되었으며 Atmel의 AVR CPU 탑재 가장 널리 활용 | 영국 라즈베리 파이 재단이 '12년 정식 출시한 초소형 싱글 보드 컴퓨터 | 초기 비글보드를 거쳐 '13년 Texas Instrument 출시 가장 뛰어난 성능 | 인텔-아두이노의 합작 개발 저전력 소형 코어 제품인 Quark 칩 장착 |

## 2.6 산업별 오픈소스 활용(2/5)



OS

### 무료로 사용 및 수정, 배포가 가능한 개방형 Operation System

- 프로그래머들이 자유롭게 수정하고 배포할 수 있음
- 개방형 OS를 사용함으로써 비용을 절감할 수 있음
- 리눅스, 페도라, 솔루스, 리눅스 민트 등

Linux

ubuntu

리눅스 기반의 국내 개방형 OS

베일 벗은 개방형 OS `하모니카`

[AD] '맛있는 4차 산업혁명' 푸드테크 코리아 2018 (11/30일)

특정 소프트웨어(SW) 의존도를 줄이기 위해 정부와 민간이 추진했던 개방형 운용체계(OS) '하모니카 프로젝트'가 베일을 벗었다. 기존 윈도 사용자환경(UI)에 익숙한 사용자를 배려한 한글화 작업에 초점을 맞췄다. 향후 OS 확산과 적용을 위한 업그레이드 작업에 오픈소스 SW 개발자가 참여할 수 있도록 커뮤니티를 활성화할 계획이다.



## 2.6 산업별 오픈소스 활용(3/5)



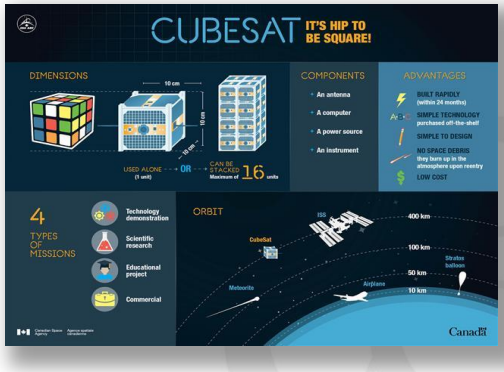
인공위성

### 오픈소스 기반의 인공위성 큐브셋(Cubesat)

- 부피 1리터, 질량 1.33kg을 넘지 않는 초소형 인공위성
- 오픈소스 기반의 인공위성으로 웹상에서 직접 인공위성 설계도면을 찾아 제작할 수 있음
- 1999년 캘리포니아 폴리테크닉 주립대학과 스탠포드대학이 공동으로 학생의 교육을 위한 목적으로 개발

특징

| | |
|---|---|
| 간단한 디자인 | 작고 단순한 디자인이지만 튼튼한 구조를 가지고 있음 |
| 오픈소스 | 설계도 및 제작 방법이 웹사이트에 공개되어 있음 |
| 대량생산 | 기존의 인공위성과 다르게 발사체 자체가 정해져 있으며 별도의 비용이 필요 없음 |
| 동시성 | 하나의 임무가 아닌 특정 임무 여러 개를 수행할 수 있음 |



## 2.6 산업별 오픈소스 활용(4/5)



인공지능

### 글로벌 IT기업에서 AI 오픈소스 기술을 공개

- 인공지능 생태계 진화를 앞당기고 개발자 커뮤니티와의 관계를 강화하기 위한 목적
- 또한, 시장 영향력을 확대할 수 있음

| 기업 | 서비스명 | 설명 |
|---|---|---|
| 야후 | CaffeOnSpark | • 딥러닝 SW<br>• 아파치 스파크 프레임워크에 기반<br>• 음성패턴 인식 및 사진 또는 비디오내용 식별을 통한 딥러닝에 활용 |
| 바이두 | WARP-CTC | • 컴퓨터가 음성인식을 하기 위해 필요한 머신러닝 기술 적용<br>• 이를 통해 Deep Speech 2 엔진 개발 |
| 마이크로소프트 | Cortana | • 인공지능 도우미<br>• 그 외 딥러닝 툴킷인 CNTK, 분산 머신러닝 툴킷인 DMTK 오픈 |
| 구글 | TensorFlow | • 기계학습과 딥러닝을 위한 기술<br>• 데이터 플로우 그래픽 방식을 사용<br>• 인공지능 신경망 연구에 한 획을 그었다는 평가를 받고 있음 |
| 페이스북 | Big Sur | • 머신러닝 데이터 학습 시 사용되는 서버<br>• 데이터 처리속도를 높여줌 |
| 삼성전자 | Veles | • 딥러닝 응용프로그램 개발을 위한 분산형 플랫폼<br>• 개방형 범용 병렬 컴퓨팅 프레임워크인 오픈치 또는 GPU에서 수행하는 알고리즘을 산업 표준 언어를 사용해 작성할 수 있도록 하는 GPGPU기술인 쿠다 사용 |

IT Chosun '인공지능(AI), 오픈소스 경쟁 시작됐다. '



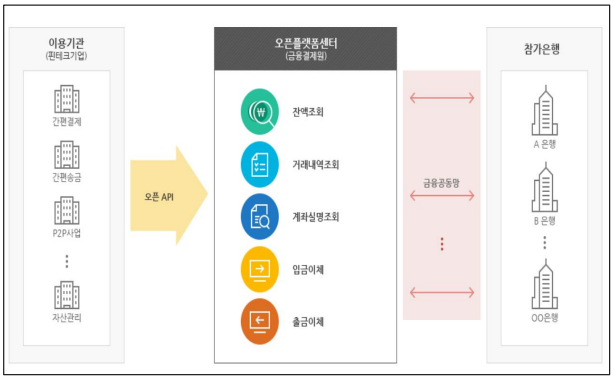
## 2.6 산업별 오픈소스 활용(5/5)



은행권 공동 오픈플랫폼

### 핀테크기업이 금융서비스를 편리하게 개발할 수 있도록 제공하는 표준 인프라

- 핀테크 서비스 출시를 위해 은행 모두와 개별적으로 협약을 맺어야 하는 번거로움을 해소하고 전산표준을 통일화 하기 위해 16개 시중 은행이 자발적으로 참여하여 참가은행과 핀테크기업이 서비스 개발 과정에서 서로 소통할 수 있는 오픈 플랫폼 구축




기대효과

- 이용기관은 참신한 아이디어와 기술을 가지고 금융분야에 진출하여 다양한 핀테크 서비스를 제공할 수 있게 됨
- 고객은 금융에 대한 접근이 쉬워지고 선택권이 넓어지는 효과가 생김
- 참가은행은 이용기관이 제공하는 다양한 서비스를 통하여 신규 고객과 만날 수 있게 됨으로써 새로운 수익 기회 창출

은행권 공동 오픈플랫폼(https://www.open-platform.or.kr/)

## Contents

# Ⅲ. 블록체인 분야 이슈



## 3.1 4차산업 블록체인의 등장



### 블록체인의 역사 및 특징

- 2008년 사카시 나까모도의 P2P기반 암호 화폐인 비트코인에 대한 논문에서 비트코인의 이중지불방지를 위한 개념으로 도입
- 이후, 블록체인 기술의 일반화는 부탈린의 이더리움에 의해 완성됨

**4차 산업혁명에 맞는 새로운 기술로서 블록체인은 주목할 만한 기술이다.**

| 효율성 | 신기술 | 사용 예시 | 기대효과 |
|---|---|---|---|
| • 분산장부 시스템을 통한 투명한 거래로 보안, 감독 규제 비용 절감 가능<br>• 블록체인은 기술 특성상 IT 비용과 인력이 수반되는 대규모 인프라를 필요로 하지 않음 | • 2016 초 세계 경제 포럼에서 제 4차 산업혁명 시대를 이끌 핵심기술 중 하나로 블록체인이 선정됨<br>• 글로벌 시장 조사기관인 가트너 (Gartner) 와 딜로이트(Deloitte)도 2017년 트렌드중 하나로 블록체인 선정 | • 효율적인 계약 자동화<br>• 스마트 계약(Smart Contract) 의 실현<br>• 계약 성립까지 걸리는 시간의 획기적 단축<br>• 글로벌 시장의 규제 준수 비용 절감 | • 모든 종류의 자산의 등록, 보관, 거래에 블록체인 기술을 적용 할 수 있음<br>• 전 세계적으로 블록체인을 이용한 국가 차원의 시스템 개발이 활성화 될 수 있음 |

출처 : 블록체인패러다임과 핀테크 보안 (박성준)과학기술 정책 연구원 -기술동향과 시사점

## 3.2 블록체인의 장점



### 블록체인 기술의 장점

| 장점 | 내용 |
|---|---|
| 보안성 향상 | ▪ 분산원장 기술은 암호화된 데이터와 암호화된 키 값으로 거래가 이루어지기 때문에 보안성이 향상됨<br>▪ 새로운 블록은 기존의 블록과 연결되므로 하나의 데이터를 변조 하거나 탈취하려면 전체 블록 안의 데이터의 변조 또는 탈취를 해야 한다. |
| 거래 속도 향상 | ▪ 거래의 인증과정에서 제 3자를 배제시키는 실시간 거래가 이루어지므로 거래 기록의 신뢰성 확보<br>▪ 분산원장 기술로 오류와 실수를 최소화 시킬 수 있으므로 오류의 정정과 수정을 위한 시간이 줄어듬 |
| 비용 감소 | ▪ 거래 정보와 인증을 위한 중앙 서버와 집중화 된 시스템이 필요 없기 때문에 비용이 적게 듬<br>▪ 거래 정보가 분산되어 있어 해킹 위험도 낮음 |
| 가시성 극대화 | ▪ 네트워크 참여자들의 실시간 거래 모니터링이 가능하므로 가시성 극대화<br>▪ 거래상의 가시성은 투명성과 자기부인 방지의 기능을 지님 |
| 익명성 보장 | ▪ 개인정보를 요구하지 않기 때문에 은행계좌, 신용카드 등 기존 지급수단에 비해 높은 익명성 제공 |
| 확장성 | ▪ 공개된 소스에 의해 쉽게 구축, 연결, 확장이 가능함 |
| 안정성 | ▪ 일부 참가 시스템에 오류 또는 성능저하 발생 시 전체 네트워크가 받는 영향 미비 |

출처 : 블록체인패러다임과 핀테크 보안 (박성준)과학기술 정책 연구원 -기술동향과 시사점

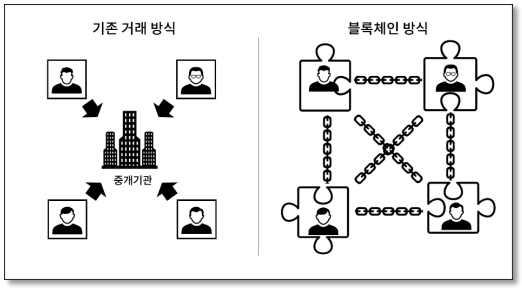


## 3.3 블록체인의 원리



### 블록체인에 기반한 거래과정

#### 기존 거래 방식과 블록체인 방식 비교

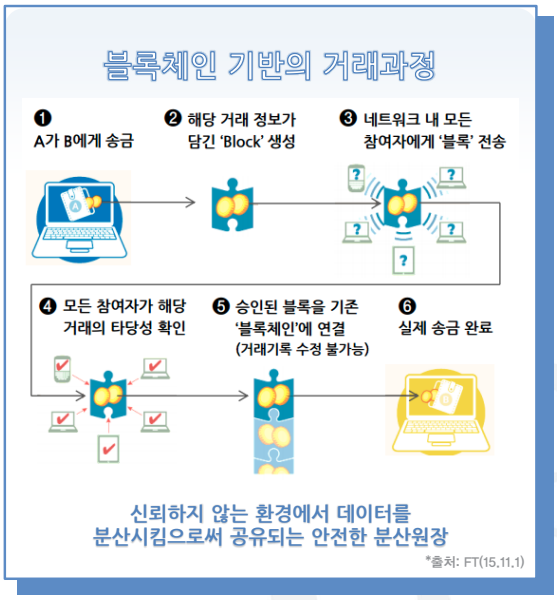



**기존 거래 방식**

저장된 장부가 있는 중앙 집중식 시스템

**블록체인 방식**

분산원장이 있는 분산 시스템

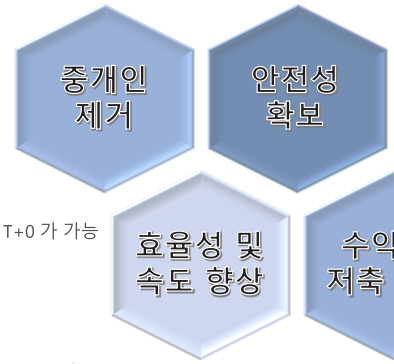


## 3.4 블록체인의 분산원장

3 블록체인 분야 이슈

### 분산 원장(Distributed ledger)이란?

산업이 새로운 비즈니스 모델을 재정의하거나 만들 수 있도록 함




높은 안전성 및 투명성으로 기록 변경이 거의 불가능

거래 간소화 및 결재시간 T+0 가 가능

효율적인 프로세스 및 비용 절감을 통한 잠재비용 절감 및 새로운 수익 기회 창출

**분산 원장(Distributed ledger) 이란?**

- 분산 원장이란, 거래가 발생했을 때 데이터를 중앙집중형 장부에 기록을 보관하는 기존의 방식과 달리, 거래 참가자 모두에게 내용을 공개하는 분산형 디지털 장부를 뜻함.
- 블록체인의 데이터구조는 분산원장기술(Distributed ledger technology)의 사용
- 기존의 원장은 중앙집중화 되어 있으며 거래를 승인, 기록하기 위해 제 3자와 중개인을 활용
- 블록체인은 전체 네트워크의 원장을 안전하게 배포하며 중개자가 필요하지 않음
- 이 기술은 P2P 토렌트 파일 공유와 같은 여러 개의 복제본을 유지함

Blockchain Security SECURITY

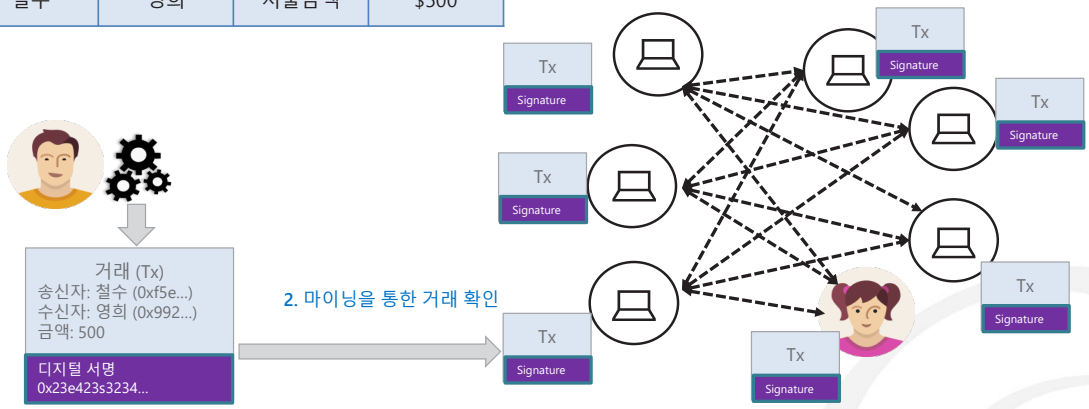


## 3.5 블록체인의 합의 시스템

3 블록체인 분야 이슈

### 분산 원장 예시

| 송신자 | 수신자 | 자산 | 금액 |
|---|---|---|---|
| 철수 | 영희 | 지불금액 | $500 |




1. 거래 정보는 해시 함수를 통해 전달 (타임 스탬프 생성 및 보안 유지)

Blockchain Security SECURITY

## 3.6 블록체인의 종류

3 블록체인 분야 이슈

### 블록체인의 종류

| | 퍼블릭 블록체인 | 프라이빗 블록체인 |
|---|---|---|
| 개념 | 누구나 쉽게 네트워크에 참여할 수 있는 블록체인으로 대표적으로 비트코인이나 이더리움이 해당한다. | 하나의 기관에서 독자적으로 블록체인을 운영하는 것 |
| | 블록체인의 종류는 그 성격에 따라 크게 3가지 형태로 나눌 수 있다. 퍼블릭 블록체인/프라이빗 블록체인/컨소시움 블록체인 | |
| 참여대상 차이점 | 누구나 참여 가능하며 누구나 운영 할 수 있다. 안정성을 위한 연산이 추가적으로 수행한다. | 운영주체가 명확하기 때문에 법적인 규제를 준수해야 한다. |
| | 퍼블릭 블록체인은 누구나 참여하고 트랜잭션의 내용이 모두 공개되며 검증 또한 모든 노드들이 참여함. → 성능 저하 가능<br>프라이빗 블록체인은 노드간 권한을 다르게 설정할 수 있고, 허가 받은 대상들만 노드로 참여할 수 있음. → 성능 향상 가능 | |
| 장점 | 운영 주체가 광범위하며 불분명하기 때문에 법적 구속력에 상대적으로 자유롭고, 거래의 투명성이 보장된다. | 블록체인 엔진을 수정할 수 있으며, 비용도 상대적으로 저렴하다. 각 노드들의 권한을 다르게 설정하는 운영상의 자유도가 보장된다. |
| | 퍼블릭 블록체인은 모든 사람에게 공개되며 익명성과 거래의 투명성을 보장하여 비트코인, 이더리움 등에 활용된다.<br>프라이빗 블록체인은 미리 인증된 참여자만 컨소시엄을 이뤄 수행하기 때문에 운영상의 자유도가 보장된다. | |

Blockchain Security SECURITY

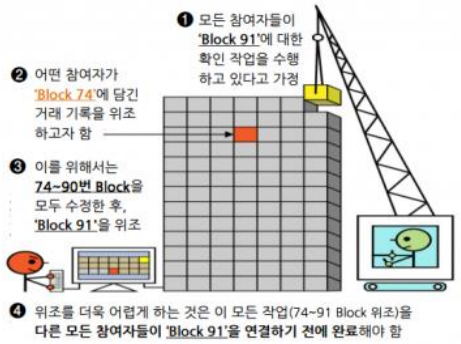


## 3.7 블록체인의 특징

3 블록체인 분야 이슈

### 블록체인의 특징

블록체인 개념도




자료: IEEE Spectrum (2015. 7)

| | |
|---|---|
| 脫 제3자 [참여자 정보공유] | 공인된 제3자 불필요<br>→ 비용절감, 시스템 안전성<br>*기존 시스템은 제3자에 대해 수수료 지불 |
| 확장능력 [공개된 소스] | 쉽게 블록체인을 구축, 연결 가능<br>→ 강력한 확장성 및 아이디어 수용성<br>*기존 시스템은 비공개, 폐쇄적으로 확장 제약 |
| 보안능력 [높은 보안능력] | 모든 장부를 해킹하려면 고비용 발생<br>중앙집중관리 불필요<br>→ 내부자 조작 및 정보유출 위험 감소 |
| 투명성 [공개된 장부] | 모든 참여자가 장부를 공유, 공개<br>→ 거래기록의 투명성<br>* 투명성이 중요한 금융거래, 회계관리에 활용 가능 |

Blockchain Security SECURITY

# 3.8 블록체인의 적용단계

3 블록체인 분야 이슈

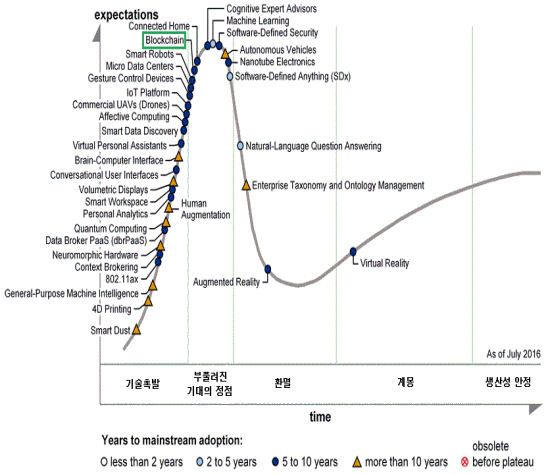
## 블록체인의 특징

### 블록체인의 장단점 및 적용단계

- 블록체인은 하이프사이클 상에서 "부풀려진 기대의 정점" 단계에 위치

| 구분 | 특징 | 내용 | 효과/제약사항 |
|---|---|---|---|
| 장점 | 탈중앙화 | P2P 기반으로 중개기관 없이 참여자 간 직접거래 가능 | 인프라 구축비용 및 중개수수료 절감 |
| | 보안성 | 다수의 참여자가 거래 정보를 공유하여 해킹이 어려움 | IT 보안비용 절감 |
| | 확장성(오픈소스) | 오픈소스를 이용해 구축, 연결, 확장 가능 | IT 구축비용 절감 |
| | 투명성 | 모든 거래기록에 공개적 접근 가능 | 관리감독 및 규제비용 절감 |
| | 신속성 | 거래의 승인 및 기록이 자동적으로 실행됨 | 신속성 향상 |
| 단점 | 확장성(처리속도) | 시간당 거래 처리속도가 제한적 | 주식시장에서와 같은 대량거래 구현이 어려움 |
| | 확장성(저장공간) | 모든 거래기록을 저장해야 하므로 저장공간이 점점 증가 | 저장용량 문제가 나타날 소지가 있음 |
| | 비가역성 | 한 번 집행된 거래는 다시 되돌릴 수 없음 | 이전된 자산이 강제로 반환될 수 없음 |

자료 : Santander InnoVentures, KB금융지주 경영연구소, 한국은행, 신영증권 리서치센터




자료 : Gartner, 신영증권 리서치센터



# 3.9 블록체인 어플리케이션 종류

3 블록체인 분야 이슈

## 블록체인에 대한 각 어플리케이션 분류

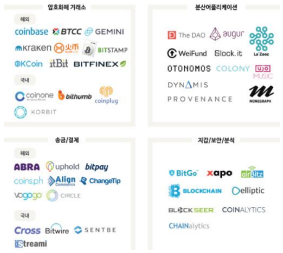
자료 1.1 출처: EBA "Cryptotechnologies, a major IT innovation and Catalyst for Change (재구성)

시가총액 상위 주요 디지털통화

| | 시가총액(백만$)[1] | 가격($)[1] | 공개시기 | 화폐단위 | 특 징 |
|---|---|---|---|---|---|
| Bitcoin | 6,347 ( 91.3) | 422.55 | 2009 | BTC | 최초의 디지털통화 |
| Ripple | 213 ( 3.1) | 0.0063 | 2012 | XRP | 이종통화간 자금이체서비스 |
| Litecoin | 152 ( 2.2) | 3.47 | 2011 | LTC | 작업증명체계 개선, 결제시간 단축(2.5분) |
| Ethereum | 64 ( 0.9) | 0.84 | 2015 | Ether | 계약처리·실행 플랫폼 결제시간 단축(12초) |
| Dash | 18 ( 0.3) | 3.03 | 2014 | DASH | 익명성 강화 구Xcoin, Darkcoin |
| Dogecoin | 14 ( 0.2) | 0.0001 | 2013 | DOGE | 소셜미디어 소액지급 |
| Peercoin | 9 ( 0.1) | 0.41 | 2012 | PPC | 채굴효율성 개선 발행한도 없음 |

주: 1) 2015.12.29일 기준, ( )내는 전체 디지털통화 시가총액 비중(%)
자료: http://www.coinmarketcap.com

공공 블록체인 (비트코인, 이더리움 기반 스타트업

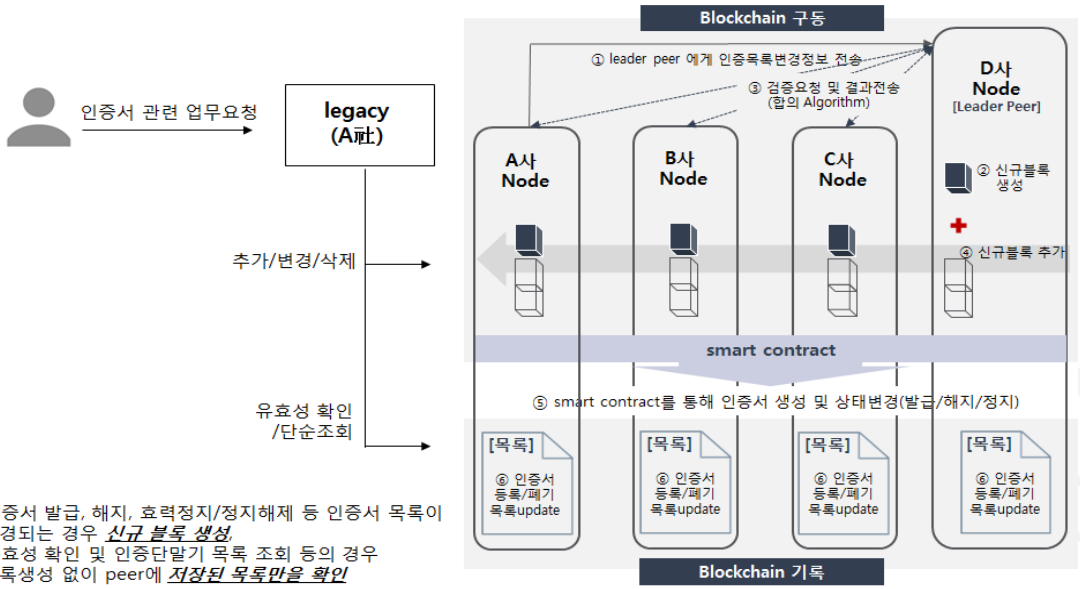


금융권대상 프라이빗 블록체인 기반 스타트업

## 3.10 블록체인 활용 예시

3 블록체인 분야 이슈

블록체인 방식 장외주식 거래과정 예시




- 인증서 발급, 해지, 효력정지/정지해제 등 인증서 목록이 변경되는 경우 ***신규 블록 생성***
- 유효성 확인 및 인증단말기 목록 조회 등의 경우 블록생성 없이 peer에 ***저장된 목록만을 확인***

출처: 금융투자협회



## 3.11 블록체인 활용 분야

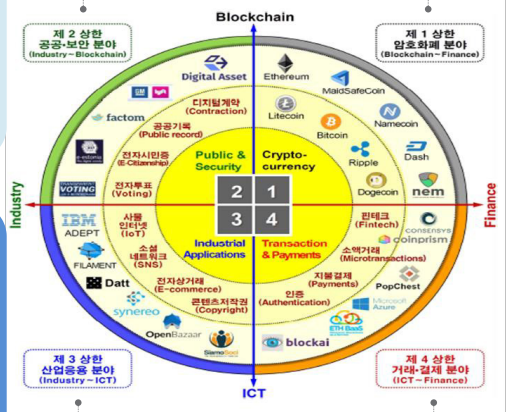
3 블록체인 분야 이슈

**공공, 보안 분야**

•활용 분야 : 디지털계약, 공공기록, 전자신분증, 전자투표 등에서 블록체인을 활용
• 사례 : 에스토니아는 블록체인과 연계한 전자시민권을 도입했으며, 스웨덴 정부는 토지등기부에 블록체인을 적용하고 있음

**산업분야**

• 활용분야 : 사물인터넷(IoT), 소셜네트워크, 전자상거래, 콘텐츠 저작권 분야에서 활용 가능, 이에 따라 IBM, 마이크로소프트, 삼성전자 등 대기업들이 모두 블록체인에 투자하고 있다.
• 사례 : 영국 가수 이머진 힙은 블록체인 기반의 플랫폼에서 음반을 발표함




**암호화폐 분야**

• 비트코인, 이더리움, 리플 등이 이에 해당되며, 이 암호화폐 분야의 기반기술이 블록체인이다.

**거래, 결제 관련 부문**

•활용분야 : 핀테크, 소액거래, 지불결제, 인증 분야 활용

• 현황 : 국내에서도 장외 주식 거래소에 블록체인 솔루션 도입이 시작되는 등 국내 금융권의 블록체인 투자가 늘어날 전망이다.

# 3.12 블록체인 대표 어플리케이션 비트코인

3 블록체인 분야 이슈

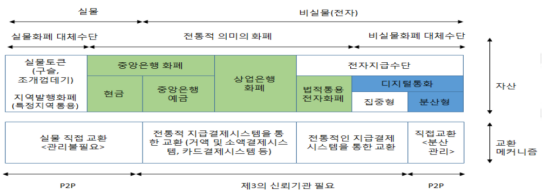
## 비트코인이란?

- 화폐(Money)는 '실물화폐'에서, 화폐의 소유 및 이전이 디지털 기록에 의해 입증되는 '가상화폐'의 형태로 진화
- 돈의 소유 여부가 공인기관에 저장된 '기록'에 의존하므로, 기록의 정확성에 대한 신뢰가 매우 중요
- 블록체인은 자산의 소유권 이력을 관리하는 거래 체인을 만듬

## Peer-to-peer 전자 화폐 시스템

- 순수한 peer-to-peer 전자 화폐는 금융 기관을 통하지 않고 온라인 지불이 한 쪽에서 다른 쪽에게 직접
- 디지털 서명은 솔루션의 일부를 제공하지만 신뢰할 수 있는 제 3자가 여전히 이중 지출을 방지해야 하는 경우 주요 이점은 상실
- 피어 투 피어 네트워크를 사용하여 이중 지출 문제에 대한 해결책을 제안
- 네트워크는 해시 기반 작업 증명 체인을 해싱하여 트랜잭션을 타임 스탬프 처리하여, 작업 증명을 다시 실행하지 않는한 변경할 수 없는 레코드 생성
- 가장 긴 체인은 발생한 일련의 이벤트에 대한 증거가 될 뿐만 아니라 CPU 전력이 가장 큰 곳에서 발생한 것으로 입증
- 대다수의 CPU 전력이 네트워크 공격을 위해 협력하지 않는 노드에 의해 제어되는 한, 가장 긴 체인을 생성하고 공격자를 앞설 것입니다. 네트워크 자체는 최소한의 구조만 필요로 함
- 메시지는 최선의 방법으로 발송되며, 노드를 떠나도 네트워크에서 재결합 할 수 있으며, 작업 증명 체인 중 가장 긴 작업 증명 체인을 사라지면 어떤 일이 일어 났는지를 증명 가능

화폐 및 교환 메커니즘 분류체계




자료: BIS(2015)



# 3.13 블록체인 비트코인 거래소의 보안 위험

3 블록체인 분야 이슈

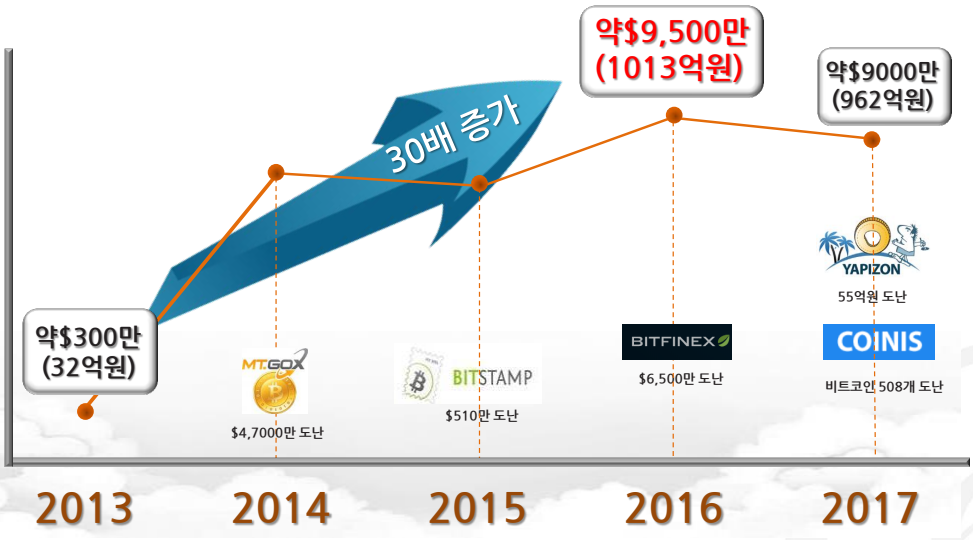
## 비트코인 거래소의 위험성

- 뉴스에서 알리고 있는 비트코인 거래소의 해킹 위험 증가

## 3.14 블록체인 코인거래소의 보안 위험

3 블록체인 분야 이슈

2014년부터 2017년까지 **3년 새 비트코인 탈취 규모가 30배 넘게 증가**했다.
미국 사이버 보안 업체인 '체이널리시스'가 공개한 '가상화폐 범죄의 본질적 변화 ' 보고서에 따르면 2013년 부터 2017년 12월까지 해킹으로 도난당한 비트코인의 액수는 약 1억 7,200만달러(도난 당시 가치 기준)에 달한다.




Blockchain Security SECURITY



## 3.15 블록체인 코인 기술 변화 - 이더리움 플랫폼

3 블록체인 분야 이슈

**이더리움이란?**

- 이더리움(Ethereum)은 **블록체인 기술을 기반으로 스마트 계약 기능을 구현하기 위한 분산 컴퓨팅 플랫폼**
- 이더리움이 제공, 이더(Ether)는 비트코인과 마찬가지로 사이버 공간에서 암호화된 가상화폐의 일종으로 거래
- 이더리움의 화폐 단위는 ETH로 표시

### 대표적인 블록체인 기술의 플랫폼 비교

**비트코인**

bitcoin

- 비트코인은 튜닝 불완전한(Turing-incompleteness) 언어인 '스크립트 언어 ' 사용
- 사용 범위 : **화폐**로서의 기능만 실행
- 비트코인의 UTXO가 표현할 수 있는 상태는 사용 했거나/ 안했거나 둘 중 하나이기 때문에 '상태 표현의 제한(Lack of state)'이 존재함
- UTXO가 블록체인의 블록헤더 데이터들을 해독하지 못해, 화폐 이외의 다른 분야의 어플리케이션 기능 실행에 한계가 있음

**이더리움**

ethereum

- 이더리움은 튜링 완전한 (Turing-completeness) 언어인 'Solidity(JAVA script)'와 'Serpent(Python) ' 을 사용
- 사용 범위 : **화폐 기능 뿐만 아니라 여러 어플리케이션들(금융, 신원관리, SNS, 의료, 예술, 정부행정, 보험 등)**을 실행
- 튜링 완전한 언어를 사용하기 때문에 복잡한 다중계약인 Smart Contract와 분산 어플리케이션 구현이 가능하다.

Blockchain Security SECURITY

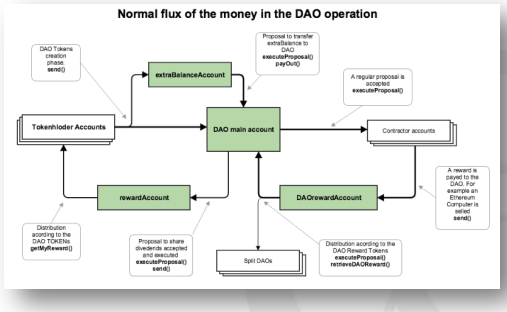
## 3.16 블록체인 DAO 해킹 사례(1/2)

3 블록체인 분야 이슈

**DAO 사례** : 2016년 6월 7일 DAO Contract 취약점을 이용해 약 360만개의 이더리움(당시 시세 640억 상당)이 도난당한 사례이다. 도난당한 코인은 전체 이더리움의 약 10%에 해당되며, 해당 사건으로 인하여 코인당 21달러에서 13달러까지 엄청난 가치 하락이 있었다.

### The DAO(Decentralized Autonomous Organization)란?

- 탈 중앙화된 자율조직으로 이더리움 창시자인 비탈릭 부테릭을 필두로 이더리움 개발진들이 개발한 시스템
- 코드로만으로 이루어진 기업
  - ☞ DAO는 실제 주소, 경영진이 없고, 모든 내용은 코드로 이루어짐
  - ☞ 모든 업무가 코드로 수행되므로 누구나 github에서 코드를 통해 업무내용을 감사할 수 있음
- DAO 토큰에 의해 경영됨
  - ☞ DAO 토큰 보유자들은 그들이 보유한 토큰에 따라 투표권을 행사하고 배당금을 분배받음






## 3.16 블록체인 DAO 해킹 사례(2/2)

3 블록체인 분야 이슈

DAO에는 DAO토큰 보유자들이 이더를 환불받을 수 있게 하는 splitDAO 기능이 있었다. 해커는 DAO.sol을 분석하면서 이 **splitDAO(이더 환불 명령 함수)가 재귀호출에 취약**하다는 사실을 발견했다. 재귀호출은 하나의 명령문으로 자신을 다시 호출하여 작업을 수행하는 방식을 의미한다.

### 해킹 프로세스

**1 DAO Token**

Split(스마트 컨트랙트) 기능 보유

* Split : 보유한 DAO Token을 일정비율의 Ether로 되돌려 받는 일종의 투자금 반환 시스템

**2 Split 결함 존재**

Split은 투자금 반환요청이후 일정시간 ' 이 지난 뒤에야 잔고가 반환요청 금액만큼 감소한다는 결함 존재

**3 해커들 Split 공략**

해커들은 자신의 투자잔고가 감소하기 전, 이 일정시간동안 투자금에 대한 반환요청을 어마어마한 수로 반복 (recursive attack)

**4 해킹 성공**

약 360만개의 이더리움 흠칫

## 3.17 블록체인 국내 코인 거래소 보안 이슈

3 블록체인 분야 이슈

방통위·과학기술정보통신부·한국인터넷진흥원(KISA) 등 관계 기관들은 2017년 10~12월 **국내 대형 가상화폐거래소 10곳의 보안실태를 점검 실시**, 서버 구조상 조사가 불가능한 2곳을 제외한 **8곳 모두 보안기준을 충족하지 못함**

두나무(업비트)·리플포유·씰렛(코인피아)·이야랩스·야피안(유빗)·코빗·코인원·코인플러그 8곳에 **총 1억4천100만원의 과태료를 부과**

8곳 중 나무(업비트), 리플포유와 야피안 3곳은 해킹 사고로 사이트가 폐쇄되고 거래가 중단된 상태

8곳 중 업비트, 빗썸, 코인원, 코빗 등 4곳은 올해부터 ***정보보호관리체계(ISMS) 인증 의무대상자***

☞ 정보통신서비스 매출액(전년도 기준)이 100억원 이상이거나 하루 평균 이용자수(전년도말 기준 직전 3개월간)가 100만명 이상인 업체는 ISMS 인증 의무대상이다.

Blockchain Security SECURITY

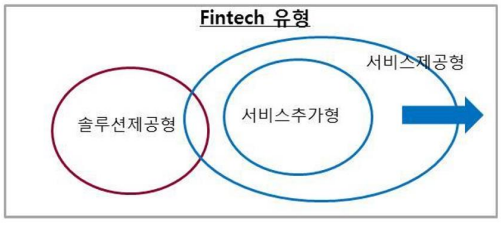


## 3.18 4차산업 모바일 핀테크

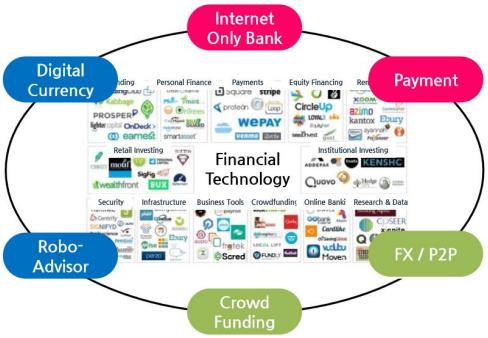
3 블록체인 분야 이슈

### 핀테크 개념 및 유형

- 핀테크(Fintech) = 금융(Finance) + 기술(Technology)
- 온라인(웹, 모바일 등)및 오프라인 상에서 제공되는 금융 서비스를 위한 정보통신기술
- 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭(금융위원회)
- 국내는 정부규제로 시장진입이 어려우나, 전세계적 非금융업 의 금융업진출화두, 핀테크관심도상승




- 솔루션 제공형(기술 솔루션을 제공하여 다양한 금융기업의 서비스를 지원하는 기업)
- 서비스 추가형(기존 핵심서비스 보유기업이 금융서비스를 추가하는 기업)
- 서비스 제공형(자체 기술을 기반으로 금융서비스를 직접 제공하는 중소형 기업)




핀테크 서비스의 유형

Blockchain Security SECURITY

## 3.19 모바일 핀테크 성장 배경

3 블록체인 분야 이슈

### 1. 소비환경의 변화

**모바일소비 및거래확대**

모바일로 인한PC에서의시간공간적 제약해소 24시간 동안언제어디서든 물건구매가능 모바일소비시장 폭발적성장 핀테크성장잠재력에 대한기대감상승

### 2. 빠른 기술혁신 속도

**빠른기술혁신 속도 융합기술발달 (핀테크)**

빠른기술혁신으로 시장잠재력 현실화,모바일 시장확대 융합기술의 발달로 결제, 송금에서 대출, 증권, 자산운용 등 서비스제공범위확대 소비자편익제공의기반조성

### 3. 現 금융시장의한계

**現금융시장성장 한계,**
**혁신금융기법 활용한 수익모델필요**

글로벌금융위기 이후 美, 유럽등글로벌금융시장 성장정체 은행대출수익확대한계, 증권업거래대금 감소수익성 저하 새로운수익모델에 대한니즈발생

### 4. 글로벌 IT기업들의 경쟁 심화

**글로벌IT기업경쟁심 화 모바일금융**

핀테크를 활용한금융시장 진출 E-commerce와 스마트폰 확산 ⇒IT기업의 금융진출 애플구글등글로벌IT 기업의 경쟁심화

Blockchain Security SECURITY



## 3.20 모바일 핀테크 글로벌 컨소시엄

3 블록체인 분야 이슈

**핀테크의 권역 별 컨소시엄 및 사례**

- 미, 중, 일 등 해외 금융기관을 중심으로 컨소시엄 구성 및 확산

### Global

R3CEV

DBS J.P.Morgan UBS HSBC + 70개 금융기관

- **Founded:** 2015년 9월
- **Description:**
  - 분산장부기술 기반의 해외송금 및 트레이딩 시스템 구현
  - 블록체인 기반 디지털 화폐 개발

### China

The Financial Blockchain Shenzhen Consortium

平安银行 PING AN BANK 腾讯 Tencent + 30개 기술사 및 금융기관

- **Founded:** 2016년 5월
- **Description:**
  - 보험 및 트레이딩 플랫폼 적용
  - 블록체인 기술이 적용 가능한 금융분야에 블록체인 적용 예정

### Japan

The Japan Bank Consortium

MIZUHO 住信SBIネット銀行 SBI Sumishin Net Bank SMFG MUFG + 30개 은행

- **Founded:** 2016년 10월
- **Description:**
  - 24시간 운영되는 실시간 국내외 송금 인프라 구현 목표
  - 2017년 봄 PoC 거쳐 서비스 출시 예정

### Korea

Financial Investment Blockchain Consortium

신한금융투자 true friend 한국証券증권 금융투자협회 Korea Financial Investment Association NH투자증권 MIRAE ASSET 미래에셋대우 + 26개 증권사

- **Founded:** 2016년 12월
- **Description:**
  - 증권사 간 인증 공동 플랫폼 구축
  - 청산결제 자동화와 장외거래 등 단계적으로 연구 및 추진

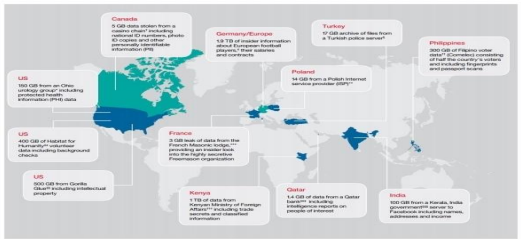
Blockchain Security SECURITY

## 3.21 모바일 핀테크 보안 이슈(1/4)

3 블록체인 분야 이슈

산업 전체가 융합되면서 보안사고의 **피해규모는 점차 커지고 있고, 전 산업에 걸쳐** 보안 이슈는 중요해지고 있습니다.

### 2016 주요데이터유출사고

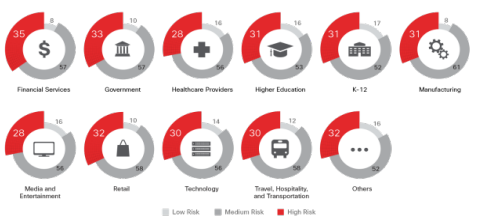


◇ 2016년 주요 데이터 유출 사고

(참고자료 : IBM X-Force 보안 동향 및 위험 보고서)

### 2016 산업별 고위험군 응용프로그램 분포도

Figure 8 Distribution of Low-, Medium-, and High-Risk Applications, by Industry




(참고자료 : CISCO CloudLock)

### 대규모 보안사고

- **정보유출건수 2년 합한 수치 2배 이상**
  40억(2016) > 10억(2014) + 6억(2015)
- **방대한 정보 유출**
- **공개된 취약점 건수 기록적**
- **유출대상** : 개인정보 (신용정보, 의료정보 등) → 비정형데이터 (이메일 내용 등)

### 전 산업에 걸쳐 노출된 보안 위협

- 금융, 공공, 유통, IT, 제조 등 거의 **전 산업에서 고위험군 어플리케이션 분포가** 약 30% 정도로 **높은 사용률**

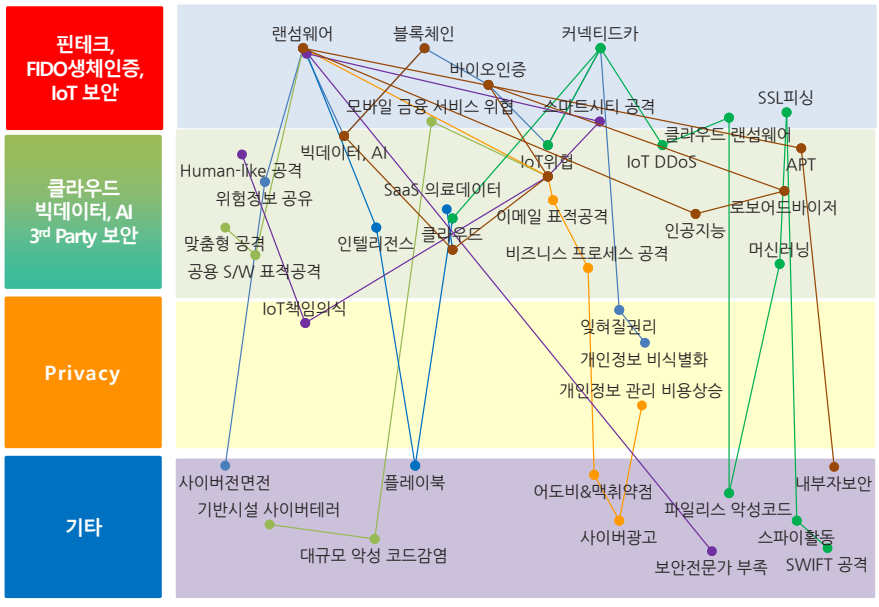
Blockchain Security SECURITY



## 3.21 모바일 핀테크 보안 이슈(2/4)

3 블록체인 분야 이슈

### 보안 시장 이슈




### 차세대 중점 보안

- **랜섬웨어, IoT 기기를 이용한 공격, 빅데이터, 클라우드, AI, 머신러닝** 등 신기술의 지속적 이슈 예상
- **새롭게 파일리스 악성코드(메모리 상주 악성코드), 공용 S/W 표적 공격, SWIFT 공격이 대두**

- KISA정보보호10대이슈
- 사이버위협 인텔리전스 선정 사이버공격
- 트렌드마이크로 보안예측보고서
- 팔로알토 보안전망
- 시만텍 10대 보안 전망
- 포티넷 보안 위협 전망
- 금융보안원 10대 이슈

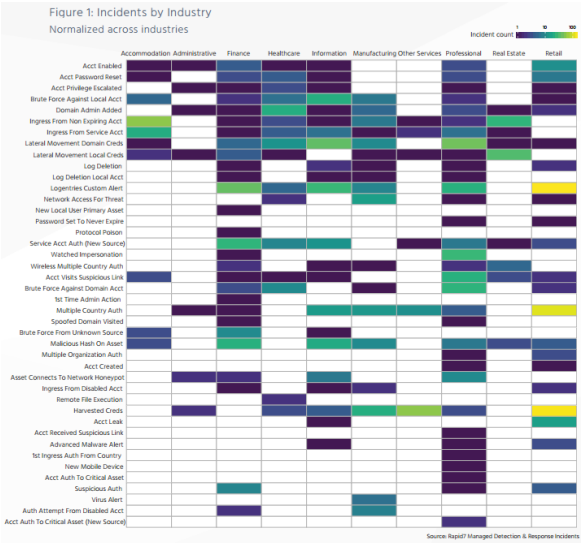
Blockchain Security SECURITY

## 3.21 모바일 핀테크 보안 이슈(3/4)

3 블록체인 분야 이슈

금융권의 사고는 전문가 집단 다음으로 종류가 많았으며, 그 중에서도 **심각성이 높은 사고가 23종으로 가장 많이 나타나고 있어 다양한 위협에 대한 보안을 할 수 있어야 합니다.**

**2017 1분기 산업별 사건 분류**




(참고자료 : Rapid7 Threat Intelligence Report 2017 Q1)

**금융권 사고 분류**

**총 42개 사고분야 중**
- **금융분야 :** 28종 집계, **상위 23종 심각**
- **전문가 집단 :** 33종 집계, **상위 23종 심각**

**2017년 대표적인 사건**

- 해커조직 **신용카드 정보 등 탈취**해 12억 원 빼돌려(1.4, KBS)
- 핸디소프트 그룹웨어 **코드서명 악성코드 유포**에 활용(1.19 전자신문)
- 사이트 접속자 정보 다 빨아들인다, **북한 원홀 해킹**(1.24, 중앙일보)
- 미국 동부 인터넷 마비 시킨 **'미라이' 악성 파일, 국내서도 발견**(1.25, 이데일리)
- 또 뚫린 **사이버 안보**...이번엔 **프린터 해킹** (2.9, 채널A) o "10만원 내면 풀어줄게"... **에레보스 랜섬웨어** 감염 주의 (2.17, 전자신문)
- 설문지로 위장한 **국내 맞춤형 랜섬웨어 주의**(2.8, 아이티데일리)
- **아시아나항공 홈페이지 해킹** 당해...접속 불가능(2.20, YTN)
- 국내 **홈페이지 디도스 공격** 주의, **웹 최신버전 업데이트** 필요(3.7, 이데일리)
- 3.20 악몽 재현? **금융사 표적** 北 사이버 공격(3.8, 전자신문)

Blockchain Security SECURITY 블록체인 시큐리티



## 3.21 모바일 핀테크 보안 이슈(4/4)

3 블록체인 분야 이슈

2016년 해킹사고는 **금전목적의 공격성향이 강해졌습니다.** 공격자들이 피해자에게 간접적인 방식이 아닌 직접적인 과금 또는 금전탈취를 통해서 수익을 창출하게 되면서 **금융권(은행, 증권사, 보험, 카드사 등)의 직접적인 공격이 발생**하였습니다. 이전에는 금융권공격의 대다수가 국외 금융권이 대상이라면, 최근 몇 년간 2015년 DD4BC의 지방은행 및 증권사 디도스 공격, 2016년 방글라데시의 스위프트(SWIFT)공격 사례와 같이 직/간접적인 공격대상에 국내 금융권이 포함되는 경우가 급격히 증가하였습니다.

| 2016년 | 국가 | 사건요약 | 상세내용 |
|---|---|---|---|
| 2월 | 한국 | 선불카드 정보 유출로 3억원 상당 피해 | • 국내 카드회사의 인터넷 홈페이지가 중국 해커의 소행으로 보이는 공격을 당해 수백 장의 50만 원권 기프트카드(무기명 선불카드) 정보가 유출<br>• 카드번호 생성기를 이용해 유효기간이 같은 카드번호 16자리를 확인하고, 무작위 숫자 입력 프로그램으로 CVC 번호도 알아낸 것으로 추정 |
| | 방글라데시 | SWIFT를 이용한 금전탈취 | • 국제 은행 간 자금결제 통신망 기구인 '스위프트'(SWIFT)'를 이용하여 방글라데시 중앙은행의 미국 뉴욕 연방준비은행 계좌에서 약 8100만달러(약 905억원)를 이체<br>• 이후 베트남과 필리핀, 에콰도르에서도 비슷한 해킹사고 발생 |
| 5월 | 일본 | ATM기에서 14억엔 인출 | • 위조 신용카드로 전국 17개 광역지자체의 현금자동입출금기(ATM)에서 2시간 반 만에 14억4000만엔(약 155억5000만원)이 인출<br>• 남아프리카은행에서 유출된 신용카드 정보로 제작한 위조카드 사용 |
| | 한국 | 한국은 홈페이지 디도스 | • 어나니머스(Anonymous)가 우리나라의 중앙은행인 한국은행을 대상으로 디도스 공격을 감행<br>• 12일 저녁 8시 50분께부터 13일 새벽까지 수차례에 걸쳐 디도스 공격을 시도하였으나 피해 미발생 |
| 11월 | 영국 | 테스코뱅크 해킹사고로 2만명 금전피해 | • 당좌예금(Current account) 고객 13만 6000명 중 4만명이 해킹 공격을 받았으며 이중 2만여 명은 직접적인 금전적 피해 발생하였으나 정확한 금액은 미확인 |

Blockchain Security SECURITY 블록체인 시큐리티

## Contents

# Ⅳ. 보안 위협





## 4.1 오픈 소스 보안 취약점 – Structs2 (1/4)

### Apache Structs2

- 오픈소스는 소스코드가 공유되어 있기 때문에 코드리뷰를 통해 취약점이 빠르게 검토되어 제거될 것이라는 예상과는 다르게 오히려 취약점을 이용한 공격이 확산되고 있음
- 다음은 오픈소스 배포 시점과 취약점 발견 시점에 대한 표

오픈소스에서 발생한 취약점의 배포 시점과 발견 시점

| | Apache Structs2 | HeartBleed | 쉘쇼크 | Freak | 고스트 | 베놈 |
|---|---|---|---|---|---|---|
| 배포시점 | 2006 | 2011 | 1989 | 1990 | 2000 | 2004 |
| 발견 시점 | 2013 | 214 | 2014 | 2015 | 2015 | 215 |
| Component | Structs | OpenSSL | Bash | OpenSSL | GNU C Library | QEMU |

# 4.1 오픈 소스 보안 취약점 – Structs2 (2/4)

4 보안 위협

## Apache Structs2

- 2013년 Apache에서 개발한 'Structs2'에 존재하는 보안 취약점을 이용한 공격도구가 만들어짐
- 공격자는 특정 매개변수를 통해 공격 구문을 전송할 수 있으며, 원격 명령 및 파일 생성으로 시스템 권한 획득 가능

### 2013년 Apache Structs2 취약점으로 인한 피해

"Apache Structs2 공격 툴에 의한 집중 공격으로
사이트 접속 장애 및 정보유출 피해 발생 "

'Apache Structs2' 보안 취약점을 악용한
신종 해킹 주의 및 업데이트 권고

### 2017년 Apache Structs2 취약점으로 인한 피해

'중국발 사드 보복' 명분 내건 사이버공격 확산
민관 홈페이지 피해…한국인터넷진흥원 "홈페이지 보안 관리 주의 권고"

[긴급] 중국 해커들, Struts2 자동화 공격툴과 공격방법 공유중...주의

중국발 해킹 공격 이미 진행형! 두려움보다 철저함 필요하다

중국 해커조직의 한국 웹사이트 공격 루트 '아파치 스트럿츠'

아파치 스트럿츠 취약점 노린 공격 확산
"원격코드실행 공격에 2.3.5~2.3.31 버전, 2.5~2.5.10 버전 노출"

韓 사이버공습 계획 中 해커들, 아파치·SQL 등 보안 취약점 노린다



# 4.1 오픈 소스 보안 취약점 – Structs2 (3/4)

4 보안 위협

## Apache Structs2

- 최근에 Apache Strutcs2 취약점을 이용한 원격 코드 실행 가능 취약점 (CVE-2017-5638)이 발견됨
- 해당 취약점은 Jakarta Multipart 파서를  기반으로 한 파일 업로드 수행 시 HTTP Request 헤더의 Content-type을 변조해 원격 코드 실행
- 중국 해커 집단이 이 취약점을 이용해 공격할 예정이라는 기사 보도로 이슈가 됨

Jakarta Struts

| Summary | |
|---|---|
| Who should read this | All structs2 developers and users |
| Impact of vulnerability | Possible RCE when performing file upload based on Jakarta Multipart parser |
| Maximum security rating | High |
| Recommendation | Upgrade to Structs 2.3.32 or Structs 2.5.10.1 |
| Affected Software | Structs 2.3.25-Structs2.3.31, Structs2.5-Structs2.5.10 |
| CVE identifier | CVE-22017-5638 |

보안전문가, '아파치 스트럿츠(Apache Struts) 2 취약점'을 이용한 웹서버 공격 경고
KISA, 아파치 스트럿츠 원격 코드 실행 취약점 업데이트 권고

[보안뉴스 원병철 기자] 중국의 유명 해커조직들이 총동원령을 내리며 우리나라 웹사이트를 무차별적으로 공격하고 있다. 해커조직들은 디페이스 공격을 통해 홈페이지를 변조한 후 사드배치 반대와 롯데그룹에 대한 반감을 노골적으로 드러내고 있다. 특히, 3월 7일 한국에서 개최되는 국제대회 관련 웹사이트는 물론 패션브랜드와 교육관련 웹사이트 등을 공격한 후, 총동원령이 내려진 상태다. 외에도 중국독수리연합(Ch 이 우려되는 상황이다.

아파치 스트럿츠(Struts)가 원격코드실행(RCE) 취약점을 품은 것으로 드러났다. 스트럿츠는 국내외서 널리 쓰이는 자바 웹애플리케이션용 오픈소스 프레임워크다. 이를 사용 중인 다수 웹서버 개발자와 운영자에게 취약점이 해결된 새 버전 업데이트가 요구된다.

한국인터넷진흥원(KISA) 보호나라 인터넷침해대응센터(KrCERT/CC)는 지난 7일 보안공지를 통해 아파치 스트럿츠 RCE 취약점(CVE-2017-5638)에 대응한 최신 버전 업데이트를 권고했다.

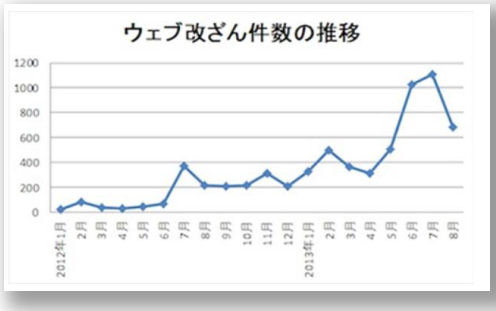
## 4.1 오픈 소스 보안 취약점 – Structs2 (4/4)

4 보안 위협

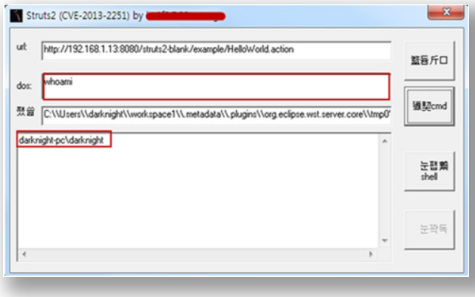
### 발생 내용

- 일본의 JPCERT/CC에 접수된 피해 신고 건수는 2013년 5월부터 급증

### JPCERT/CC에 접수된 피해 신고 건수 추이




### 툴을 이용한 원격 명령 실행




Blockchain Security SECURITY

이글루시큐리티 '보안 위협 사례로 보는 오픈 소스'



## 4.1 오픈 소스 보안 취약점 – OpenSSL (1/3)

4 보안 위협

### OpenSSL(HeartBleed)

- OpenSSL은 PC와 서버간에 데이터를 주고 받을 때 통신 내용의 암호화를 지원
- HeartBleed는 공격자가 정해진 크기보다 많은 데이터를 요청함으로써 발생

### HeartBleed

OpenSSL
HeartBleed

통신 구간 암호화를 위해 많이 사용되는 OpenSSL라이브러리에서 서버에 저장된 중요 메모리 데이터가 노출되는 취약점

### 관련 기사

Blockchain Security SECURITY

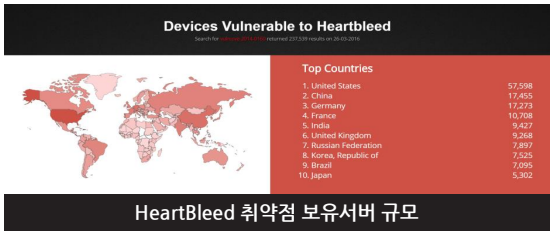
ZDNet Korea '한국, 세계2위 하트블리드 취약점 보유국'

# 4.1 오픈 소스 보안 취약점 – OpenSSL (2/3)

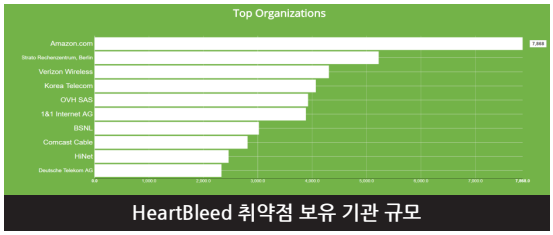
4 보안 위협

## OpenSSL(HeartBleed)

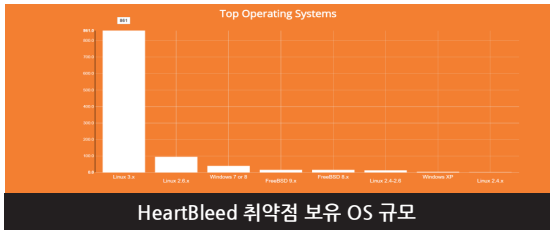
- 2016년 3월 쇼단에서 공개한 HeartBleed 취약점 보고서의 우리나라 순위는 아래와 같음
- 취약점 서버 보유 국가  8위, 취약점 보유 기관 : 4위(Korea Telecom)



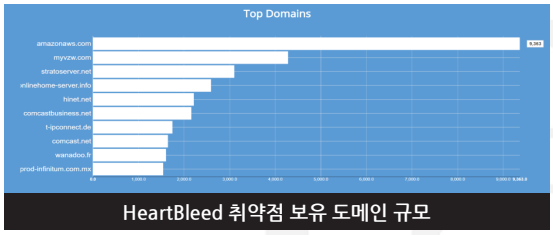

HeartBleed 취약점 보유서버 규모




HeartBleed 취약점 보유 기관 규모




HeartBleed 취약점 보유 OS 규모




HeartBleed 취약점 보유 도메인 규모

Blockchain Security SECURITY

쇼단 'Sample Report onHeartbleed'



# 4.1 오픈 소스 보안 취약점 – OpenSSL (3/3)

4 보안 위협

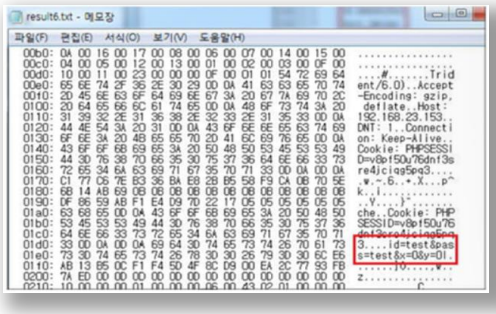
## 발생 내용

- SSL 사용 및 취약한 사이트 통계에서 우리나라는 SSL사이트 중 약 56%가 취약

### SSL 사용 및 취약한 사이트 통계

| DOMAIN | VULNERABLE SITES | TOTAL NO. OF SITES USING SSL | TOTAL NO. OF SITES | PERCENTAGE |
|---|---|---|---|---|
| KR | 57 | 102 | 2839 | 56% |
| JP | 534 | 1195 | 17852 | 45% |
| RU | 2708 | 6298 | 38573 | 43% |
| CN | 66 | 164 | 10430 | 40% |
| GOV | 26 | 69 | 829 | 38% |
| BR | 866 | 2648 | 16328 | 33% |
| AU | 553 | 1743 | 7811 | 32% |
| UK | 1073 | 3765 | 19062 | 28% |
| DE | 1544 | 6324 | 34275 | 24% |
| FR | 594 | 3068 | 13033 | 19% |
| IN | 611 | 3462 | 13204 | 18% |
| Total | 8632 | 28838 | 174336 | 30% |

### 서버 메모리 정보 노출




Blockchain Security SECURITY

이글루시큐리티 '보안 위협 사례로 보는 오픈 소스'

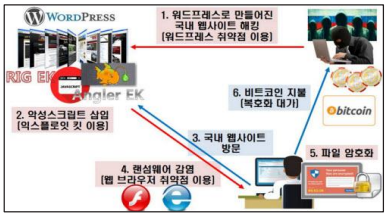
# 4.1 오픈 소스 보안 취약점 – 워드프레스 (1/2)

4 보안 위협

## 워드프레스

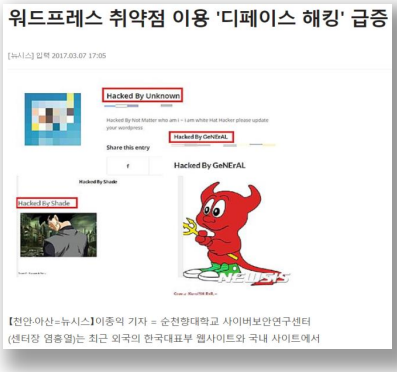
- 워드프레스는 누구나 무료로 설치형 홈페이지를 만들 수 있는 오픈 소스 소프트웨어
- 개방 커뮤니티에 공개된 플러그인, 테마를 추가하여 운영 가능

### 워드프레스




워드프레스 취약점을 이용해 악성스크립트를 삽입하여 랜섬웨어에 감염시킨 사례
워드프레스 취약점은 위와 같이 악성스크립트를 삽입하는 방식으로 공격함

### 관련 기사


워드프레스 취약점 이용 '디페이스 해킹' 급증

[뉴시스] 입력 2017.03.07 17:05

Hacked By Unknown
Hacked By GeNErAL
Hacked By Shade

【천안·아산=뉴시스】이종익 기자 = 순천향대학교 사이버보안연구센터 (센터장 염흥열)는 최근 외국의 한국대표부 웹사이트와 국내 사이트에서

보안뉴스 '워드프레스 취약점 악용한 랜섬웨어 주의보'



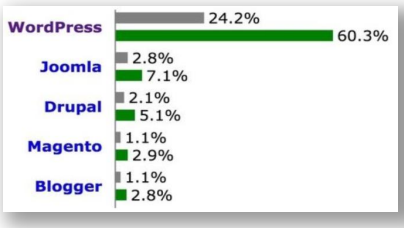
# 4.1 오픈 소스 보안 취약점 – 워드프레스 (2/2)

4 보안 위협

## 워드프레스

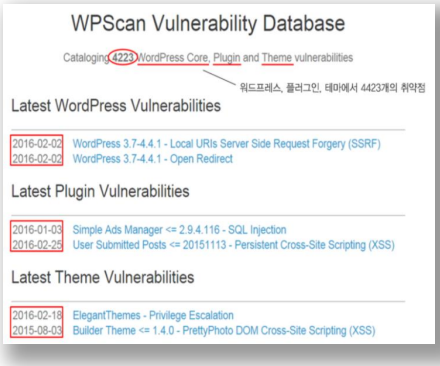
- 워드프레스의 한 취약점을 이용해 수 십만개의 워드프레스 사이트를 감염시킬 수 있음

### 워드프레스 취약점 통계




W3TECHS에 따르면 워드프레스 사이트가 전체 웹의 24%를 차지함
따라서 워드프레스 취약점 발견 시 피해가 클 것으로 예상

### 워드프레스 취약점 데이터베이스




이글루시큐리티 '보안 위협 사례로 보는 오픈 소스'

## 4.2 타겟형 랜섬웨어 확산

4 보안 위협

2016년 **다양한 종류의 신종 랜섬웨어들이** 등장하였던 반면, 2017년에는 기업을 대상으로 전사적으로 감염을 시키는 등 **특정 표적을 선정한 타겟형 랜섬웨어**가 확산될 전망입니다.

**2016 랜섬웨어의 해(年)**

**작년 한 해 발견된 대표적인 랜섬웨어**
- 모바일 결제방식이 추가된 록쿠(Rokku)
- 매크로 기능 이용, 한글문서까지 감염시킨 록키(Locky)
- 암호화된 파일의 몸값 낮아짐
- **랜섬웨어 감염소요시간 = 3초**
- 블랙마켓 랜섬웨어 제작비 : 약 45만원
- **국내 피해액 : 3000억원 이상,** 1900억원 (2015)

랜섬웨어 몸값줘도 복구 확률 50% 미만

**2017 타겟형 랜섬웨어**
- 기업 및 공공기관, 사회기반시설 등 **특정 표적을 선정하여 시스템 내부의 모든 파일을 암호화하여 몸값을 요구하는 형태가 증가**할 것
- 로컬 주요 보안위협 세력의 랜섬웨어 유포 가세
- **기업 대상 주요 서버 및 중앙관리 통한 전사 랜섬웨어 감염**
- 모바일 및 IoT **디바이스 대상 랜섬웨어 유포**

Blockchain Security SECURITY



## 4.3 4차산업 IOT의 위협이 되는 오픈 소스 위협 (1/3)

4 보안 위협

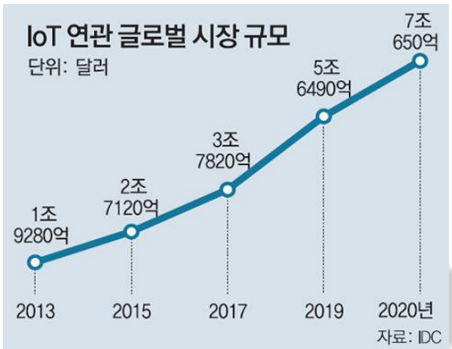
**IoT 생명은 '연결', 핵심은 오픈소스 SW!**

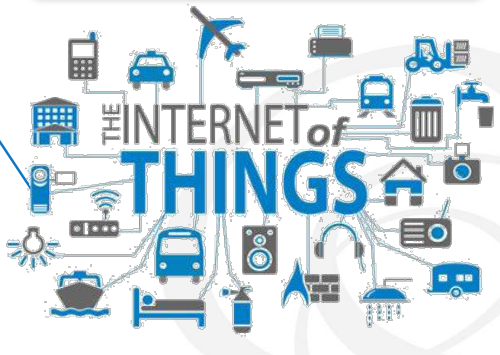
오픈소스의 가장 큰 장점은 우수한 상호 호환성!

동일한 소스코드가 다양한 사물에 탑재되면
IoT 확산에 있어 가장 효과적 방법

**오픈소스의 위협 = IoT 전체의 위협**

- 동일한 소스코드가 다양한 사물에 탑재 되므로 하나의 취약점 발견으로도 IoT 전체 위협 가능




**4차 산업혁명과 위협 - IoT 위협**

IoT를 구성하는 연결기기의 수
2014년 37억 5000여대
2015년 48억 8000여대
2020년 2,500억대 예상

Blockchain Security SECURITY

## 4.3 4차산업 IOT의 위협이 되는 오픈 소스 위협 (2/3)

4 보안 위협

위키리크스가 CIA의 '해킹 전략'이 담긴 내부 문건을 폭로했다

뉴스1
게시됨: 2017년 03월 08일 09시 20분 KST | 업데이트됨: 2017년 03월 08일 09시 28분 KST

25 0

CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA
Larry Downing / Reuters

미국의 폭로 전문 웹사이트 위키리크스가 미국 중앙정보국(CIA)의 해킹 정보 관련 문건 9000여 건을 폭로했다. 삼성전자의 스마트 TV나 애플의 아이패드 등도 감청 도구로 활용한 것으로 드러났다. 문건의 양이나 내용 등만 봐도 큰 파문이 일 것으로 보인다.

7일(현지시간) AFP통신에 따르면 위키리크스는 웹사이트에 CIA 사이버 정보센터의 문건을 게재했다. CIA 사이버 정보센터는 미국 버지니아주 랭리에 본부를 둬, 육일 프랑크루트에 지사를 두고 있는 조직이다.

"TV·스마트폰이 CIA 해킹·감시도구"…위키 폭로에 보안 우려↑

송고시간 | 2017/03/08 11:13

삼성애플구글 등 제품 활용…"스노든 폭로보다 파장 커"

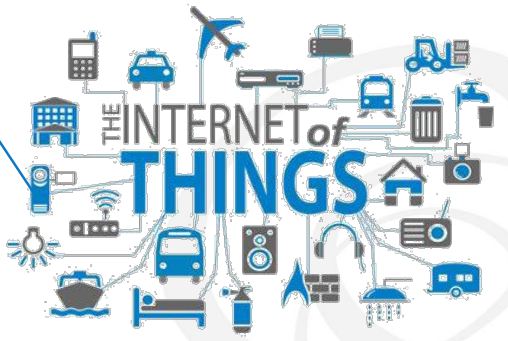
(서울=연합뉴스) 김남권 기자 = 미국 중앙정보국(CIA)이 TV와 스마트폰 등을 해킹·감시 도구로 이용했다는 웹사이트 위키리크스의 폭로로 보안 우려감이 더욱 커지고 있다.

위키리크스가 7일(현지시간) 공개한 CIA 사이버 정보센터의 문서가 사실로 밝혀질 경우 정보기관이 마음만 먹으면 일상생활의 필수품으로 자리 잡은 제품들을 얼마든지 도감청 도구로 활용할 수 있음을 보여준다.



위키리크스 폭로 "TV·스마트폰이 CIA 해킹·감시도구"
[EPA=연합뉴스 자료사진]

스마트 TV, 냉장고 등
연결된 IoT로 번지는 위협




**TV 스마트폰 등 IoT 기기들, CIA 해킹도구로 활용**

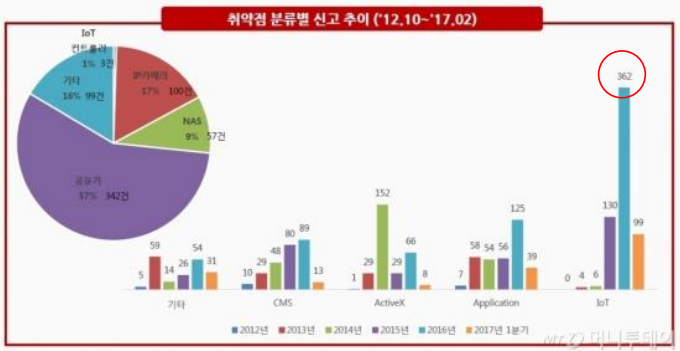
위키리크스가 가 미국 중앙정보국(CIA)의 해킹 정보 관련 문건 9000여건 폭로…. 삼성전자의 스마트 TV 등 감청 도구로 활용….

Blockchain Security SECURITY



## 4.3 4차산업 IOT의 위협이 되는 오픈 소스 위협 (3/3)

4 보안 위협

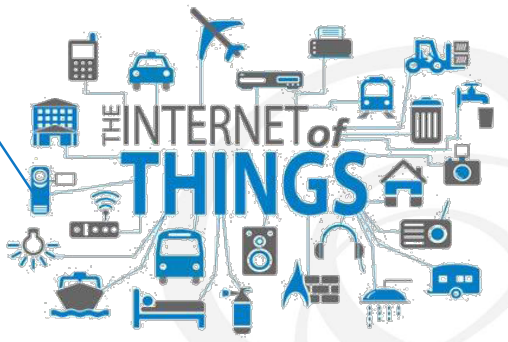



(참고자료 : 한국인터넷진흥원(KISA)이 집계한 지난 1분기 신고포상제 통계)

**IoT 공격으로 인한 피해액**

13조4000억 원 (2015) → **17조7000억 원(2020년)**

(참고자료 : KT경제경영연구소)




**IoT 취약점 신고 건수 및 피해액 증가**

2015년 기준 13조4000억 원 에서 2020년 17조7000억 원 으로 증가할 것이라는 예상

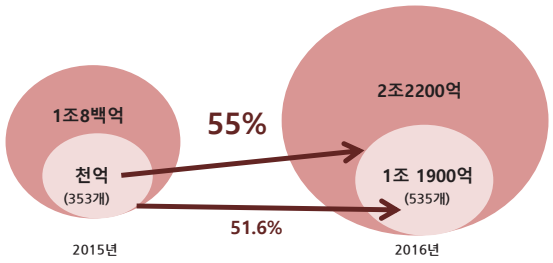
Blockchain Security SECURITY

## 4.4 4차산업 클라우드의 위협이 되는 오픈 소스

4 보안 위협

### 클라우드의 성장

AI, 빅데이터 등 혁신기술이 이끄는 4차 산업혁명 시대에 클라우드로의 전환이 필수적이라는 인식이 확산되면서 국내 클라우드를 사용하는 이용자가 증가하고 있으며, 재작년에 비해 작년은 5배, 올해 10배 이상 증가하는 추세




(참고자료 : Cisco CloudLock)

**클라우드로 인한 대표적인 보안 위협**

- 자원 공유 및 집중화에 따른 서비스 장애
- 법규, 규제의 문제
- 정보 위탁 및 사용 단말에 따른 정보 유출
- 사용 단말 다양화에 따른 정보유출
- 가상화 취약점 상속
- 분산 처리에 따른 보안 적용의 어려움

**CSA에서 발표한 9대 보안 위협**

1. 데이터 취약점
2. 데이터 손실
3. 계좌 하이재킹
4. 안전하지 않은 API
5. 서비스거부공격
6. 내부자 위협
7. 클라우드 서비스 남용
8. 불충분한 Due diligence
9. 공유 기술

(참고자료 : Cloud Security Alliance)

Blockchain Security SECURITY



## 4.5 4차산업 빅데이타 보안 위협

4 보안 위협

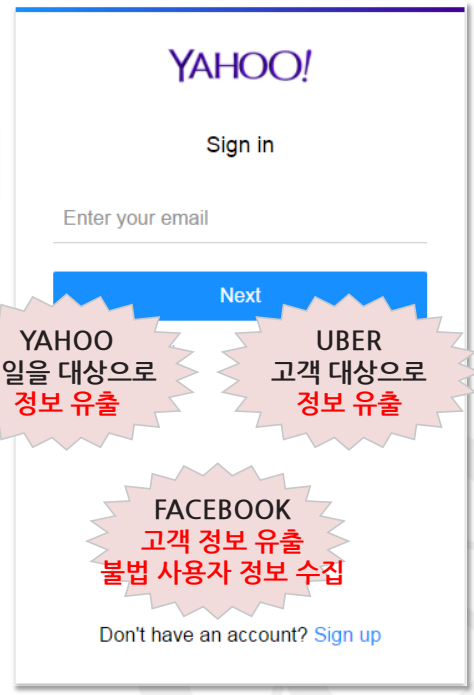
야후 또 털렸다. 10억 명 개인 정보 유출 뒤늦게 확인
Posted 2016. 12. 15 오전 10:44:28

"또 털렸다"...야후 해킹으로 10억명 개인정보 유출

야후가 2013년에 해킹을 당했고 사상최대인 10억명의 개인정보가 유출됐다
연합뉴스
게시됨: 2016년 12월 15일 09시 56분 KST | 업데이트됨: 2016년 12월 15일 09시 56분 KST

사상최대 10억명의 개인정보 유출

- 사용자 이름
- 이메일주소
- 암호화된 비밀번호
- 전화번호
- 생년월일




YAHOO 메일을 대상으로 정보 유출

UBER 고객 대상으로 정보 유출

FACEBOOK 고객 정보 유출 불법 사용자 정보 수집

Blockchain Security SECURITY

## 4.6 4차산업 모바일 보안 위협

4 보안 위협

**최신 스마트폰, 보안 취약점이 200개**

**문자 받기만 해도 무차별 해킹, "안드로이드 기기 95%가 보안 취약점에 노출되어 있다"**

### 스마트폰 영역 별 보안 위협 요소

| 영역 | 위협요소 |
|---|---|
| 디바이스 | 이동 저장매체 감염 |
| | 분실 및 도난 |
| | 데이터 노출 |
| 네트워크 | 데이터 스피닝 및 변조 |
| | Wi-Fi 해킹 |
| | DDoS 공격 |
| | 음성 도청 및 감청 |
| | 비인가 AP |
| 플랫폼 | 스마트폰과 PC 연결을 통한 악성코드 전파 및 접근 |
| | 외장메모리를 이용한 악성코드 전파 |
| | 루팅 및 탈옥 |
| | OS 보안 취약점 |

| 영역 | 위협요소 |
|---|---|
| 애플리케이션 | 보안 매커니즘을 우회한 악성 프로그램 등록 |
| | GPS를 통한 위치 정보 노출 |
| | 이메일을 통한 악성코드 첨부 및 스팸 메일 발송 |
| | 웹사이트를 통한 피싱 및 악성코드 다운로드 |
| | 개인 정보 유출 |
| | 장치이용 제한 |
| | IoT 연결 기기에 대한 컨트롤 장악 |
| | 패스워드 크랙 |
| | 애플리케이션 취약점을 이용한 악용 |
| | 애플리케이션 설치 동의 우회 |
| | 부정과금 유발 |
| | 공개된 Exploit 공격 |

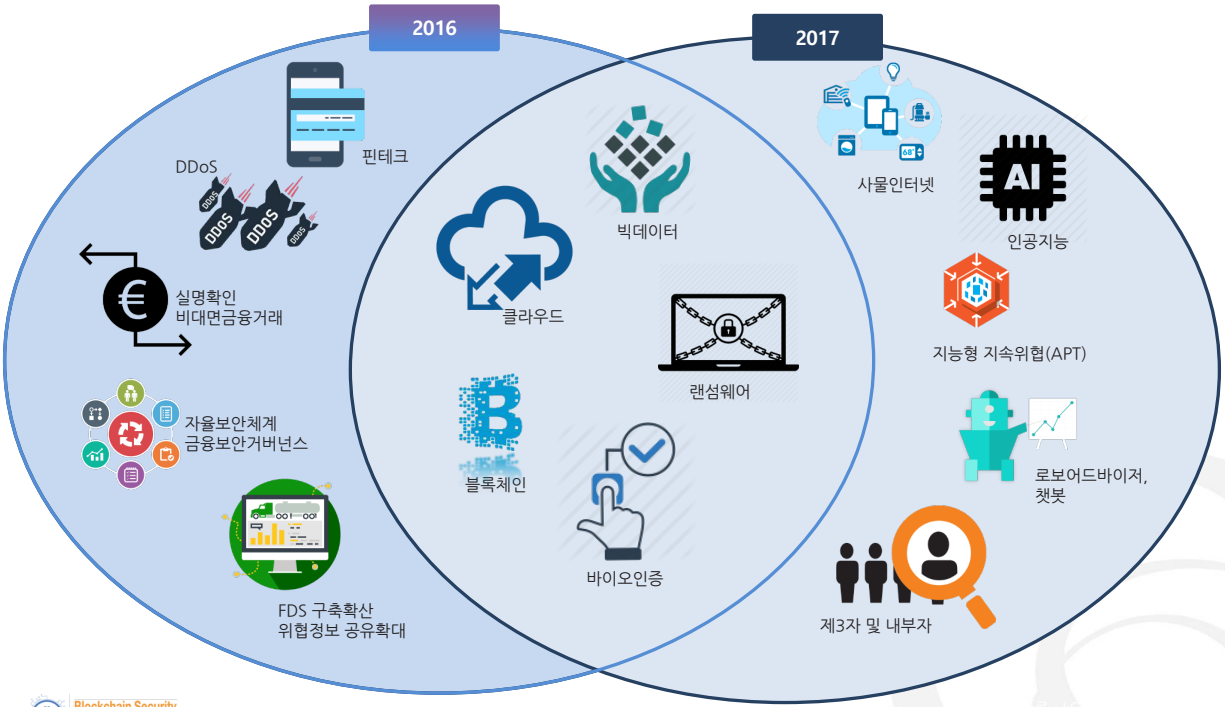
(참고자료 : LG CNS 블로그)

Blockchain Security SECURITY



## 4.7 금융권 보안 위협 (1/3)

4 보안 위협

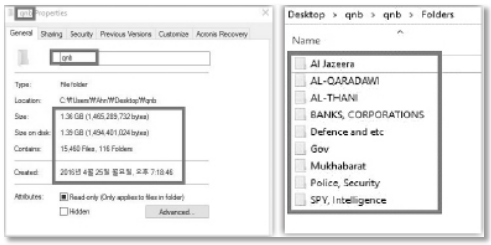



Blockchain Security SECURITY

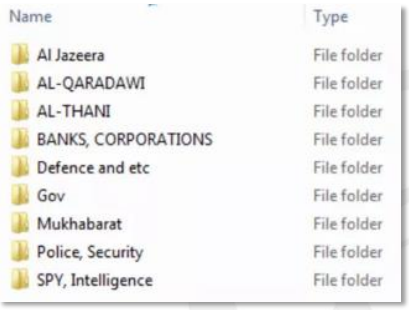
## 4.7 금융권 보안 위협 (2/3)

4 보안 위협

북아프리카의 대표적 은행인 카타르중앙은행의 고객계좌정보가 무더기로 유출되었다. '카드마스터'파일에는 수백명의 한국인 개인정보도 포함된다고 한다.



QNB 압축파일 압축해제내역, QNB파일 중 폴더내역의 폴더명




데이터 덤프파일

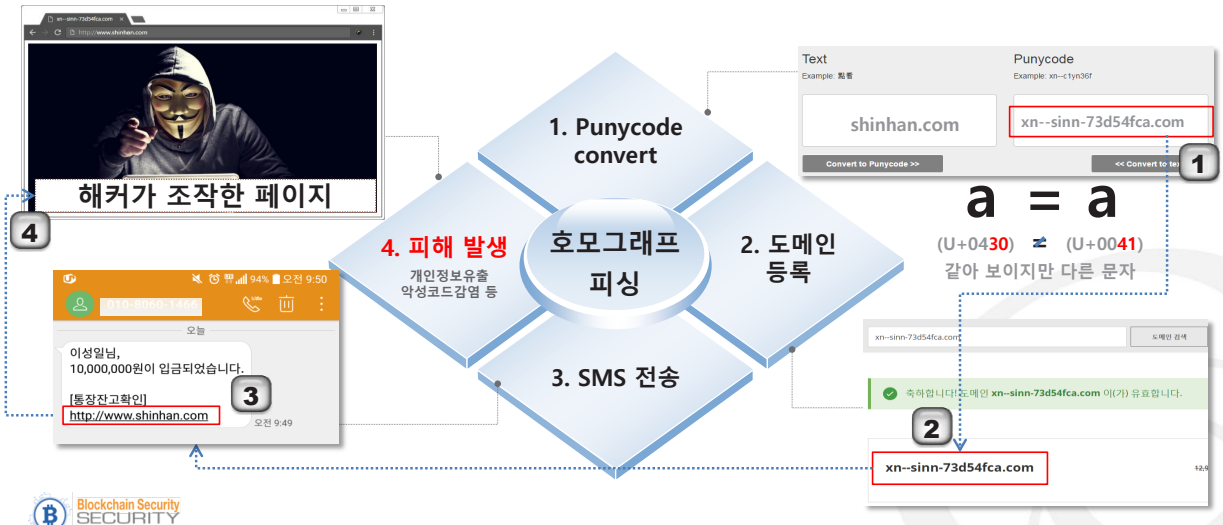


## 4.7 금융권 보안 위협 (3/3)

4 보안 위협

### IDN 호모그래프 공격

- Punycode를 이용한 도메인 피싱공격
- 평범한 알파벳처럼 보이는 특수문자를 도메인으로 등록하여 shinhan.com으로 보이게 함으로써 사용자에게 피싱 공격이 가능합니다.

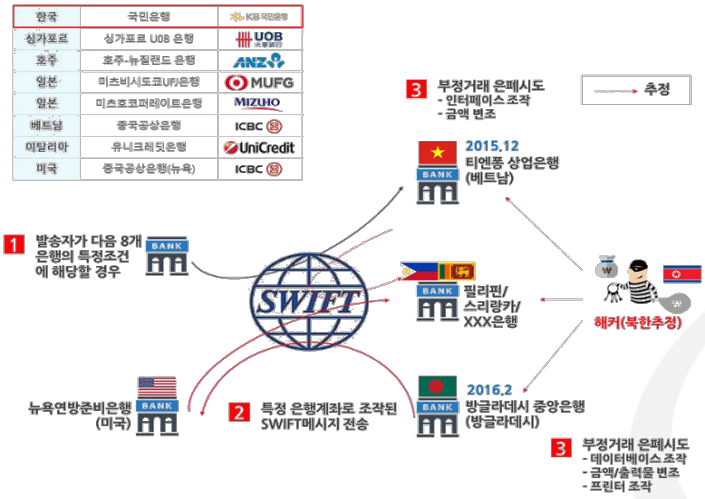


# 4.8 금융권 보안 위협 사례 (1/7)

4 보안 위협

## SWIFT 취약점 동향

- 2016년 금융권 대상 해킹사고 중 대표적인 사례로, 공격자들은 글로벌 금융거래 정보를 은행과 기타 금융기관 간 연결 전송기능을 제공하는 SWIFT(Society for Worldwide Interbank Financial Telecommunication)를 이용해 제작된 악성코드로 방글라데시 중앙은행 계좌에서 8,100만 달러(약 966억)원을 탈취



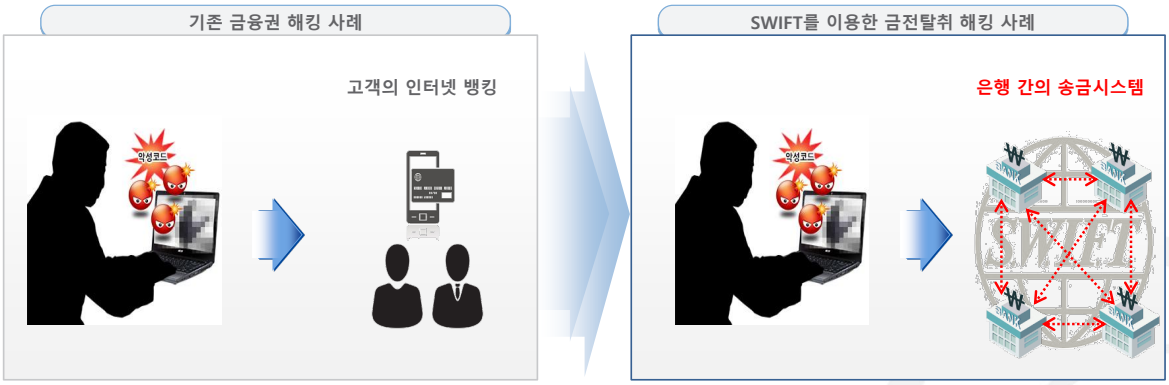



# 4.8 금융권 보안 위협 사례 (2/7)

4 보안 위협

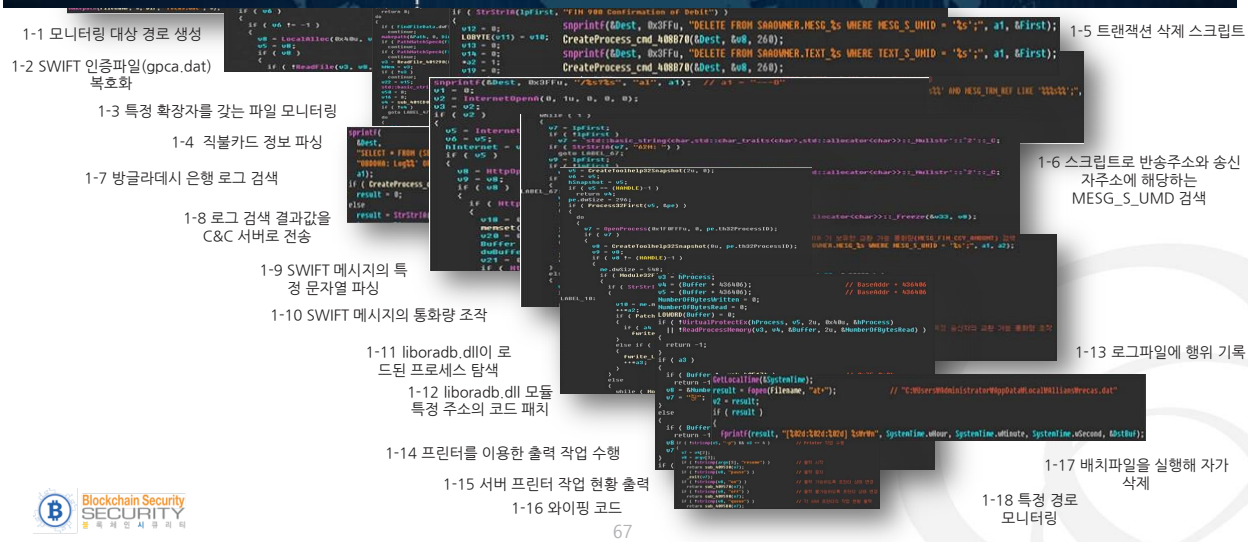
## SWIFT 취약점 동향 2

- SWIFT는 1973년 은행들 간의 정보전달 체계 및 표준화된 지불체계를 구축하기 위해 만들어진 은행연합 기구로 현재 200개국 이상에서 10,800개 이상의 은행들이 참여
- SWIFT는 ISO 9362에 정의된 “은행들 간의 지불 체계를 위한 금융기관 식별코드”를 의미



## 4.8 금융권 보안 위협 사례 (3/7)

4 보안 위협



1-1 모니터링 대상 경로 생성
1-2 SWIFT 인증파일(gpca.dat) 복호화
1-3 특정 확장자를 갖는 파일 모니터링
1-4 직불카드 정보 파싱
1-5 트랜잭션 삭제 스크립트
1-6 스크립트로 반송주소와 송신 자주소에 해당하는 MESG_S_UMD 검색
1-7 방글라데시 은행 로그 검색
1-8 로그 검색 결과값을 C&C 서버로 전송
1-9 SWIFT 메시지의 특정 문자열 파싱
1-10 SWIFT 메시지의 통화량 조작
1-11 liboradb.dll이 로드된 프로세스 탐색
1-12 liboradb.dll 모듈 특정 주소의 코드 패치
1-13 로그파일에 행위 기록
1-14 프린터를 이용한 출력 작업 수행
1-15 서버 프린터 작업 현황 출력
1-16 와이핑 코드
1-17 배치파일을 실행해 자가 삭제
1-18 특정 경로 모니터링

Blockchain Security SECURITY



## 4.8 금융권 보안 위협 사례 (4/7)

4 보안 위협

### 영국테스코뱅크 해킹사고

- 테스코뱅크의 약 2만 명의 고객 계정에서 돈이 빠져나간 사태가 발생
- 약 4만 개의 계좌에서 수상한 행동 및 거래가 발견되었고, 그 중 절반 정도가 돈이 빠져나간 금전피해 사고

### 관련 기사

영국 테스코은행 4만여명 계좌 해킹

영국의 테스코뱅크 4만 개 계좌 해킹당하다

절반인 2만 여개 계좌에서는 실제 금전 피해 발생
테스코뱅크는 전액 보상해줄 계획…고객은 여전히 불안

[보안뉴스 문가용 기자] 영국의 가장 큰 슈퍼마켓 체인인 테스코(Tesco)가 소유한 은행, 테스코뱅크(Tesco Bank)에서 해킹 사건이 발생했다. 테스코뱅크에 따르면 일부 고객들의 계정에서 온라인 범죄 행위가 발생했고, 현금이 인출되는 경우도 있었다고 한다. 아직 더 자세한 내용은 공개되지 않은 상태지만 여러 매체들의 보도에 따르면 2만 명 정도의 고객들이 금전적인 피해를 입은 것으로 보인다.

사이버 보안 서비스 ECSC의 이안 맨 (Ian Mann) 최고 경영자는 침해의 규모가 테스코의 내부 시스템이나 모바일 애플리케이션이 해킹 당했을 가능성이 있음을 나타냄

Blockchain Security SECURITY

# 4.8 금융권 보안 위협 사례 (5/7)

4 보안 위협

## CIA IoT기기 해킹도구로 사용

- 위키리크스가 공개한 문건에 따르면 CIA는 바이러스, 트로이 등 전자기기의 소프트웨어 시스템에 침투할 수 있는 1000여 종류의 멀웨어 시스템을 개발하고 애플의 아이폰  안드로이드 스마트폰, 마이크로소프트(MS)의 소프트웨어, 자동차에 설치된 소프트웨어 프로그램
- 삼성전자의 스마트 TV 등을 해킹 도구로 사용

1. ext3 형태로 TV에서 USB로 채널을 보냄
2. Usb_mount 디렉토리로 zip파일과 file1.txt를 추가시킴 (추가시키기 전에 777로 디렉토리 허용으로 세팅하면 좋다)
3. 다음 코드로 몇 개의 파일을 생성 (나중에 USB로 복사본을 가질 수 있음)

Blockchain Security SECURITY 블록체인 시큐리티

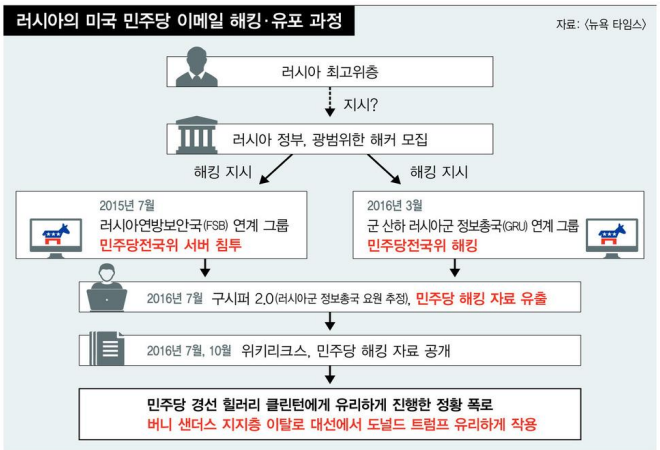


# 4.8 금융권 보안 위협 사례 (6/7)

4 보안 위협

## 러시아의 미 대선 개입 해킹

- 위키리크스가 공개한 문건에 따르면 CIA는 바이러스, 트로이 등 전자기기의 소프트웨어 시스템에 침투할 수 있는 1000여 종류의 멀웨어 시스템을 개발하고 애플의 아이폰  안드로이드 스마트폰, 마이크로소프트(MS)의 소프트웨어, 자동차에 설치된 소프트웨어 프로그램




Blockchain Security SECURITY 블록체인 시큐리티

## 4.8 금융권 보안 위협 사례 (7/7)

4 보안 위협

1. 국정원 국내 가상화폐 거래소 해킹 사례
   https://youtu.be/X7CKsG-CrlU
2. 핀테크 금융거래 해킹 사례
   https://youtu.be/pGfioFNWYNo
3. 뉴욕 연방 준비(Fed) 은행 해킹 사례
   https://youtu.be/ex0ULQ3CEYg
4. 가상화폐 거래소 '유빗' 해킹 사례
   https://youtu.be/Ls-o5mqFJsQ
5. 일본 가상화폐 거래소 'coincheck ' 해킹 사례
   https://youtu.be/Bd9J6KNskIs



## 4.9 해커 입장에서 공격 추이 변화

4 보안 위협

APT(Advanced Persistent Threat) 등 보호해야 할 시스템은 갈수록 복잡해지고, 시스템을 침해하기 위한 공격기법은 꾸준히 진화하고 새롭게 개발되고 있습니다.

| | 과거 | 현재 | 미래 |
|---|---|---|---|
| 공격 규모 | 개인 | 단체 | 국가 |
| 공격 목적 | 자랑, 편의 | 금전적인 이익 | 테러, 전쟁, 사이버전 |
| 공격 기술 | 서버, 네트워크, CVE 위주 | 랜섬웨어, 악성코드 | APT, STUXNET |
| 인터넷 환경 | PC 통신 | 4G, 무선, 광통신, 클라우드 | 고도화된 IoT 환경 |

## Contents

# V. 대응방안

Blockchain Security SECURITY

## 5.1 오픈 소스 보안 위협에 대한 대응 방안

5 대응 방안

### 대응 방안

› 오픈소스의 취약점을 대응하기 위한 방안으로 다음과 같은 두 가지 방안이 있다.

**가시성 확보**

매년 취약점 발표 수 **4,000** 개

**98%** 회사는 자신들이 사용하는 오픈소스에 대해 모름

**68%** 회사는 보안 취약점에 감시 안함

**투자와 집중**

오픈소스 안정성과 질을 평가하는 CII(Core Infrastructure Initiative) 비영리 단체를 통한 안정성 평가 시행

미래창조과학부와 한국인터넷진흥원에서 주관하는 취약점 신고포상제를 통한 취약점 발굴

오픈소스 코드의 분류와 추적
각 제품에 사용된 오픈소스 리스트 작성

**가시성 확보가 필요**

향후 보안 관련 사고예방

**이러한 활동에 꾸준한 투자 및 관심 표현 필요**

Blockchain Security SECURITY

이글루시큐리티 '보안 위협 사례로 보는 오픈 소스'

## 5.2 전자금융기반시설 가이드 (1/7)

5 대응 방안

### 전자금융기반시설 취약점 분석/평가 항목

- 금융보안원은 **금융 분야 특성을 반영한 정보보호관리체계(ISMS) 인증기준 점검항목**을 제시하였다.
- 정보통신(IT) 분야에 초점이 맞춰진 기존 ISMS 점검항목에서 1개 항목을 삭제하고 72개 항목을 추가, 총 324개 점검항목으로 구성된다.

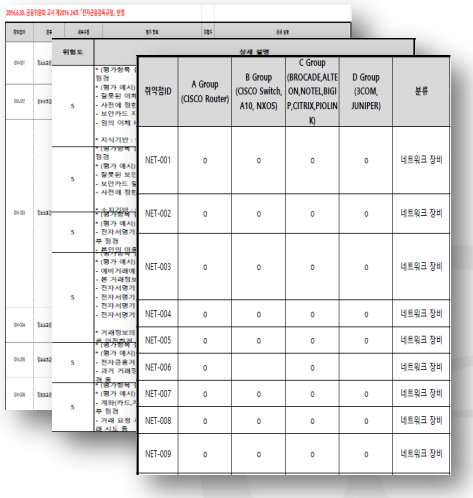
금보원, 금융 분야 맞춤 `정보보호관리체계` 점검항목 제시

발행일 : 2017.03.09

[AD] AJ전시몰 2017 전시가전 연말총결산

금융보안원이 금융 분야 특성을 반영한 정보보호관리체계(ISMS) 인증기준 점검항목을 제시했다. 정보통신(IT) 분야에 초점이 맞춰진 기존 ISMS 점검항목에서 1개 항목을 삭제하고 72개 항목을 추가, 총 324개 점검항목으로 구성됐다. 금융기관 자율보안체계 구축과 정보보호 역량 강화에 기여할 것으로 기대된다.

금융보안원 FINANCIAL SECURITY INSTITUTE



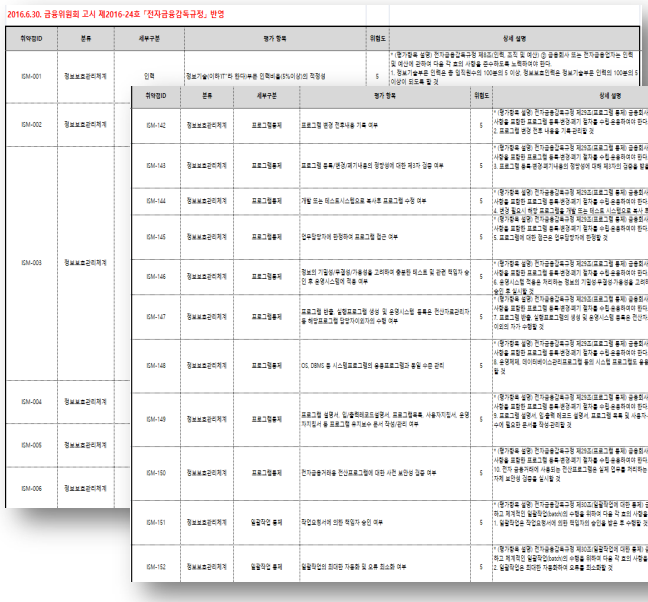
| 취약점ID | A Group (CISCO Router) | B Group (CISCO Switch, A10, NXOS) | C Group (BROCADE,ALTEON,NOTEL,BIGIP,CITRIX,PIOLINK) | D Group (3COM, JUNIPER) | 분류 |
|---|---|---|---|---|---|
| NET-001 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-002 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-003 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-004 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-005 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-006 | 0 | | 0 | | 네트워크 장비 |
| NET-007 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-008 | 0 | 0 | 0 | 0 | 네트워크 장비 |
| NET-009 | 0 | 0 | 0 | 0 | 네트워크 장비 |



## 5.2 전자금융기반시설 가이드 (2/7)

5 대응 방안

### 정보보호관리체계 항목



2016.6.30. 금융위원회 고시 제2016-24호 「전자금융감독규정」 반영

| 취약점ID | 분류 | 세부구분 | 평가 항목 | 위험도 | 상세 설명 |
|---|---|---|---|---|---|
| ISMS-001 | 정보보호관리체계 | 정책 | 정보기술부문 및 전자금융부문 정책(보안정책, 지침 등)의 수립 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |
| ISMS-002 | 정보보호관리체계 | 조직 | 정보보호 및 개인정보보호 조직 구성 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |
| ISMS-003 | 정보보호관리체계 | 조직 | 정보보호 및 개인정보보호 자원 할당 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |
| ISMS-004 | 정보보호관리체계 | 조직 | 정보보호 및 개인정보보호 교육 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |
| ISMS-005 | 정보보호관리체계 | 조직 | 외부자 보안 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |
| ISMS-006 | 정보보호관리체계 | 조직 | 정보보호 위반 시 조치 | 5 | • 「전자금융 감독규정」 제15조(프로그램 등록) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록 변경관리 절차를 수립·운용하여야 한다.<br>1. 프로그램 변경 전후 내용을 기록·관리할 것 |

### 세부항목

- 건물 및 설비
- 전산실/전산 자료/전산망
- 정보처리/정보보호 시스템
- 공개용웹서버
- IP주소
- 정보기술 계획/사업/계약/감리
- 용량/성능 관리
- 직무분리
- 전산원장/거래/프로그램/일괄작업 통제
- 암호프로그램/키관리 통제
- 내부사용자/이용자 비밀번호 관리
- 정보기술 아웃소싱
- 정보기술부문 실태평가
- 전자금융거래시 준수사항
- 이용자 유의사항 공지
- 보안성 심의
- 악성코드 감염방지
- 비상대책
- 침해사고 예방/대응훈련
- 재해복구 센터/훈련
- 정보기술부문/전자금융사고 보고
- 조직

## 5.2 전자금융기반시설 가이드 (3/7)

5 대응 방안

### 서버(Server) 항목

| 취약점ID | AIX | HP-UX | LINUX | SOLARIS | WINDOWS | 분류 | 세부구분 | 평가 항목 | 위험도 | 상세 설명 |
|---|---|---|---|---|---|---|---|---|---|---|
| SRV-001 | O | O | O | O | O | 서버 | 비밀번호 관리 | SNMP 서비스 Get community 스트링 설정 오류 | 4 | * (평가항목 설명) SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통할하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP 통신시 이용되는 SNMP community string 기본 이름인 public/private 등의 유추하기 쉬운 이름으로 설정하여 이용하고 있는지 여부를 점검 |
| SRV-002 | O | O | O | O | O | 서버 | 비밀번호 관리 | SNMP 서비스 Set community 스트링 설정 오류 | 5 | * (평가항목 설명) SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통할하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP 통신시 이용되는 SNMP community string 기본 이름인 public/private 등의 유추하기 쉬운 이름으로 설정하여 이용하고 있는지 여부를 점검 |
| SRV-003 | | | | | O | 서버 | 권한 관리 | SNMP 접근 통제 설정 | 3 | * (평가항목 설명) SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통할하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP서비스를 사용할 수 있는 호스트에 특정하여 이용하고 있는지 여부를 점검 |
| SRV-004 | O | O | O | O | O | 서버 | 설정 관리 | 불필요한 SMTP 서비스 실행 여부 | 2 | * (평가항목 설명) SMTP 서비스는 인터넷에서 메일을 전송하는 SMTP 프로토콜을 기반으로 하는 서비스로, 악의적인 공격자는 SMTP 서비스를 이용하여 SMTP 서비스를 실행 중인 컴퓨터의 정보를 획득하거나 다양한 공격이 가능하므로 불필요한 SNMP 서비스가 가동 여부를 점검 |
| SRV-005 | O | O | O | O | | 서버 | 설정 관리 | SMTP 서비스 expn/vrfy 명령어 실행 가능 여부 | 2 | * (평가항목 설명) SMTP 서비스는 인터넷에서 메일을 전송하는 프로토콜로, SMTP 서비스에서 이용되는 expn/vrfy 명령어 지원여부를 점검하여 해당 명령어를 통해 시스템에 등록된 특정 사용자 계정 이용 여부를 파악할 수 있는지 여부를 점검 |
| SRV-006 | O | O | O | O | | 서버 | 권한 관리 | Sendmail Log Level 미설정 | 1 | * (평가항목 설명) Sendmail은 널리 사용되는 MTA(Mail Transfer Agent)로써 유닉스에 기본적으로 포함되어 있는 서비스로 서비스 가용성 확보 및 지속적인 보안취약점에 대한 모니터링이 필요하며, Senmail의 loglevel은 서비스 운영상의 이벤트에 대한 로그를 남기는 구분으로 loglevel 설정의 적절성을 점검 |
| SRV-007 | O | O | O | O | | 서버 | 설정 관리 | 취약한 버전의 Sendmail 사용 여부 | 2 | * (평가항목 설명) 특정 버전의 Sendmail 에서 SMTP 헤더 분석(parsing) 구성 요소에 버퍼 오버플로우 등의 서버 권한을 획득할 수 있는 심각한 침해유형이 발생하고 있으므로 취약한 Sendmail 버전을 사용하고 있는지 여부를 점검 |
| SRV-008 | O | O | O | O | | 서버 | 설정 관리 | Sendmail 서비스 거부 방지 기능 미설정 | 2 | * (평가항목 설명) 네트워크 회선 용량 및 서버 처리 용량 초과로 인한 메일 서비스 거부 및 시스템 다운을 방지하기 위해 보안설정의 적절성 여부를 점검 |
| SRV-009 | O | O | O | O | | 서버 | 설정 관리 | 스팸 메일 릴레이 제한 | 2 | * (평가항목 설명) SMTP 서비스는 인터넷에서 메일을 전송하는 프로토콜로, 다른 메일 서버가 보낸 메일을 다시 발송하는 relay 기능을 제공하는데 해당 기능은 공격자가 정당한 인증 과정 없이 다량의 메일스팸메일을 발송 가능하므로 이에 대한 안전성 여부를 점검 |
| SRV-010 | O | O | O | O | | 서버 | 설정 관리 | 일반사용자의 Sendmail 실행 방지 | 2 | * (평가항목 설명) SMTP 서비스 사용 시 일반 사용자의 q 옵션을 사용한 Sendmail 실행을 방지하여 메일큐 내용과 sendmail 설정을 보거나, 메일큐를 강제적으로 drop 시킬 수 있는 기능을 막아야 하며 그렇지 않을 경우 비인가자에 의한 SMTP 서비스 오류 발생할 수 있으므로 적절한 보안 설정이 되었는지 여 대한 점검 |
| SRV-011 | O | O | O | O | | 서버 | 설정 관리 | ftpusers 파일 내 시스템 계정 존재 여부 | 2 | * (평가항목 설명) ftp 운영시 신뢰할 수 있는 사용자에 대한 사용 제한 필요하며, ftpusers 파일 미존재 시 모든 사용자가 파일을 업/다운로드 가능하여 비정상적으로 만들어진 계정 사용자나 신뢰할 수 없는 사용자도 파일 전송이 가능하여 불법적인 자료의 업/다운로드 위협이 존재하여 ftpusers 파일 안에 시스템 계정이 존재하지 않으면 비인가자가 이를 악용하여 불법적인 시스템 접근이 가능하므로 ftpusers 내 적절한 시스템 계정을 설정이 적절성 여부를 점검 |
| SRV-012 | O | O | O | O | | 서버 | 설정 관리 | .netrc 파일 내 호스트 정보 노출 | 4 | * (평가항목 설명) .netrc 파일은 ftp에서 자동으로 파일 송/수신을 위해 사용되는 서비스로, 관련 서비스를 이용하기 위해서는 .netrc 파일에 FTP 접근 IP와 비밀번호를 평문으로 보관하도록 되어 있으므로, 해당 파일에 대한 권한설정의 적절성 여부를 점검 |
| SRV-013 | O | O | O | O | O | 서버 | 설정 관리 | Anonymous FTP 비활성화 | 4 | * (평가항목 설명) FTP 서비스는 인터넷에서 파일을 전송하기 위한 프로토콜을 기반으로 하는 서비스로 계정과 패스워드가 암호화하지 않고 평문 전송을 기반으로 하며, 모든 사용자가 FTP 서비스를 이용할 수 있는 익명(Anonymous) FTP 기능이 활성화된 경우 악의적인 사용자도 손쉽게 접근 가능하므로 이에 대한 보안설정의 적절성 여부를 점검 |
| SRV-014 | O | O | O | O | | 서버 | 권한 관리 | NFS 접근통제 | 3 | * (평가항목 설명) NFS 서비스는 원격지의 시스템에 위치한 파일을 마치 자신의 컴퓨터에 있는 것처럼 검색하고, 마음대로 저장하거나 수정할 수 있도록 지원하는 서비스로 잘못된 설정에 의해 원치않는 자료 또는 디렉토리 등이 외부에 노출되고 있는지 여부를 점검 |
| SRV-015 | O | O | O | O | | 서버 | 설정 관리 | NFS 서비스 비활성화 | 2 | * (평가항목 설명) NFS 서비스는 원격지의 시스템에 위치한 파일을 마치 자신의 컴퓨터에 있는 것처럼 검색하고, 마음대로 저장하거나 수정할 수 있도록 지원하는 서비스로 해당 서비스가 업무에 관계없이 이용/활성화되고 있는지 여부를 점검 |

### 세부항목

- 비밀번호 관리
- 권한 관리
- 설정 관리
- 사용자 인증
- 감사
- 패치 관리
- 파일 및 디렉터리 관리
- 서비스 관리
- 보안 관리
- 계정 관리
- DB 관리
- 로그 관리

Blockchain Security SECURITY 블록체인 시큐리티

77

## 5.2 전자금융기반시설 가이드 (4/7)

5 대응 방안

### 데이터베이스 항목

| 취약점ID | ORACLE | MSSQL | MYSQL | 분류 | 세부구분 | 평가 항목 | 위험도 | 상세 설명 |
|---|---|---|---|---|---|---|---|---|
| DBM-001 | o | o | o | 데이터베이스 | 비밀번호 관리 | 유추가능한 비밀번호 설정여부(DB계정) | 4 | * (평가항목 설명) 공격자에 의해 비밀번호 도용을 방지하기 위해 DB계정명과 동일하거나 유추가능한 비밀번호로 설정 여부 등을 점검 |
| DBM-002 | o | o | o | 데이터베이스 | 비밀번호 관리 | 기본 계정 및 패스워드 변경(디폴트 ID 및 패스워드 변경 및 잠금) | 4 | * (평가항목 설명) DB설치 시 생성된 DB계정의 비밀번호가 디폴트(default) 상태로 설정되어 있는 경우 해당 정보를 이용하여 DBMS 시스템에 무단접근할 수 있으므로 DB계정에 대한 초기 비밀번호 사용 여부를 점검 |
| DBM-003 | o | o | o | 데이터베이스 | 사용자 인증 | 비인가자의 접근 차단을 위한 사용자 계정 관리 | 2 | * (평가항목 설명) 필요에 의해 생성된 DB계정이 여러가지 이유로 이용되지 않는 등, 관리되지 않는 DB계정에 대한 적절성 여부를 점검 |
| DBM-004 | o | o | o | 데이터베이스 | 권한 관리 | DBA 계정 권한 관리 | 4 | * (평가항목 설명) DBMS 계정이 접근할 필요가 없는 테이블에 대한 접근권한이 있거나 DBA권한이 주어져 해당 DBMS 계정 권한을 공격자가 획득할 경우 전체 DB 데이터의 조회/변경/삭제 등이 가능하므로 관련 테이블에 대한 접근권한의 적절성 여부를 점검 |
| DBM-005 | o | o | o | 데이터베이스 | 관리적 물리적 보안 | DB서버 중요정보 암호화 적용 여부 | 3 | * (평가항목 설명) 주민등록번호/비밀번호 등의 중요 정보가 암호화되지 않은 평문 형태로 DBMS에 저장되어 있는 경우 해당 정보가 누출될 위험이 존재하므로 중요정보에 대한 암호화 적용 여부를 점검 |
| DBM-006 | o | | | 데이터베이스 | 사용자 인증 | 로그인 실패 횟수에 따른 잠금시간 등 계정 잠금 정책 설정 | 3 | * (평가항목 설명) DBMS 계정을 통한 로그인 시도 시 로그인 실패 횟수에 따른 계정 잠금 시간이 설정되어 있지 않아 유추 가능한 비밀번호나 무작위 대입공격(Brute Force Attack)으로 로그인 시도가 가능하므로, 이에대한 보안설정의 적절성 여부를 점검 |
| DBM-007 | o | o | o | 데이터베이스 | 비밀번호 관리 | 비밀번호 복잡도 설정 | 5 | * (평가항목 설명) 쉬운 비밀번호 설정시 외부 공격자들로부터 쉽게 유추될 수 있는 위험이 존재하므로, DB 계정 비밀번호의 특수 문자 등을 혼합하는 등 회사에서 정한 비밀번호 관리정책에 대한 준수 여부를 점검 |
| DBM-008 | o | o | o | 데이터베이스 | 비밀번호 관리 | 비밀번호의 주기적인 변경 | 3 | * (평가항목 설명) 비밀번호의 주기적 미교체 및 쉬운 비밀번호 설정시 외부 공격자들로부터 쉽게 유추될 수 있는 위험이 존재하므로, 회사에서 정한 비밀번호 관리정책에 대한 준수 여부를 점검 |
| DBM-009 | o | o | o | 데이터베이스 | 설정 관리 | 세션 idle timeout 설정 | 3 | * (평가항목 설명) 세션 idle timeout은 DBMS와 사용자 클라이언트 사이에서 클라이언트의 요청이 없는 상태로 DBMS가 기다릴 수 있는 최대 시간을 의미(즉, 세션 타임아웃으로 설정된 시간이 지날 때까지 클라이언트의 요청이 없다면 DBMS에서 자동으로 세션을 종료)<br>* (평가 예시)<br>- 운영자가 이석 중이거나 해당 DB를 사용하지 않을 경우, 특정시간 후 세션의 종료하고 있는지에 대한 점검 |
| DBM-010 | o | o | o | 데이터베이스 | 사용자 인증 | SYSDBA 로그인 제한 설정 | 2 | * (평가항목 설명) DBMS가 설치된 시스템 상에서 SYSDBA 권한을 가진 DB계정으로 계정명/비밀번호 입력없이 접속 가능한지 여부를 점검 |
| DBM-011 | o | o | o | 데이터베이스 | 감사 | 기본적인 감사(사용자, 권한, 객체 등) 기능 사용 여부 | 3 | * (평가항목 설명) DBMS에 대한 침해사고 발생시 원인 파악 및 문제 해결을 위한 정보보호관련 로그를 관리하고 있는지 여부를 점검 |
| DBM-012 | o | | | 데이터베이스 | 비밀번호 관리 | listener 비밀번호 설정 및 디폴트 포트 변경 | 5 | * (평가항목 설명) TNS(Trasnparent Network Substrate) Listner는 원격 클라이언트들의 요라클 서버 접속 요청을 처리하고 기본적으로 TNS Listener는 공백의 비밀번호로 설정되어 있어 권한이 없는 원격 사용자가 TNS Listener에 접근하거나, Listener의 작동을 중지 가능하므로 listener 디폴트 포트인 1521을 변경하고 비밀번호 설정이 되어 있는지에 대한 점검 |
| DBM-013 | o | o | o | 데이터베이스 | 권한 관리 | 원격에서 DB 서버로의 접속 제한 | 3 | * (평가항목 설명) 공격자가 원격 시스템에서 DB 에 접근하여 중요한 데이터를 얻기 위한 공격이 증가하고 있으므로, 관련 DBMS에 운영과 관계 없는 불필요 접속을 허용하고 있는지 여부를 점검 |
| DBM-014 | o | | | 데이터베이스 | 권한 관리 | OS_ROLES, REMOTE_OS_ROLES 설정 | 4 | * (평가항목 설명) OS_ROLES, REMOTE_OS_ROLES에 대한 보안설정이 미비한 경우, 원격 사용자가 OS의 다른 사용자로 위장하여 관련 DMBS에 무단 접근 가능한 위험이 발생 할 수 있으므로 이에 대한 보안설정의 적절성 여부를 점검<br>* (평가 예시)<br>- OS_ROLES, REMOTE_OS_ROLES의 파라미터 값을 FALSE로 설정하는 등 |
| DBM-015 | o | o | | 데이터베이스 | 권한 관리 | 응용프로그램 또는 DBA 계정의 Role의 Public 설정 점검 | 4 | * (평가항목 설명) Role이 Public으로 설정된 경우, 일반 계정에서도 응용 프로그램 테이블 또는 DBA 테이블로의 접근이 가능하므로 관련 내용에 대한 권한설정의 적절성 여부를 점검 |
| DBM-016 | o | o | o | 데이터베이스 | 패치 관리 | 데이터베이스 최신 보안패치와 밴더 권고사항 적용 | 4 | * (평가항목 설명) DBMS 설치 파일에 대한 보안패치 미실시한 경우, 알려진 취약점에 의해 DBMS가 해킹될 수 있는 위험이 있으므로 관련 DBMS에 대한 최신 보안패치 적용 여부를 점검 |

### 세부항목

- 비밀번호 관리
- 사용자 인증
- 권한 관리
- 관리적 물리적 보안
- 감사
- 패치 관리
- 계정 관리
- 접근 관리
- 옵션 관리
- 로그 관리

Blockchain Security SECURITY 블록체인 시큐리티

78

## 5.2 전자금융기반시설 가이드 (5/7)

5 대응 방안

### 인프라 구성 항목

| 취약점ID | 분류 | 세부구분 | 평가 항목 | 위험도 | 상세 설명 |
|---|---|---|---|---|---|
| INF-001 | 인프라 구성 | 서버/네트워크 가용성 | 네트워크 최신(ISP) 이중화 구성 | 3 | * (평가항목 설명) 네트워크(ISP) 회선의 장애와 같은 상황에 안정적 운영을 위해 장애시 서비스 장애가 발생할 우려가 있으므로 네트워크 회선(ISP)을 이중화 구성하고 있는지 점검 |
| INF-002 | 인프라 구성 | 서버/네트워크 가용성 | 네트워크 장비 이중화 구성 | 3 | * (평가항목 설명) 네트워크 장비가 단일장비로 구성되어 있을 경우 장애 장애시 서비스 장애가 발생할 우려가 있으므로 네트워크 장비를 이중화 구성하고 있는지 점검 |
| INF-003 | 인프라 구성 | 서버/네트워크 가용성 | 정보보호시스템의 이중화 구성 | 3 | * (평가항목 설명) 정보보호시스템이 단일장비로 구성되어 있을 경우 장애 장애시 서비스 장애가 발생할 우려가 있으므로 정보보호시스템을 이중화 구성하고 있는지 점검 |
| INF-004 | 인프라 구성 | 서버/네트워크 가용성 | 중요 서버 이중화 구성 | 3 | * (평가항목 설명) 서버의 단일장애 구성으로 운영 중 장애 장애시 서비스 장애가 발생할 우려가 있으므로 중요서버를 이중화 구성하고 있는지 점검 |
| INF-005 | 인프라 구성 | 서버/네트워크 가용성 | 소프트웨어 및 하드웨어 서비스가 중단(EOS) 된 노후장비 존재 | 4 | * (평가항목 설명) 벤더의 소프트웨어 및 하드웨어의 지원이 종료된 경우 장애의 원인 파악이 힘들 장애 근구 해결을 위한 추가 패치업데이트 적용 등 지원으로 지원이 종료된(End of Service) 노후장비가 존재하는지 점검 |
| INF-006 | 인프라 구성 | 서버/네트워크 가용성 | 장애 대응 장애발생 시 복구를 위한 별도 구인 확보 여부 | 3 | * (평가항목 설명) 장애 장애 장애

## 5.2 전자금융기반시설 가이드 (7/7)

5 대응 방안

### 웹 모바일 HTS 항목

| 취약점ID (WEB) | 취약점ID (Mobile) | 취약점ID (HTS) | Sub NUM | 분류 | 세부구분 | 평가 항목 | 위험도 | 상세 설명 |
|---|---|---|---|---|---|---|---|---|
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 001 | 전자금융보안 | 거래 인증 | [전자금융] 거래 인증수단 검증 오류 (지식기반) | 5 | * (평가항목 설명) 전자금융거래에 적용된 거래 인증수단(지식기반)에 대한 검증절차의 적절성 여부를 점검<br>* (평가 예시)<br>- 질문된 이체 또는 계좌 비밀번호 입력 후 정상거래 가능 여부 점검<br>- 사전에 정한 인증절차 우회 가능 여부 점검<br>- 보안카드 지시번호 변경 오류<br>- 임의 이체 비밀번호 사용 가능 여부 등을 점검<br>* 지식기반 : 이용자가 알고 있는 지식으로 인증(예 : ID/비밀번호, 이체/계좌비밀번호, 신용카드 비밀 |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 002 | 전자금융보안 | 거래 인증 | [전자금융] 거래 인증수단 검증 오류 (소지기반) | 5 | * (평가항목 설명) 전자금융거래에 적용된 거래 인증수단(소지기반)에 대한 검증절차의 적절성 여부를 점검<br>* (평가 예시)<br>- 질문된 보안카드 지시번호 입력 후 정상거래 가능 여부 점검<br>- 보안카드 일련번호 조작 후 임의 보안매체 사용 가능 여부 점검<br>- 사전에 정한 인증절차 우회 가능 여부 점검 등<br>* 소지기반 : 이용자가 소지하고 있는 인증매체로 인증(예 : 보안카드, OTP발생기, HCM 등) |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 003 | 전자금융보안 | 거래 인증 | [전자금융] 이용자 인증정보 재사용 | 5 | * (평가항목 설명) 전자금융거래 시 이용되는 이용자 인증 정보의 재전송 가능 여부를 점검<br>* (평가 예시)<br>- 전자서명기술 이용 시 전자서명 값을 저장하고 일정 시간 이후 해당 전자서명 값의 재사용 가능 여부 점검<br>- 보안카드 일련번호 인증 후 단말기에서 재사용 가능 여부 점검 등 |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 004 | 전자금융보안 | 거래 무결성 | [전자금융] 거래정보 무결성 검증 | 5 | * (평가항목 설명) 전자금융거래 시 이용되는 거래정보의 무결성 검증 여부를 점검<br>* (평가 예시)<br>- 예비거래에 이용된 거래정보와 본거래에서 이용된 거래정보의 일치 여부 점검<br>- 본 거래정보와 최종 승인된 거래정보의 일치 여부 점검<br>- 전자서명기술 이용 시 타인인증서로 서명 후 거래 가능 여부 점검<br>- 전자서명기술 이용 시 전자서명 검증절차 오류 여부 점검<br>- 전자서명기술 이용 시 전자서명 무결성 검증 오류 여부 점검<br>- 전자서명기술 이용 시 매번 동일한 전자서명값 이용 여부 점검 등<br>* 거래정보의 무결성 : 이용자가 단말기(PC/모바일 등)를 통해 입력한 거래정보가 금융회사 시스템으로 이용자 전송 중에 위변 |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 005 | 전자금융보안 | 거래 인증 | [전자금융] 거래정보 재사용 | 5 | * (평가항목 설명) 전자금융거래 시 이용되는 거래정보의 재사용 가능 여부를 점검<br>* (평가 예시)<br>- 전자금융거래 시 정상 로그인 이용자가 아닌 타인의 이용자 거래정보 무단 이용 가능 여부 점검<br>- 과거 거래정보(거래정보 암호값, 해쉬값 등)를 별다른 인증 및 확인절차 없이 지속 이용 가능 여부 점검 등 |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 006 | 전자금융보안 | 거래 무결성 | [전자금융] 거래시 소유주 확인 여부 | 5 | * (평가항목 설명) 전자금융거래 시 이용자의 이용 권한 검증 여부를 점검<br>* (평가 예시)<br>- 계좌(카드,계약)정보 조회 시 타 이용자의 계좌(카드,계약)번호 입력 후 타 이용자 계좌 조회 가능 여부 점검<br>- 거래 요청 시 계좌 번호를 현재 로그인 중인 이용자가 아닌 다른 이용자의 계좌번호로 변조하여 거래 시도 등 |
| WEB-FIN- | MOB-FIN- | HTS-FIN- | 007 | 전자금융보안 | 거래 무결성 | [전자금융] 사전에 정한 조회기간 이상으로 거래내역 조회가능 여부 | 5 | * (평가항목 설명) 거래내역 조회 시 금융회사가 정한 기간 이상의 내역 조회 가능 여부를 점검<br>* (평가 예시)<br>- 3개월로 정한 거래내역 조회가능 시 3개월 이상으로 변경 후 확인 여부 점검<br>- 거래가 종료된 계좌에 대해 거래내역을 입력 조회 가능 여부 점검 등 |

**세부 항목**

- 거래 인증/무결성
- 단말 보안
- 서비스 보호
- 이용자 인증
- 데이터 보호

### (시범운영 분야) SmartWatch항목

| (2017.12.19) 시범운영 -SmartWatch- | Sub NUM | 분류 | 세부구분 | 평가 항목 |
|---|---|---|---|---|
| MOW-FIN- | 001 | 전자금융보안 | 거래 인증 | [전자금융] 거래 인증수단 검증 오류 (지식기반) |
| MOW-FIN- | 002 | | | |
| MOW-FIN- | 003 | | | |
| MOW-FIN- | 004 | | | |
| MOW-FIN- | 005 | | | |

| 위험도 | 상세 설명 |
|---|---|
| 5 | * (평가항목 설명) 전자금융거래에 적용된 거래 인증수단(지식기반)에 대한 검증절차의 적절성 여부를 점검<br>* (평가 예시)<br>- 질문된 이체 또는 계좌 비밀번호 입력 후 정상거래 가능 여부 점검<br>- 사전에 정한 인증절차 우회 가능 여부 점검<br>- 보안카드 지시번호 변경 오류<br>- 임의 이체 비밀번호 사용 가능 여부 등을 점검<br>* 지식기반 : 이용자가 알고 있는 지식으로 인증(예 : ID/비밀번호, 이체/계좌비밀번호, 신용카드 비밀번 |
| 5 | * (평가항목 설명) 전자금융거래에 적용된 거래 인증수단(소지기반)에 대한 검증절차의 적절성 여부를 점검<br>* (평가 예시)<br>- 질문된 보안카드 지시번호 입력 후 정상거래 가능 여부 점검<br>- 보안카드 일련번호 조작 후 임의 보안매체 사용 가능 여부 점검<br>- 사전에 정한 인증절차 우회 가능 여부 점검 등<br>* 소지기반 : 이용자가 소지하고 있는 인증매체로 인증(예 : 보안카드, OTP발생기, HCM 등) |
| 5 | * (평가항목 설명) 전자금융거래 시 이용되는 이용자 인증 정보의 재전송 가능 여부를 점검<br>* (평가 예시)<br>- 전자서명기술 이용 시 전자서명 값을 저장하고 일정 시간 이후 해당 전자서명 값의 재사용 가능 여부 점검<br>- 본인의 이용자 인증정보(SSO)를 다른 단말기에서 재사용 가능 여부 점검 등 |
| 5 | * (평가항목 설명) 전자금융거래 시 이용되는 거래정보의 무결성 검증 여부를 점검<br>* (평가 예시)<br>- 예비거래에 이용된 거래정보와 본거래에서 이용된 거래정보의 일치 여부 점검<br>- 본 거래정보와 최종 승인된 거래정보의 일치 여부 점검<br>- 전자서명기술 이용 시 타인인증서로 서명 후 거래 가능 여부 점검<br>- 전자서명기술 이용 시 전자서명 검증절차 오류 여부 점검<br>- 전자서명기술 이용 시 전자서명 무결성 검증 오류 여부 점검<br>- 전자서명기술 이용 시 매번 동일한 전자서명값 이용 여부 점검 등<br>* 거래정보의 무결성 : 이용자가 단말기(PC/모바일 등)를 통해 입력한 거래정보가 금융회사 시스템으로 이용자 전송 중에 위변 |
| 5 | * (평가항목 설명) 전자금융거래 시 이용되는 거래정보의 재사용 가능 여부를 점검<br>* (평가 예시)<br>- 전자금융거래 시 정상 로그인 이용자가 아닌 타인의 이용자 거래정보 무단 이용 가능 여부 점검<br>- 과거 거래정보(거래정보 암호값, 해쉬값 등)를 별다른 인증 및 확인절차 없이 지속 이용 가능 여부 점검 등 |
| 5 | * (평가항목 설명) 전자금융거래 시 이용자의 이용 권한 검증 여부를 점검<br>* (평가 예시)<br>- 계좌(카드,계약)정보 조회 시 타 이용자의 계좌(카드,계약)번호 입력 후 타 이용자 계좌 조회 가능 여부 점검<br>- 거래 요청 시 계좌 번호를 현재 로그인 중인 이용자가 아닌 다른 이용자의 계좌번호로 변조하여 거래 시도 등 |

Blockchain Security SECURITY 블록체인 시큐리티

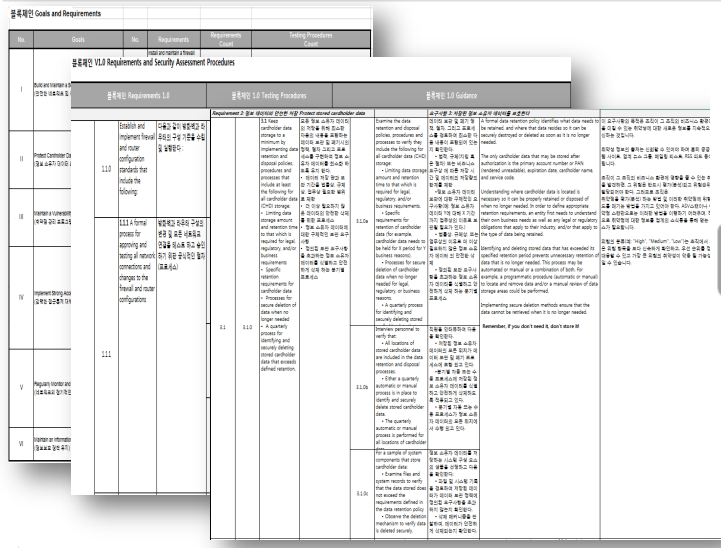


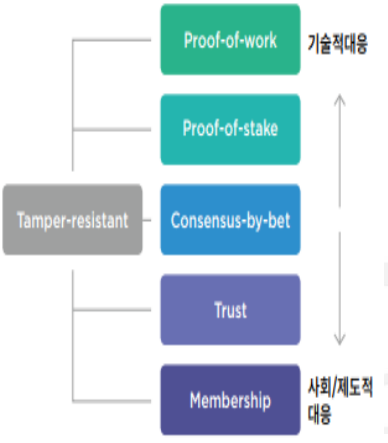
## 5.3 블록체인 구축 보안 가이드 (1/4)

5 대응 방안

### 블록체인 체크리스트

- 모든 블록체인이 가지고 잇는 다음의 본원적 공통요소를 기반으로 체크리스트를 고안하였다.
  - 분산구조, 참여자 네트워크와 참여자 스스로 제공하는 컴퓨터를 활용, 암호학과 디지털서명으로 이용자식별, 기록 조작/변경을 어렵게 만드는 메커니즘, 타임스탬핑, 개별 거래를 프로그램화 (programmable transaction)




위변조에 대응하는 블록체인 메커니즘 분류

Blockchain Security SECURITY 블록체인 시큐리티

## 5.3 블록체인 구축 보안 가이드 (2/4)

5 대응 방안

### 서버 항목 - Requirement 1: 방화벽 설치 및 관리

| No. | Goals | No. | Requirements | Requirements Count | Testing Procedures Count |
|---|---|---|---|---|---|
| I | Build and Maintain a Secure Network and Systems (안전한 네트워크 및 시스템 구축 및 유지) | 1 | Install and maintain a firewall configuration to protect cardholder data (방화벽 설치 및 관리) | 23 | 38 |
| | | 2 | Do not use vendor-supplied defaults for system passwords and other security parameters (시스템 패스워드 및 보안 파라미터) | 12 | 36 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.1.0 | router configuration standards that include the following: | | 1.1.0 | documentation specified below and verify that standards are complete and implemented as follows: | 이 완전하며, 다음과 같이 실시되고 있는지 확인한다 : | that block unwanted access and manage authorized access into and out of the network.<br>Configuration standards and procedures will help to ensure that the organization's first line of defense in the | 에어 또는 하드웨어 장치들입니다. 구성 기준과 절차는 데이터를 보호하기 위해 조직의 첫번째 방어선으로써 그 강도를 유지하는 데 도움이 됩니다. |
| 1.1.1 | **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations | 방화벽과 라우터 구성의 변경 및 모든 네트워크 연결을 테스트 하고 승인하기 위한 공식적인 절차(프로세스) | 1.1.1a | Examine documented procedures to verify there is a formal process for testing and approval of all:<br>• Network connections and<br>• Changes to firewall and router configurations | 문서화된 절차를 통해 다음의 모든 항목들을 테스트하고 승인하기 위한 공식적인 절차가 있는지 확인한다:<br>• 네트워크 연결<br>• 방화벽과 라우터의 구성 변경 | A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall.<br>Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration. | 방화벽과 라우터의 모든 연결과 변경을 승인 및 테스트하기 위해 문서화되어 실시되고 있는 프로세스는, 네트워크 라우터 또는 방화벽의 잘못된 구성에 의해 발생하는 보안 문제를 방지하는데 도움이 됩니다.<br>변경에 대한 공식 승인과 테스트 없이 변경 기록이 업데이트 되어서는 안되며, 이는 곧 (네트워크) 문서상의 기록과 실제 구성 사이에 불 일치가 발생하는 원인이 됩니다. |
| | | | 1.1.1b | For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. | 네트워크 연결중 샘플을 선정한 후, 해당 네트워크 책임자를 인터뷰하고 기록을 검토하여 네트워크 연결이 승인되고 테스트 되고 있는지 확인한다 | | |
| | | | 1.1.1c | Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | 방화벽과 라우터 구성의 실질적 변화를 샘플을 선정하고 확인한 후 기록의 변경을 비교하며, 그리고 책임자를 인터뷰해 그 변경이 승인되고 테스트 되었는지 확인한다. | | |



## 5.3 블록체인 구축 보안 가이드 (3/4)

5 대응 방안

### DB 항목 - Requirement 3: 데이터의 안전한 저장

| No. | Goals | No. | Requirements | Requirements Count | Testing Procedures Count |
|---|---|---|---|---|---|
| II | Protect Cardholder Data (카드 소유자 데이터 보호) | 3 | Protect stored cardholder data (카드 소유자 데이터의 안전한 저장) | 22 | 46 |
| | | 4 | Encrypt transmission of cardholder data across open, public networks (공개망 전송 시 암호화) | 4 | 13 |

### 네크워크 항목 - Requirement 10 : 네트워크 및 데이터 접근 모니터링

| No. | Goals | No. | Requirements | Requirements Count | Testing Procedures Count |
|---|---|---|---|---|---|
| V | Regularly Monitor and Test Networks (네트워크의 정기적인 모니터 및 테스트) | 10 | Track and monitor all access to network resources and cardholder data (네트워크 및 데이터 접근 모니터링) | 32 | 41 |
| | | 11 | Regularly test security systems and processes (보안시스템 및 프로세스에 대한 정기적 점검) | 16 | 32 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| are documented, in use, and known to all affected parties. | 있는지 확인한다. | | protecting stored cardholder data are:<br>• Documented,<br>• In use, and<br>• Known to all affected parties.. | 는지 확인한다 :<br>• 문서화되어 있다.<br>• 사용되고 있다.<br>• 영향을 받는 관계자 전원에게 알려져 있다. | | | 의 지속적인 관리를 위하<br>운영 절차를 인식하고 |

## 5.3 블록체인 구축 보안 가이드 (4/4)

5 대응 방안

**접근통제 항목**

| No. | Goals | No. | Requirements | Requirements Count | Testing Procedures Count |
|---|---|---|---|---|---|
| IV | Implement Strong Access Control Measures (강력한 접근통제 대책 적용) | 7 | Restrict access to cardholder data by business need to know (업무상 알 필요에 근거한 접근 제한) | 10 | 11 |
| | | 8 | Assign a unique ID to each person with computer access (1인 1계정 부여) | 23 | 44 |
| | | 9 | Restrict physical access to cardholder data (물리적 접근 제한) | 27 | 44 |

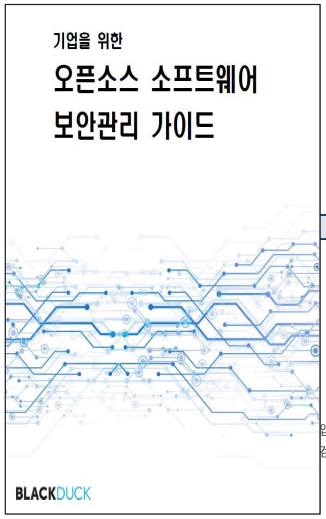
| | | | | | | |
|---|---|---|---|---|---|---|
| **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.<br><br>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network | 시스템을 네트워크에 설치하기 전에 반드시 공급업체에서 제공하는 기본값을 변경하고, 불필요한 디폴트 계정을 비활성화 한다.<br><br>이것은 운영 체계, 보안 서비스를 제공하는 소프트웨어, 응용 프로그램, 시스템 계정, 포인트 오브 세일즈(POS) 단말기, 결제 어플리케이션, 단순 네트워크 관리 프로토콜(SNMP), 커뮤니티 문자열 등에서 사용되지만 이에 한정되지 않으며, 모든 기본 패스워드에 적용된다. | 2.1.0a | Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) | 시스템 구성 요소의 샘플을 선정하고 그 공급업체에서 제공하는 기본 계정과 패스워드를 사용하여 장치에 로그온을 시도하고(시스템 관리자의 도움을 받아) 모든 기본 패스워드(운영 체제(OS), 보안 서비스를 제공하는 소프트웨어, 응용 프로그램, 시스템 계정, POS 단말기, 단순 네트워크 관리 프로토콜(SNMP), 커뮤니티 문자열 에서 사용되는 것을 포함)가 변경되어 있는지 확인한다.(공급업체의 설명서 및 인터 넷 소스를 사용하여 공급업체 제공의 계정 / 패스워드를 확인한다.) | Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.<br><br>Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password. | 악의적인 사용자(조직의 내외에 관계없이)는 흔히 공급업체의 기본 설정, 사용자 계정 및 패스워드를 사용하여 설치되어 있는 운영 체제(OS), 소프트웨어, 응용 프로그램, 시스템을 위협합니다. 이러한 기본 설정은 네트워크 및 해커 커뮤니티 등에 많이 공개되어 있으며, 해커들 사이에서도 잘 알려져 있지만, 설정을 변경함으로 써 공격에 대한 시스템의 취약점을 줄일 수 있습니다.<br><br>기본 계정을 사용할 예정이 없는 경우에도 기본 패스워드를 강력한 고유 패스워드 로 변경 한 후 해당 계정을 비활성화함으로써 악의적인 사용자가 계정을 다시 활성 화한 후 기본 패스워드를 통하여 접근하는 것을 방지 할 수 있습니다. |



## 5.4 오픈소스 구축 보안 가이드 (1/2)

5 대응 방안

**보안가이드**




**오픈소스 보안 요구항목**

| 구분 | 분·석설계단계 보안요구항목 | 구현단계 보안취약점 |
|---|---|---|
| 입력데이터 검증 및 표현 | DBMS 조회 및 결과 검증 | SQL 삽입 |
| | XML 조회 및 결과 검증 | XQuery 삽입<br>XPath 삽입 |
| | 디렉토리 서비스 조회 및 결과 검증 | LDAP 삽입 |
| | 시스템 자원 접근 및 명령어 수행 입력값 검증 | 경로조작 및 자원삽입<br>운영체제 명령어 삽입 |
| | 웹 서비스 요청 및 결과 검증 | 크로스사이트 스크립트 |
| | 웹 기반 중요기능 수행 요청 유효성 검증 | 크로스사이트 요청 위조 |
| | HTTP 프로토콜 유효성 검증 | 신뢰되지 않은 URL 주소로 자동 HTTP 응답분할 |
| | 허용된 범위내 메모리 접근 | 포맷스트링 삽입<br>메모리 버퍼 오버플로우 |

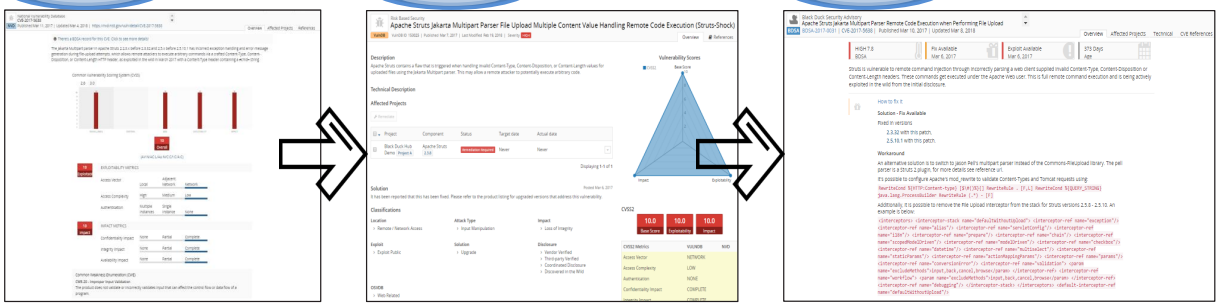
**보안 체크리스트**

| 세부통제 영역 | 세부통제 항목 | 결과 이행 (Y) | 부분 이행 (P) | 미이행 (N) | 해당 없음 (N/A) | 평가 근거 및 의견 |
|---|---|---|---|---|---|---|
| SQL 삽입 | 예약어를 사용하는 경우에는 DB쿼리에 사용되는 외부 입력값에 대하여 특수문자 및 쿼리 예약어를 필터링하는가? | | | | | |
| | 스트러츠(Struts), 스프링(Spring) 등과 같은 프레임워크를 사용하는 경우 에는 외부입력값 검증모듈 및 보안모듈을 상황에 맞추어 적절하게 사용하는가? | | | | | |
| XQuery 삽입 | XQuery에 사용되는 외부 입력데이터에 대하여 특수문자 및 쿼리 예약어를 필터링하는가? | | | | | |
| | XQuery를 사용한 쿼리문은 문자열을 연결하는 형태로 구성하지 않고 파라미터(Parameter)화된 쿼리문을 사용하는가? | | | | | |
| XPath 삽입 | Xpath 쿼리에 사용되는 외부 입력데이터에 대하여 특수문자(', [ ], /, =, @ 등) 및 쿼리 예약어 필터링을 수행하고 파라미터화된 쿼리문을 지원하는 XQuery를 사용하는가? | | | | | |

## 5.4 오픈소스 구축 보안 가이드 (2/2)

5 대응 방안

1단계 2단계 3단계



### NVD (CVE, CWE)

- 일반인에게 공개된 보안취약점 정보
- 보안취약점 상세설명, CVSS 스코어 및 CVE, CWE 메트릭스 포함

### VulnDB

- 가장 많은 보안취약점 DB를 보유하고 있는 보안취약점 데이터베이스
- 보안취약점에 대한 기술적 상세설명, 패치여부확인 및 솔루션, VulnDB 메트릭스 및 레퍼런스 링크 포함

### Black Duck Security Advisory

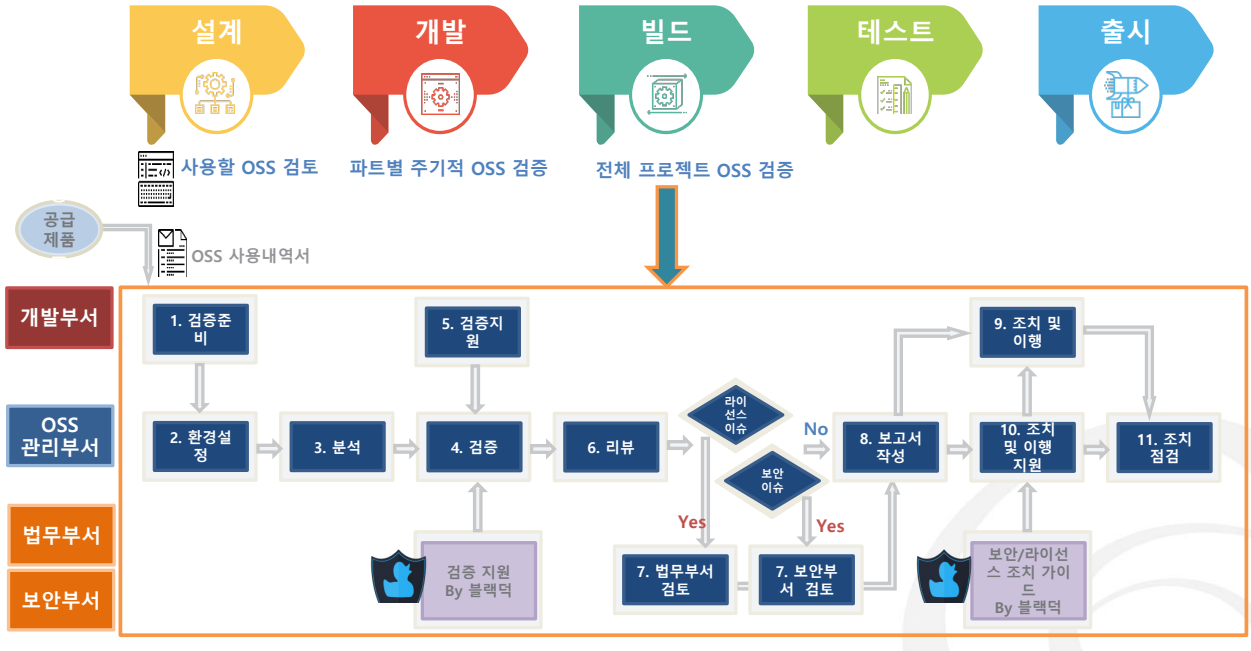
- 블랙덕 보안 연구기관 (Center for Open Source Research & Innovation, COSRI)의 오픈소스 보안 전문 리서치를 통해 검토
- 보안취약점 업데이트 버전, 패치 방법 제공

Blockchain Security SECURITY



## 5.4 오픈소스 보안 관리 사례 –블랙덕 허브 (1/4)

5 대응 방안




Blockchain Security SECURITY

## 5.4 오픈소스 보안 관리 사례 –블랙덕 허브 (2/4)

5 대응 방안

**검증대상 코드 분석 및 오픈소스 식별**

Black Duck Hub를 통해 검증대상 코드로부터 오픈소스 및 보안취약점 식별

**우선순위 조치대상 보안취약점 분류**

블랙덕의 오픈소스 보안가이드를 통해 고위험도 우선조치대상의 오픈소스 보안취약점 리스트업

**Hub를 통한 조치 솔루션 확인**

Black Duck Hub를 통해 조치 가능한 오픈소스 보안취약점 솔루션 및 대체버전의 오픈소스 확인

단계별 보안 조치 참조

"오픈소스 보안취약점 관리 프로세스"

**조치 프로세스 시행**

Black Duck Hub의 조치 프로세스를 통해 유관부서 담당자들과 협업하여 오픈소스 보안취약점 조치 시행

**지속적인 모니터링**

식별한 오픈소스를 Black Duck Hub를 통해 실시간으로 지속적인 모니터링을 하며 향후 발생할 수 있는 오픈소스 보안취약점에 대해 신속한 조치 시행

Blockchain Security SECURITY 블록체인 시큐리티

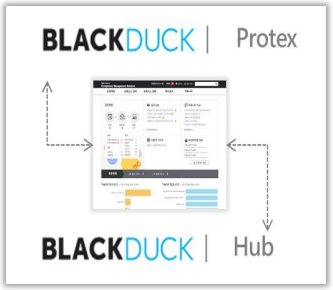


## 5.4 오픈소스 보안 관리 사례 –블랙덕 허브 (3/4)

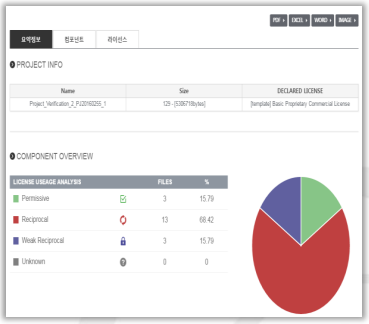
5 대응 방안

- 블랙덕 솔루션을 바탕으로 오픈소스 사용 가이드라인을 제공하고 개발SW에 인용된 오픈소스의 보안취약점 및 저작권 침해와 라이선스 위반을 관리함으로써 체계적인 오픈소스 통합관리 기능을 제공함

**오픈소스 라이선스/보안 솔루션과의 연동 및 관리**




**실시간 현황 통계 및 오픈소스 사용 정보 모니터링**



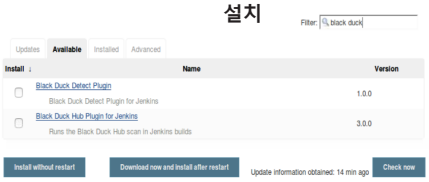

**관리에 필요한 기능 자동화 및 관리 효율성 증대**

Blockchain Security SECURITY 블록체인 시큐리티

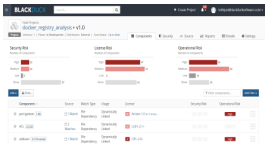
## 5.4 오픈소스 보안 관리 사례 –블랙덕 허브 (4/4)

5 대응 방안

젠킨스 플러그인 저장소에서 블랙덕 허브 플러그인 설치

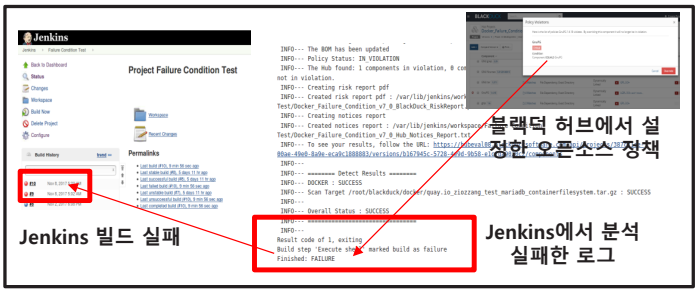


젠킨스 빌드 프로세스를 통해 프로젝트 자동분석

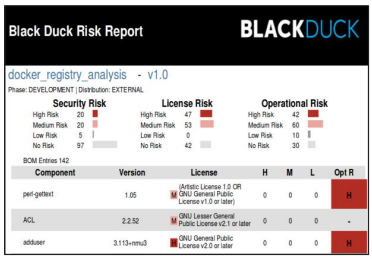


자동분석된 프로젝트

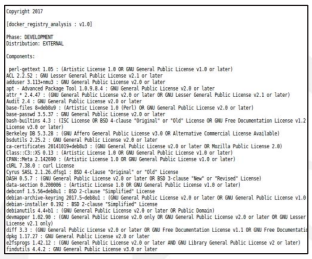
기능 1. 오픈소스 정책에 따라 빌드실패 유도




기능 2 : 블랙덕 리스크 리포트 자동산출




기능 3. 라이선스 고지문 산출



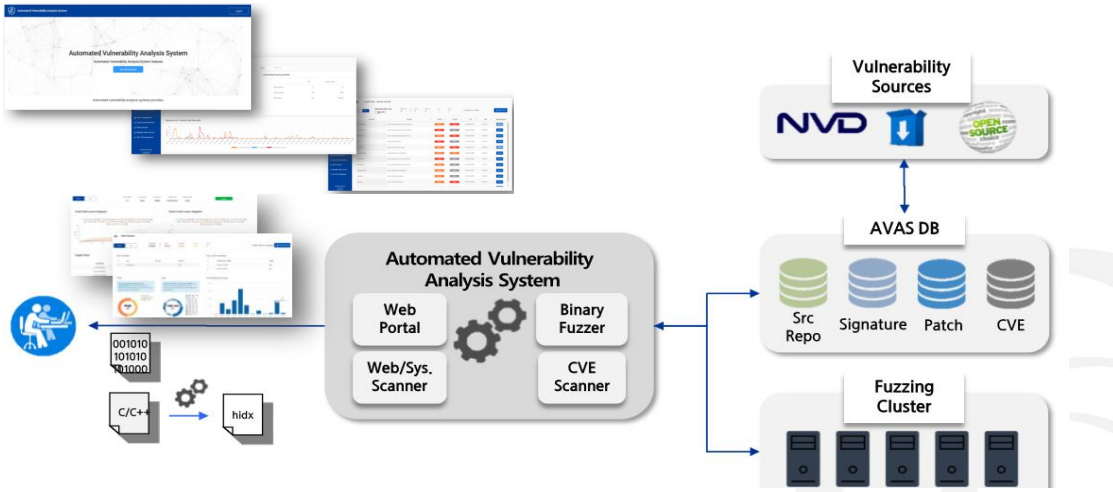


## 5.4 오픈소스 보안 관리 사례 – S사 AVAS (1/3)

5 대응 방안

### S사 AVAS

- 사용하기 쉬운 웹베이스 관리 도구
- to analyze CVEs in source code (Known vulnerabilities)
- to find memory corruption bug in binary (Unknown vulnerabilities)
- to scan Web/System vulnerabilities (Known vulnerabilities)

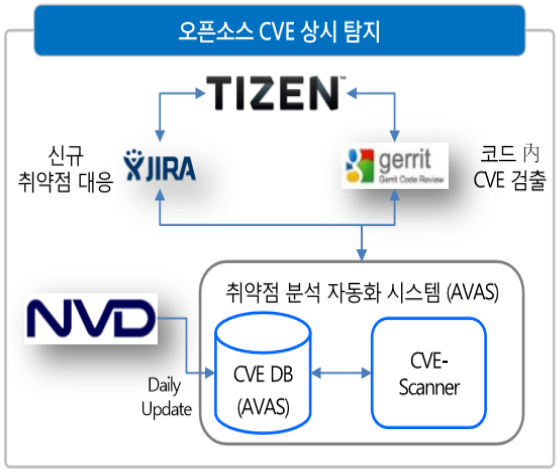


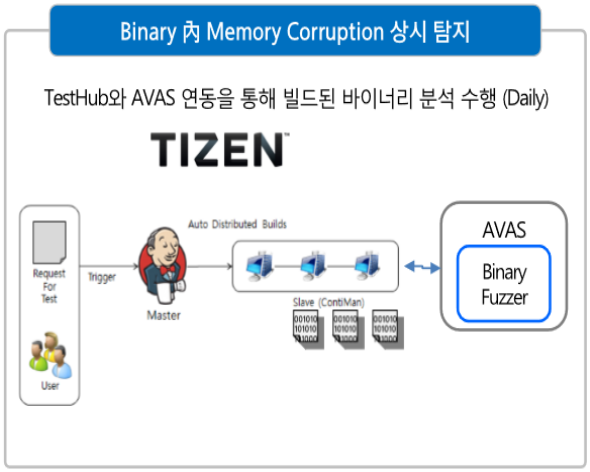
## 5.4 오픈소스 보안 관리 사례 – S사 AVAS (2/3)

5 대응 방안

### S사 AVAS

- When a new CVE is released, AVAS will alert the Tizen team within 24 hours.
- Every time a Tizen developer pushes code, AVAS checks CVE by default.
- AVAS will perform Fuzzing tests on Tizen binaries daily soon.




Blockchain Security SECURITY



## 5.4 오픈소스 보안 관리 사례 –S사 AVAS (3/3)

5 대응 방안

### S사 AVAS

**CVE Scanner**

**CVE**

OVER 80,000 NVD

**Patch**

10,000

**Crawling**

24h

**Automated Fuzzing**

**Architecture**

ARM
x86/x64
TIZEN

**Engine**

2 AFL Smart Fuzzer

**Computing Power**

40 cores

Blockchain Security SECURITY

## 5.5 지능형 대응방안 - 사이버 킬체인 모델

5 대응 방안

### 개요

- 킬체인은 선제타격시스템 또는 공격형 방위 시스템을 뜻하는 군사용어(타격순환제)
- 1991년 걸프전부터 사용된 언어로 미국 방위업체 록히드마틴의 컴퓨터 과학자들이 네트워크 방어를 위한 사이버 보안과 관련해서도 이 용어를 사용하기 시작

### 관련 기사

최근 사이버 킬체인 구축 및 전략에 대한 관심이 높아지고 있음

### 1 사이버 킬체인 개념

- 사이버 공격을 대응하기 위한 개념

### 2 사이버 킬체인 모델 및 활용

- 록히드마틴, 미 국방부, 가트너, 베다시스, 휴랫패커드, 델, 시스코

### 3 사이버 킬체인 기반 대응 방책

- 공격 유형, 유형 별 대응 방책, 경로별 대응 방책, 단계별 대응 방책



## 5.6 지능형 대응방안 - 사이버 킬체인 개념

5 대응 방안

### 사이버 킬체인

- 전쟁터에서 적군의 공격 체인을 선제 공격하여 적의 공격을 무력화시키는 군사적 개념에서 시작
- 최근 지능형 지속 공격에 의한 사이버 피해 사례를 대응하기 위한 체계

**사이버 공격도 일련의 공격 과정에서 방어자가 공격의 공격 과정 상의 한 단계만 차단해도 공격을 무력화하거나 지연시킬 수 있음을 제안하는 모델**

### 사이버 킬체인 모델

록히드마틴 | 미 국방부 | 가트너 | 베다시스 | 휴랫패커드 | 델 | 시스코

## 5.7 사이버 킬체인 7단계

5 대응 방안

**록히드마틴**

- 록히드마틴은 정찰, 무기화, 유포, 악용, 설치, 명령 및 제어, 목적 달성의 7단계로 구성된 모델 제시

| | | |
|---|---|---|
| 1단계 | 정찰 Reconnaissance | • 공격자가 의도한 목적을 달성하기 위해 공격 대상을 탐색하고 식별 및 선정하는 단계 |
| 2단계 | 무기화 Weaponization | • 공격자가 정찰 단계를 통해 표적을 선정한 후, 표적을 공격하기 위한 사이버 무기를 준비하는 단계 |
| 3단계 | 유포 Delivery | • 만들어진 사이버 무기를 표적으로 전달하는 단계(메일 첨부파일, 웹 사이트, USB) |
| 4단계 | 악용 Exploitation | • 사이버 무기가 표적 시스템에 전달된 후 악성 코드의 작동이 촉발되는 단계(취약점 이용) |
| 5단계 | 설치 Installation | • 공격자가 표적 시스템에 트로이목마, 백도어 등을 설치하여 표적에서 활동할 환경 조성 단계 |
| 6단계 | 명령 및 제어 Command & Control | • 공격자가 외부에서 표적 시스템을 통제할 수 있도록 채널을 구축하고 접근하는 단계 |
| 7단계 | 목적 달성 Actions on Objectives | • 공격자가 의도한 목적을 달성하는 단계(내부자료 정찰, 정보 수집, 데이터 훼손, 시스템 파괴 등) |

Blockchain Security SECURITY



## 5.8 미국방부 대응 모델 (1/2)

5 대응 방안

**미 국방부**

- 미 국방부는 공격과 방어의 주요 활동과 목적 등을 기술한 사이버안보 킬체인 제시
- 록히드마틴과 다르게 설치단계를 제외하고 목적달성 이후 유지 단계 추가

| 공격자 | 방어자 |
|---|---|
| 정찰 (Recon) | 탐지 (Detect) |
| 무기화 (Weaponize) | 거부 (Deny) |
| 유포 (Deliver) | 교란 (Disrupt) |
| 악용 (Exploit) | 약화 (Degrade) |
| 통제 (Control) | 기만 (Deceive) |
| 시행 (Execute) | 파괴 (Destroy) |
| 유지 (Maintain) | |

장기간 지속적으로 다양한 경로를 이용해 지능적 공격

공격을 분석하고 대응 방안을 결정

Blockchain Security SECURITY

## 5.8 미국방부 대응 모델 (2/2)

5 대응 방안

### 미 국방부

› 록히드마틴은 미 국방부 정보작전 팀 대응 방안을 적용하여 각 유형별로 활용할 수 있는 기술을 제시

| 정찰 (Reconnaissance) | 탐지 (Detect) | 거부 (Deny) | 교란 (Disrupt) | 약화 (Degrade) | 기만 (Deceive) | 파괴 (Destroy) |
|---|---|---|---|---|---|---|
| 정찰 (Reconnaissance) | Web Analytics | Firewall ACL | | | | |
| 무기화 (Weaponization) | NIDS | NIPS | | | | |
| 유포 (Delivery) | Vigilant user | Proxy filter | In-line AV | Queuing | | |
| 악용 (Exploitation) | HIDS | Patch | DEP | | | |
| 설치 (Installation) | HIDS | Chroot jail | AV | | | |
| 명령 및 제어 (Command and Control) | NIDS | Firewall ACL | NIPS | Tarpit | DNS redirect | |
| 목적 달성 (Actions on Objectives) | Audit log | | | Quality of Service | Honeypot | |

Blockchain Security SECURITY



## 5.9 디도스 공격에 대한 사이버킬체인 분석

5 대응 방안

### 디도스 공격

› 록히드마틴의 사이버 킬체인 모델을 디도스 공격절차에 활용

정찰 Reconnaissance

- 공격자가 공격할 특정 웹사이트 선정
- 공격에 활용할 컴퓨터 후보군 선발

무기화 Weaponization

- 공격자가 직접 프로그래밍하여 실행 파일에 악성코드 주입
- 자동화 도구를 이용한 악성코드 제작

유포 Delivery

- 이메일 파일 첨부 및 웹 사이트 등을 통해 악성코드 유포

악용 Exploitation

- 사용자가 악성코드를 다운로드하여 실행 시 감염
- 감염 후 공격자가 침투하여 시스템 정보 탐색 및 취약점 조사

설치 Installation

- 시스템의 취약점을 활용해 추가 악성코드 설치 유도

명령 및 제어 Command & Control

- 유입된 악성코드는 감염된 컴퓨터에 잠복
- 공격자의 명령에 따라 활성화 및 통제

목적 달성 Actions on Objectives

- 특정 웹 사이트에 동시 접속하여 사용자들이 웹 사이트에 접근하지 못하도록 함

Blockchain Security SECURITY

## Contents

# VI. 보안 인텔리전스



### 대응 방책 프레임워크

- 사이버 킬체인에 기반한 대응 방책 프레임워크
- 사이버 공격의 대표적이 공격방법에 대한 대응방법은 다음과 같음

| 보안 대상 | 대응 방법 | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 네트워크 보안 | 방화벽 | IDS | IPS | Anti-Spam Virus Wall | VPN | TMS | 유해 사이트 차단 | 통신 암호화 (SSL 등) | 무선 보안 | NAC | Anti-DDoS | ESM / 종합분석시스템 | 통합로그분석 / 디지털포렌식 | 통합정보유출 모니터링 / 통합정보 모니터링 시스템 | IAM(Identity and Access Management) | RMS(Risk Management System) / ESP / 보안 포털 |
| | UTM/XTM | | | | | | | | | | | | | | | |
| 시스템 보안 | 서버보안 (Secure OS) | | | 원격접속통제 | | | 취약점 스캐너 | | | | | | | | | |
| 애플리케이션 보안 | PKI | HSM | SSO | EAM | 앱 가상화 (SBC) | 웹 방화벽 | 웹 취약점 스캐너 | 소스코드 취약점 스캐너 | | | | | | | | |
| 데이터베이스 보안 | 데이터베이스 취약점 스캐너 | | 데이터 마스킹 | | 데이터베이스 암호화 | | 데이터베이스 접근제어/감사 | | | | | | | | | |
| 클라이언트 보안 | PC보안 (DLP) | Anti-Virus | PMS | Anti-Phishing | Anti-Spyware | 키보드 보안 | Client 가상화 | 스마트폰 보안 (MDM 등) | | | | | | | | |
| 컨텐츠 보안 | 문서보안 (DRM) | 위변조 방지 | 출력 보안 | 보안 메일 | 컨텐츠 검색/필터링 | HDD 암호화 | 데이터 완전삭제 | 보안 USB | 문서 중앙화 | 데스크탑 가상화(SBC) | | | | | | |
| 물리/융합 보안 | 출입통제 | 검색대 | EAS | RFID | 보안종이 | 생체인식 | OTP | 보안토큰 | 디가우저 | 지능형 영상감지 | 복합기 보안 | 스마트 카드 | | | | |

# 6.1 보안인텔리전스 프레임워크 (2/3)



## 대응 방책 프레임워크

- 사이버 킬체인에 기반한 대응 방책 프레임워크
- 사이버 공격의 대표적이 공격방법에 대한 대응방법은 다음과 같음

### 사이버 킬체인 현황

- 현재 사이버 킬체인은 공격자가 하는 행위를 근거로 추적하여 차단하는 개념
  - ➔ 단편적인 피해 복구만 중요시되는 한계 존재
  - ➔ 적의 의도 탐지 기술 및 체계에 대한 보완 필요
- 국방 정보보호 체계와 민간 체계에서 산출되는 빅데이터를 활용해 적의 의도를 선제적으로 파악하고, 관련 기관 간의 실시간 정보공유
  - ➔ 적의 공격 무력화 및 공격 지연 대응 체계 구축 필요
- 국방 및 군 관련 정부 기관 인력의 보안 의식 향상
  - ➔ 인식 교육 훈련 강화
- 엔드포인트 보안 체계 도입 시 전체를 보호하기 위한 탐지 및 차단 기술 필요
- 데이터 보호 및 무단 유출 방지 통합 플랫폼 도입 필요

### 보안 대상 별 예방, 탐지, 추적 및 교정 방안

<table>
<tr><th></th><th colspan="4">예방</th><th>탐지</th><th colspan="2">추적 및 교정</th></tr>
<tr><td rowspan="3">네트워크</td><td>방화벽</td><td>VPN</td><td>IDS</td><td>TMS</td><td rowspan="6">통합로그분석/<br>디지털포렌식</td><td rowspan="6">취약점진단/<br>사고대응 프로세스</td></tr>
<tr><td colspan="4">IPS / UTM</td><td>네트워크 스캐너</td></tr>
<tr><td colspan="4">Anti-DDoS</td><td rowspan="2"></td></tr>
<tr><td>서버</td><td>서버보안</td><td>원격접속통제</td><td>HIDS</td><td>시스템 스캐너</td></tr>
<tr><td>데이터베이스</td><td>DB암호화</td><td colspan="3">DB 접근제어 / 감사</td></tr>
<tr><td rowspan="3">애플리케이션</td><td colspan="3">PKI / OTP / SSO / EAM / IAM</td><td></td><td>소스취약점 스캐너</td></tr>
<tr><td colspan="4">웹 방화벽</td><td>웹 취약점 스캐너</td></tr>
<tr><td colspan="5">웹 개발보안 체계</td></tr>
<tr><td>통합관리</td><td colspan="6">ESM / RMS / 종합분석시스템</td></tr>
<tr><td></td><td colspan="6">사전 영향성 검토 프로세스 / 보안관제 체계</td></tr>
</table>



# 6.1 보안인텔리전스 프레임워크 (3/3)



## 방책 유형 분류 및 세부 방책

| 정보보안체계 유형 분류 | 방책 유형 분류 | 세부 방책 |
|---|---|---|
| 네트워크 보안 | 1. 네트워크 공격 대응 방책 | 레거시 방화벽 |
| | | 차세대 방화벽 |
| | | DDoS 방어 |
| | | DNS 보안 |
| | | 보안AP·WIPS·VPN |
| | | 보안 스위치 |
| | | TAP·방화벽 관리 |
| | | 능동형 보안 아키텍처 |
| | 2. 웹·이메일·애플리케이션 공격 대응 방책 | 이메일 보안 |
| | | 웹방화벽 |
| | | 웹쉘 방어 전용 솔루션 |
| | | 보안웹게이트웨이 (SWG) |
| | | SSL 가시성 |
| | | 시큐어코딩·소스코딩 보안 |
| | 3. 접근 제어 방책 | 네트워크접근제어(NAC)·IP관리 |
| | | 망분리·망연계 |
| | | 통합계정접근관리(IAM)·시스템접근제어 |
| | | 사용자인증·SSO·비밀번호관리 |

| 정보보안체계 유형 분류 | 방책 유형 분류 | 세부 방책 |
|---|---|---|
| 시스템 (단말) 보안 | 4. 엔드포인트 공격 대응 방책 | 안티바이러스·통합엔드포인트보안 |
| | | 엔드포인트 침해탐지 및 대응 (EDR) |
| | | 엔드포인트 추적, 침해탐지 및 대응 (ETDR) |
| 콘텐츠(데이터) /정보유출방지보안 | 5. 데이터 보안 방책 | 정형 데이터 암호화·키관리·접근 제어 |
| | | DB 접근 제어 체계 |
| | | 비정형 데이터 암호화·유출방지 |
| | | 문서 중앙화 |
| | 6. 랜섬웨어 대응 방책 | - |
| | 7. 중요정보 유출 대응 방책 | - |
| 보안관리 | 8. 보안 관리 방책 | 통합로그관리·SIEM·네트워크포렌식 |
| | | 사용자 및 계정 행위 분석 (UBA/UEBA) |
| | | 보안관리·보안관제·침해대응 |
| | | 취약점 진단·모의해킹 |

## 6.2 보안인텔리전스 세부 방책 (1/10)

6 보안 인텔리전스

### 1. 네트워크 공격 대응 방책

#### 레거시 방화벽

- 하드웨어 플랫폼에 보안 기능들을 직렬로 배치하여 각 모듈 별로 패킷-리패킷을 진행하여 장비 성능이 낮았으며 관리가 복잡해져 대규모 환경이 아닌 이상 필요한 보안 시스템을 갖추지 못함
- 통합보안위협관리(UTM)솔루션을 통해 네트워크 보안의 모든 기능을 통합시킴

#### 차세대 방화벽

- 성능 저하 없이 방화벽, IPS, VPN, 안티바이러스 등의 네트워크 보안기능을 모두 사용할 수 있으며 SSL트래픽 복호화 가능
- 세션단위로 분석
- 프로토콜 이상행위를 분석해 악성코드의 C&C통신을 찾을 수 있음

#### DDoS 방어

- DDoS공격은 애플리케이션 계층을 공격해 서비스 장애를 일으키는 지능적인 공격으로 최근 대규모 공격이 증가하고 있음
- IDG에 따르면 DDoS공격 중 35%가 네트워크 공격 ,34%는 네트워크 볼륨 공격, 30%는 애플리케이션 계층 공격
- 따라서 DDoS 방어 솔루션이 다시 성장하고 있으며, 대규모 공격 방어를 위한 대형 장비와 클라우드 기반의 방어 기술이 대응책으로 부각됨

#### DNS 보안

- DNS는 정상 사용자의 요청인지 공격자의 요청인이 구분하지 않고 IP주소만을 알려주므로 보안이 고려되지 않고 설계됨
- DNS서버 자체가 저렴하므로 DNS 서버를 증설해 일정 수준의 DNS 증폭 공격을 막을 수 있지만 대규모 공격은 서버 증설로 예방이 어려움
- DNS는 빠른 속도가 생명이므로 가볍고 빠르면서 지능적인 보안 기술이 요구됨



## 6.2 보안인텔리전스 세부 방책 (2/10)

6 보안 인텔리전스

### 1. 네트워크 공격 대응 방책

#### 보안 AP•WIPS•VPN

- 보안에 취약한 사물인터넷과 BYOD 환경에서 주소를 변조한 파밍 공격은 막을 수 없음
- WIPS는 컨트롤 서버가 비싸서 도입이 부담스러운 솔루션
- WIPS와 VPN은 외부 접속 차단 및 내부정보 유출 방지, 스마트폰 테더링 서비스 통제, 불법 네트워크 접속 등을 위해 유무선 통신 네트워크를 사용하는 환경에서 반드시 요구됨

#### 보안 스위치

- L2/L3에서 주로 발생하는 MAC 플러딩, MAC 변조, ARP 스푸핑, IP 스푸핑, DHCP 및 ICMP 공격 등을 차단함
- VoIP 환경에서 도감청 방지
- 사용자 단말의 유해 트래픽을 차단하고 정상 트래픽은 유입시키는 반면 NAC 위험이 있는 단말의 네트워크 접근 차단

#### TAP•방화벽 관리

- 바이패스 스위치를 설치, 이중화 구성, 많은 보안장비가 있을 수록 네트워크 가시성 확보가 어려움
- 따라서 TAP을 설치하여 네트워크 트래픽 분석
- 패킷 브로커는 장비로 패킷을 전달하는 스위치로서 패킷 필터링과 로드밸런싱 역할을 함

#### 능동형 보안 아키텍처

- 진화하는 공격에 대한 대응 방법으로 능동형 보안 아키텍처가 제안
- 네트워크 경계에서 레거시 방화벽의 역할, 애플리케이션 계층에서 차세대 방화벽의 역할, 내부 네트워크에서는 확산되는 공격을 탐지하는 APT 방어 역할에 집중
- 능동형 보안 아키텍처를 위해 네트워크 내부를 더 작은 단위로 보안 범위 분할(ISFW)

## 6.2 보안인텔리전스 세부 방책 (3/10)



### 2. 웹•이메일•애플리케이션 공격 대응 방책

#### 이메일 보안

- 이메일에 악성 링크 및 악성 첨부파일을 삽입하여 보내는 공격
- 샌드박스에서 의심스러운 첨부파일을 실행하여 위험요소 유무를 확인
- 문서를 분해해 안전한 콘텐츠로 재조합 하는 기술과 이메일 암호화로 인증된 사용자로 부터만 수신하는 방법도 있음

#### 웹방화벽

- 전체 해킹의 75%가 웹 애플리케이션에서 발생하고 대부분의 공격은 정상적인 패킷으로 위장하여 방화벽 등을 통과
- 기존의 시그니처 기반 공격 차단 솔루션 외에 SSL 복호화, 고성능, 최신 웹 환경 지원이 가능한 지능형 웹 방화벽 서비스가 요구됨
- 클라우드 기반의 위협 인텔리전스를 이용하면 실시간으로 공격 탐지 및 차단이 가능

#### 웹쉘 방어전용 솔루션

- 웹쉘 공격자는 짧은 코드를 사용하거나 정상적인 스크립트 파일 삽입, 웹소스 보호 등을 위한 스크립트 인코더, 시그니처 문자열 분산 삽입 등의 방법으로 안티바이러스, 웹 방화벽 등을 우회
- 웹쉘 공격 방어는 보안관제 및 방어 전용 솔루션이 요구됨

#### 보안웹게이트웨이(SWG)

- 웹을 통해 진행되는 대규모 감염과 지능형 지속 공격을 막기 위해 사용자 단말과 내부 네트워크를 악성 웹으로부터 보호하는 체계
- 클라우드 인프라를 이용해 지속적으로 전 서계 웹사이트를 모니터링하고 유해 사이트리스트 업데이트



## 6.2 보안인텔리전스 세부 방책 (4/10)



### 2. 웹•이메일•애플리케이션 공격 대응 방책

#### SSL 가시성

- 악성코드를 암호화 트래픽에 숨겨 유입하거나 중요정보를 암호화하여 탈취하는 등을 통해 솔루션 우회
- 인바운드 트래픽 뿐만 아니라 아웃바운드 트래픽의 분석이 필요

#### 시큐어코딩•소스코딩 보안

- 공격은 애플리케이션 취약점을 이용해 진행되므로 설계부터 테스트, 운영까지 전 단계에서 취약점을 고려해야 함
- 소프트웨어 개발 과정에서 시큐어 코딩의 중요성이 높아지고 있음
- 모바일 앱 보호를 위해 개발 과정에서 시큐어 코딩을 적용하고, 개발 완료 시 난독화로 보호하며 정기적으로 점검해야 함

## 6.2 보안인텔리전스 세부 방책 (5/10)



### 3. 접근 제어 방책

#### 네트워크접근제어(NAC)•IP관리

- 네트워크에 접근하는 모든 단말의 인증정보 및 보안 무결성을 검증하는 NAC는 위험한 단말의 접근을 차단해 내부 네트워크 보안
- 우리나라에서는 IP관리 솔루션을 기반으로 한 NAC 주로 사용
- 차세대 NAC는 사물인터넷과 클라우드를 위한 엔드포인트 제어 기능이 있으며, 단말 통제를 위해 수집하는 빅데이터를 이용해 지능적인 보안 모니터링 및 침해탐지/대응 지원 예정

#### 망분리•망연계

- 망분리 기술도 중요하나 운영 기술도 중요
- 망분리 예외조치를 취한 사이트와 자료 등은 모니터링을 통해 감시를 해야 하며 보안 정책 등을 적용해야 함

#### 통합계정접근관리(IAM)•시스템접근제어

- 업무환경이 복잡해질 수록 계정관리와 접근권한 문제가 중요시 되고 있음
- 통합계정접근관리 시스템은 계정관리와 접근관리 기능을 통합하여 사용자에게 부여된 권한 내에서만 시스템에 접근할 수 있도록 함
- 멀티팩터 인증을 적용하여 강력한 본인인증을 거치도록 함

#### 사용자 인증•SSO•비밀번호 관리

- 사이버 활동 시 사용자, 단말, 네트워크 등에 대해 정상/비정상을 인증해야 하며 데이터가 위변조되었는지 아닌지 유무를 확인해야 함
- SSO는 한 번의 강력한 인증을 완료하면 연계된 시스템에서 인증을 하지 않아도 되는 기술이므로 더 강력한 보안이 필요시 됨



## 6.2 보안인텔리전스 세부 방책 (6/10)



### 4. 엔드포인트 공격 대응 방책

#### 안티바이러스•통합엔드포인트보안

- AV는 악성코드의 시그니처 매칭, 정적/동적 분석, 평판분석 기술을 이용해 웹/이메일 필터링으로 유입/확산 경로를 감시
- 최근 AV는 통합엔드포인트보안으로 진화하여 다양한 엔진을 하나의 에이전트에 통합시켜 오탐/미탐 없이 악성코드를 차단
- 또한, 모바일 기기, 다양한 사물인터넷, ICS/SCADA 보안을 위한 차세대 엔드포인트 보안 체계로 발전하고 있음

#### 엔드포인트 침해탐지 및 대응(EDR)

- AV보다 진보한 모델인 통합엔드포인트보안(EPP) 솔루션은 신변종 악성코드를 탐지하지만 완벽한 차단이 어려움
- EDP 는 AV와 EPP한계를 극복하기 위해 제안된 체계
- 엔드포인트 행위 모니터링과 분석 및 IOC를 참고해 보안사고 탐지

#### 엔드포인트 추적, 침해탐지 및 대응(ETDR)

- 스마트폰, 태블릿 PC, 사물인터넷, POS, 산업용 장비 등도 엔드포인트로 분류되어 관리 범위가 확대됨
- EPP와 DER이 통합하여 방대한 위협 인텔리전스와 고도의 이상행위 탐지 기술을 접목하여 공격의 선제 방어부터 탐지대응까지 가능한 ETDR로 진화하고 있음

## 6.2 보안인텔리전스 세부 방책 (7/10)



### 5. 데이터 보안 방책

**정형 데이터 암호화•키관리•접근제어**

- 대부분의 사이버 공격의 목표는 데이터 위변조 및 탈취이며 이 데이터들은 DBMS를 통해 관리됨
- 중요데이터를 암호화하고 강력한 암호화 키관리 시스템을 도입
- 머신러닝 기술을 이용해 중요정보를 지능적으로 탐지하고, 보안 시스템을 우회하는 공격을 탐지/차단하는 기술로 진화 중

**DB 접근 제어 체계**

- 네트워크상에서는 기존 DB 접근제어 시스템을 통해 암호화 통신, 접속 및 사용에 대한 권한 제어 등의 기본적인 기능으로 정보유출을 방지
- 보안 강화를 위해 엔드포인트를 강력한 보안정책으로 제어하고 로그를 기록하여 감시하도록 엔드포인트컨트롤(DEC)를 도입해야 함
- DEC는 DB 접속 도구, DB 접근제어, 데이터 마스킹, 데이터 암호화 등의 기능을 제공함

**비정형 데이터 암호화•유출방지**

- 비정형 데이터 보호는 문서 암호화 기술인 DRM, 내부 정보 유출 방지 기술인 DLP이나 두 기술 모두 한계점이 존재함
- 사용중인 데이터, 저장된 데이터 등을 모두 보호할 수 있는 데이터 라이프사이클에 맞춘 데이터 보안 기술이 필요

**문서 중앙화**

- DRM을 이용한 문서 암호화는 운영체제 및 애플리케이션 종속성이 높아 효율성이 떨어지며 관리 업무를 증가시킴
- 또한 DLP는 오탐/미탐이 많고 우회 공격을 방어하지 못함
- 따라서 문서의 체계적인 관리와 불법 유통 방지, 다양한 협업 환경 지원과 투명한 버전 관리등의 효과를 제공하는 문서 중앙화 사용
- 문서의 악성코드 감염 방지와 랜섬웨어 피해 방지 효과도 제공



## 6.2 보안인텔리전스 세부 방책 (8/10)



### 6. 랜섬웨어 대응 방책

| | |
|---|---|
| 지능형 지속 공격방식 랜섬웨어 | • 엔드포인트, 네트워크, 웹, 이메일 등 공격이 진행될 수 있는 모든 지점을 모니터링 및 평판기반분석, 글로벌 인텔리젼스를 이용한 차단 필요 |
| 랜섬웨어 차단 기술 | • 웹 사이트 방문 전 유해 여부를 탐지하는 웹 보안게이트웨이(SWG)<br>• 유해사이트 차단 URL필터링 기술<br>• 유해사이트 접속 차단 기본 기능<br>• 머신러닝 기술을 이용한 프로세스 악성행위 학습 및 분석/차단<br>• 데이터 유실 대비를 위한 백업 |
| 차단 행위 | • 악성코드 배포로 의심스러운 사이트 및 외부 네트워크와의 통신이 감지되었을 경우<br>• 다량의 파일에 접근해 변경을 시도하는 경우<br>• 이메일에 첨부된 파일이 의심스러운 경우<br>• 메크로 기능 차단<br>• 새로운 실행 파일 유입 및 사용 시 평판 분석 및 샌드박스 내에서 조사 |

# 6.2 보안인텔리전스 세부 방책 (9/10)



## 7. 중요정보 유출 대응 방책

- 중요 정보를 안전하게 보호하기 위해서는 정보의 라이프사이클에 적합한 보안 정책을 마련해야 함
- 생산되는 모든 문서와 정보를 중앙 서버에 보관하고 조직의 정책에 따라 보호하는 문서 중앙화가 효율적인 데이터 관리/보호 방안이 떠오르고 있음

# 6.2 보안인텔리전스 세부 방책 (10/10)



## 8. 보안 관리 방책

### 통합로그관리•SIEM•네트워크포렌식

- 진행중인 공격과 이미 완료된 침해사고의 흔적을 찾아 격리하고, 피해 확산을 방지하며, 공격을 역추적하여 전체 공격 시나리오를 찾아 향후 유사 공격에 대비하기 위해 사용됨
- 네트워크와 시스템 내부에서 침해 흔적을 추적하는 포렌식과 네트워크 패킷 및 로그를 분석하는 모니터링 기술, 취약점 진단 및 모의해킹을 하며 공격 루트를 제거하는 기술이 포함됨

### 사용자 및 계정 행위 분석(UBA/UEBA)

- 로그관리 시스템은 탐지 패턴을 알고 있는 공격자들에 의해 무력화될 수 있음
- 임계치 및 시나리오 기반 UBA는 쉽게 우회할 수 있으나, 인공지능 접목 시 임계치 이하의 행위도 이상행위로 탐지 가능함
- UBA에서 탐지한 이벤트를 SIEM에서 다른 이벤트와 상관 분석하면 더 정확한 공격 탐지 기능을 얻을 수 있음

### 보안관리•보안관제•침해대응

- 침해 탐지 및 대응은 공격 시작에서 완료까지의 시간을 줄이는 것이 관건이며, 지능형 보안관리/관제시스템을 이용해 빠르게 대응해야 함
- 로그분석 뿐만 아니라 보호 자산을 식별하고 네트워크 장비 등 관련 기기에 대한 가시성 확보가 필요
- 공격 시나리오를 보안 정책에 적용하여 유사 공격 방지 및 빠른 대응을 진행해야 함

### 취약점 진단•모의해킹

- 취약점 진단과 모의해킹은 공격이 일어날 가능성을 낮추는 예방적 보안 전략으로 실제 공격자의 관점에서 테스트를 진행해야 함
- 테스트 결과 취약점이 발견되면 올바르게 조치해야 하며 다시 테스트를 진행하여 조치 확인을 해야 함
- 방대하고 복잡한 시스템에 대해서 자동화 도구를 사용하기도 함

# 6.3 공격 경로별 대응 방안 (1/4)

6 보안 인텔리전스

공격 경로 분석

## 내부자 행위와 정보체계 취약점에 따른 공격 경로 분류

| 경로•요인 | 내부•체계 취약점 | 공격 경로 |
|---|---|---|
| 감염경로 | 내부자 행위 X | • 네트워크를 통한 악성코드 전파 |
| | 내부자 행위 O | • 해킹된 웹 사이트 접속하여 드라이브 바이 다운로드 기법에 의해 악성코드 감염.<br>• 악성 액티브엑스 설치 및 업데이트.<br>• 감염파일 다운로드 및 실행.<br>• 감염된 첨부 파일 실행.<br>• 감염된 USB 연결하여 자동 실행. |
| 감염 요인 | 정보 체계 내 취약점 O | • 운영체제 보안 패치 적용 미흡.<br>• 응용 소프트웨어 보안 패치 미흡.<br>• 제로데이 공격<br>• 공유폴더와 관리자 패스워드 등 PC 보안 설정 취약<br>• 사용자 실수, 무지, 부주의 |
| | 정보 체계 내 취약점 X | • 사용자 실수, 무지, 부주의 |
| | 방영 채계 미흡 | • 백신 미설치<br>• 백신 업데이트 미흡<br>• 백신이 검출 못 하는 신종 악성코드 |

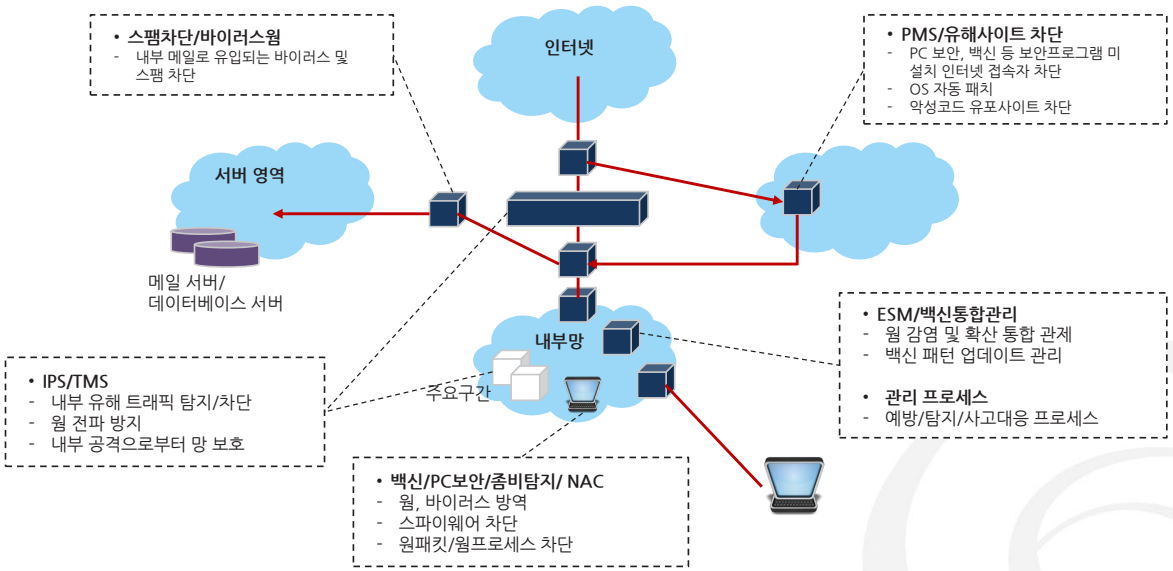


# 6.3 공격 경로별 대응 방안 (2/4)

6 보안 인텔리전스

공격 경로별 대응 방책

## 공격 경로별 대응 방책



# 6.3 공격 경로별 대응 방안 (3/4)



## 공격 경로별 대응 방책

### 정보 유출 경로별 대응 방안과 보안 솔루션

| 구분 | | 대응방안 | 내용 | 보안 솔루션 | | | | |
|---|---|---|---|---|---|---|---|---|
| 정보 획득 | 응용 | 권한 재정비 | • 정보 및 사용자에 대한 등급 세분화<br>• 최소권한의 원칙에 따라 업무적으로 반드시 필요한 정보만 접근 가능하도록 적용 | • ERM<br>• IAM | | | | • SBC |
| | | 서버 DRM 적용 | | • DRM | | | | |
| | DB | 서버 DRM 적용 | • PC로 다운로드된 파일에 대한 통제<br>• 암호화, 열람횟수/기간/출력 제한, 이력로깅을 통한 통제 | • 데이터베이스 보안 | | | | |
| 온라인 유출 | 사내에서 전송 | 유해사이트 차단 | • 웹하드, P2P등 정보유출 위협 사이트 접속 차단 | • 유해사이트 차단 | | | | |
| | | 사외전송 모니터링 | • 메일/게시판/메신저/웹하드/FTP 등 전송 내역 로깅 | • 외부전송모니터링/DLP | | | | |
| | 사외에서 전송 | VPN통제 | • VPN 계정 통제/인증 강화 및 접속 환경 가상화 | • SBC | | | | |
| | | 전송 모니터링/차단 | • 메일/게시판/블로그 등 외부 전송 내역 로깅<br>• P2P. 메신저 등 위험 프로그램 실행 차단 | • PC보안 | • NAC | • 출입통제<br>• 장비 반출입 통제 | • PC DRM | |
| | | 반출 통제 | • 노트북 등 장비 반출 통제 | | | | | |
| 오프라인 유출 | 외부 저장매체 | 매체 차단 및 로깅 | • USB/FDD/CD-RW 등 외부저장매체 차단 및 로깅 | • PC보안<br>• DLP<br>• 보안 USB | | | | |
| | 내장 HDD | HDD 암호화 및 봉인 | • HDD 전체 암호화 또는 봉인 스티커 부착 | • HDD 암호화 | | | | |
| | 출력물 | 워터마킹 및 로깅 | • 출력 시 출력자 정보 강제 삽입 및 출력 이력 로깅 | • 출력 보안<br>• OA기기 보안 | | | | |
| 통합 분석 관리 | | 증거 수집과 분석 | • 사고 조사, 법적 증거 확보 | • 디지털 포렌식 | | | | |
| | | 통합보안 모니터링 | • 통합분석, 정보유출징후 탐지, 블랙리스트 관리 등 | • 통합정보유출모니터링 시스템 | | | | |



# 6.3 공격 경로별 대응 방안 (4/4)



## MITRE 모델

- MITRE는 2014년도에 사이버 위협 정보 전송 규격인 사이버 위협 정보 전송 규격(Trusted Automated eXchange of Indicator Information, TAXII)과 사이버 위협 정보 표현 규격(The Structured Threat Information eXpression, STIX)를 발표함
- 사이버 위협 정보 표현 규격에는 공격 기법 관련 킬체인에 대한 전술, 기술, 절차에 식별자를 부여

### MITRE PRE-ATT&CK 모델

- PRE-ATT&CK은 공격자가 들어오기 전에 공격을 막는 능력을 제공
- 7단계의 사이버 킬체인의 앞 4단계에서 파생된 17개의 전술 카테고리가 있음
- 방어하는 조직에 다음과 같은 질문에 대답할 수 있는 능력 제공
  - 공격자들이 공격 대상을 목표로 삼고 있다는 신호의 유무
  - 공격자가 일반적으로 사용한 기법
  - 공격 발생 전 공격자를 볼 수 있는 추가적 정보를 얻기 위한 사이버 위협 인텔리전스 데이터 수집 및 분석의 우선순위 결정

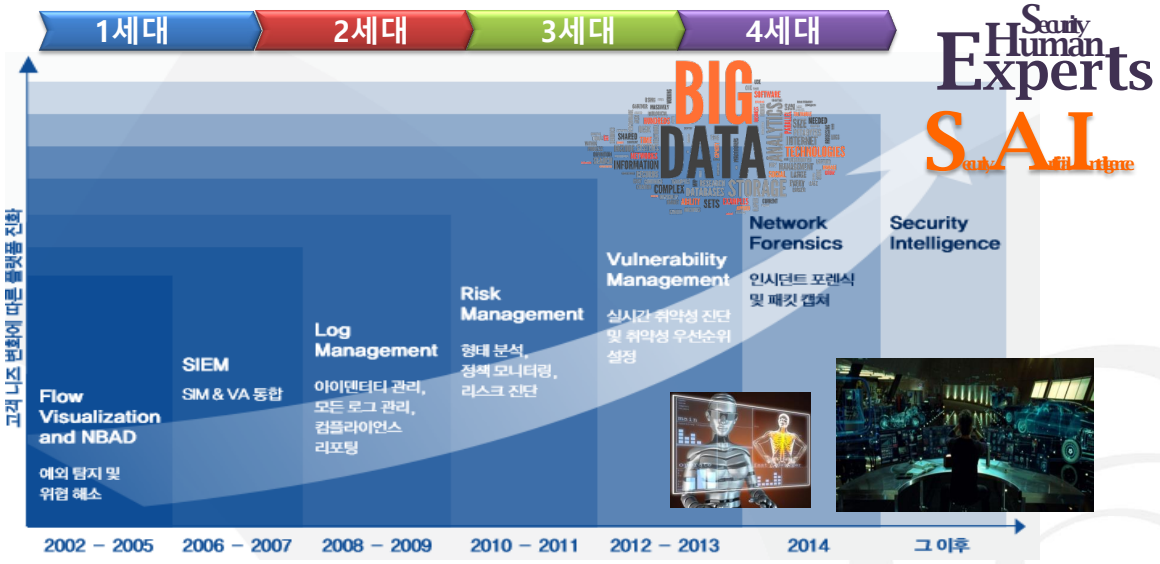
### MITRE ATT&CK 모델

- PRE-ATT&CK은 알려진 보안 위협에 대해 이해하고 방어에 대한 수준을 높이는데 유용
- 공격자가 목표를 실행하기 위해 사용하는 공격 전술, 기술 및 절차를 상세히 설명함으로써 네트워크 방어 우선순위 지정에 도움
- 방어 조직및 의사결정권자는 특정 공격 기술의 체크리스트 뿐만 아니라 다양한 용도로 ATT&CK에서 위협 정보를 사용할 수 있음
- 공개적으로 알려진 샘플들을 이용한 예측에 기반

## 6.4 보안인텔리전스 – SHIP (시큐리티 휴먼 인텔리전스 플랫폼)

6 보안 인텔리전스

세계 최고의 전문인력(Security Human Expert)과 4세대 혁명을 이끄는 보안에 최적화된 인공지능 솔루션(Security Artificial Intelligence)을 통합한 보안 인텔리전스 플랫폼(Security Human Intelligence Platform)을 연구합니다.




Blockchain Security SECURITY



## 6.4 보안인텔리전스 – IOMS 컴플라인언스 관리

6 보안 인텔리전스

**업무 연속성**

사용자의 OS, 웹브라우저에 상관없이 ISMS / ISO27001 / PIMS 를 통합관리 할 수 있으며 위험관리에서 인증심사 문서의 자동생성 까지 모든 기능을 전자 문서로 제공하여 업무 연속성을 제공합니다.

**ISMS-P 와 FISMS 로의 확장성**

ISMS 와 PIMS 가 결합된 ISMS-P 로 확장이 가능함과 동시에 FISMS 의 운영관리 시스템으로 즉시 적용이 가능. (해외 ISO27001, PCI-DSS 가능)

**취약점 점검의 무료 서비스**

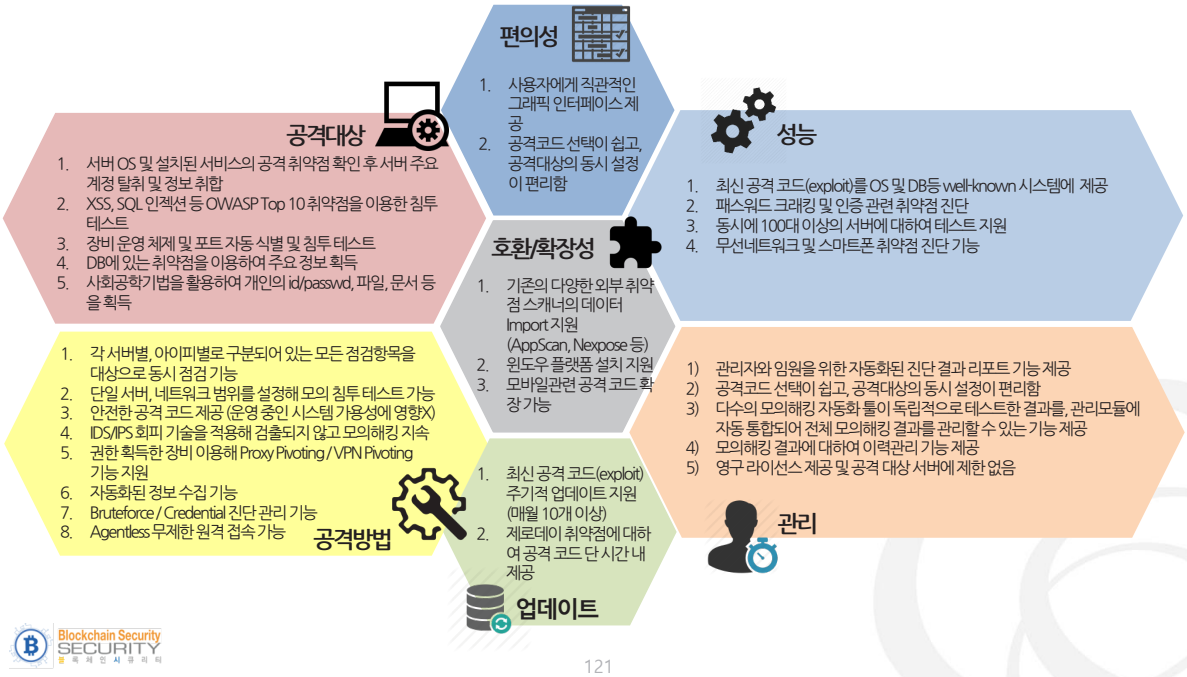
IOMS 를 구매하는 모든 고객에게 Agent / Agentless 방식의 기반의 주요정보 통신기반시설 취약점점검 기능을 무료로 서비스 실시
CCE, CVE, CWE 등의 소프트웨어 방식 지원, HW 기반 악성코드 탐지 지원 (옵션)

Blockchain Security SECURITY

## 6.4 보안인텔리전스 – Rapid7 모의해킹 및 취약성 점검 툴

6 보안 인텔리전스

외부 공격자와 같은 공격 방법을 사용하여 조직의 다양한 네트워크 방어체계에 대한 통합 모의해킹 검증 테스트를 수행합니다.






## 6.4 보안인텔리전스 – 하드웨어 기반 악성코드 탐지

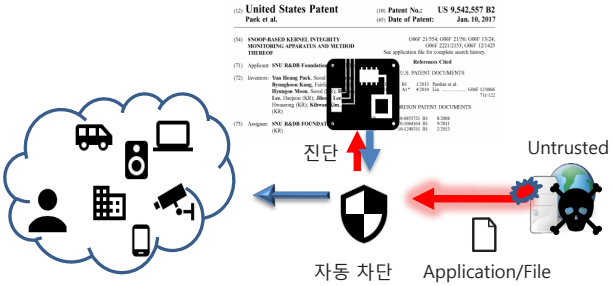
6 보안 인텔리전스

**하드웨어 기반 악성코드(APT, 랜섬웨어, 멀웨어 등) 탐지 하는 기술로 세계 유일의 특허 보유 기술 적용, 현존하는 최고의 탐지기술 (삼성 스마트 TV 적용 등 최다 적용사례 보유)**

**HW 기반 악성코드 (APT, 멀웨어, 랜섬웨어 류) 실시간 활동 대비**

- 하나의 network를 이루는 시스템의 보호를 위해 network 내의 단말로 유입되는 새로운 application/file의 진단이 필수적
- 현재는 대부분 SW기반의 sandbox 기술을 활용하여 진단
- ➔ 앞서 언급한 바와 같이 malware가 진단을 회피 가능
- 최신 malware의 분석이 가능한 HW기반 진단 도구가 sandbox의 역할을 대체해야 함
- 특히 Smart city / Smart home을 이루는 주요 기기들이 ARM 기반의 embedded device이기 때문에 ARM기반 환경의 진단 도구가 필요

**특허 번호 - US09542557 기반**




**[ 진단 특징 ]**

**필요성**

**Evasive malware의 등장으로 기존의 SW 기반 진단 무력화**

SW 기반 진단 도구에 반드시 나타날 수 밖에 없는 특징(fingerprint)을 감지하여 회피 ➔ Fingerprint를 남기지 않는 진단 도구 필요
SW 기반 구현에서는 그 fingerprint를 숨기는 것에 한계가 존재 ➔ HW기반 접근이 필요

**진단방식**

**Malware에서 확인 가능한 zero- Fingerprint 진단**

최신 Malware 진단을 위해 필요한 동적 정보 (dynamic behavior) 추출 HW를 활용
- Data access를 확인할 수 있는 Snooper 기술
- Code 수행 흐름을 확인할 수 있는 Branch tracing 기술 (서울대 보유)

## 6.4 보안인텔리전스 – 인프런 (프리미엄 정보 제공, 교육)

6 보안 인텔리전스

온/오프 라인의 교육, 실무 연구, 프리미엄 컨설팅 등을 다년간의 경험을 통한 다각적 정보 제공 서비스를 제공합니다.

**최신 이슈 업데이트**

웹 해킹, 악성코드 분석, 모바일 보안 등 사람과 기술에 대한 보안 정보를 통합하여 중요도 순으로 배치되며, 여러 보안 관련 기관 정보를 모두 확인할 필요가 없도록 최신 이슈 정보를 제공합니다.

**연구협력을 통한 최신보안기술 연구**

지식과 정보의 흐름이 안팎으로 열린 시스템을 구축하고 학제간 공동연구를 통해 지식이 개발, 선순환되는 지식 커뮤니티를 만들어가고 있습니다.

**관련 추천 기술 및 컨설팅**

오렌지 리포트 내 정보에 관한 추가적인 내용 및 기술 문의, 각 기업에서 어려움을 겪고 있는 내용에 대한 컨설팅까지 문의 가능합니다.

**실무 연구**

보안 컨설팅을 지속적으로 제공하고 있으므로 기업에서 최근 고민하는 문제점을 파악하고 있으며 종합적인 시각으로 폭넓게 진단하여 눈높이에 맞는 실용적인 해결방안을 마련합니다.

**경영층 보고 및 발표에 바로 활용 가능한 형식**

경영층에 보고할 자료를 별도로 작성할 필요가 없도록 경영층에게 바로 보고 및 발표할 수 있는 형식으로 작성됩니다.

**글로벌 연구**

보안은 글로벌 동향을 잘 아는 것이 중요합니다. 급변하는 글로벌 IT산업과 기술환경을 체계적으로 분석,연구하여 기업경영 및 보안정책에 대한 가이드라인을 제시합니다.

Blockchain Security SECURITY



## 6.5 보안인텔리전스 기대효과

6 보안 인텔리전스

**기대효과**

- 사이버 킬체인을 통해 사이버 공격에 대응하기 위한 효과적인 방어 전략 구축 가능
- 사이버 국방 환경의 보안에 적용할 수 있는 체계적인 기반 마련 가능

| | |
|---|---|
| 분석 틀 제공 | • 공격자의 침투 방식에 대한 정보를 조사하고 획득함으로써 사후 공격 예방 및 피해 최소화를 위한 분석 틀 제공 |
| 공격 방지 | • 공격자가 목적 달성을 하기 전에 공격 체인을 끊거나 공격을 지연시킴으로써 공격자의 공격을 위한 자원을 빠른 시간안에 소진 및 무력화 가능 |
| 선제적 대응 | • 사이버 국방 차원에서 사이버 공격의 각 단계에 대해 선제적이고 체계적인 대응을 가능하게 하여 사이버 국방 체계와 중요 자원의 피해를 사전에 예방할 수 있고 피해의 신속한 복구 가능 |
| 다양한 활용 | • 국방 사이버 방어 체계 구축을 위해 필요한 새로운 기술, 체계, 도구, 절차, 전술 등을 식별하고 합리적인 투자 및 활용 가능 |

Blockchain Security SECURITY

Blockchain Security SECURITY 블 록 체 인 시 큐 리 티

# 감사합니다.

주소 : 서울대학교 컴퓨터공학 연구소 암호화연구실 (블록체인시큐리티)
블록체인시큐리티 in 싱가폴 Founder
영남이공대학교 사이버보안학과 기태현 겸임 교수
: 010-8435-7979, skykey@mite.co.com

The 24th Network Security Conference -Korea

# 바이너리 코드에 기반한 오픈소스 정보 및 관련된 취약점 분석 기술

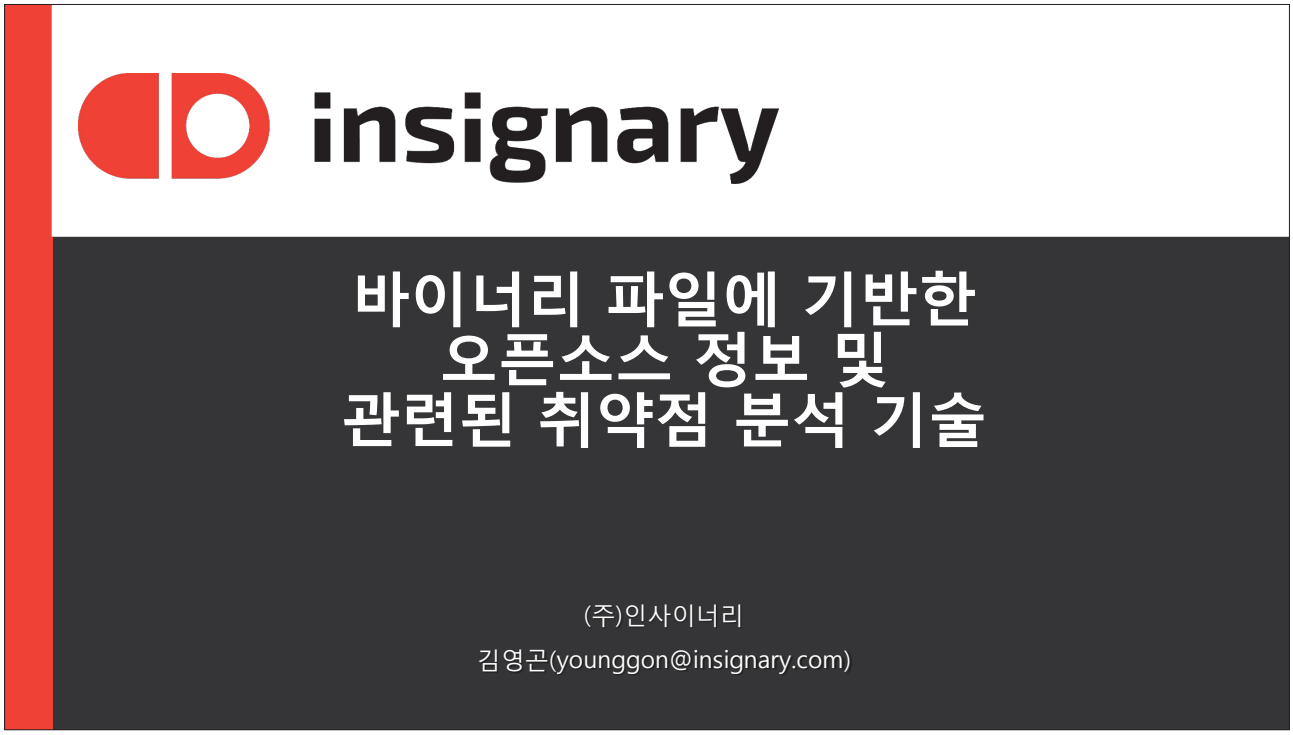
**김영곤** 인사이너리 팀장

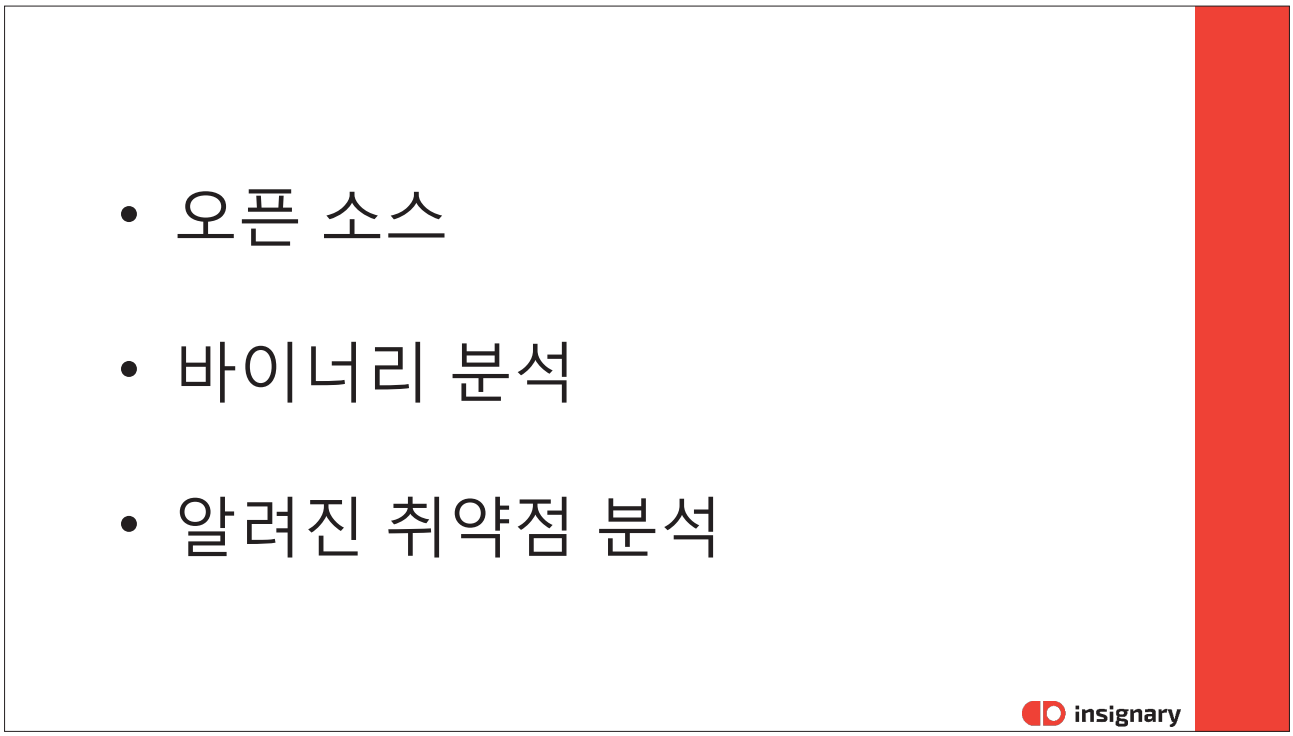
### 학력 및 경력사항

현 (주)인사이너리 개발팀장
전 (주)퓨처시스템 개발이사
전 (주)윈스 개발팀장
전 (주)안랩 책임연구원
울산대학교 공학박사

### 강연요약

많은 상용 소프트웨어 개발사 및 판매 소프트웨어에서 다양한 오픈소스를 사용하고 있습니다. 오픈소스 사용이 증가함에 따라 오픈소스 취약점도 증가하는 추세에 있으며, 이를 정확히 파악하고 취약점에 대응하는 것이 점점 중요해 지고 있습니다. 본 강연에서는 소프트웨어 최종 산출물인 바이너리에 대해 실제 사용한 오픈소스 정보와 오픈소스에 존재하는 취약점을 분석하는 기술을 제시합니다. 이를 위해 fingerprint 기반으로 사용한 오픈소스를 분석하는 기술과 실제 사용한 오픈소스 코드에 존재하는 취약점을 분석하는 기술을 설명합니다.


insignary
바이너리 파일에 기반한
오픈소스 정보 및
관련된 취약점 분석 기술
(주)인사이너리
김영곤(younggon@insignary.com)

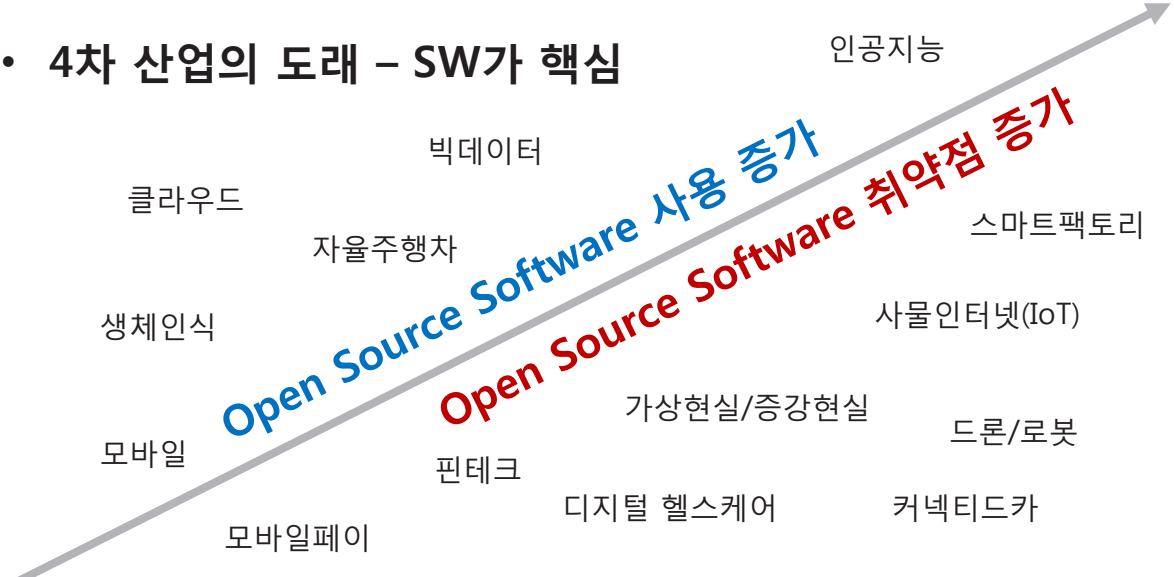

• 오픈 소스
• 바이너리 분석
• 알려진 취약점 분석
insignary

# 오픈소스

Copyright © 2017 Insignary Inc. Not for redistribution without written permission. insignary

## 컴퓨팅 환경의 변화

- **4차 산업의 도래 – SW가 핵심**

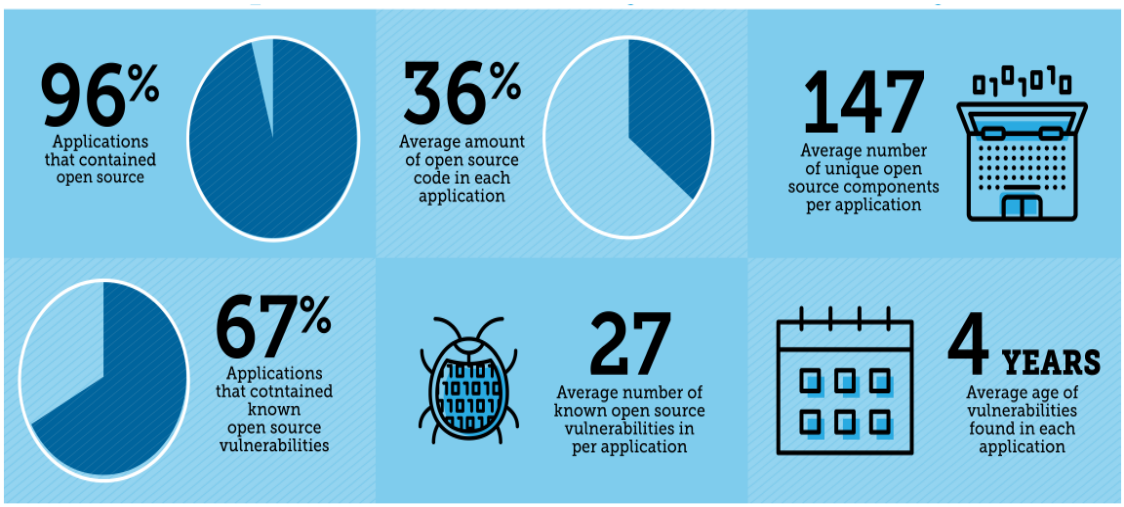



Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary

# 오픈 소스

Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary


# 2017년 오픈소스 통계

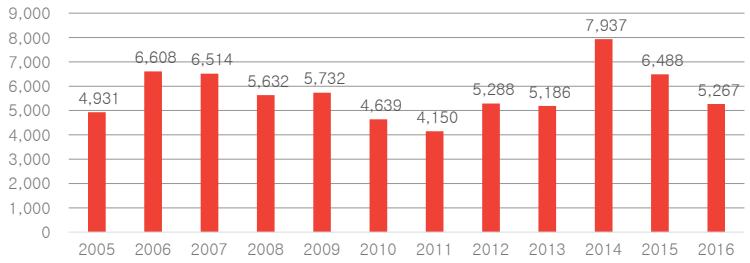



*참조: BLACKDUCK FLIGHT 2017*
*Software Security Assurance for DevOps*

Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary

# 오픈 소스 주요 보안 취약점

| | Heartbleed | Shellshock | Freak | Ghost | DROWN | SambaCry | Apache Structs |
|---|---|---|---|---|---|---|---|
| 발견 시점 | 2014 | 2014 | 2015 | 2015 | 2016 | 2017 | 2017 |
| 배포 시점 | 2011 | 1989 | 1990s | 2000 | 1990s | 2010 | 2007 |
| Component | OpenSSL | Bash | OpenSSL | GNU C Library Library | OpenSSL | SAMBA | Apache Struts |



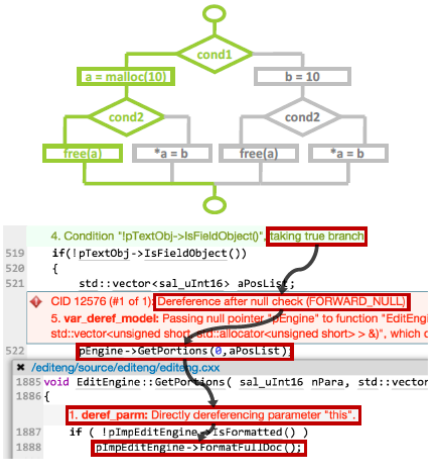

참조: CVE Trend (http://www.cve.mitre.org)

- 불행하게도, SAST/DAST의 자동화된 툴보다 수동으로 Code Review를 하는 보안 연구자들의 의해 발견됨
- 오픈소스에 대한 가시성 부족으로 인해 모르는 상태에서 공격받을 가능성이 많고, 보안 대책을 세우는 것은 더 어려움

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary


# SAST – Static Analysis

- Static Code Analysis for Security
- Source code 파싱을 통해 문제점 분석
- 소스 파일과 코드에 존재하는 취약점 분석

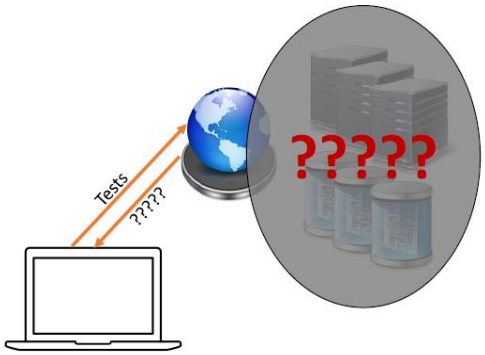



- Coding phase
- Build verification

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary

# DAST – Dynamic Analysis

- Web Application Scanner
- 동작중인 어플리케이션 테스트를 통한 분석
- 악의적인 사용자를 시뮬레이션하여 취약점 분석

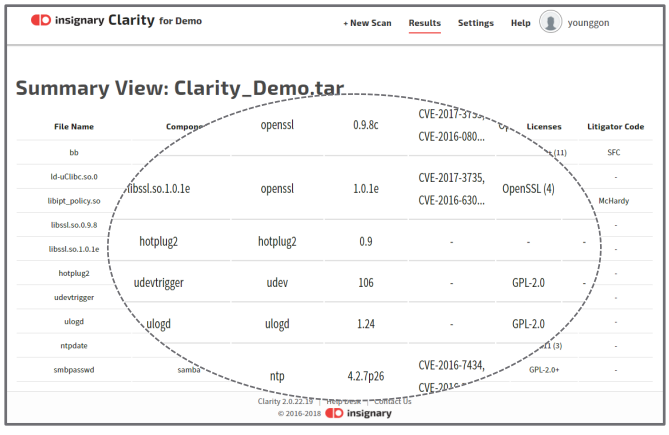



- QA testing
- Pre-production testing

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary


# SCA – Software Composition Analysis

- Open Source Library Scanning
- 어플리케이션 내에 존재하는 오픈소스 컴포넌트 분석
- 오픈소스 라이선스 위반 여부 분석
- 오픈소스 취약점 분석

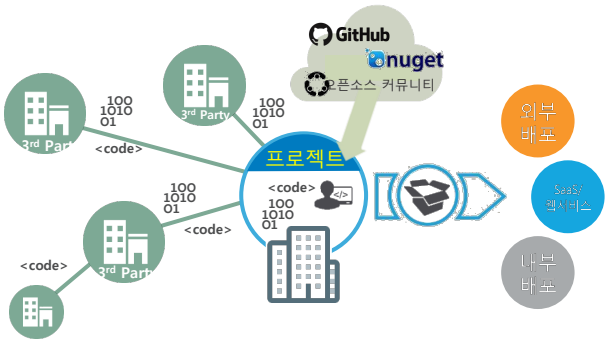



- First commit & build
- Continuous monitoring

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary

# 3Rd Party 코드와 오픈 소스

## 기업은 3rd Party의 코드에 대해서도 보안 및 라이선스에 대한 책임이 있음




- 많은 기업들이 비용 절감 및 효율성 향상을 위해 3rd Party 코드를 이용
- 3rd Party 코드에는 오픈 소스가 포함되는 경우가 많음
- 소스 코드 없이 **바이너리**만 전달되는 경우도 많음
  - 어떤 오픈 소스가 사용되었는지 알 수 없음
  - 그 당시에는 문제가 없더라도 나중에 보안 취약점이 발견될 경우 보안 대책에 큰 문제 발생

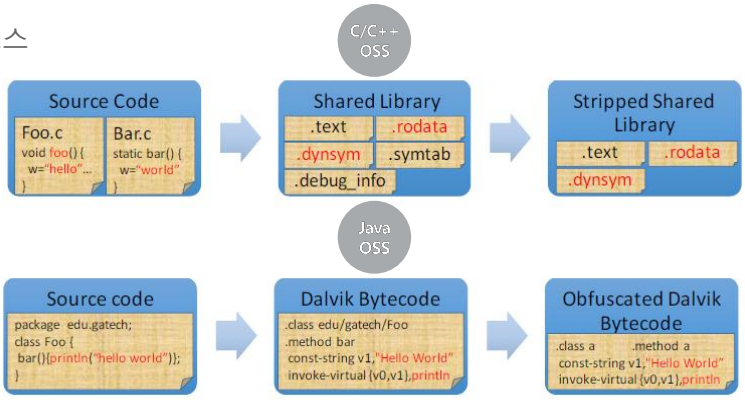
Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary


# 바이너리 분석

Copyright © 2017 Insignary Inc. Not for redistribution without written permission. insignary

# 바이너리 분석

- 바이너리에 대해 사용한 오픈소스 정보 분석
- 사용한 오픈소스 패키지 인식
- 정확한 오픈소스 버전 인식

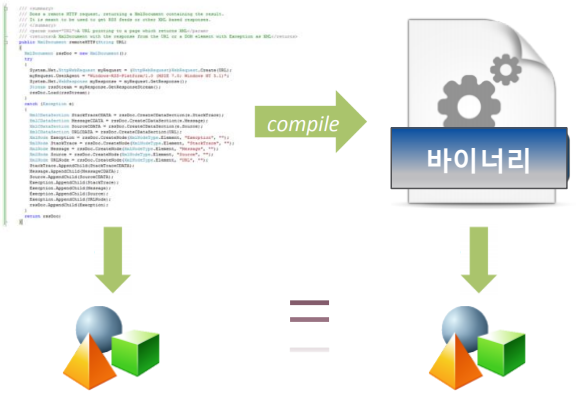



- 개발사는 소프트웨어를 바이너리 형태로 제공
- 회사간(supply chain) 소프트웨어 전달은 바이너리 형태로 제공

Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary


# 바이너리 분석

- 컴파일 후에도 변화하지 않고 유지되는 고유 식별자 정보 추출
- 고유 식별자 정보에 따라 사용한 오픈 소스 정보 분석
- 오픈 소스에 존재하는 알려진 취약점 분석

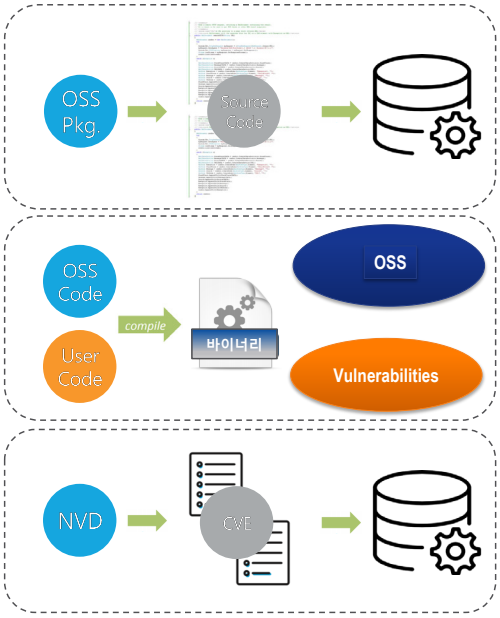



- 식별자를 포함하는 컴포넌트 추출
- 유일한 컴포넌트 정보로 대상 OSS 판별

Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary

# 바이너리 분석

- 오픈소스 데이타베이스
- 바이너리 분석 엔진
- 알려진 취약점 분석




- 사용한 소스파일 기반 라이선스
- 사용한 소스파일 기반 취약점

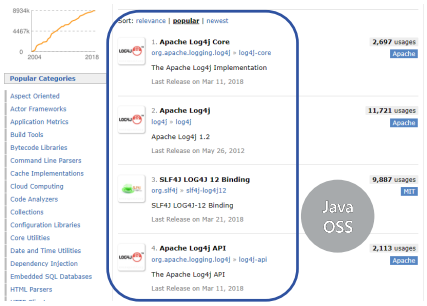
Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary

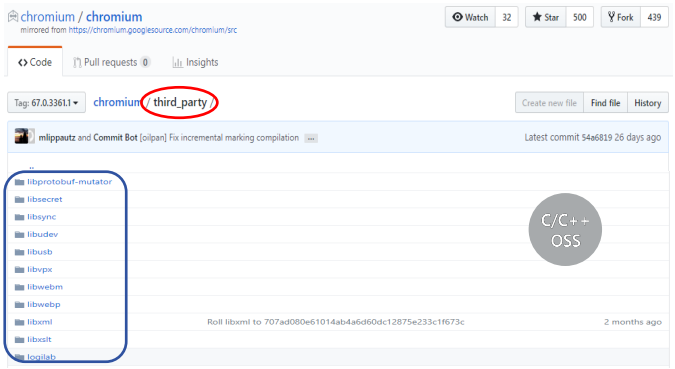

# 코드클론 분석

Copyright © 2017 Insignary Inc. Not for redistribution without written permission. insignary

# 코드 클론

- 많은 오픈소스에서 다른 오픈소스를 복사해서 사용하고 있음
- Java 관련 오픈소스의 경우 코드 클론 이슈가 심각하게 존재함

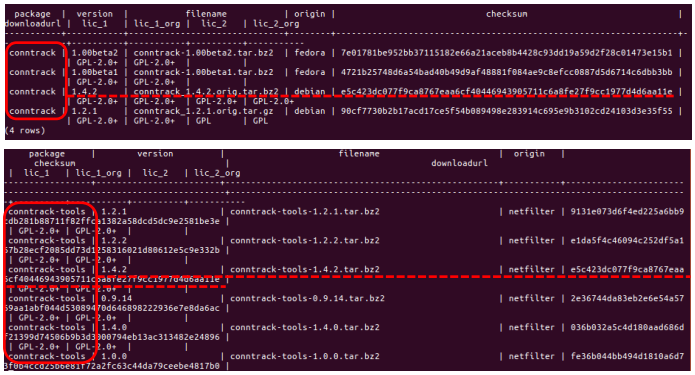



Copyright © 2018 Insignary Inc. Not for redistribution without written permission.


# 코드 클론 분석

- Rename Code Clone
- 특정 버전부터 컴포넌트 이름이 변경되어 유지되는 컴포넌트
- 컴포넌트 이름을 동일하게 처리



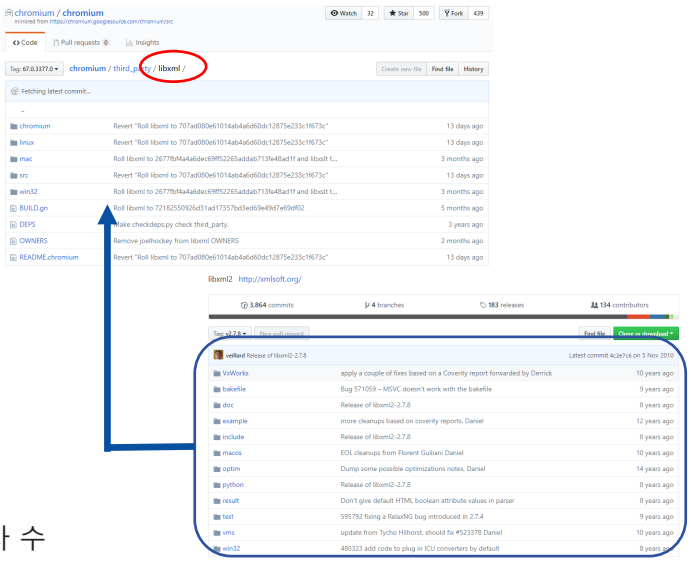




Copyright © 2018 Insignary Inc. Not for redistribution without written permission.

# 코드 클론 분석

- Internal Code Clone
- 한 컴포넌트가 다른 오픈소스 컴포넌트 전체를 포함하는 경우
- 원본 컴포넌트 판단 필요

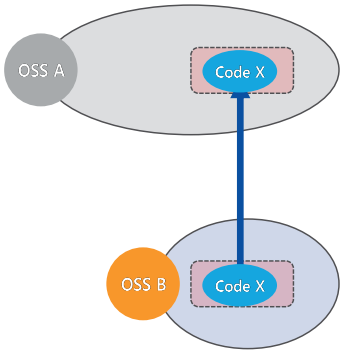



- 식별자를 포함하는 컴포넌트의 소스파일 정보에 기반한 클론 탐지
- 컴포넌트별 파일 버전 수, 고유식별자 수

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.


# 코드 클론 분석

- Partial Code Clone
- 한 컴포넌트가 다른 오픈소스 컴포넌트 일부 파일을 포함하는 경우
- 원본 컴포넌트 또는 현재 컴포넌트 판단 필요




- 식별자를 포함하는 컴포넌트의 소스파일 정보에 기반한 파일 탐지

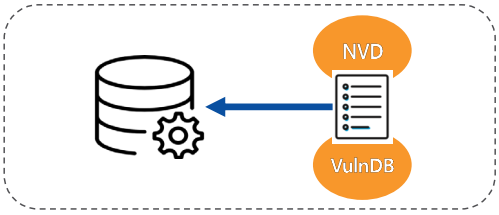
Copyright © 2018 Insignary Inc. Not for redistribution without written permission.

# 알려진 취약점 분석

Copyright © 2017 Insignary Inc. Not for redistribution without written permission. insignary

## 취약점 데이타베이스

- 알려진 취약점 DB 활용
- 취약점이 존재하는 소스파일정보 또는 취약점이 존재하는 오픈소스 컴포넌트 정보 DB화
- 실제 사용한 오픈소스 파일에 존재하는 알려진 취약점 분석




| cve | checksum |
|---|---|
| CVE-2000-1210 | cacdde95b79568dcacd215dd46a6e8607514b5b56255a34ec68fa4413f05025e |
| CVE-2000-1254 | 6bfbeb9e752d611901e6420b0a5497a cf47cbf30f38849a70ac8e983e7c217b |
| CVE-2001-1593 | efc767689ccbad250297f6792bd34a6 a95801f14080c046e1ea46c178748493 |
| CVE-2001-1593 | 06d83c85b7c48bc8511bc0fa6eea1e8 b227a6f63bdf32a4e65f5a7f4b967ad0 |
| CVE-2001-1593 | 11022ecd6cb3a88e1ecc176ca710adf a80504202f0d3ebc349dc6fa8c9cd8c3 |
| CVE-2001-1593 | 79803d81a6ac8e367a8408fa736dff5 12bf488bd14c42d4edd0e218ec289c85 |
| CVE-2002-0400 | 76dca6b76c6444092379335ec9a2225 0b9d1283c70b9b2cdb481f022be3d800 |
| CVE-2002-0400 | 886991f89e35b3eeecfb1dcac29df91 7791886f3cb3302fea2a737657126825 |
| CVE-2002-0400 | 4e6c2169565e1908ad09406ff9d219f 2837b4e3daa7ab891b2e170757195409 |
| CVE-2002-0429 | e3c5390d3a12f8dcc701d539aad8411 45a18a151b4934d5b1ac7af79b87ecee |

| cve | package | version |
|---|---|---|
| CVE-1999-0002 | linux | 2.0 |
| CVE-1999-0002 | linux | 2.1 |
| CVE-1999-0002 | linux | 3.0.3 |
| CVE-1999-0002 | linux | 4.0 |
| CVE-1999-0002 | linux | 4.1 |
| CVE-1999-0002 | linux | 4.2 |
| CVE-1999-0002 | linux | 5.0 |
| CVE-1999-0002 | linux | 5.1 |
| CVE-1999-0004 | pine | 4.02 |
| CVE-1999-0005 | imap | 10.234 |

| package | version | filename |
|---|---|---|
| tomcat | 3.0 | source.jsp |
| tomcat | 3.1 | source.jsp |
| tomcat | 3.1.1 | source.jsp |
| tomcat | 3.2 | source.jsp |
| tomcat | 3.2.1 | source.jsp |
| tomcat | 3.2.3 | source.jsp |
| tomcat | 3.2.4 | source.jsp |
| tomcat | 3.3.1 | source.jsp |
| tomcat | 3.3.1a | source.jsp |
| tomcat | 3.3a | source.jsp |
| tomcat | 4.0 | source.jsp |

Copyright © 2018 Insignary Inc. Not for redistribution without written permission. insignary

# 취약점 분석

- 사용한 오픈소스 컴포넌트 분석

## Summary View: libcrypto.so.1.0.2g

| File Name | Component | Component Version | Security Risks | Licenses | Litigator Code |
|---|---|---|---|---|---|
| libcrypto.so.1.0.2g | openssl | 1.0.2g | CVE-2017-3738, CVE-2017-373... | Others (5) | Patent module |

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.


# 취약점 분석

- 사용한 오픈소스 버전 및 취약점 분석

## Detail View: libcrypto.so.1.0.2g

Overview | Unique Matches | Other Matches | No Matches | ELF Analysis

| | |
|---|---|
| Name | libcrypto.so.1.0.2g |
| Path | - |
| Size | 2720392 bytes |
| File type | ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=f3e5e7f0b05269b4adf1e12be069f1e44483165a, not stripped |
| SHA 256 | 7934cc224e02c054fac4281d01277769e8da2050002804e7ff9e3cdc512cc050 |
| Declared shared libraries | libdl.so.2, libc.so.6 |
| Tags | binary, ranking, toplevel, dynamic, elf, elfdynamic, knownlitigator, architecture, libs, identifier |

### Matched Components by Score (Top 10)

### Matched Components Detail

| Rank | Component | Version | Scores | Unique Matches | Other Matches | Security Risks | Licenses |
|---|---|---|---|---|---|---|---|
| 1 | openssl | 1.0.2g | 65407 | 3345 | - | CVE-2017-3738<br>CVE-2017-3737<br>CVE-2016-8610<br>CVE-2016-2182<br>CVE-2016-2181<br>CVE-2016-2180<br>CVE-2016-2179<br>CVE-2016-2178<br>CVE-2016-2176<br>CVE-2016-2107 | Others (5) |

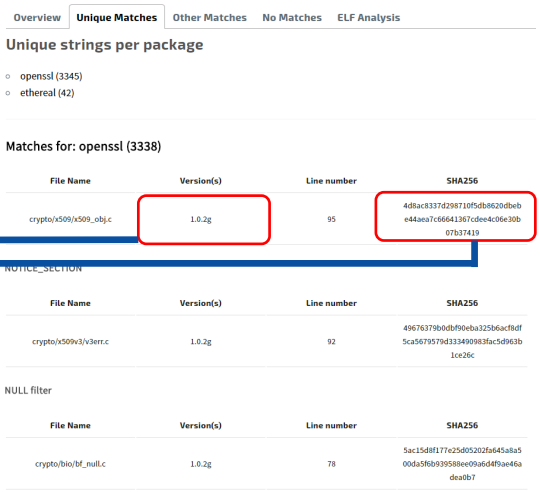
Copyright © 2018 Insignary Inc. Not for redistribution without written permission.

# 취약점 분석

- 사용한 오픈소스 파일 분석

```
    cve      | package | version
-------------+---------+---------
CVE-2016-2107 | openssl | 1.0.2g
CVE-2016-2179 | openssl | 1.0.2g
CVE-2016-2181 | openssl | 1.0.2g
CVE-2016-2181 | openssl | 1.0.2g
CVE-2016-8610 | openssl | 1.0.2g
CVE-2017-3738 | openssl | 1.0.2g
(6 rows)
```

```
    cve      |                             checksum
-------------+------------------------------------------------------------------
CVE-2016-2176 | 4d8ac8337d298710f5db8620dbebe44aea7c66641367cdee4c06e30b07b37419
(1 row)
```




Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary


# 오픈소스 보안대책

- 조직 내에 사용 중인 오픈소스 현황 파악이 중요함
- 최종 전달 형태인 바이너리 형태에 대한 검증이 필요함
- 새로운 취약점에 대한 발견 못지않게 이미 알려진 취약점을 정확히 파악하는 것이 중요함

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary

# 오픈소스 보안대책의 변화 시작

| 지금까지는... | 이제부터는... |
| --- | --- |
| • 오픈 소스 보안도 기술적인 문제이다 | • 기술적인 대응도 필요하지만 보안 관리와 정책, 프로세스가 우선 |
| • 오픈 소스 보안도 기존 강력한 정보보호용 도구나 솔루션을 사용하면 해결된다 | • 사건 사후대응에는 필요함<br>• 사전 대응에는 오픈 소스 가시성이 필수 |
| • 오픈 소스 코드 검증만으로 충분하다 | • 실제 배포되는 바이너리 검증이 필수 |
| • 정보보호는 보안 담당자의 업무이기 때문에 오픈 소스 보안도 마찬가지이다 | • 오픈 소스 전담 담당팀과 담당자가 필요 |
| • 바이너리 코드만으로 무엇을 알 수 있겠어? | • 바이너리만으로도 모든 것을 알 수 있음 |
| • 나는 개발자인데… | • 오픈 소스 보안은 개발자가 보안 담당자라는 것을 인식해야 함 |

Copyright © 2018 Insignary Inc. Not for redistribution without written permission.
insignary
27

# 바이너리 파일에 기반한 오픈소스 정보 및 관련된 취약점 분석 기술

# Q&A

㈜인사이너리
김영곤(younggon@insignary.com)

insignary

# 국내 대상 위협 인텔리전스

**곽경주** 금융보안원 과장

### 학력 및 경력사항

성균관대학교 컴퓨터공학과 학사 (~ 2011.2)
성균관대학교 전자전기컴퓨터공학과 석사 (~ 2013.2)
금융결제원 침해대응부 (~ 2015)
금융보안원 침해대응부 (~ 현재)
경찰청 사이버 범죄 전문가 그룹 자문위원
사이버치안대상 행정자치부 장관상 수상 (2016)

### 강연요약

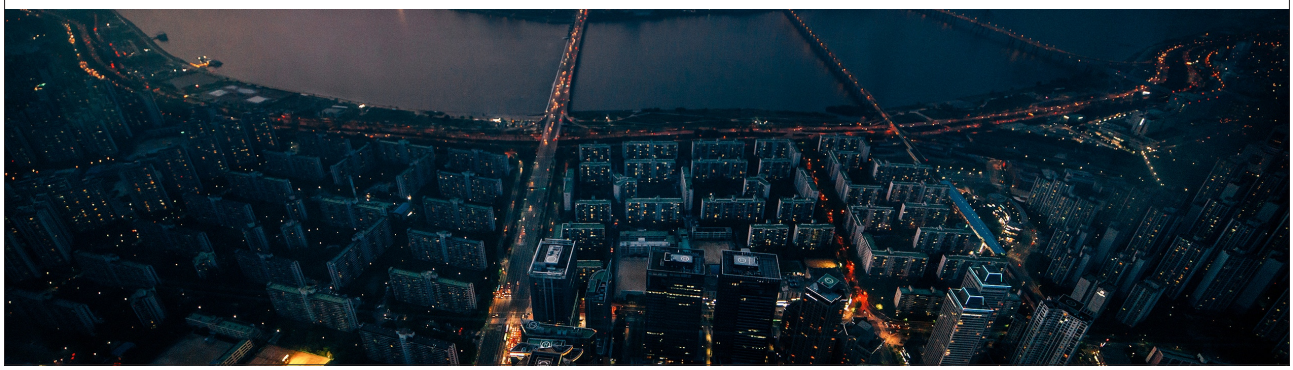
국내는 오래전부터 다수의 위협 그룹으로부터 수많은 공격을 받고 있으며 신변종 악성코드가 끊임없이 제작되어 유포되고 있고 이를 통해 주요 기관 및 기업들에 대한 침투를 시도하고 있다. 2017년 이후, 많은 그룹들이 금전적 이득을 목적으로 하는 공격에 집중하고 있는 양상을 보이고 있다.

본 발표에서는 국내를 대상으로 지속적인 공격을 수행하고 있는 다수의 위협 그룹과 각 그룹별 특징을 살펴보고자 한다. 이를 위해 최근 공격에 사용된 악성코드들간의 유사도 분석과 TTP (Tactics Techniques and Procedures) 프로파일링 결과를 공유하고 해당 그룹들에 의해 발생한 사고들의 원인과 각 공격 방식에 대한 분석 결과를 통해 향후 유사 공격에 대한 대응 전략을 수립하는데 도움을 주고자 한다.

# 국내 대상 위협 인텔리전스

## Landscape of Threats in South Korea

곽경주 (kjkwak@fsec.or.kr)
금융보안원 침해위협분석팀



## 발표자 소개

곽경주 (郭炅周)
과장, 금융보안원 침해위협분석팀

금융결제원 침해사고대응팀 (~2015.4)
금융보안원 침해위협분석팀 (현재)

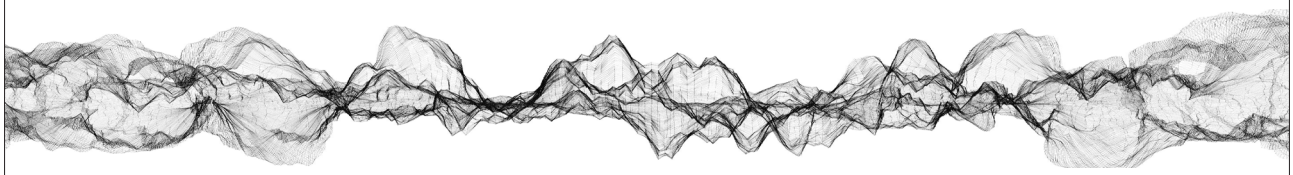
경찰청 사이버 위협 전문가 그룹 자문위원
사이버치안대상 행정자치부 장관상
BoB 디지털포렌식 트랙 멘토

**주요 발표**

International Symposium on Cyber Crime Response (2014, 2017), K-ISI, CIISCON, WhitehatContest, PACSEC, HITCON, HACKCON, KimChiCon, Kaspersky Security Analyst Summit, Blackhat Europe, Blackhat Asia

CONTENTS

01. 배경지식
02. 위협그룹별 사고 사례
03. 위협 인텔리전스 데이터
04. 결론



# 배경지식

# 용어 정의

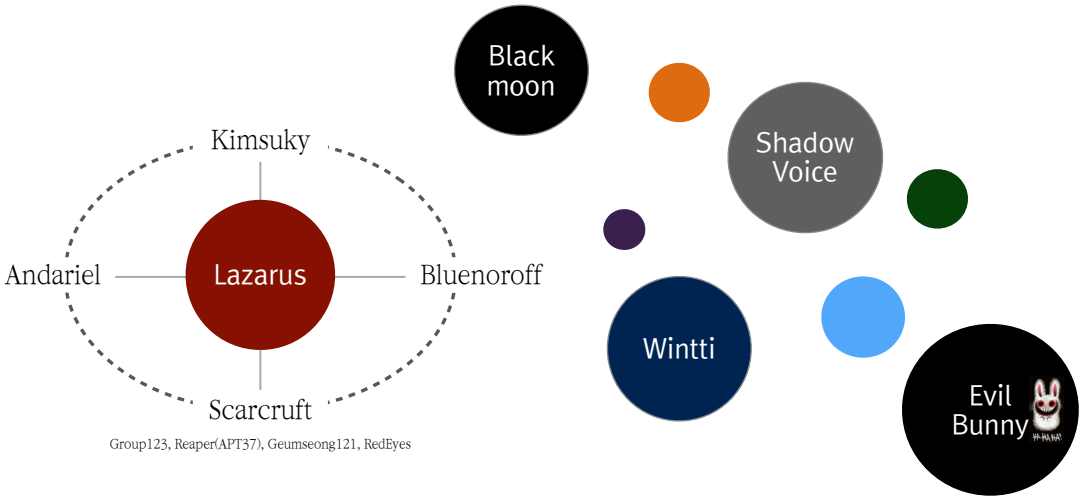
## 용어 정의

http://stixproject.github.io/documentation/idioms/campaign-v-actors/

Threat Actor
Campaign
Incident or Operation
TTP (Tactics Techniques and Procedures)
Confidence

# 국내 대상 위협그룹

## 국내 대상 위협 그룹




Group123, Reaper(APT37), Geumseong121, RedEyes

## 국내 대상 위협 그룹

| | Lazarus | Bluenoroff | Scarcruft & Kimsuky | Andariel | Wintti | Evil Bunny (랜섬웨어) |
|---|---|---|---|---|---|---|
| Target | 정부, 금융, 방송 | 전세계 금융산업 암호화폐 거래소 금융 | 탈북자, 통일 관련 연구원 및 정부기관 | 국내 금융, 방산, 민간기업, 보안 솔루션 업체, 정부기관 등 | 게임산업, 소프트웨어 개발 업체 | 불특정 다수 |
| Purpose | 사회적 혼란 | 금전 이득 | 정보 수집 | 금전 이득 자료 탈취 | 자료 탈취 | 금전 이득 |
| Incidents | 3.20 사이버테러 소니픽쳐스 | 2016 SWIFT 2017 A은행 망분리 취약점 공격 2017~2018 암호화폐 | 탈북자 커뮤니티 및 언론사 장악 후 악성코드 유포 | Campaign RIFLE | N사 제품 변조 다수 게임회사 해킹 | - |
| Attack Vector | Spearphishing, Watering-hole | | | | | |
| | Document Malware, 0 or 1day | | | | | CVE-2017-4878 CVE-2016-0189 Sundown GF |
| | Supply Chain Attack | Mobile APP | | Supply Chain Attack | | |
| | | - | Flash, Kakaotalk Phishing | | | |

# 위협 그룹별 사고 사례

# 안다리엘 (Andariel)

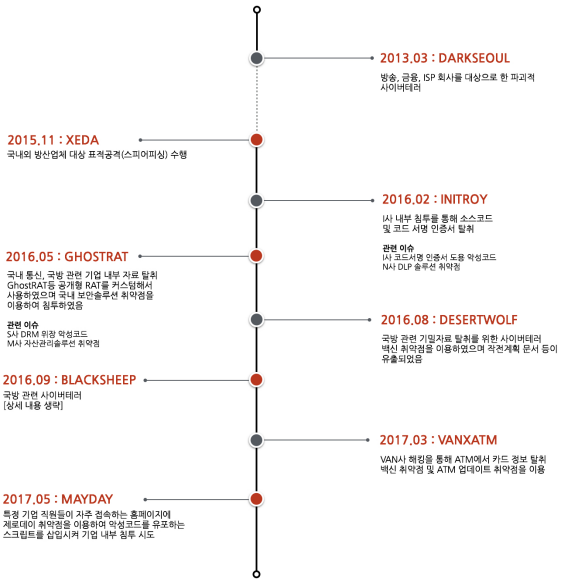
Campaign RIFLE : Andariel, The Maiden of Anguish

보고서 다운로드 : 금융보안원 홈페이지 공지사항 (fsec.or.kr)

## CAMPAIGN RIFLE

### 관련 오퍼레이션 및 주요 키워드

1. DARKSEOUL : 3.20 사이버테러
2. XEDA : 방산업체 스피어피싱
3. INITROY : 코드서명 인증서 / 소스코드 탈취
4. GHOSTRAT : 대기업 계열사 및 항공사
5. DESERTWOLF : 국방
6. BLACKSHEEP : 국방
7. VANXATM : ATM
8. MAYDAY : 금융회사 노동조합 / 워터링홀
9. BOWCASTER : 특정 자산관리 프로그램(PMS) 서버 취약점 이용



## CAMPAIGN RIFLE

**관련 오퍼레이션 주요 내용 : XEDA**

공격발생 : 2015년 11월
공격대상 : 서울 국제 항공우주 및 방위산업전시회 (ADEX) 참가 기업
공격방법 : 엑셀 매크로를 이용한 추가 악성코드 다운로드 및 실행 유도

## CAMPAIGN RIFLE

**관련 오퍼레이션 주요 내용 : GHOSTRAT**

공격인지 : 2016년 2월
공격기간 : 2014년 7월
공격대상 : H그룹 (D항공), S그룹 (17개 계열사)
피해규모 : 27개 회사 (140,000대 PC) 감염, 1TB(42,600건) 문서 유출
- 유출 문서 : 방위산업 자료, 네트워크 전산 자료

이용된 취약점 : M사 자산관리 솔루션 (취약 포트 3511/tcp, 3526/tcp)

## CAMPAIGN RIFLE

**관련 오퍼레이션 주요 내용 : VANXATM**

공격발생 : 주요 정보 유출 2017년 3월

공격대상 : VAN사

이용된 취약점

- 백신 및 내부 업데이트 서버

## CAMPAIGN RIFLE

**관련 오퍼레이션 주요 내용 : BOWCASTER**

최초 공격발생 : 2017년 중순

공격대상 : 금융, 여행사, 제조, IT 업권 등 다양

공격방법 : (주로) PMS 취약점

Special Report

[Special Report] 유명 기업 보안 시스템을 연달아 뚫다, 대범한 해커 조직의 공격 -1편-

2018. 3. 22. 10:17 URL 복사

<SK인포섹 블로그>

# 블루노로프 (Bluenoroff)

## BLUENOROFF

### CRYPTOFORCE

공격대상 : PoS (Point-of-Sale)

공격방법 : 전문 전송용 VAN사 모듈 후킹 후 카드정보 탈취

```
equal = strchr((const char *)ApprovalMSG, '=');// ThreadParameter가 = 을 포함하고 있는지 확인
if ( equal )
{
  Card_Track2_Data = 0;
  memset(&ApprovalMSG_v13, 0, 259u);
  C2_URL = 0;
  memset(&v13, 0, 259u);
  strncpy(&Card_Track2_Data, equal - 16, 37u);// =을 기준으로 앞 16바이트부터 총 37바이트 전체 복사 (equal은 = 이 있는 위치)
  loop_index = 0;
  if ( &Card_Track2_Data + strlen(&Card_Track2_Data) + 1 != &ApprovalMSG_v13 )
  {
    do                                          // 치환 암호 이용해 암호화
    {
      *(&Card_Track2_Data + loop_index) = SubstitutionTable_10014CB0[*(&Card_Track2_Data + loop_index)];
      ++loop_index;
    }
    while ( loop_index < strlen(&Card_Track2_Data) );
  }
```

## BLUENOROFF

### ENIUMESCAPE

최초 공격발생 : 2017년 초

공격대상 : 금융

공격방법 : VDI 취약점 (Namedpipe를 이용한 파일 송수신) 이용하여 내부 정보 탈취 시도

```
v14 = 260;
GetComputerName_dword_1001A954(&v21, &v14);
v3 = _strnicmp(&v21, "pb", 2u);
if ( v3 )
```

<pb로 시작하는 특정 호스트명 탐색>

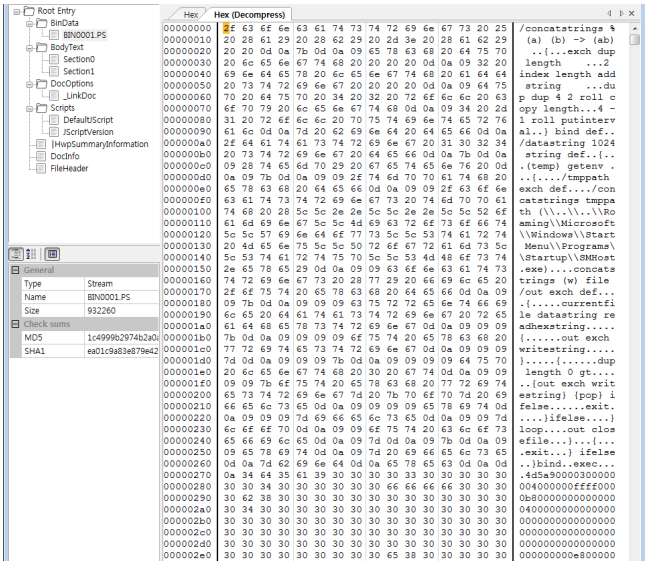
```
if ( strcmp(&String, (const char *)&word_10
{
  if ( v40 & 0x10 )
    lstrcpyA((LPSTR)MARKER_v2, ":FZ:");
  else
    lstrcpyA((LPSTR)MARKER_v2, ":GY:");
  *(_DWORD *)(MARKER_v2 + 4) = *(_DWORD *)&
  *(_DWORD *)(MARKER_v2 + 8) = *(_DWORD *)&
  FileTimeToLocalFileTime((const FILETIME *
  v6 = LocalFileTime.dwHighDateTime;
```

<블루노로프 코드 패턴 : 파일 Marker>

## BLUENOROFF

### HWP 악성코드 및 모바일 악성앱

공격대상 : 암호화폐 거래소 및 관련 회사

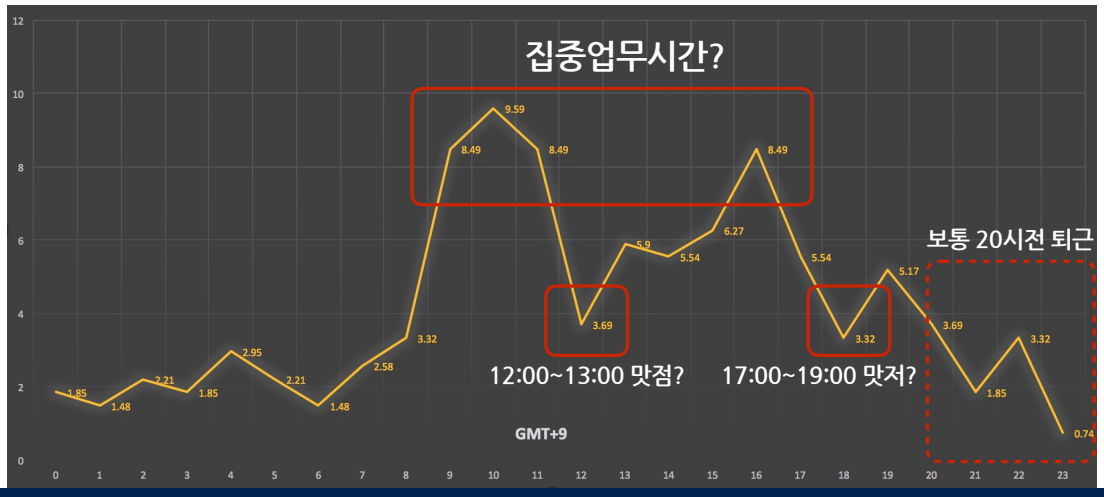


# 그룹별 위협 인텔리전스 데이터

## 안다리엘 (Andariel)

# Threat Intelligence : Andariel

## Malware Buildtime - Working-time 추측




# Threat Intelligence : Andariel

## Rifle Transform : XOR 트랜스폼

- 특징 : 다수의 XOR 연산 이용. 인코딩/디코딩에 모두 사용 가능

```
LOBYTE(v5) = 0x48;
v6 = 0x90u;
v11 = 0x2B3C48;
result = 0x654321;
if ( v3 > 0 )
{
  v8 = a3 - (_DWORD)v4;
  v10 = v3;
  do
  {
    *v4 = v6 ^ result ^ v5 ^ v4[v8];
    v6 = v6 & result ^ v5 & (v6 ^ result);
    v5 = ((((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20) | (v11 >> 8);
    result = (((result << 7) ^ (result ^ 16 * (result ^ 2 * result)) & 0xFFFFFF80) << 17) | (result >> 8);
    ++v4;
    v9 = v10-- == 1;
    v11 = ((((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20) | (v11 >> 8);
  }
  while ( !v9 );
}
return result;
```

# Threat Intelligence : Andariel

## Rifle Transform : FE 트랜스폼

- 특징 : XOR 트랜스폼과 거의 유사하나, Bit Manipulation에 사용되는 값이 다소 상이

```
if ( a3 )
{
  do
  {
    *(_BYTE *)(v6 + a4) ^= v4 ^ (unsigned __int8)result;
    v8 = v5 >> 8;
    v4 = BYTE3(result) ^ BYTE1(result) & (result >> 16) ^ v5 & BYTE1(v5) & (v5 >> 16) ^ v10 & result;
    result = (result >> 8) | (v9 << 24);
    v5 = (v5 >> 8) | (((v7 ^ (unsigned __int16)(2 * v7)) & 0x1FE) << 22);
    ++v6;
    v10 = v4;
    v9 = v8 | (((v7 ^ (unsigned __int16)(2 * v7)) & 0x1FE) << 22);
    v7 = result;
  }
  while ( v6 < a3 );
}
return result;
```

# Threat Intelligence : Andariel

## Rifle Transform : S 트랜스폼

- 특징 : S^로 시작하는 문자열에서 S^를 제외한 문자열을 추출하는데 사용됨

```
v2 = RIFLE_S_Decoding("S^HeapCreate");
dword_412E64 = (int)GetProcAddress(v1, (LPCSTR)v2);
v3 = RIFLE_S_Decoding("S^GetProcessHeap");
dword_412E08 = (int)GetProcAddress(v1, (LPCSTR)v3);
v4 = RIFLE_S_Decoding("S^HeapDestroy");
dword_412E58 = (int)GetProcAddress(v1, (LPCSTR)v4);
v5 = RIFLE_S_Decoding("S^HeapAlloc");
dword_412F08 = (int)GetProcAddress(v1, (LPCSTR)v5);
v6 = RIFLE_S_Decoding("S^HeapReAlloc");
dword_412F20 = (int)GetProcAddress(v1, (LPCSTR)v6);
v7 = RIFLE_S_Decoding("S^HeapFree");
dword_412E7C = (int)GetProcAddress(v1, (LPCSTR)v7);
v8 = RIFLE_S_Decoding("S^GetModuleFileNameA");
dword_412EF8 = (int)GetProcAddress(v1, (LPCSTR)v8);
v9 = RIFLE_S_Decoding("S^DeleteFileA");
dword_412E10 = (int)GetProcAddress(v1, (LPCSTR)v9);
v10 = RIFLE_S_Decoding("S^CreateMutexA");
dword_412DB0 = (int)GetProcAddress(v1, (LPCSTR)v10);
v11 = RIFLE_S_Decoding("S^CreateThread");
dword_412E94 = (int)GetProcAddress(v1, (LPCSTR)v11);
```

```
if ( *(_BYTE *)v1 != 'S' || *((_BYTE *)v1 + 1) != '^' )
{
  v4 = *(_WORD *)v1;
  if ( *(_WORD *)v1 > 0xBB7u )
    v4 = 0xBB7;
  if ( (unsigned __int16)v4 > 0u )
  {
    v5 = (char *)v1 + 2;
    v6 = (unsigned __int16)v4;
    v7 = BYTE1(v10);
    v8 = Dst;
    do
    {
      *v8++ = v7 ^ *v5++;
      --v6;
    }
    while ( v6 );
  }
  result = Dst;
}
else
{
  if ( strlen((const char *)v1) - 2 >= 0xBB7 )
    v2 = 0xBB7;
  else
    v2 = strlen((const char *)v1) - 2;
  strncpy_s(Dst, 0xBB8u, (const char *)v1 + 2, v2);
  result = Dst;
}
```

# Threat Intelligence : Andariel

## Rifle Transform : SUBS 트랜스폼

- 특징
  내부에 저장되어 있는 문자 치환 테이블을 이용하여
  특정 문자로 치환 후 Shift, OR 연산을 이용하여
  최종 문자열 생성 -> 해당 문자열 XOR 트랜스폼으로 전달

```
dwSize = 0;
v0 = RIFLE_SUBS_Decoding(16, "978FF5eqF2YM01+4", (int *)&dwSize);
RIFLE_XOR_Decoding(v0, dwSize);
v1 = LoadLibraryA(v0);
```

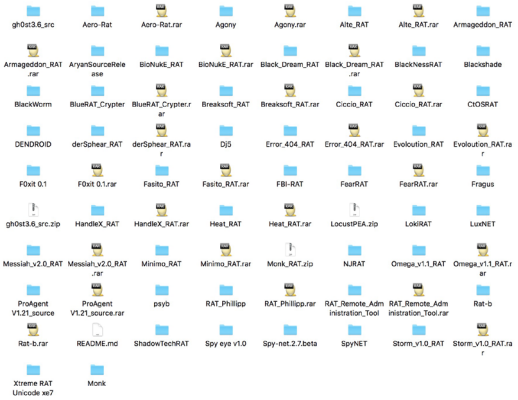
```
if ( result )
{
  for ( i = *v4; *v4; i = *v4 )
  {
    v9 = v3;
    ++v4;
    --v3;
    if ( v9 <= 0 || i == '=' )
      break;
    if ( i == ' ' )
      i = '+';
    v10 = word_414B90[i];
    if ( v10 >= 0 )
    {
      switch ( v5 % 4 )
      {
        case 0:
          result[v6] = 4 * v10;
          break;
        case 1:
          result[v6++] |= v10 >> 4;
          result[v6] = 16 * v10;
          break;
        case 2:
          result[v6++] |= v10 >> 2;
          result[v6] = (_BYTE)v10 << 6;
          break;
        case 3:
          result[v6++] |= v10;
          break;
        default:
          break;
      }
      ++v5;
```

# Threat Intelligence : Andariel

## 오픈소스 RAT

- 안다리엘은 자체 개발 RAT 외에도 인터넷에 공개된 RAT 소스코드를 수정하여 공격에 활용
- Aryan, XtremeRAT, GhostRAT, FBI RAT 등

<실제 공격자가 다운로드 받은 RAT 소스코드>



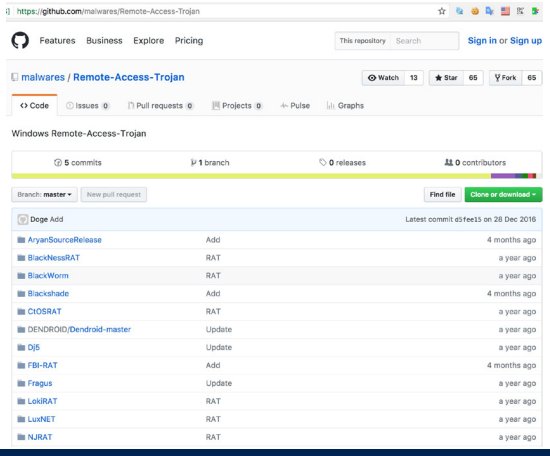
# Threat Intelligence : Andariel

## 오픈소스 RAT

| | | | |
|---|---|---|---|
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/ACMConvertor.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/ACMOut.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/AS_ShellUtils.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/AS_Ver.inc |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/BTMemoryModule.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Common.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.cfg |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.dof |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.dpr |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.dproj |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.dproj.local |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.identcache |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CryptFile.res |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/CustomIniFiles.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/DeviceHelper.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/English.ini |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Espa[illegible]ol.ini |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/GeoIP.dat |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/GeoIP.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/IdCompilerDefines.inc |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/IdIOHandler.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/IdIOHandlerSocket.pas |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Images/ |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Images/Xtremelco.ico |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Images/Xtremelco.png |
| 'Carved_Zip_1448749083.zip | Remote-Access-Trojan-master | Xtreme RAT | Unicode xe7/Images/XtremeRAT1.jpg |

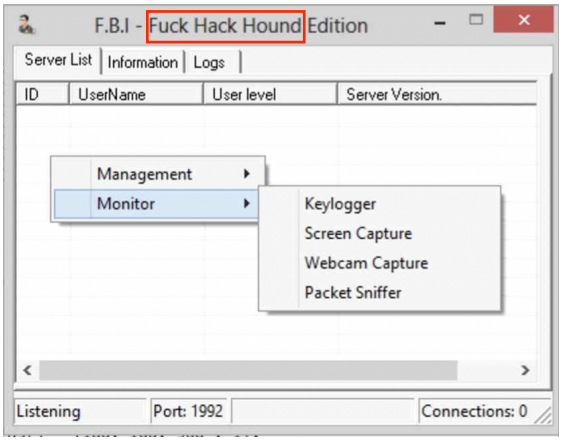
〈실제 공격자가 다운로드 받은 RAT 소스코드 GitHub〉

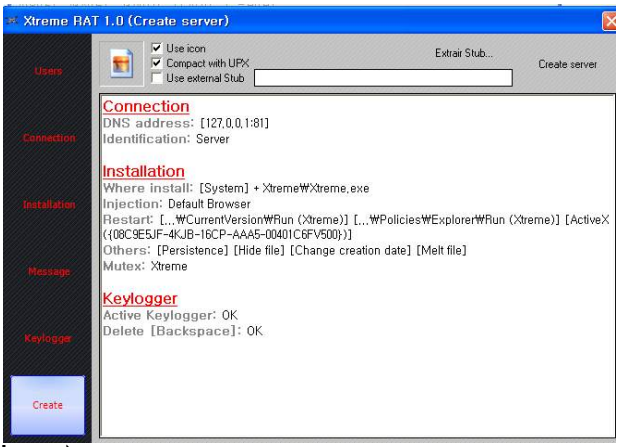
https://github.com/malwares/Remote-Access-Trojan




# Threat Intelligence : Andariel

## 오픈소스 RAT




〈실제 공격에 사용된 RAT〉

# Threat Intelligence : Andariel

## 오픈소스 RAT

- 뮤텍스 생성

2017년 6월 제작된 파일에서는 악성코드 동작 시 주요 서브루틴으로 바로 진입하지만, 2017년 8월 제작된 변종 파일에서는 뮤텍스(Mutex)를 생성하는 코드가 추가되었다. 뮤텍스(Mutex)는 일반적으로 악성코드가 기존에 감염되었던 시스템인지 여부를 확인하여 중복 실행을 방지하기 위한 목적으로 사용된다.

```
int __stdcall __noreturn WinMain(HINSTANCE hInstance,
{
  InitializeCriticalSection(&CriticalSection);
  sub_405000();
}
```

[2017년 6월 제작 파일]

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance,
{
  char *v4; // eax@2
  char *v5; // ecx@3
  if ( !OpenMutexA(0x1F0001u, 0, "ASDASDADSA") )
  {
    CreateMutexA(0, 0, "ASDASDADSA");
    v4 = &name;
    if ( name )
    {
      v5 = &name;
      do
      {
        *v4 ^= 0xFu;
        v4 = ++v5;
      }
      while ( *v5 );
    }
    InitializeCriticalSection(&CriticalSection);
    sub_405000();
  }
  return 0;
}
```

[2017년 8월 제작 파일]

<SK인포섹 블로그>

```
int APIENTRY WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow)
{
    HANDLE  Mutex = OpenMutex(MUTEX_ALL_ACCESS, FALSE, "ASDASDADSA");
    if(Mutex == NULL)
    {
        Mutex = CreateMutex(NULL, FALSE, "ASDASDADSA");
    }
    else
    {
        return 0;
    }
//MessageBox(NULL, "Injected", "Injected", MB_OK);
    Inject=CreateDialog(GInstance,(LPCTSTR)MAIN,NULL,(DLGPROC)MainWndProc);
    //  ShowWindow(Inject,SW_HIDE);
    MSG msg;
    while(GetMessage(&msg,Inject,0,0)==TRUE)
    {
        TranslateMessage(&msg);
        DispatchMessage(&msg);
```

<FBI RAT 소스코드>

"Andariel의 오퍼레이션에서
자주 사용되고 있는 오픈소스 RAT의 코드"

# Threat Intelligence : Andariel

## 인코딩 / 디코딩 함수 변경

```
v3 = a1;
v4 = a2;
v5 = 0x1D91E44;
v6 = 0x40E0E1E;
v12 = 0x1D91E44;
v11 = 0x40E0E1E;
if ( a3 > 0 )
{
  v7 = v4 - (_DWORD)v3;
  do
  {
    v8 = v5 >> 8;
    *v3 = v11 ^ v12 & BYTE1(v5) ^ v3[v7] ^ (v12 >> 16) & BYTE3(v12) ^ BYTE1(v6) & (v6 >> 16) & BYTE3(v6);
    result = (v6 >> 8) | (v12 << 24);
    v5 = (v5 >> 8) | ((16 * v11 ^ (v11 ^ 2 * (v11 ^ 4 * v11)) & 0xFFFFFFF0) << 20);
    v6 = result;
    ++v3;
    v12 = v8 | ((16 * v11 ^ (v11 ^ 2 * (v11 ^ 4 * v11)) & 0xFFFFFFF0) << 20);
    v10 = a3-- == 1;
    v11 = result;
  }
  while ( !v10 );
}
return result;
```

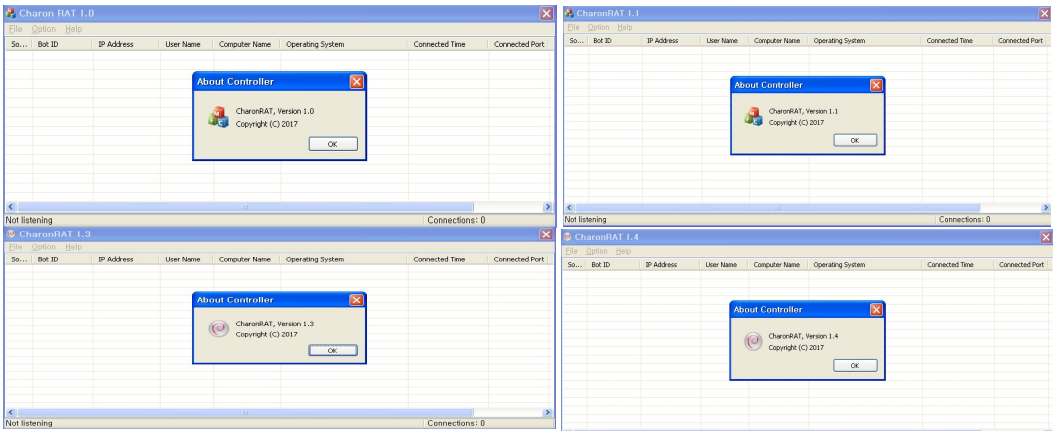
**<2017년 5월 MAYDAY 오퍼레이션 샘플에서 발견된 신규 트랜스폼 함수>**

## Threat Intelligence : Andariel

### RAT 업그레이드 및 버전 관리 : CharonRAT

## Threat Intelligence : Andariel

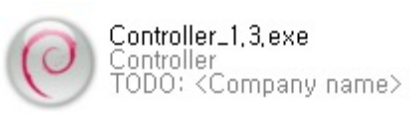
### RAT 업그레이드 및 체계적 버전 관리 : CharonRAT

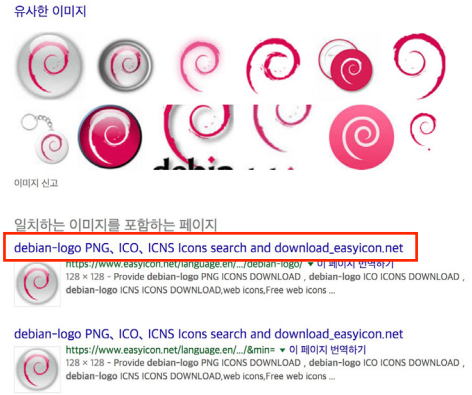


## Threat Intelligence : Andariel

### RAT 업그레이드 및 버전 관리 : CharonRAT

아이콘으로 사용되는 이미지

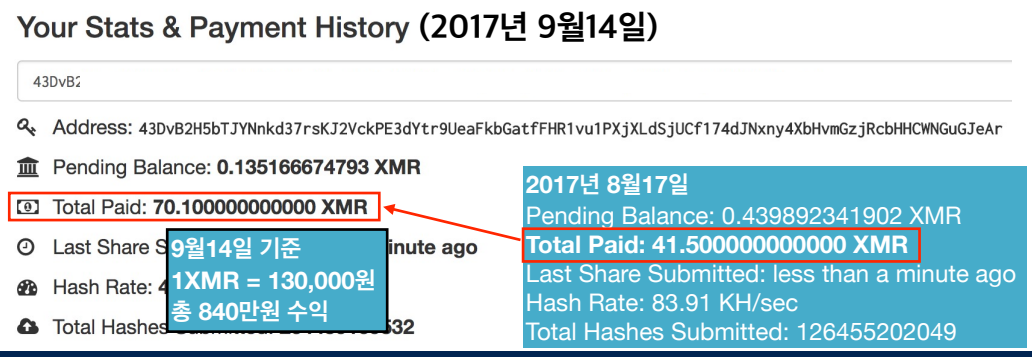



## Threat Intelligence : Andariel

### 모네로 채굴기 (Monero Miner)

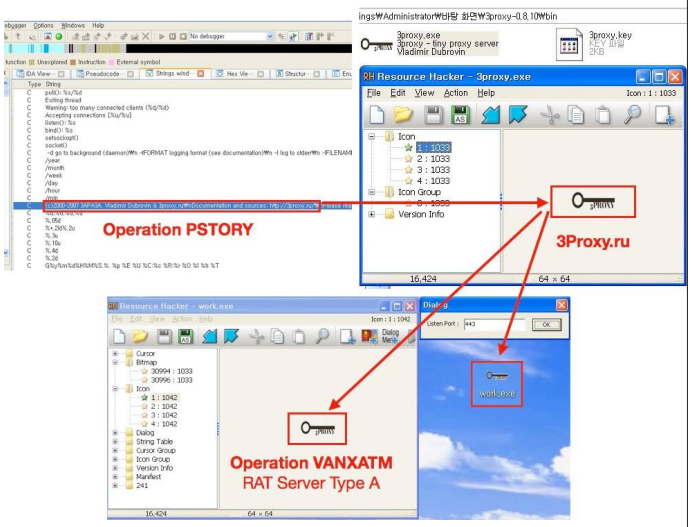
```
C:\Windows\system\rmgr\rar.exe  x -hp                    2 C:\Windows\system\rmgr\1.rar C:\Windows\system\rmgr\
"C:\Windows\system\rmgr\update.exe" -a cryptonight -o stratum+tcp://mine.moneropool.com:443 -u
43DvB2                                                                                  r -p x -t 2
```



## Threat Intelligence : Andariel

### IP 은닉 기법의 변화

- 과거에는 VPN을 이용하였으나 VPN 소프트웨어 오류로 인해 실제 IP가 자주 노출되었음
- 최근에는 국내 서버를 Proxy로 이용하여 최종 C&C로 바로 자료를 유출시키는 방법도 사용
  => 유출 자료 확보가 어려워지고 있으며 따라서 피해 규모를 파악하기 어려워짐
  => 공격 원점 IP를 찾기도 어려워짐




## Threat Intelligence : Andariel

### 기타 공격 도구

- 3proxy, AngryScanner, Webshell (404 not found webshell 등), pcon.exe, plink.exe, vpn.exe (키로거), Mimikatz 등

# 블루노로프 (Bluenoroff)

## Threat Intelligence : Bluenoroff

### 코드 패턴

- File Marker

```
$delimiter1 = ":FZ:" fullword ascii wide
$delimiter2 = ":GY:" fullword ascii wide
$delimiter3 = ";**;" fullword ascii wide
```

- Logging 파일 이름

```
$filename1 = "MD*.tmp" fullword ascii wide
$filename2 = "DWS*.tmp" fullword ascii wide
$filename3 = "PM*.tmp" fullword ascii wide
$filename4 = "WM*.tmp" fullword ascii wide
$filename5 = "FM*.tmp" fullword ascii wide
$filename6 = "CS*.tmp" fullword ascii wide
```

- Fake SSL 도메인

```
$fakedomain1 = "www.google.com" ascii
$fakedomain2 = "www.apple.com" ascii
$fakedomain3 = "uk.yahoo.com" ascii
$fakedomain4 = "www.bing.com" ascii
$fakedomain5 = "www.debian.org" ascii
$fakedomain6 = "dropbox.com" ascii
$fakedomain7 = "facebook.com" ascii
$fakedomain8 = "github.com" ascii
$fakedomain9 = "tumblr.com" ascii
$fakedomain10 = "twitter.com" ascii
$fakedomain11 = "wetransfer.com" ascii
$fakedomain12 = "wikipedia.org" ascii
$fakedomain13 = "xbox.com" ascii
$fakedomain14 = "microsoft.com" ascii
```

# Threat Intelligence : Bluenoroff

## 코드 패턴

- 로깅 포멧 및 디버깅 메시지

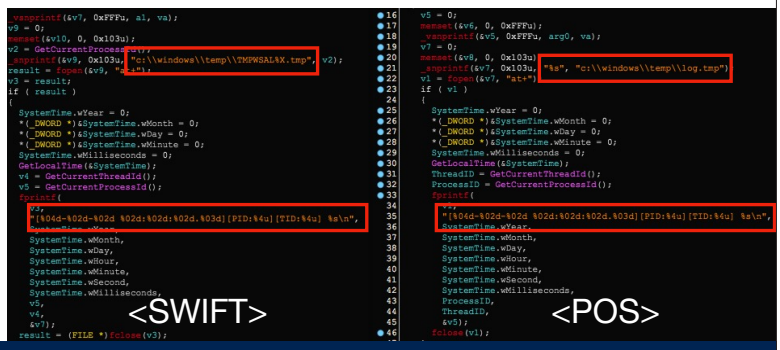
$a1 = "[%04d-%02d-%02d %02d:%02d:%02d.%03d][PID:%4u][TID:%4u] %s"

$a2 = "c:₩₩windows₩₩temp₩₩log.tmp"

$a3 = "initialize_func(%s, %s) %s"

$a4 = "Success"

$a5 = "Failed"




# Threat Intelligence : Bluenoroff

## 코드 패턴

- 인코딩된 HTTP 패킷

Acceyk: */*;
Cxwkewk-Kpye: vlukryaik/fxiv-daka; bxlwdaip=
Acceyk-Ewcxdrwg: gzry,defuake,jdch
Acceyk-Uawglage: tx-TI
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"bxaid_rd\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"ljei_rd\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\";
fruewave=\"rvg01_29.syg\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"vp.dxc\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\";
fruewave=\"yiakrce.ydf\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"trwg.syg\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"dieav.amr\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"hy01.amr\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"jkai.amr\"
Cxwkewk-Drjyxjrkrxw: fxiv-daka; wave=\"frue1\"; fruewave=\"jkai.amr\"
Cxwkewk-Kpye: ayyurcakrxw/xckek-jkieav

- 디코딩된 HTTP 패킷

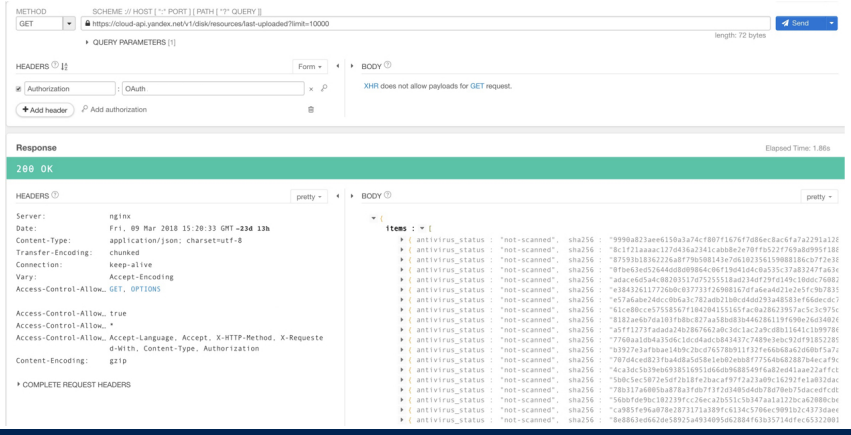
Accept: */*;
Content-Type: multipart/form-data; boundary=
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR
Content-Disposition: form-data; name="board_id"
Content-Disposition: form-data; name="user_id"
Content-Disposition: form-data; name="file1";
filename="img01_29.jpg"
Content-Disposition: form-data; name="file1"; filename="my.doc"
Content-Disposition: form-data; name="file1";
filename="pratice.pdf"
Content-Disposition: form-data; name="file1"; filename="king.jpg"
Content-Disposition: form-data; name="file1";
filename="dream.avi"
Content-Disposition: form-data; name="file1"; filename="hp01.avi"
Content-Disposition: form-data; name="file1"; filename="star.avi"
Content-Disposition: form-data; name="file1"; filename="star.avi"
Content-Type: application/octet-stream

# 스카크러프트 (Scarcruft)

## Threat Intelligence : Scarcruft (a.k.a Red Eyes, 금성121, Group123, Reaper)

### 특징

- 탈취 데이터 클라우드 (Yandex, Dropbox, Pcloud)로 전송



## Threat Intelligence : Scarcruft

### 특징

- PDB Path
  *:₩FirstBackDoor*
  *:₩TASK₩ProgamsByMe*
  C:₩Users₩NaughtyDevelop*
  *:₩work₩4th₩plugin*
  *:₩work₩n1st₩plugin*
  *:₩HighSchool₩*
  *:₩Happy₩Work₩Source₩*
  *₩First-Dragon₩*₩Dog[Call|Print].pdb

Special Thanks to Ahnlab (Minseok Cha)

## Reference

### GeomSeong121, Est Security

http://www.boannews.com/media/view.asp?idx=67660&kind=1

### Red Eyes, Ahnlab

http://download.ahnlab.com/kr/site/library/%5BReport%5DRed_Eyes_Hacking_Group_kor.pdf

### Group123, Cisco Talos

http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

### APT37 (Reaper), FireEye

https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

Wintti

## Threat Intelligence : Wintti (Shadowpad)

### 쉘코드 디코딩 코드

```
rule Shadowpad_Transform
{
    strings:
        $mz = {4D 5A}
        $hex = {81 7D F8 ?? ?? ?? ?? 73 3C 8B 4D F4 03 4D F8 0F B6 11 0F B6 45 FC 33 D0 8B 4D F0 03 4D F8 88 11 8B 55 FC C1 E2 10 8B 45 FC C1 E8 10 03 D0 89 55 FC 8B 4D FC 69 C9 ?? ?? ?? ?? 81 E9 ?? ?? ?? ?? 89 4D FC EB B2}
    condition:
        $mz at 0
        and filesize < 30MB
        and any of ($hex*)
}
```

```
for ( i = 0; i < 0xFB44; ++i )
{
  *((_BYTE *)v3 + i) = v5 ^ *((_BYTE *)&unk_1000F718 + i + 4);
  v5 = 0xC9BED351 * ((v5 >> 16) + (v5 << 16)) - 0x57A25E37;
}
if ( (unsigned int)v3(0) < 0x1000 )
  MessageBoxA(0, "###ERROR###", 0, 0);
return v2;
```

## Reference

**Winnti Analysis, Noveta**
https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

**Winnti : More than just a game, Kaspersky**
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf

**Winnti Polymorphism, Takahiro Haruyama (Symantec)**
https://hitcon.org/2016/pacific/0composition/pdf/1201/1201%20R2%201610%20winnti%20polymorphism.pdf

**ShadowPad in corporate networks, Kasperksy**
https://securelist.com/shadowpad-in-corporate-networks/81432/

# EvilBunny
(Matrix, Magniber, GlobeImposter, Hermes, GandCrab)

## Threat Intelligence : Ransomware

### Matrix Ransomware

- http://www.boannews.com/media/view.asp?idx=57755

매트릭스 랜섬웨어 암호파일에서 '주체·평양' 단어 발견됐다

좋아요 53개 | 입력 : 2017-10-30 11:56 가 가

**암호화된 파일에 영문으로 '주체', '평양' 단어 있는 매트릭스 랜섬웨어 변종 발견**
**공격자 추정의 11개 메일주소 포착...여기에도 영문으로 '주체', '평양' 단어 포함**
**지난 27일 매트릭스 랜섬웨어 변종 유포...유포시점은 약 1주일 전후로 유포**

가장 많이 본 기사 [주간]
1 [긴급] 26만대 이상 기기
2 북한 배후 해커조직, 국내
3 버터플라이 랜섬웨어 유포
4 난리 난 페이스북, 삭제
5 [한국정보보호학회 칼럼]

## Threat Intelligence : Ransomware

### GandCrab Ransomware

- http://www.boannews.com/media/view.asp?idx=67364

'버전업'해 돌아오겠다던 약속 지킨 랜섬웨어 공격자들

좋아요 28개 | 입력 : 2018-03-08 16:18 가 가

**경찰과 보안 업체 공조로 무력화된 이전 랜섬웨어 공격자들, '컴백'**
**개발된 복호화 툴 무력화시켜...그 외 자잘한 변화들 있어**

[보안뉴스 문가용 기자] 갠드크랩(GandCrab)이라는 랜섬웨어 개발자들이 자신들이 장담했던 바를 지켰다. 보안 업체 비트디펜더(Bitdefender)가 무력화시킨 자신들의 무기를 새롭게 업그레이드 하여 돌아오겠다던 이들이 갠드크랩 2.0을 들고 나타난 것이다. 이는 비트디펜더의 복호화 툴에 풀리지 않는다.

가장 많이 본
1 [긴급] 2
2 북한 배후
3 버터플라
4 난리 난
5 [한국정보
6 네이버 부
7 신한데이
8 [주말판]
9 리눅스
10 [보안다

## Threat Intelligence : Ransomware

### GlobeImposter Ransomware

– http://blog.alyac.co.kr/1249

악성코드 분석 리포트

**유효한 디지털서명을 탑재한 랜섬웨어 GlobeImposter 변종 등장**

알약(Alyac) 2017.08.01 11:03

안녕하세요? 이스트시큐리티 시큐리티대응센터(ESRC) 입니다.

GlobeImposter 랜섬웨어 변종 중 유효한 디지털 서명을 탑재한 형태가 해외에서 등장하고 있어 이용자분들의 각별한 주의가 요망됩니다.

잘 아시는 분들도 계시겠지만, 일반적으로 특정 파일에 유효한 디지털 서명이 탑재되어 있다는 것은 무결성이 보장된다는 의미와 함께 정상적인 파일(화이트 리스트)임을 증명하는 용도로 활용되기도 합니다.

## Threat Intelligence : Ransomware

### Hermes Ransomware

– http://www.boannews.com/media/view.asp?idx=66525

**Hermes 랜섬웨어 변종 출현! 안랩 V3 우회 노렸다**

좋아요 36개 | 입력 : 2018-02-01 18:10 가 가

가장 많

1 [긴

2 북한

3 난리

4 신한

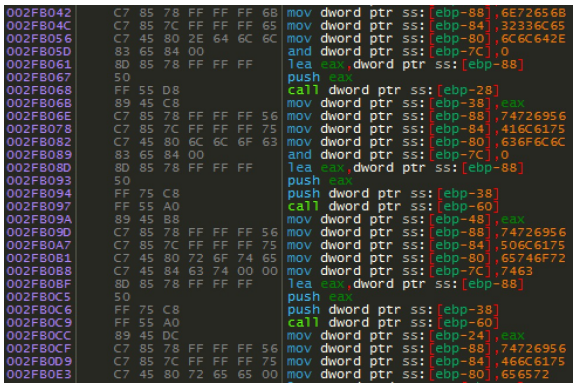
**Hermes 랜섬웨어, 국내 유포 중...최근 안랩 타깃 공격 포착**

**2017년 제외됐던 감염 제외 폴더에 최근 안랩도 포함시켜 변형**

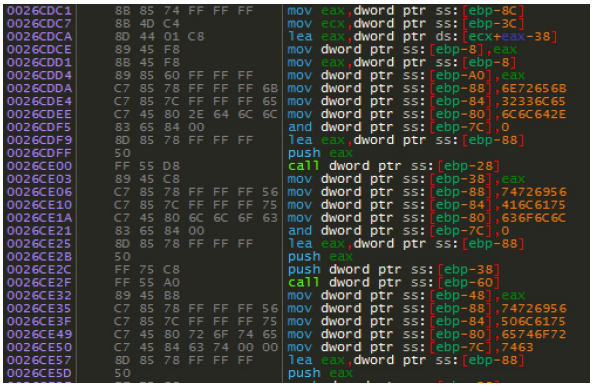
## Threat Intelligence : Ransomware

### 연관성 분석

Trigger code (Shellcode)




〈Magniber〉

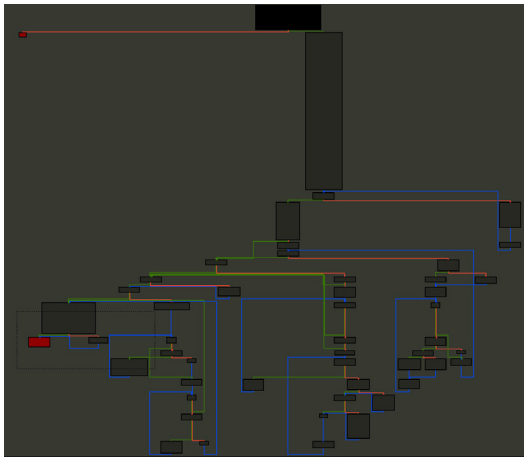



〈GandCrab〉

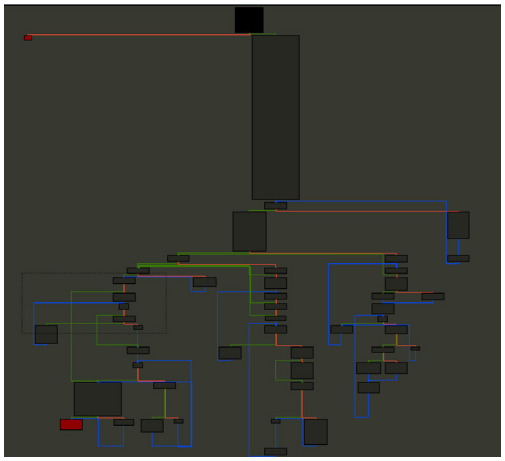
## Threat Intelligence : Ransomware

### 연관성 분석

Trigger code (Shellcode)



〈Magniber〉

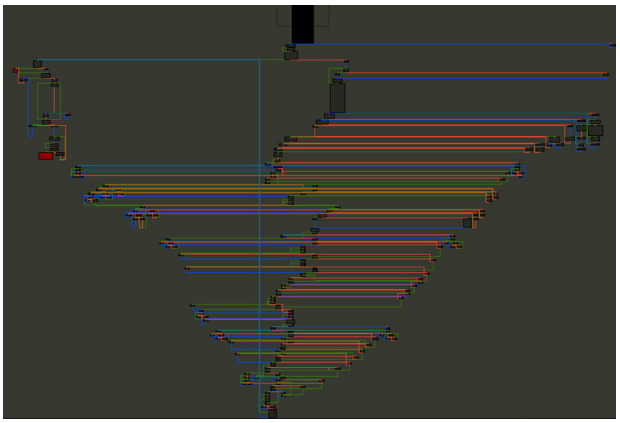


〈GandCrab〉

## Threat Intelligence : Ransomware

### 연관성 분석

Trigger code (Shellcode)



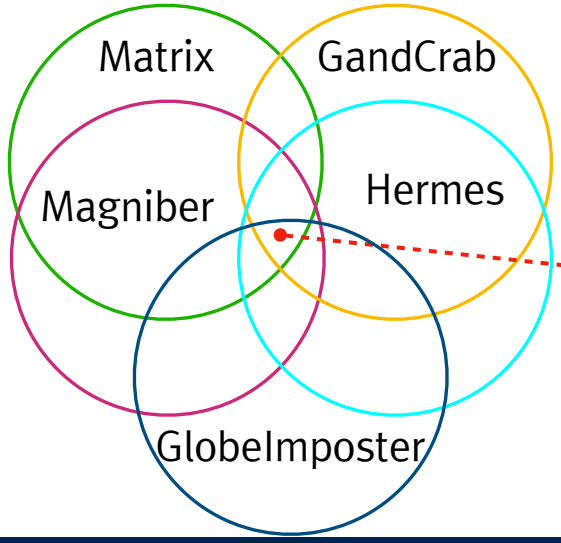
〈Magniber〉

〈GandCrab〉

## Threat Intelligence : Ransomware

### 연관성 분석

Decoding




```
v2 = 0xC6EF3720;
v7 = *a2;
v8 = a2[1];
v3 = *a1;
v4 = a1[1];
v9 = a2[2];
v10 = a2[3];
v11 = 32;
do
{
  AddAtomW(0);
  GetLastError();
  v4 -= (v2 + v3) ^ (v9 + 16 * v3) ^ (v10 + (v3 >> 5));
  v5 = (v2 + v4) ^ (v7 + 16 * v4) ^ (v8 + (v4 >> 5));
  v2 += 0x61C88647;
  v3 -= v5;
  --v11;
}
while ( v11 );
result = a1;
a1[1] = v4;
*a1 = v3;
return result;
```

〈Decoding Pseudocode〉

## Threat Intelligence : Ransomware

연관성 분석
Decoding

```
v2 = 0xC6EF3720;
v7 = *a2;
v8 = a2[1];
v3 = *a1;
v4 = a1[1];
v9 = a2[2];
v10 = a2[3];
v11 = 32;
do
{
  AddAtomW(0);
  GetLastError();
  v4 -= (v2 + v3) ^ (v9 + 16 * v3) ^ (v10 + (v3 >> 5));
  v5 = (v2 + v4) ^ (v7 + 16 * v4) ^ (v8 + (v4 >> 5));
  v2 += 0x61C88647;
  v3 -= v5;
  --v11;
}
while ( v11 );
result = a1;
a1[1] = v4;
*a1 = v3;
return result;
```

```
void decrypt (uint32_t* v, uint32_t* k) {
    uint32_t v0=v[0], v1=v[1], sum=0xC6EF3720, i;  /* set up
    uint32_t delta=0x9e3779b9;                     /* a key
    uint32_t k0=k[0], k1=k[1], k2=k[2], k3=k[3];   /* cache
    for (i=0; i<32; i++) {                         /* basic
        v1 -= ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
        v0 -= ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
        sum -= delta;
    }                                              /* end cy
    v[0]=v0; v[1]=v1;
}
```

〈TEA Implementation〉

〈from Magniber〉

## Threat Intelligence : Ransomware

연관성 분석
Decoding

### Tiny Encryption Algorithm

From Wikipedia, the free encyclopedia

In cryptography, the **Tiny Encryption Algorithm** (**TEA**) is a block cipher notable for its simplicity of description and implementation, typically a few lines of code. It was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory; it was first presented at the Fast Software Encryption workshop in Leuven in 1994, and first published in the proceedings of that workshop.[4]

https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm

## Threat Intelligence : Ransomware

연관성 분석
Decoding

```
v5 = 0xC6EF3720;
v6 = 0x20;
do
{
  result -= (v5 + *(_DWORD *)(4 * ((v5 >> 11) & 3) + 0x1002951C)) ^ (v4 + (0x10 * v4 ^ (v4 >> 5)));
  v5 += 0x61C88647;
  v4 -= (v5 + *(_DWORD *)(4 * (v5 & 3) + 0x1002951C)) ^ (result + (0x10 * result ^ (result >> 5)));
  --v6;
}
while ( v6 );
```

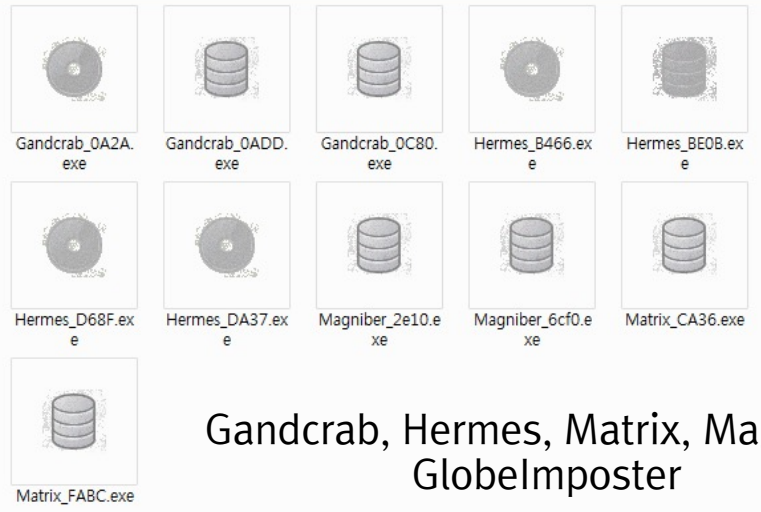
MD5 : B84293FEEDC66909F3D3B517B5396DCE
<BMdoor, Andariel>

```
v4 = 0xC6EF3720;
v5 = 32;
do
{
  v3 -= (v4 + dword_100150F8[(v4 >> 11) & 3]) ^ (v2 + (16 * v2 ^ (v2 >> 5)));
  v4 += 0x61C88647;
  --v5;
  v2 -= (v4 + dword_100150F8[v4 & 3]) ^ (v3 + (16 * v3 ^ (v3 >> 5)));
}
while ( v5 );
```

MD5 : F795B22676BAC9AC1D21E278BF184E4F
<3.20 Cyberterror, Lazarus>

## Threat Intelligence : Ransomware

연관성 분석
icons




Gandcrab, Hermes, Matrix, Magniber, GlobeImposter

# 연관성 분석

## Threat Intelligence : Ransomware

icons

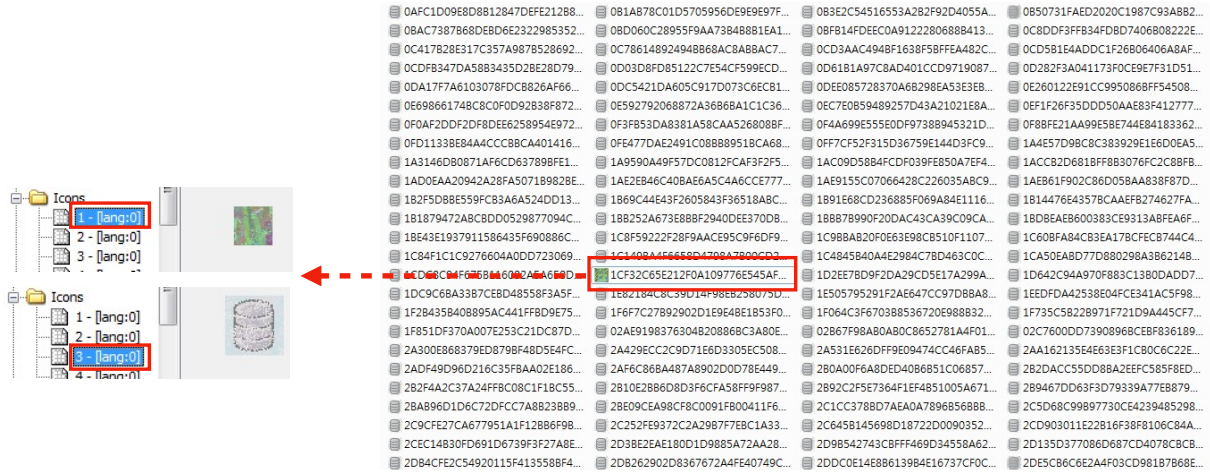
```
rule magniber_icon_db : dbicon
{
        strings:
                $icon = {77 16 27 37 76 E2 DC FD FF FF FE B2 3B F1 DC FD FF FD CD C7 8B EA DC FD 7F D8 00 02 77 FC DC FD FF C8 00 00 1F D0 DC FD FF E0 00 00 0F F3 DC FD FF 80 00 00 03
F6 DC FD 6F 00 00 00 01 EF DC FD CF 00 00 00 00 FD DC FD 9E 00 00 00 00 7F DC FD EE 00 00 00 00 FF DC FD FE 00 00 00 00 DD DC FD CC 00 00 00 00 CD DC FD 74 00 00 00 00 F7 DC FD
D8 00 00 00 00 D7 DC FD B8 00 00 00 00 3D DC FD F4 00 00 00 00 74 DC FD 56 00 00 00 00 62 DC FD 54 00 00 00 00 7A DC FD 78 00 00 00 00 F0 DC FD 72 00 00 00 00 FE DC FD FE 00
00 00 00 F5 DC FD B6 00 00 00 00 F9 DC FD 7C 00 00 00 00 FF DC FD FE 00 00 00 00 FF DC FD 3E 00 00 00 00 FC DC FD D2 00 00 00 00 FC DC FD FE 00 00 00 00 F4 DC FD DE 00 00 00 00
B7 DC FD 20 00 00 00 00 DE DC FD 2C 00 00 00 00 DE DC FD C6 00 00 00 00 7D DC FD 20 00 00 00 00 D1 DC FD 3A 00 00 00 00 D3 DC FD 04 00 00 00 00 FA DC FD FE 00 00 00 00 3E DC
FD FE 00 00 00 00 7D DC FD 5E 00 00 00 00 96 DC FD 06 00 00 00 00 2D DC FD 4E 00 00 00 01 7E DC FD A9 00 00 00 01 FE DC FD 8B 00 00 00 02 36 DC FD A3 20 00 00 03 9F DC FD F3 18
00 00 10 8F DC FD DF FF 80 00 0C 5F DC FD 56 FD DA FB 9F 30 DC FD DD F6 FD 1A B6 F7 DC FD EF EB FF E1 C4 C7 DC FD}
        condition:
                all of them
}

rule magniber_icon_cd : cdicon
{
        strings:
                $icon = {F9 FE F7 DF FB BE 00 00 EF 95 F7 6B BE FF 00 00 EF 2C BB EB F4 FD 00 00 FF BB E0 06 FE 1F 00 00 FF CD 00 00 FE F1 00 00 F7 D4 00 00 3F 2F 00 00 7F D0 00 00 0F
7F 00 00 FF E0 00 00 07 FF 00 00 FF C0 00 00 03 FD 00 00 DE 80 00 00 01 FD 00 00 FF 00 00 00 00 F8 00 00 FE 00 00 00 00 7B 00 00 FC 00 00 00 00 36 00 00 FC 00 00 00 00 37 00 00 F0
00 00 00 00 1B 00 00 F8 00 00 00 00 1D 00 00 D0 00 00 00 00 0E 00 00 E0 00 00 00 00 0F 00 00 F0 00 00 00 00 0F 00 00 E0 00 03 C0 00 05 00 00 A0 00 07 60 00 07 00 00 A0 00 0F 70
00 07 00 00 A0 00 17 F8 00 07 00 00 C0 00 1D E8 00 07 00 00 C0 00 1F F8 00 07 00 00 00 00 1F F8 00 07 00 00 60 00 09 F0 00 07 00 00 60 00 07 60 00 07 00 00 E0 00 03 C0 00 07 00
00 F0 00 00 00 00 0F 00 00 D0 00 00 00 00 0F 00 00 B0 00 00 00 00 0F 00 00 F8 00 00 00 00 1F 00 00 78 00 00 00 00 1F 00 00 BC 00 00 00 00 0F 00 00 BC 00 00 00 00 3F 00 00 FE 00
00 00 00 7F 00 00 FE 00 00 00 00 FF 00 00 9F 00 00 00 00 FF 00 00 FD C0 00 00 03 9F 00 00 DF E0 00 00 07 FF 00 00 FF F0 00 00 06 FF 00 00 FF DC 00 00 3E FF 00 00 FF FF 00 00 FD DF
00 00 FF FF 60 07 FB FF 00 00 FF FF FF BE BF FF 00 00 FF FF 7F 7F 3F FF 00 00 FF FF FF 75 FF FF 00 00}
        condition:
                all of them
}

rule magniber_icon_fractal : fractalicon
{
        strings:
                $icon = { 7B 49 5A FC 78 4B 59 FD D4 DC 87 FB D1 DB 86 FD D5 DD 86 FC D3 DC 87 FB AF 30 61 FC AD 30 63 FB AE 31 60 FF AF 31 61 FE AF 30 64 FE 09 F4 66 FE 08 F1 67 FD
43 3B 6A FC 07 F1 65 FB 07 F3 67 FE 2B DB 39 FE 09 F3 64 FC 07 F4 65 FE C0 D5 12 FB C1 D7 11 FC ED 14 08 FD F0 12 09 FD F1 12 07 FE F0 14 0B FD ED 15 0A FE F0 15 07 FC DC 15 9F FD
DE 15 9F FE DC 14 9E FE DC 16 9C FD CF 13 50 FE D1 12 51 FD 7F 2A 8F FD 7D 29 90 FC 3A 93 94 FC 3A 91 92 FE}
        condition:
                all of them
}
```

〈yararules to detect  Evil Bunny icons〉

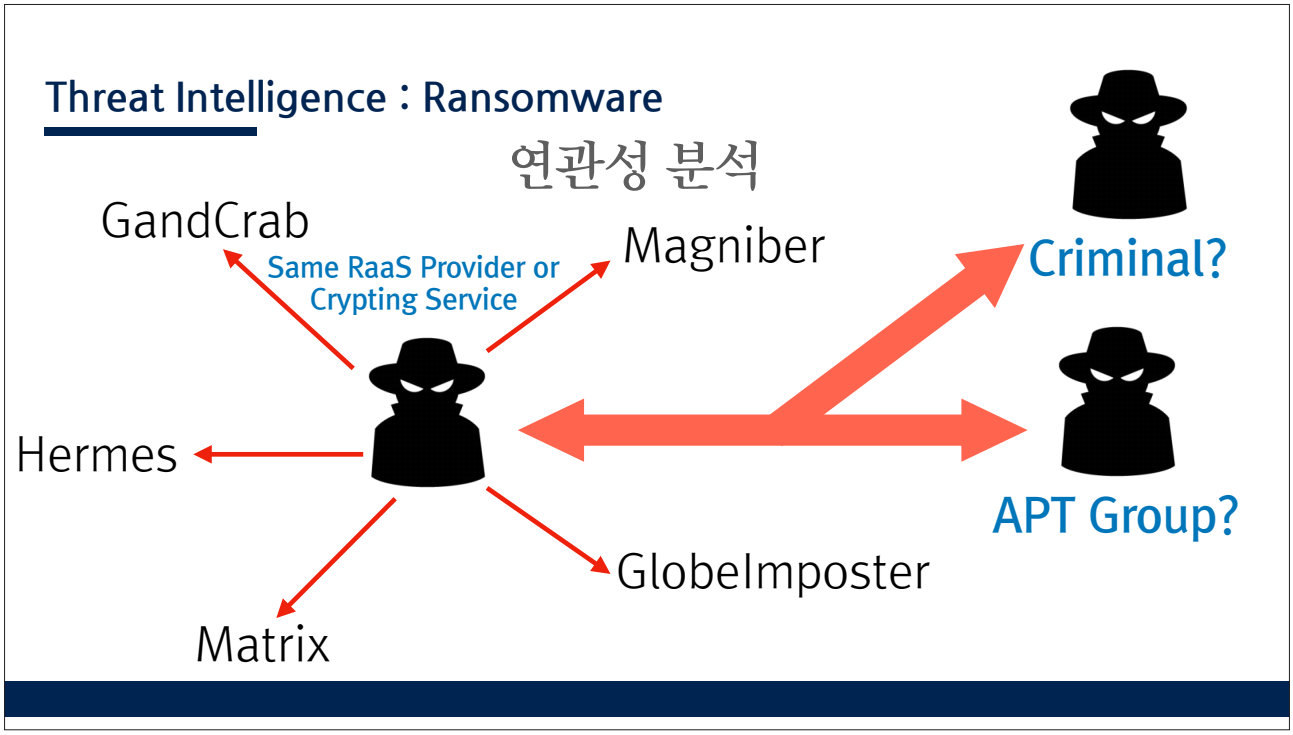
# 연관성 분석

## Threat Intelligence : Ransomware

icons




Retrohunting : 총 7,100개 탐지


Threat Intelligence : Ransomware
연관성 분석
GandCrab
Same RaaS Provider or
Crypting Service
Magniber
Criminal?
Hermes
APT Group?
GlobeImposter
Matrix

# 결론

## CONCLUSION

왜 우리는 지속적으로 같은 공격 그룹에게 당하고 있는가?

Q&A

감사합니다.

kjkwak@fsec.or.kr

The 24th Network Security Conference -Korea

# KOSIGN : 대용량 악성파일의 자동화 분석 플랫폼과 분석 대응 기술

**조학수** 윈스 전무

### 학력 및 경력사항

現 (주)윈스 전무이사/연구개발본부장
서울대학교 전산과학과 석사
서울대학교 계산통계학과 전산과학전공

### 강연요약

맥아피 Threat Report '17.12월 보고서에 따르면 '17년 3Q에 매일 200만 건의 신종 및 변종 악성파일이 등장하고 있다.

각 기관은 2003년 ISAC 출범이후 사이버위협대응센터를 운영하며 사이버 위협정보에 대해 자체 수집 및 분석, 정보 공유에 대한 필요성이 증대되고 있다. 하지만 폭증하는 악성코드에 대해 자체 분석하기에는 인력,자원이 턱없이 부족한 상황이다.

이에 효과적인 사이버위협 탐지/대응을 위해 자동화된 플랫폼을 도입하여 위협정보 분석하는 것이 현 상황을 타계하기 위한 방안이 될 수 있다. 또한 각 사이버위협대응센터는 자체 생산된 정보를 체계적으로 공유하기 위한 다자간 정보 공유체계를 구축하여 방어비용을 절감하는 것이 필요하다.

Global Leading Security

# KOSIGN: 위협정보 공유 및 대용량 악성파일 자동화 분석 플렛폼

All In Sniper

㈜윈스 연구소장 조학수

2018. 04. 13

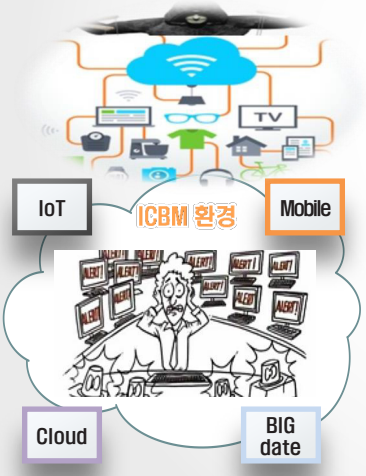
## 목 차

1. 배경소개
2. 위협정보 공유 표준
3. KOSIGN 프로젝트
4. CTI 플렛폼
5. Malware Analysis
6. Malware Labeling
7. KOSIGN 서비스
8. 향후 계획

# 1. 배경소개 - 보안기술 변화 요구

**다양한 보안장비에서 발생되는 위협 의심이벤트를 분석/대응하기에는 운용 효율성이 낮음**

새로운 사이버 위협 증가와
새로운 보안장비 도입에 대한
**운용관리 효율성 증대 요구**




**요구 01 보안 제품별 상이한 이벤트 통합**
보안 제품별 상이한 이벤트 생성 체계로 이벤트 통합 어려움

**요구 02 분리된 보안위협 관제 솔루션 통합**
다수의 보안 관제 솔루션으로 인한 운용관리 효율성 저하

**요구 03 새로운 보안 위협에 대한 신속한 인지**
Zero-Day 취약점에 대한 인지/대응 불가 현상

**요구 04 위협 분석/대응 효율화**
대량의 보안이벤트 분석 시간 부족, 부족한 분석으로 정확한 대응 어려움

**요구 05 자동화된 사이버 위협 대응 컨트롤 센터**
자동화된 수집/분석/대응 프로세서 구축을 통한 신속한 보안 체계 구축

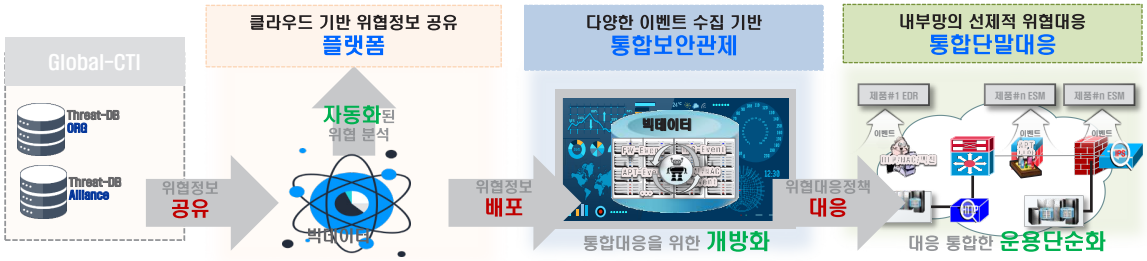

Copyright © 2017 All rights reserved by WINS co., Ltd.

# 1. 배경소개 - 차세대 보안

**실시간 방어 중심의 체계에서 피해 최소화를 위한 선제적 예방대응 중심으로 진화**

선제적 범죄 대응

**미래 보안 서비스 플랫폼 및 위협 대응 Flow**

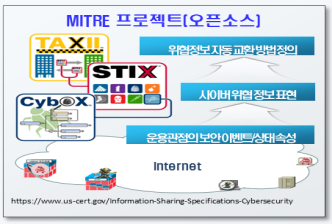


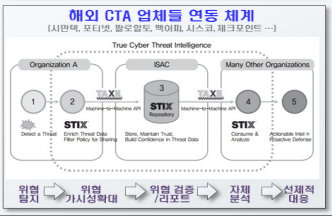


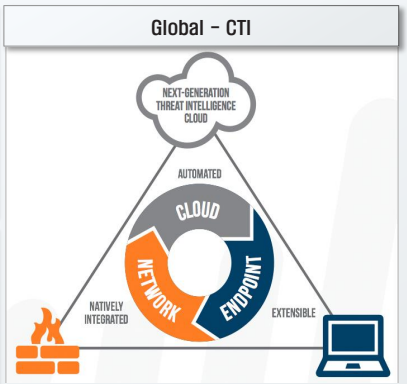
Copyright © 2017 All rights reserved by WINS co., Ltd.

# 1. 배경소개 - 위협정보공유 기술동향

## 해외



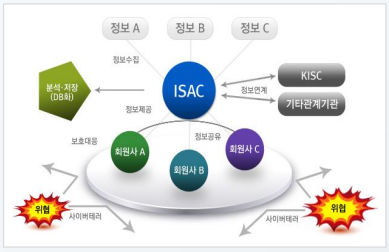




| | 업체 | Cloud기반 TI 서비스 |
|---|---|---|
| CTA 가입 벤더 | Symantec | DeepSight™ Intelligence |
| | 포티넷 | Security Fabric |
| | McAfee | Global Threat intellignece |
| | Palo Alto | WildFire |
| | Check Point | ThreatCloud |
| | Cisco | Talos |
| 기타 | HP | Threat Central |
| | IBM | X-Force Exchange |

**클라우드 위협정보 공유/협업 방식으로 제품 탐지 성능 향상**

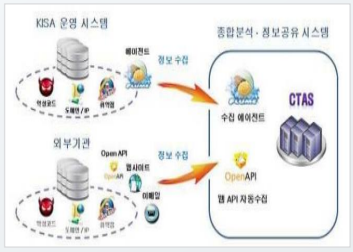
## 국내

### 금융/공공/국방 ISAC




2002 금융공유분석센터, 증권, 통신, 전력
취약점 정보 공유 및 대응

### KISA C-TAS




320 대응 2014년 8월 서비스
CTEX 포맷,

### 정보보호 산업계

- 위협정보DB는 기업의 경쟁력
  => **정보 공유의 어려움**
- STIX/TAXII 기술은 연구단계
  => **보안 기업들 위기감**

Copyright © 2017 All rights reserved by WINS co., Ltd.


# 1. 배경소개 - 해외 동향

**미국**

- 사이버정보공유법안(CISPA), 2011
  정보기관과 민간사이 사이버보안 위협시 '제한없는' 개인정보 공유
- 사이버보안법(CISA of 2015), 2015
  정보공유 협력 활성화 근거
  사이버위협정보 통합센터(CTIIC) 설립

**유럽**

- 유럽네트워크정보보안청(ENSIA) 설립, 2004
  사이버범죄 효과적 대응 초국가적 시스템
  사이버위협평가보고서 발간
- NATO 정보통신국 사이버보안데이터 교환협업기반(CDXI) 개발
  정보공유 기반시스템, 표준 호환

**일본**

- 사이버보안 기본법 제정, 2014
  사이버보안센터(NISC) 신설
  사이버보안전략 2015 발표

Copyright © 2017 All rights reserved by WINS co., Ltd.

# 2. 위협정보 공유 표준

## Cybersecurity information description specifications

| | |
|---|---|
| CVE | • Identifiers for Vulnerability information |
| CWE | • Identifiers for the software weakness type |
| CAPEC | • Identifiers for attack pattern information |
| CCE | • Identifiers for configuration issues |
| CPE | • Identifiers for IT assets such as software |
| OVAL | • Language on how to configure IT assets |
| CEE | • Language for describing computer events |
| MAEC | • Language for describing malware |


Copyright © 2017 All rights reserved by WINS co., Ltd.

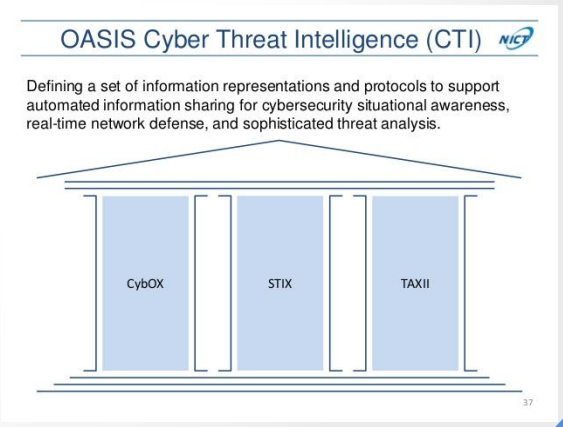
# 2. 위협정보 공유 표준

## Cybersecurity information sharing

Homeland Security

MITRE

MITRE's mission is to make it easier to secure American infrastructure, which they accomplish mostly through the release of excellent dictionary and metrics projects.





Copyright © 2017 All rights reserved by WINS co., Ltd.

# 2. 위협정보 공유 표준

**STIX**

- 사이버위협정보 표현 언어 (2013)
  STIX v2.0 확정(2017.10)

| 차이점 | 1.2 | 2.0 |
|---|---|---|
| One Standard | CybOX 미포함 | CybOX 포함 |
| Language | XML | JSON |
| Objects | 9 Data model objects | Domain object(SDO)<br>Relationship object(SRO) |
| Data markings | Xpath 사용 | Object marking<br>Granular marking |
| Indicator Pattern Language | XML 문법에 표현 | Pattern의 language 지정 |

**TAXI**

- 사이버위협정보 전송프로토콜 (2013)
  TAXII v2.0 확정(2017.10)
  JSON사용, HTTPS 암호화, 인증 지원

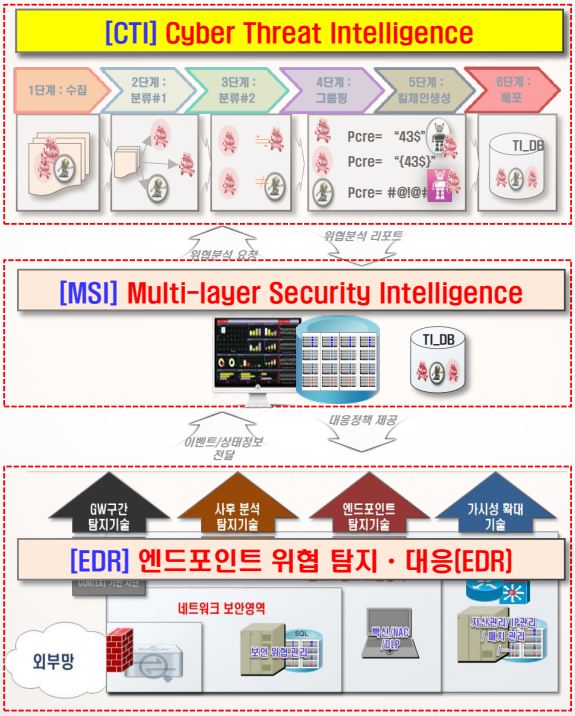
**CybOX**

- 말웨어 행위포함 증적 기술언어 (2012)
  Cyber observable은 상태 속성 또는 측정가능 한 이벤트
  STIX v2.0에 포함


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 3. KOSIGN 프로젝트

이기종 보안솔루션들의 효과적인 사이버위협 탐지 · 대응을 위한 KOSIGN 서비스 기술 개발

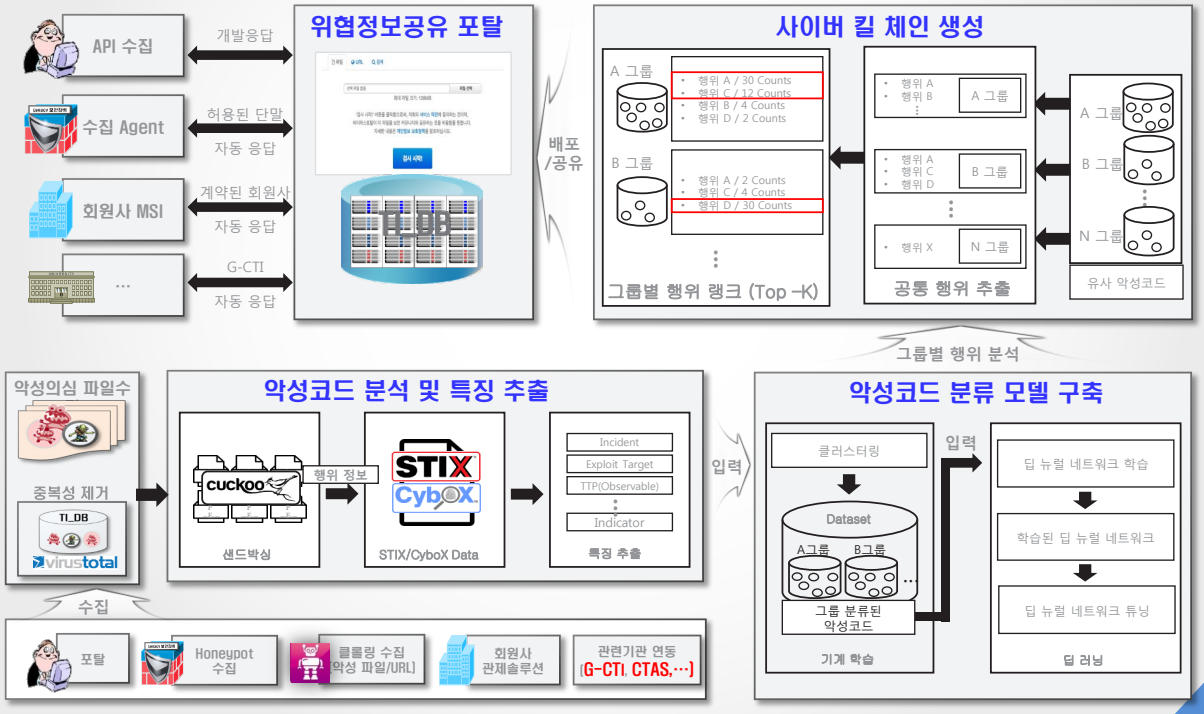



*. KOSIGN (Korea Open Security Intelligence Global Network) : 한국형 오픈 시큐리티 인텔리전스 공유 기술을 글로벌한 네트워크에 적용하기 위한 서비스 이름


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 4. CTI 플랫폼 - 개요

연동 및 자동 수집된 **사이버위협정보**를 정적/동적/유사도 분류 후 위협모델정보 **배포/공유** 하는 서비스



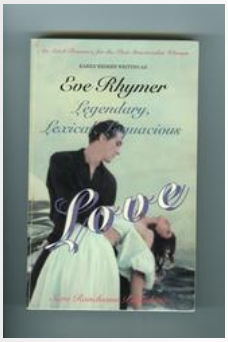


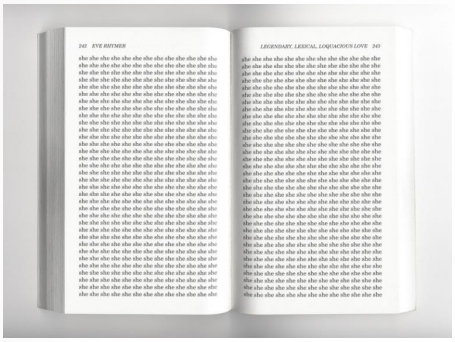

Copyright © 2017 All rights reserved by WINS co., Ltd.

# 5. Malware Analysys

## ◆ Bag of words

Karen Reimer"Legendary, Lexical, Loquacious Love",1996



- 로맨스 소설
- 알파벳순으로 등장횟수만큼 단어를 나열
- "her" 8페이지
- "his" 2.5페이지

"문학 작품에 대한 정량적 계측"

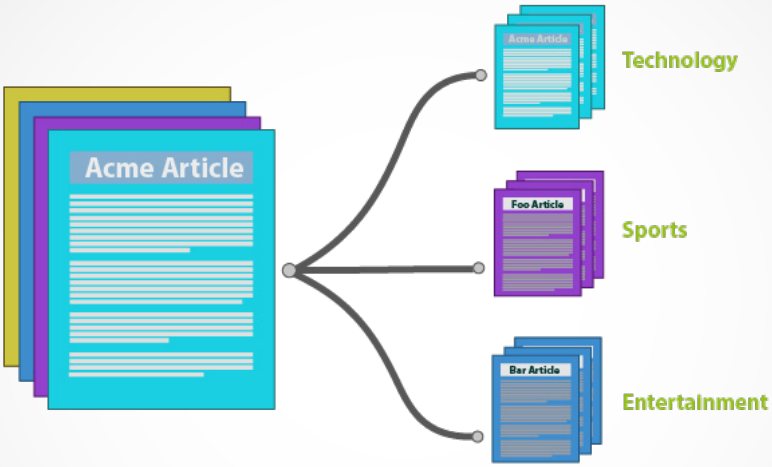
## ◆ 단어의 빈도로 소설 읽기



Copyright © 2017 All rights reserved by WINS co., Ltd.

# 5. Malware Analysys

## ◆ Text Classification & Malware




https://towardsdatascience.com/machine-learning-nlp-text-classification-using-scikit-learn-python-and-nltk-c52b92a7c73a

## ◆ 단어의 빈도수로 유사한 논문 분석할 수 있다면?

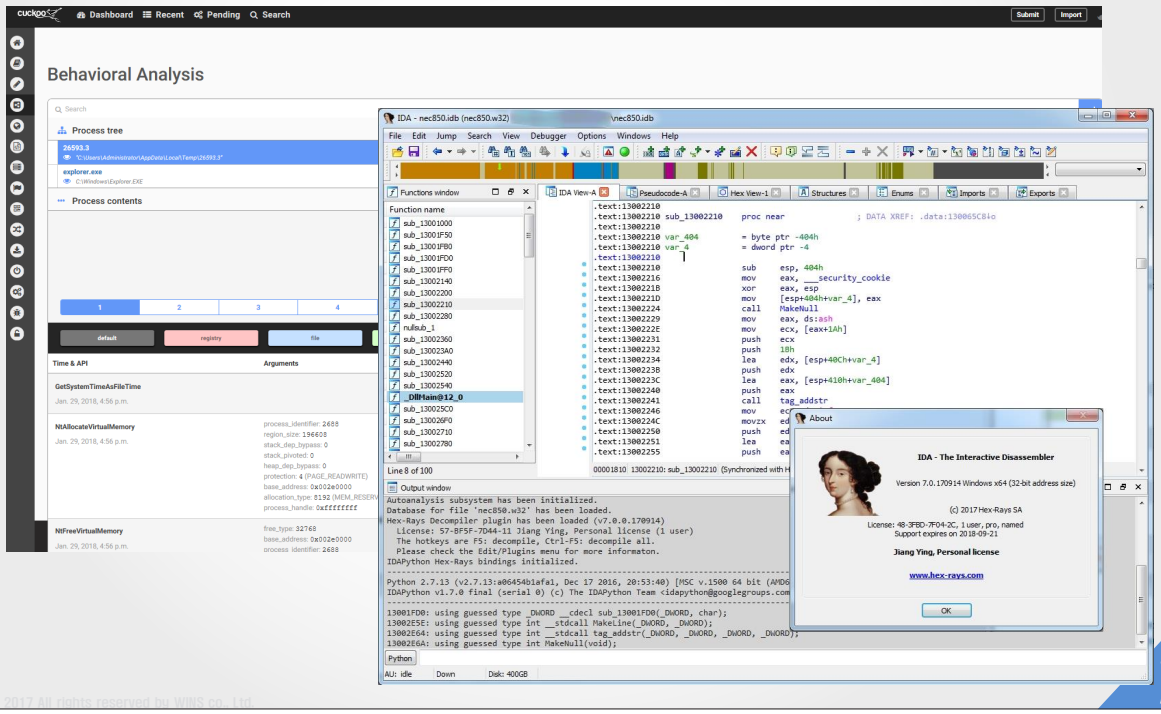

Copyright © 2017 All rights reserved by WINS co., Ltd.

# 5. Malware Analysys

## ◆ 악성코드의 단면

Cuckoo Behavioral analysis

IDA Pro

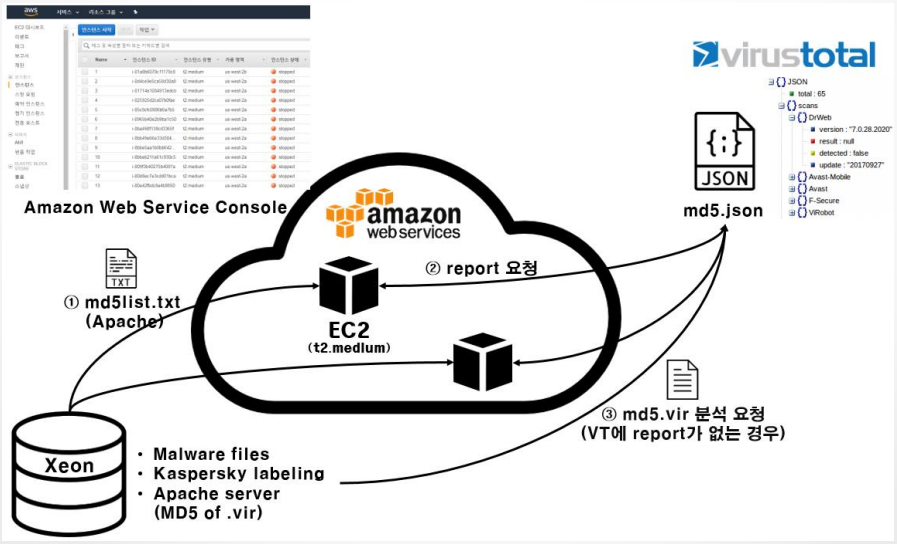




Copyright © 2017 All rights reserved by WINS co., Ltd.

# 6. Malware Labeling

- Malware Classification
  - Supervised Learning
  - Dataset 구성
  - Malware의 Label 과 Kaspersky labeling

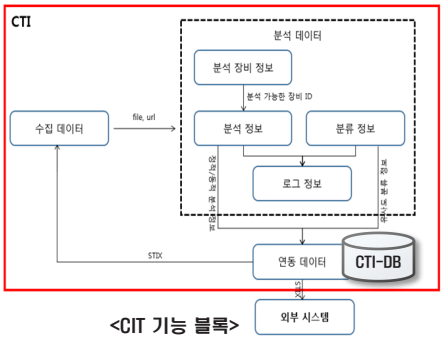




Copyright © 2017 All rights reserved by WINS co., Ltd.

# 6. Malware Labeling

- CTI 시스템 구조 및 위협정보 수집




<CIT 기능 블록>

| No. | 분류 | 수집채널 | 수집유형 | 정의 | 총 수집량 |
|---|---|---|---|---|---|
| 1 | 무료채널 | malshare | 악성파일 | 신규 출현 악성코드 공유정보 및 샘플 수집 | 75,868개 |
| 2 | | minotaur | 악성파일 | | 12,366개 |
| 3 | | vxvault | 악성파일 | | 2,308개 |
| 4 | | malc0de | 악성파일 | | 1,566개 |
| 5 | | C-TAS | 악성파일 | | 10,903개 |
| 6 | | | 악성URL | 악성코드 유포지 IP/Domain/URL 정보 | 2,832개 |
| 7 | 유료채널 | VirusSign | 악성파일 | 신규 출현 악성코드 공유정보 및 샘플 수집 | 7,003,113개 |
| 8 | 합계 | | | 전체 위협 정보 수집 합계 | 7,108,956개 |

<위협정보 수집 DB 내역 : 17년 12월 31일>

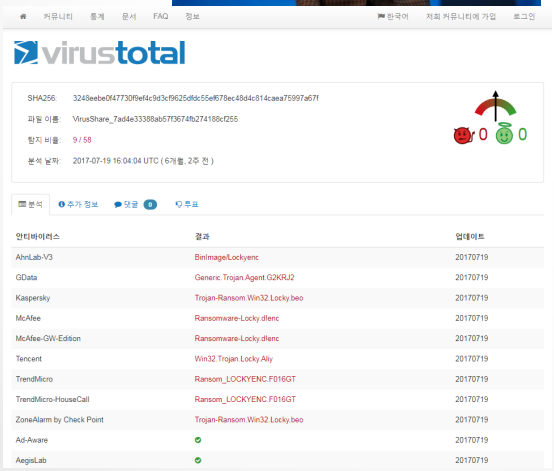
- 백신의 한계

Locky **유사도 99.98%**
https://www.virustotal.com/ko/file/3248eebe0f47730f9ef4c9d3cf9625dfdc55ef678ec48d4c814caea75997a67f/analysis/
NIMDA
https://www.virustotal.com/ko/file/3a120d08f33cd7a8fef7c61c70da6a5e858c195d2636a5999746925c900cfed8/analysis/
CAT-QuickHealTrojanPWS.ZBot20170201
https://www.virustotal.com/ko/file/37f8689b5e97eaf335cf5f63e5ceafb6ef5b88d8aff19bd68a450366655ee78a/analysis/


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 6. Malware Labeling

- Malware Labeling
  - 전문가
  - Kaspersky
  - Similarity Analysis
  - Expert & Expertee






http://blog.jpcert.or.jp/2017/03/malware-clustering-using-impfuzzy-a

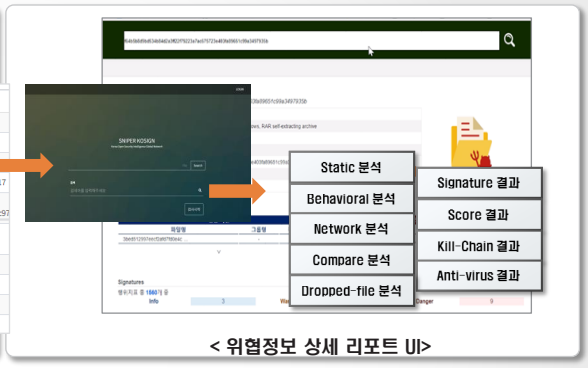


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 7. KOSIGN 서비스

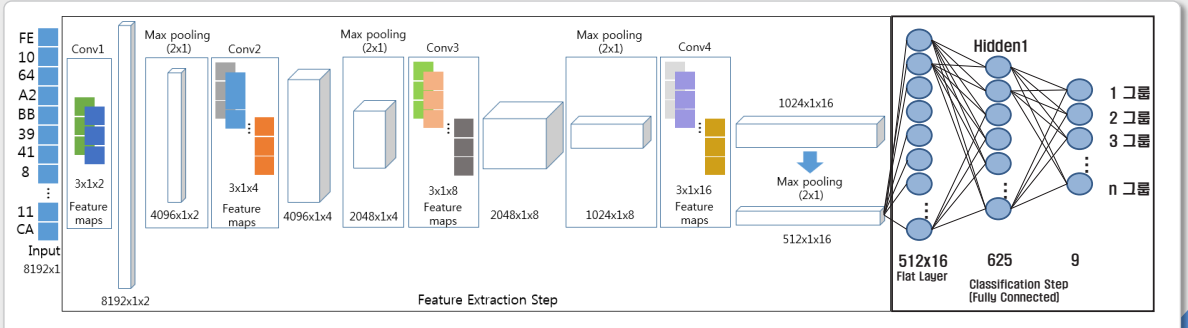
- CTI 서비스

<CTI 시스템 프로토타입 UI>




< 위협정보 상세 리포트 UI>

- 딥뉴럴 기반의 악성코드 유사도 그룹 분류 모델 알고리즘

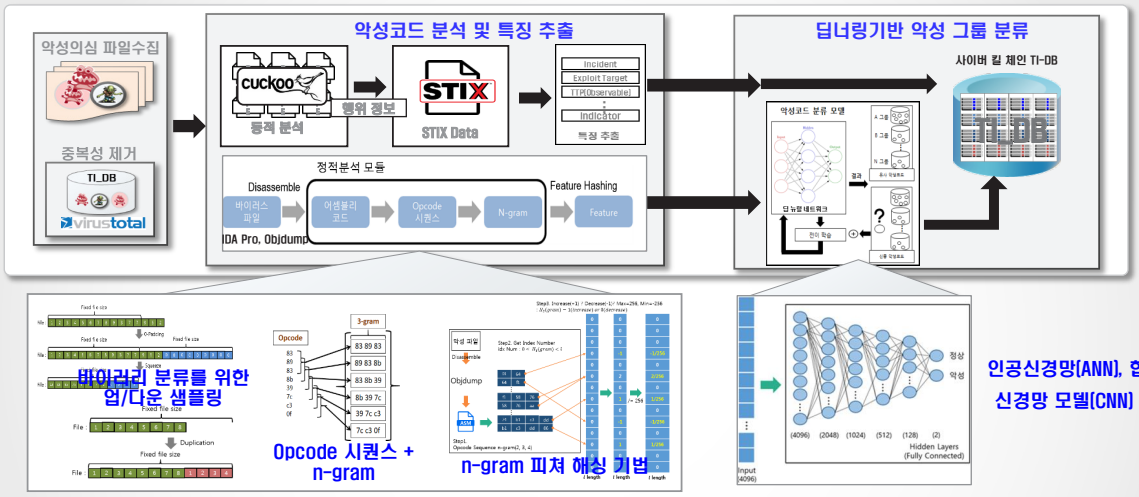





Copyright © 2017 All rights reserved by WINS co., Ltd.

# 7. KOSIGN 서비스

## ◆ 딥러닝 기반 악성코드 분류 모델




인공신경망(ANN), 합성곱 신경망 모델(CNN) 적용

## ◆ 악성코드 동작 분석 지표 추출 및 유사도 분류 성능

**악성 분류 특징**

- 바이러리 분류(고정크기 변환)
- 디스어셈블 분류(Opcode 시퀀스)
- 바이러스토탈 및 Kaspersky 진단명으로 라벨링한 지도학습

**타 기술과의 차이점**

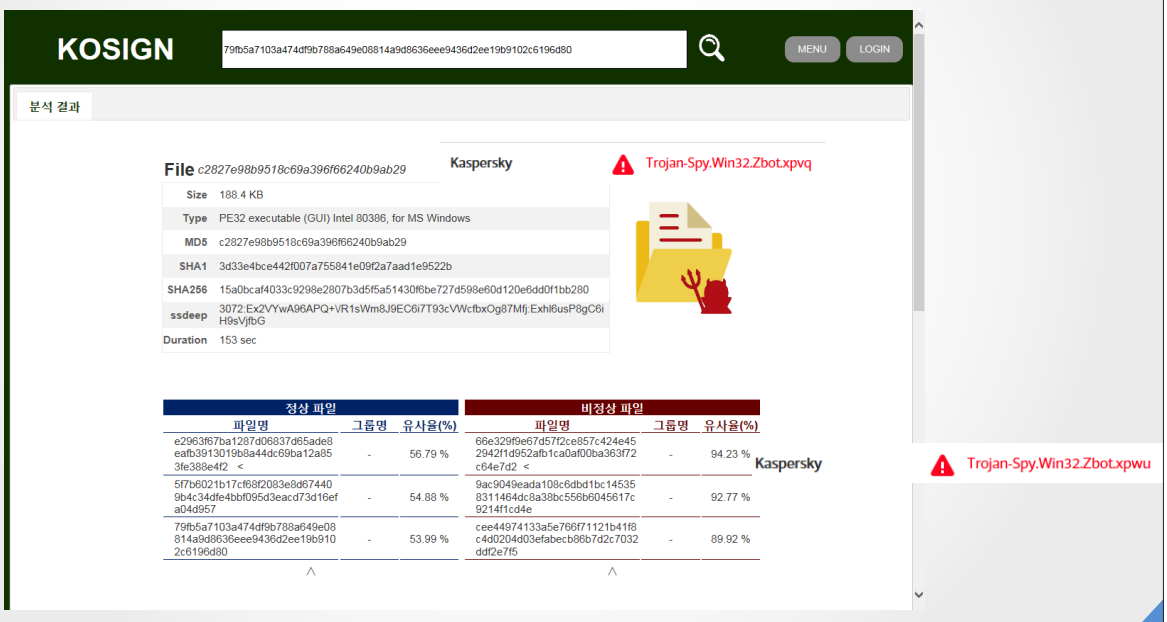
- 딥러닝 모델의 입력 벡터의 크기 제한으로 인한 **충돌 최소화하는 피쳐 해싱 기법** 적용
- **악성 파일 자체를** 이용하여 비교적 높은 분류 정확도 얻음(not 이미지 처리 방식)
  => 딥러닝 기술로 악성코드 분류 및 그룹핑의 가능성 확인
- **텐서플로우** 기반의 다양한 학습모델 적용하여 목표 성능 확보


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 7. KOSIGN 서비스 - 서비스 화면

## ◆ 알려지지 않은 악성코드

- Dynamic/Static Analysis 자료 DB 활용
- 행위 유사성 검증을 통한 유사한 정상파일, 악성파일 제시



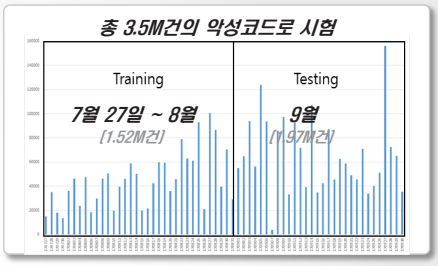


Copyright © 2017 All rights reserved by WINS co., Ltd.

# 7. KOSIGN 서비스 - 성능 검증

## ◆ 실제 분석되지 않은 악성코드를 이용하여 검증

- 바이러스사인(Virussign)의 3개월치 실제 악성코드 수집
- 수집 기간을 나누어 초기에 수집된 데이터로 학습한 모델이 나중에 수집된 악성코드에도 효과적으로 작동하는 것을 검증
  (학습 : 7.27 ~ 8.31 , 검증 : 9.01 ~ 9.30)




## ◆ 다양한 딥러닝 분류 모델 개발 및 실험 완료

- 학습모델 및 입력정보 기준 모델

| 학습모델 / 입력정보 | CNN (Convolutional Neural Network) | ANN (Artificial Neural Network) |
|---|---|---|
| 바이너리코드 | -장점: 별도 프로그램 불필요. 특징 자동 추출.<br>-단점: 입력 크기 고정화로 인한 정확도 하락 | N.A. |
| 어셈블리코드 | -장점: 실행코드 고유 특징 추출로 정확도 향상. 특징 자동 추출.<br>-단점: 별도의 디스어셈블 과정 필요. 복잡한 전처리 과정 필요 (n-gram, feature hashing) | -장점: 실행코드 고유 특징 추출로 정확도 향상.<br>-단점: 별도의 디스어셈블 과정 필요. 복잡한 전처리 과정 필요 (n-gram, feature hashing) |

- 주요 시험 환경

| | 운영체제 | Tensorflow | 기타 설치 SW | HW |
|---|---|---|---|---|
| 딥러닝 학습 및 테스트 | Windows 7 (64 bit) | 1.0.0 | -python 3.5.2<br>-anaconda3 4.2.0 | -CPU:Intel E3-1231<br>-MEM:DDR4 32GB<br>-GPU:1080Ti 1개 |
| 딥러닝 학습 및 테스트 | Windows 10 (64 bit) | 1.3.0 | -python 3.5.4<br>-anaconda3 4.2.0 | -CPU:Intel i7-6850k<br>-MEM:DDR4 64GB<br>-GPU:TITAN Xp 2개 |
| objdump 실행 | 우분투 16.04 LTS (64bit) | N.A. | -python 3.5.4<br>-objdump 2.26.1 | -CPU:Intel E5-2630<br>-MEM:DDR3 54GB |

| 모델 구분 | 입력형태 | 딥러닝 모델 | 모델 구조 | 정확도(%) | 데이터 셋(개) |
|---|---|---|---|---|---|
| Binary Classification | Binary file | CNN | -input:16384, output:2<br>-3 convolution Layer<br>-4 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax, max-pool | 96.4% | 학습(정상/악성) 35,078/1,517,011<br>검증(정상/악성) 8,769/1,955,392 |
| | Featuring hashing | ANN | -input:4096, output:2<br>-5 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax | 99.7% | 학습(정상/악성) 30,593/1,477,101<br>검증(정상/악성) 7,647/1,841,211 |
| | | CNN | -input:4096, output:2<br>-3 convolution Layer<br>-4 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax, max-pool | 98.0% | |
| Multi-class Classification (그룹 개수 : 29개) | Binary file | CNN | -input:16384, output:29<br>-3 convolution Layer<br>-4 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax, max-pool | 83.4% | 학습:1,517,011<br>검증:1,955,392 |
| | Featuring hashing | ANN | -input:4096, output:29<br>-5 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax | 88.4% | 학습: 1,477,101<br>검증: 1,841,211 |
| | | CNN | -input:4096, output:29<br>-3 convolution Layer<br>-4 Dense Layer<br>-0.7 Dropout<br>-Relu, softmax, max-pool | 83.7% | |

파일의 악성 유무 판단 정확도는 높은 것으로 판단됨

악성 특성을 통한 그룹핑 정확도를 높이기 위한 검색 기능 고도화 필요

## ◆ 연구 방향성 수립

- 대량의 악성코드 Training을 통한 빅데이터 기반 머신러닝 전처리 과정을 수행되면, **딥러닝 모델의 우수성 확인**
- 악성코드의 특성을 고려한 유사도 분석 중심의 검색 기능 개발 필요성 확인



Copyright © 2017 All rights reserved by WINS co., Ltd.

# 8. 향후 계획

## ◆ Expert-Expertise 모델에 의한 Malware Labeling

- 기존 Label은 백신 탐지명 의존
- Virus Total에 등록된 백신수 66종
- 66명의 전문가와 전문가가 생성한 Label
- Labeling에 유사도 분석 적용

## ◆ Multi-classification 정확도 향상

- Training Set과 Test Set의 Labeling 품질 강화
- Malware의 Static/Dynamic 유사도 강화학습 적용

## ◆ KOSIGN 서비스 공개

- 1000만건 Malware 수집 DB 연내 서비스
- 임의의 File 제공시 정상성 탐지, 가장 유사한 File 정보 제공
- Kill Chain 정보 제공



Copyright © 2017 All rights reserved by WINS co., Ltd.

감사합니다.

The 24th Network Security Conference -Korea

# 2017 정보보호 R&D 데이터 챌린지를 통해 살펴본 data-driven security

**김휘강** 고려대 교수

### 학력 및 경력사항

| | |
|---|---|
| 1994.03 ~ 1998.02 | KAIST 산업경영학과 학사 |
| 1998.03 ~ 2000.02 | KAIST 산업공학과 석사 |
| 2000.03 ~ 2009.02 | KAIST 산업및시스템공학과 박사 |
| 1999.08 ~ 2004.04 | 에이쓰리시큐리티컨설팅 창업자, 대표컨설턴트 |
| 2004.05 ~ 2010.02 | 엔씨소프트 Technical Director, 정보보안실장 |
| 2010.03 ~ 현재 | 고려대학교 정보보호대학원 부교수 |
| 2016.03 ~ 2017.02 | University of Canterbury, New Zealand 방문교수 |

### 강연요약

최근 정보보안 분야에 AI, machine learning을 접목하여 사람이 일일히 대응하기 어려웠던 분야들을 빠르게 자동화 해나가고 있으며, 정확도를 향상시키고 있다. 하지만, 이러한 AI, machine learning 기술을 접목하기 위해서는 양질의 data 가 필요하다.

이에, 2017년에 국내에서 최초로 정보보호학회와 KISA 공동으로 "정보보호 R&D 데이터 챌린지"를 개최한 바 있다. (http://datachallenge.kr)

이 대회에서 실제 데이터셋을 이용하여 어떠한 방식으로 대회가 이루어졌으며, 참가팀들의 주요 결과물들은 어떠하였는지 소개한다. 또한 data에 기반하여 machine learning 을 응용하여 악성코드/악성앱 탐지, 침입탐지를 구현하고자 하는 연구자들이 알아두면 도움될 만한 기법들을 소개하고자 한다.

## About me

### 김휘강

- KAIST 재학시절 KUS, SPARCS, Security KAIST 동아리 활동 (1994~)
- A3 Security Consulting 창업/CEO (1999.8~2002.4), CTO (~2004.4)
- NCSOFT 정보보안실장 (2004.5~2010.2)
- 고려대학교 정보보호대학원 부교수 (2010.3~현재)

- 주요 논문 실적
  - International Conferences: NDSS 2016, WWW (2014, 2017, 2018)
  - International Journals: IEEE Trans. On Information Forensics and Security (2017), Computer & Security (2016), Digital Investigation (2015)

- https://blog.hksecurity.net


©2018. 해킹대응기술연구실

## Main Research Area

- **Data-driven security**
  - Online Game Security
    - Game Bot, Gold-Farmer Group Detection and Prevention
    - In-game Fraud Detection
    - Pirate Server Detection and Prevention
  - Fraud Detection System
    - Internet Portal, Banking, Online Game Service
  - Network and System Security
    - Intrusion Detection with data mining and machine learning
    - Malware Analysis (Cyber Genome) – Mal-Netminer, API-MDS
    - App. Security Analysis - Andro-Profiler, Andro-Tracker, Andro-AutoPsy, Andro-Dumpsys, SAPIMMDS
  - Dataset
    - http://ocslab.hksecurity.net/Datasets


©2018, 해킹대응기술연구실


## 고려대학교 해킹대응기술연구실 (ocslab.hksecurity.net)

국내최초

국내 최초 Cyber-Genome Project 구현

악성코드, 해커/해킹그룹, 해킹사건 별 연관성 분석에 대한 구현 및 시연, IEEE CNS 2016 발표

**Malware analysis 관련 연구**

Andro-Profiler, Andro-Tracker, Andro-dumpsys 등 악성코드 분석 시스템을 개발/구축하고 정보보안 분야 유수 저널에 다수 게재

Social Network Analysis 분석 기법을 Malware Analysis 분석에 응용(Mal-Netminer)

논문실적

다수의 우수 국제학회 및 저널 논문 실적 보유

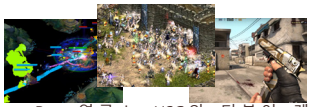
전산/보안 분야에서 **세계 최고 수준의 학회로 분류되는 WWW, NDSS에 논문을 지속적으로 게재** 중인 연구 그룹

정보보안 분야 최고수준의 국제 저널 **IEEE TIFS(Transactions on Information Forensics and Security) 등 다수의 국제 저널 논문 실적** 보유

HCRL
Hacking and Countermeasure Research Lab

세계 3대

온라인 게임 분야 세계 3대 연구 그룹



Xerox Parc 연구소, USC와 더불어 게임 유저들의 행위 분석과 게임 내 부정행위 탐지 관련 **온라인 게임 분야 세계 3대 연구 그룹임, WWW conference 에 논문을 지속적으로 게재 중**

해킹/보안 관련 기술력 보유

온라인게임, 웹사이트 등 취약점 확인을 위한 **시스템 해킹, 웹 해킹 프로젝트 다수 경험**

악성코드 분석을 통한 **리버싱 기술, 악성 행위 분석 기술 보유**

**해커 출신 및 현장 실무 경험**을 통한 수준급 해킹/보안 기술력 보유


©2018, 해킹대응기술연구실

# CONTENTS

I. 정보보호 R&D 데이터 챌린지 개요
II. 차량 이상징후 탐지
III. 모바일 악성앱 탐지

## I. 정보보호 R&D 데이터 챌린지 2017 개요

- 운영 일정
- 운영 방식
- 운영 위원회


©2018, 해킹대응기술연구실

# 2017년 정보보호 R&D 데이터 챌린지

## 국내 "최초" 데이터 챌린지 대회

- 2017 정보보호학회 동계학술대회와 연계하여 한국정보보호학회, 한국인터넷진흥원이 공동으로 개최한 대회
- 자동차보안, 악성앱 탐지 챌린지는 고려대학교 해킹대응기술연구실에서 출제, 운영
  - **홈페이지:** http://datachallenge.kr/
  - **주최:** 한국정보보호학회, 한국인터넷진흥원
  - **주관:** 고려대학교 해킹대응기술연구실, 한국인터넷진흥원(이하 키사)
  - **후원 기관**
    - 상금 후원: Ncsoft, Saint Security, EEDIOM, Penta Security
    - 상품 후원: AWS, 보안프로젝트, 카카오
      - 참가신청한 학생들은 전원 AWS Educate를 제공함

[정보보호 R&D 데이터 챌린지 본선대회 사진]


©2018, 해킹대응기술연구실


# 2017년 정보보호 R&D 데이터 챌린지

## 운영 방식

- 온라인 예선, 오프라인 본선으로 진행됨
  - 예선에 총 181팀(372명)이 지원했으며, 제출팀 중 상위 7팀을 본선 진출자로 선정함
    - 모바일 악성앱 탐지(35%, 63팀) → 악성코드 탐지(28%, 51팀) → 차량 이상징후 탐지(27%, 48팀), 악성코드 선제대응(10%, 19팀)

**온라인 예선** (2017.10.18~11.29)
- **4개 트랙 오픈**
  - 고려대학교, 키사가 각 2개의 트랙을 운영
- **홈페이지에서 신청**
  - 개인, 팀(최대 5인)으로 신청
  - 트랙 다중 신청 가능
- **각 트랙별 결과물 제출**
  - 트랙 특성에 따라 트랙별 결과물은 상이함

**예선결과 심사** (2017.11.30~12.03)
- **제출물 심사**
- **제출물 검증**
- **상위 7팀 선정**
  - 7팀 미만의 트랙일 경우, 지원자 모두 본선 진출
  - 잘못된 양식, 낮은 정확도의 제출팀은 제외

**본선진출자 발표** (2017.12.04)
- **홈페이지에 공지**
- **진출 팀 수**
  - 고려대학교
    - 모바일 악성앱 탐지 5팀 진출
    - 차량 이상징후 탐지 6팀 진출
  - 키사
    - 악성코드 탐지 7팀 진출
    - 악성코드 선제대응 2팀 진출

**오프라인 본선** 판교 KISA 정보보호 클러스터 (2017.12.08)
- **해커톤 방식**
- **운영방식**
  - 본선 진출자들은 하루동안 총 2번 새로운 데이터셋을 전달받음
  - 주어진 시간내에 *데이터 분석 → 알고리즘 개선 → 정확도 향상*을 반복함
    - 오전세션 / 오후세션
    - 각 세션마다 제출기회는 3번*
    - 가장 마지막에 제출한 정확도가 최종 정확도임

*차량 이상징후 탐지는 2번임

**수상** 고려대학교 미래융합관 (2017.12.09)
- **트랙별 상위 2개팀 수상**
  - 정확도(1차, 2차 각 50%) 70%, 발표 30%
- **수상자**
  - 차량 이상징후 탐지
    1위: CANDIS
    2위: SUNY Korea
  - 모바일 악성코드 탐지
    1위: 고려대&연세대
    2위: ASAP
  - 악성코드 탐지
    1위: 정성균
    2위: SKY의 K는 국민대
  - 악성코드 선제대응
    2위: Team IDK*

* 악성코드 선제대응은 2위(장려상)만 시상함


©2018, 해킹대응기술연구실

## 2017년 정보보호 R&D 데이터 챌린지

### 트랙 전체 요약

**(KISA) 악성코드 선제대응 챌린지**

- 백신사 제공 300개 지능형 악성코드
- 자유 기술경쟁(악성코드 공격/방어 기술)
- 1위 KISA 원장상(상금 300만원)

**(KISA) 악성코드 탐지 챌린지**

- 백신사, KISA 정상·악성코드 3만개
- 악성코드 탐지율 경쟁
- 1위 KISA 원장상(상금 300만원)

**(고려대) 차량 이상징후 탐지 챌린지**

- 자동차 정상·공격 네트워크 트래픽
- 자동차 공격 탐지 성능 경쟁
- 1위 정보보호학회 회장상(상금 300만원)

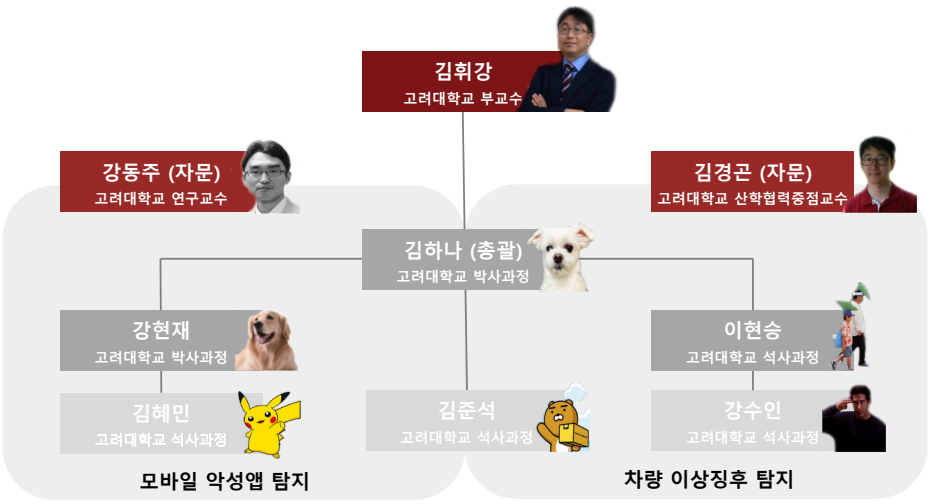
**(고려대) 악성앱 탐지 챌린지**

- 모바일 정상·악성 앱 8천개
- 모바일 악성 앱 탐지율 경쟁
- 1위 NC소프트 대표이사상(상금 300만원)

HCRL ©2018, 해킹대응기술연구실


## 2017년 정보보호 R&D 데이터 챌린지

### 운영 위원회




HCRL ©2018, 해킹대응기술연구실

# II. 차량 이상징후 탐지

- 개요
- 참가자 통계
- 데이터셋 수집 및 구성
- 챌린지
- 평가방법 및 결과
- 최종순위
- 수상자 산출물 요약

HCRL ©2018, 해킹대응기술연구실


## 차량 이상징후 탐지

### 개요

| | 예선 | 본선 |
|---|---|---|
| 진행방식 | • 제공된 데이터셋 분석<br>• 탐지 알고리즘 개발<br>• 시각화 프로그램 개발 | • 하루동안 총 2번의 세션으로 진행됨<br>- 세션별 새롭게 제공된 데이터셋 분석 →<br>1차 성능평가(테스트) → 탐지 알고리즘 개선 →<br>2차 성능평가(테스트) 순으로 진행됨<br>• 차량과 유사한 환경을 제공하기위해 소켓프로그램을 이용하여 CAN 패킷을 전달함<br>• 참가자들은 실시간으로 CAN 패킷을 받아 이상징후를 탐지해야함<br>- 분석용 데이터셋 제공<br>- 세션별 2번의 테스트 기회를 제공 (소켓프로그램) |
| 데이터셋 | • 차량 네트워크 데이터셋 (65분) | • 차량 네트워크 데이터셋 (각 10분)<br>• 총 6개의 데이터셋이 제공됨<br>- 각 세션마다 3개의 데이터셋이 제공됨<br>- 분석용, 테스트1, 테스트2 |
| 공격 유형 | • DoS<br>• Fuzzy | • DoS<br>• Fuzzy<br>• Replay |

HCRL ©2018, 해킹대응기술연구실

# 차량 이상징후 탐지

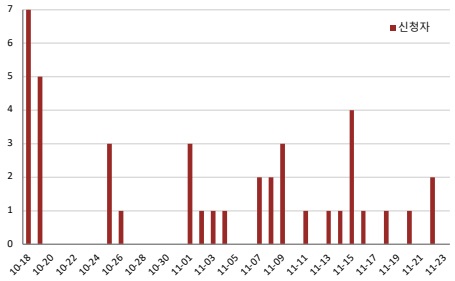
## 참가자 통계

□ 예선 참가자
- 48팀(103명)이 신청함
  - 4개 트랙중 3번째(26.52%)로 신청함
- 대학(원)생 → 기업&일반인 →고등학생&연구기관&기타 순으로 신청함

□ 본선 진출자
- 진출팀 중 상위 6개팀을 진출시킴
  - 진출팀 중 아래 조건의 팀들은 제외함
    - 제출팀 중 제출포맷이 제시한 포맷과 다를 경우
    - 기준 정확도보다 낮을 경우

| 유형 | 고등학생 | 대학(원)생 | 기업 | 연구기관 | 일반인 | 기타 | 총 합계 |
|---|---|---|---|---|---|---|---|
| 개인 | 1 | 8 | 4 | 1 | 9 | 2 | 25 |
| 팀 | 1(3) | 14(50) | 3(10) | 1(2) | 3(9) | 1(4) | 28(78) |
| **합계** | **2(4)** | **22(58)** | **7(14)** | **2(3)** | **12(18)** | **3(6)** | **48(103)** |

[소속별 신청건수]



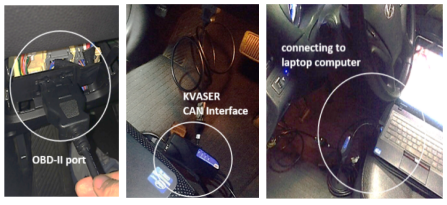

[일자별 신청건수 그래프]


©2018, 해킹대응기술연구실


# 차량 이상징후 탐지

## 데이터 수집 방법

□ 실제 차량의 CAN 트래픽 수집
- 연구실 차량을 이용하여 "DoS, Fuzzy, Replay"공격이 포함된 데이터를 추출함
  - 차량 2대(차종 A, 차종B)를 이용하여 수집
- 본 챌린지 문제에 기초가 된 참고문헌
  - Hyunsung Lee, Seong Hoon Jeong and Huy Kang Kim, *"OTIDS: A Novel Intrusion Detection System for In-vehicle Network by using Remote Frame"*, PST (Privacy, Security and Trust) 2017
  - Song, Hyun Min, Ha Rang Kim, and Huy Kang Kim. *"Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network."* Information Networking (ICOIN), 2016 International Conference on. IEEE, 2016.
- 정보보호 R&D 데이터 챌린지 본선에서 활용한 데이터셋은 공유됨
  - 키사 정보보호 R&D 데이터셋: https://www.kisis.or.kr/kisis/subIndex/283.do
  - 해킹대응기술연구실: http://ocslab.hksecurity.net/Datasets/ku-cisc2017-otids




[데이터 추출 방법]

```
Timestamp: 1481192898.075465        ID: 0587    000    DLC: 8    00 00 00 00 00 00 00 01
Timestamp: 1481192898.076242        ID: 0316    000    DLC: 8    05 1c 6a 0a 1c 13 00 7f
Timestamp: 1481192898.076480        ID: 018f    000    DLC: 8    00 21 1c 00 00 43 00 00
Timestamp: 1481192898.076712        ID: 0260    000    DLC: 8    05 1c 00 30 ff 93 63 35
Timestamp: 1481192898.076952        ID: 0080    000    DLC: 8    00 17 6a 0a 1c 13 1c 1f
Timestamp: 1481192898.077190        ID: 0081    000    DLC: 8    4d 84 5d 00 00 00 00 2f
Timestamp: 1481192898.077477        ID: 02a0    000    DLC: 8    62 00 5d 9d c2 0c b7 02
Timestamp: 1481192898.077653        ID: 0329    000    DLC: 8    85 a8 80 8c 11 2d 00 10
Timestamp: 1481192898.077901        ID: 0382    000    DLC: 8    40 fe 0f 00 00 00 00 00
Timestamp: 1481192898.078149        ID: 04b1    000    DLC: 8    00 00 00 00 00 00 00 00
Timestamp: 1481192898.078396        ID: 0164    000    DLC: 8    00 08 00 00 00 00 05 0d
Timestamp: 1481192898.078637        ID: 0370    000    DLC: 8    ff 20 00 80 ff 00 00 ec
Timestamp: 1481192898.078873        ID: 043f    000    DLC: 8    10 50 64 ff 51 54 09 00
Timestamp: 1481192898.079115        ID: 0440    000    DLC: 8    ff f0 00 00 ff 54 09 00
Timestamp: 1481192898.079357        ID: 04f2    000    DLC: 8    00 00 90 38 00 00 00 a1
Timestamp: 1481192898.079597        ID: 0110    000    DLC: 8    e0 3c 30 09 00 00 00 00
```

[추출된 데이터셋 예시]


©2018, 해킹대응기술연구실

# 차량 네트워크 데이터셋

## 차량 주행 데이터셋

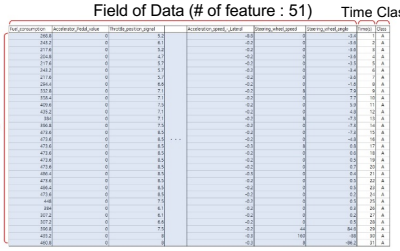
□ 주행 시 차량에 OBD-II 스캐너를 연결하여 주행 데이터를 추출

- Features : 51개(차량속도, 스티어링 휠 각도, 연료소모량, 미션오일 온도 등 추출 가능한 전체 feature) + Time + Class (운전자 10명을 A ~ J로 레이블링)
  - 차량 : KIA Soul
  - 전체 주행 시간 : 약 24시간
  - 전체 레코드 수 : 94,401개
  - 한번 주행 시 (왕복) : 약 46km

주행구간 (고려대학교 - 상암월드컵경기장)

Field of Data (# of feature : 51) Time Class

Data



데이터 샘플


©2018, 해킹대응기술연구실


# 차량 네트워크 데이터셋

## 차량 해킹 데이터셋

□ 자동차 CAN 네트워크에 대한 메시지 주입 공격 데이터셋

- OBD-II 포트를 통해 위조 메시지를 주입
  - 각 데이터셋은 300회의 주입 공격이 포함된 30~40분 동안의 CAN 트래픽 데이터
  - 1회 주입 공격은 3~5초 동안 진행됨
- Data Attributes
  - Timestamp, CAN ID, DLC, DATA, Flag

| Attack Type | # of Messages | # of normal Messages | # of injected Messages |
|---|---|---|---|
| DoS Attack | 3,665,771 | 3,078,250 | 587,521 |
| Fuzzy Attack | 3,838,860 | 2,759,492 | 1,079,368 |
| Spoofing the drive gear | 4,443,142 | 2,766,522 | 1,676,620 |
| Spoofing the RPM gauge | 4,621,702 | 2,290,185 | 2,331,517 |

데이터셋에 포함된 메시지 개수

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1478195722.75262 | 02a0 | 8 | 4 | 0 | 99 | 1d | 97 | 2 | bd | 0 | R |
| 1478195722.75842 | 430 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | R |
| 1478195722.76639 | 02b0 | 5 | ff | 7f | 0 | 5 | 2f | R | | | |
| 1478195722.76924 | 350 | 8 | 5 | 20 | 74 | 68 | 78 | 0 | 0 | 41 | R |
| 1478195722.77513 | 00df | 8 | 8c | ab | f2 | 26 | 7a | 29 | 1a | 0c | T |
| 1478195722.77595 | 06ea | 8 | 25 | 10 | 9c | ed | 5b | 16 | 2c | 18 | T |
| 1478195722.78009 | 02fd | 8 | 3f | bd | 68 | f3 | c3 | 4f | 28 | d4 | T |
| 1478195722.78639 | 02b0 | 5 | ff | 7f | 0 | 5 | c1 | R | | | |
| 1478195722.79094 | 370 | 8 | 0 | 20 | 0 | 0 | 0 | 0 | 0 | 0 | R |
| 1478195722.79640 | 02b0 | 5 | ff | 7f | 0 | 5 | f2 | R | | | |
| 1478195722.79845 | 430 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | R |
| 1478195722.79868 | 04b1 | 8 | 29 | 27 | 27 | 23 | 0 | 0 | 0 | 9a | R |
| 1478195722.79893 | 01f1 | 8 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | R |
| 1478195722.79914 | 012d | 8 | 35 | 45 | 99 | cf | 9 | 80 | c7 | 77 | T |
| 1478195722.79939 | 153 | 8 | 0 | 21 | 10 | ff | 0 | ff | 0 | 0 | R |

데이터 샘플


©2018, 해킹대응기술연구실

# 차량 네트워크 데이터셋

## CAN 침입 공격 데이터셋

- 정상 상황 (Attack Free) [2,369,868개]
  - 공격이 전혀 없는 정상 상황에서의 CAN 메시지 데이터셋
  - 공격 메시지는 없지만 탐지 노드에서 전송하는 원격 프레임이 0.01초 간격으로 전송됨
- DoS 공격 [656,579개]
  - 공격자는 다른 메시지를 무력화 시키기 위해 매우 빠른 주기로 0x000의 메시지를 주입함
  - 탐지 노드는 간격과 사이 시간을 측정하기 위해 특정 ID에 대한 원격 프레임을 전송
- Fuzzy 공격 [591,990개]
  - 공격자는 차량에서 사용되는 ID를 수집하여 차량 내 기능이 있는 ID에 대해 임의의 데이터 값을 삽입하여 주입하는 공격
- 위장 노드 공격 [995,472개]
  - 특정 타겟 노드를 선정하여 해당 노드에서 전송하는 메시지를 삭제하고 이를 대신하는 노드를 공격자가 삽입하는 공격
  - 해당 노드는 일반 노드와 같이 주기적으로 메시지를 전송하며 원격 프레임을 수신 시 응답으로 데이터 프레임을 전송


©2018, 해킹대응기술연구실


# 차량 이상징후 탐지

## 데이터셋 구성

- KU-CISC2017-OTIDS 1st ~ 4th
  - 차량 공격시도 패킷이 포함된 차량 네트워크 데이터셋
    - 예선: DoS+Fuzzy, 차종A
    - 본선: 1차(DoS+Fuzzy, 차종A), 2차(DoS+Fuzzy+Replay, 차종B)

| 구분 | 사용용도 | 데이터셋 KU-CISC2017-OTIDS | 공격 유형 | 공격 포인트 | 시간(분) | 차종 | 난이도 |
|---|---|---|---|---|---|---|---|
| 예선 | 분석 및 테스트용 | 1st | DoS Fuzzy | 20 | 65 | A | 중 |
| 본선 | 사전셋팅용 | Pre-setting | 無 | 無 | 2 | B | 無 |
| | 1차 분석용 | 2nd | DoS Fuzzy | 20 | 10 | A | 중 |
| | 1차 1회 테스트 | 2nd-test-1 | | | | | |
| | 1차 2회 테스트 | 2nd-test-2 | | | | | |
| | 2차 분석용 | 3rd | DoS Fuzzy Replay | 20 | 10 | B | 중 |
| | 2차 1회 테스트 | 3rd-test-1 | | | | | |
| | 2차 2회 테스트 | 3rd-test-2 | | | | | |
| | 예비 1회 테스트 | 4th-test-1 | DoS Fuzzy Replay | 20 | 10 | B | 상 |
| | 예비 2회 테스트 | 4th-test-2 | | | | | |

[데이터셋 구성표]


©2018, 해킹대응기술연구실

# 차량 이상징후 탐지

## 챌린지

### 차량 네트워크 이상징후 탐지 알고리즘 구현 및 시각화 프로그램 개발

**사례**

최근에 큰 마음을 먹고 자동차를 구매한 H씨는
최근 자동차 해킹이 빈번하게 시도되고 있다는 뉴스를 접하게되어
자신이 구매한 자동차에 대해서도 공격이 시도되고 있는지 K대학교 연구실에
데이터 분석 의뢰를 하였습니다. K대학교 연구실에서 분석한 결과 메시지 삽입 공격이
이뤄지고 있는 것을 발견하였습니다.
**차량 내 CAN (Controller Area Network) 프로토콜은 버스에 흐르는 메시지에 대한 검증 과정이 존재하지 않기때문에 공격자는 악의적인 명령을 위해 CAN 버스에 임의의 메시지를 삽입하더라도 차량은 메시지의 이상 여부를 측정할 수 없습니다.**
차량 공격으로는 정상 메시지를 지연시키거나 전송되는 것을 막는 도스(DoS) 공격,
차량이 이상 행위를 하도록 하는 퍼지(Fuzzy) 공격,
정상 메시지를 일정 기간 동안 덤프하여 그대로 삽입하는 재사용(Replay) 공격이
이루어질 수 있습니다.
**위 상황과 같은 공격이 시행될 때 운전자와 차량의 안전을 위해 이상 징후를 탐지할 수 있는 IDS가 필요한 실정입니다.**

**문제**

문제데이터셋을 분석하여 아래 사항을
**실시간으로 탐지**할 수 있는
**이상징후 탐지 알고리즘과**
**시각화 프로그램**을
제시해주시기 바랍니다.

- DoS / Fuzzy / Replay attack

**제출물**

- **프로그램**
  - GitHub 링크 제출 (Public 링크)
- **결과파일**
- **알고리즘 설명 문서**
- **시각화 프로그램 데모영상**
  - Youtue 영상 링크
  - 10분이내에 공격유형이 모두 포함

http://datachallenge.kr/challenge17/car/challenge/



# 차량 이상징후 탐지

## 평가방법 (F1-score)

□ F1-score

- Positive, Negative가 편향될 수 있어 Precision과 Recall의 조화평균으로 평가하는 방법

| 카테고리 | | 실제결과 | |
|---|---|---|---|
| | | Positive | Negative |
| 실험결과 | Positive | *True Positive(TP)* | *False Positive(FP)* |
| | Negative | *False Negative(FN)* | *True Negative(TN)* |

- True Positive는 실제 True를 True로 정확하게 예측한 상황을 의미함
- True Negative는 실제 False를 False로 정확하게 예측한 상황을 의미함
- False Positive는 실제 False을 True로 예측한 상황을 의미함 (오탐)
- False Negative는 실제 True를 False로 예측한 상황을 의미함 (미탐)

$$Precision = \frac{TP}{TP + FP} \qquad Recall = \frac{TP}{TP + FN} \qquad F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

- Precision은 정확률로서 제안한 알고리즘이 공격을 판단했을때 실제 공격이 이루어진 비율을 나타냄
- Recall은 재현율로서 실제 공격이 이루어졌을때 제안된 알고리즘이 공격을 판단하는 비율을 나타냄

# 차량 이상징후 탐지

## 평가결과

□ 예선에서 공동 5위를 한 CANDIS팀이 본선에서는 1위를 함

**예선**

신청건수: • 48팀(103명) 지원

본선 진출팀 정확도

| 순위 | 팀명 | 팀 유형 | F1-Score |
|---|---|---|---|
| 1위 | SUNY Korea | 팀(4명) | 100.00 |
| 2위 | 아주 | 개인 | 87.50 |
| 3위 | SEINT | 팀(4명) | 82.35 |
| 4위 | CapcorpsCert0188 | 팀(5명) | 80.00 |
| 5위 | CANDIS | 팀(3명) | 78.57 |
| 5위 | EPL | 팀(4명) | 78.57 |

**본선**

진출팀수: • 6팀(21명) 진출
• 아주팀은 중도 포기함

정확도

오전 세션

| 순위 | 팀명 | 팀 유형 | F1-Score |
|---|---|---|---|
| 1위 | CANDIS | 팀(3명) | 89.47 |
| 1위 | SUNY Korea | 팀(4명) | 89.47 |
| 3위 | CapcorpsCert0188 | 팀(5명) | 78.89 |
| 4위 | EPL | 팀(4명) | 0 |
| 4위 | SEINT | 팀(4명) | 0 |
| 6위 | 아주 | 개인 | 중도포기 |

오후 세션

| 순위 | 팀명 | 팀 유형 | F1-Score |
|---|---|---|---|
| 1위 | CANDIS | 팀(3명) | 100 |
| 2위 | SUNY Korea | 팀(4명) | 90 |
| 3위 | EPL | 팀(4명) | 88.89 |
| 4위 | CapcorpsCert0188 | 팀(5명) | 72.73 |
| 5위 | SEINT | 팀(4명) | 43.48 |
| 6위 | 아주 | 개인 | 중도포기 |


©2018, 해킹대응기술연구실


# 차량 이상징후 탐지

## 본선 최종 순위

□ 평가요소
- 예선 F1-score는 포함되지 않음
- F1-score와 발표점수는 7:3 비율로 계산
  - 각 세션별 F1-score는 5:5 비율로 계산

□ 수상팀
- 1위 CANDIS 팀
  - Ncsoft 대표이사상 수상
  - 상금(300만원), 상품(카카오 후디 라이언 1개)
- 2위 SUNY Korea 팀
  - 장려상 수상
  - 상금(200만원), 상품(카카오 대형 얼굴 쿠션 1개, 보안 프로젝트 저자 사인도서 1권)

[수상자 수상 모습]

| 구분 | CANDIS | SUNY Korea | Capcorps Cert0188 | EPL | SEINT | 아주 |
|---|---|---|---|---|---|---|
| 1차 정확도 | 89.47 | 89.47 | 78.89 | 0 | 0 | - |
| 2차 정확도 | 100 | 90 | 72.73 | 88.89 | 43.48 | - |
| 최종 정확도 점수 | 94.74 | 89.74 | 75.81 | 44.45 | 21.74 | - |
| 발표점수 | 83.75 | 84.25 | 73.25 | 88.25 | 74.25 | - |
| **최종점수** | **91.44** | **88.09** | **75.04** | **57.59** | **37.49** | **-** |

[최종 점수 정리표]

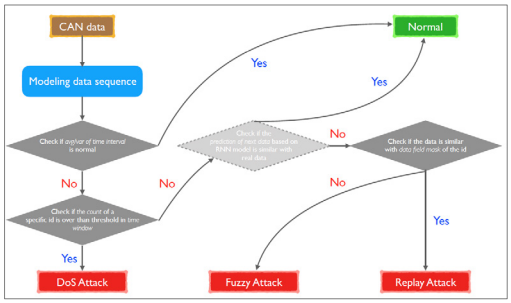

©2018, 해킹대응기술연구실

# 차량 이상징후 탐지

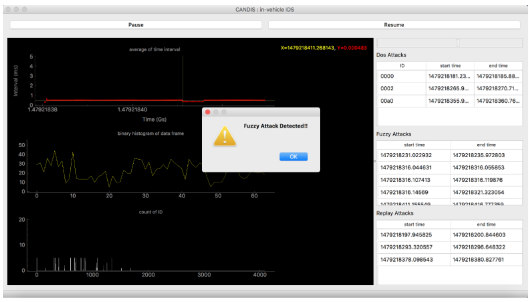
## 1위: CANDIS

□ 방법론(Deep Learning)

- 데이터 분석 통해 아래와 같은 사항들을 확인함
  - 각 ID는 발생빈도가 고정되어 있기 때문에 정상적인 패킷의 빈도는 일정함
  - 공격시, 특정 ID와 데이터가 포함된 패킷이 고정된 주기를 벗어나 발생하며, 일부 ID의 sequence가 변경됨
- RNN(Recurrent Neural Network) 알고리즘을 기반한 Data sequence modeling 기법을 이용하여 차량 이상징후를 탐지함




[방법론]




[개발한 시각화 프로그램]

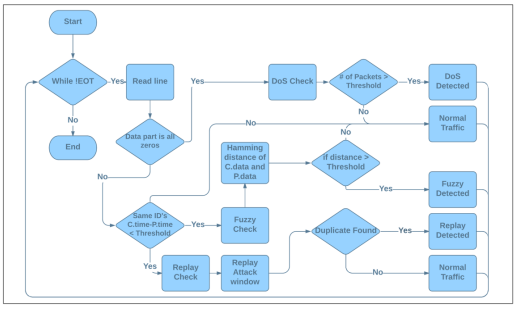


# 차량 이상징후 탐지

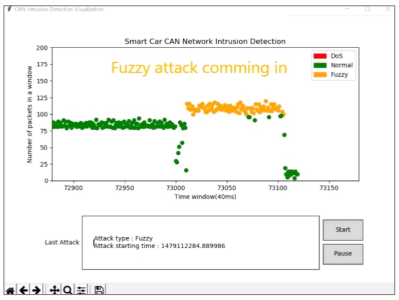
## 2위: SUNY Korea

□ 방법론(Threshold)

- 데이터셋 분석 및 시각화 프로그램을 통해 공격시, 빠른 주기와 많은 양이 데이터가 주입되는것을 확인함
  - DoS 공격의 경우, 지연시키기 위하여 모든 데이터가 00으로 구성됨
- 이를 기반으로, window당 데이터 수가 threshold 값을 넘으면, 공격으로 탐지함
  - Threshold 값을 넘으면, 공격으로 판단하고 데이터에 모두 0이 포함되어 있지 않으면 Fuzzy 공격유무를 확인함




[방법론]




[개발한 시각화 프로그램]

# III. 모바일 악성앱 탐지

- 개요
- 참가자 통계
- 데이터셋 수집 및 구성
- 챌린지
- 평가방법 및 결과
- 최종순위
- 수상자 산출물 요약

HCRL ©2018, 해킹대응기술연구실


## 모바일 악성앱 탐지

### 개요

| | 예선 | 본선 |
|---|---|---|
| 진행방식 | • 온라인제공된 데이터셋 분석<br>• 악성앱 탐지 및 패밀리 분류 알고리즘 개발 | • 하루동안 총 2번의 세션으로 진행됨<br>- 세션별 새롭게 제공된 데이터셋 분석 → 성능평가 → 탐지 알고리즘 개선을 세션시간동안 반복함<br>• 참가자들은 새로운 패밀리가 추가된 데이터셋에서 악성앱을 탐지해야함<br>- 분석용 데이터셋을 제공(추가된 악성앱 30개)<br>- 세션별 3번 테스트 기회를 제공 |
| 데이터셋 | • 정상앱(1,500개) + 악성앱(500개) / 패밀리유형 10개<br>- 정답지가 포함된 분석용 데이터셋<br>- 정답지가 미포함된 제출용 데이터셋 | • 정상앱(750개) + 악성앱(250개) / 패밀리유형 15개<br>• 총 4개의 데이터셋이 제공됨<br>- 각 세션마다 2개의 데이터셋이 제공됨<br>- 분석용(추가된 악성앱 각 30개), 제출용 |
| 공격 유형 | • 패밀리 10종 | • 패밀리 15종(예선에 없던 5개의 패밀리가 추가됨) |

HCRL ©2018, 해킹대응기술연구실

# 모바일 악성앱 탐지

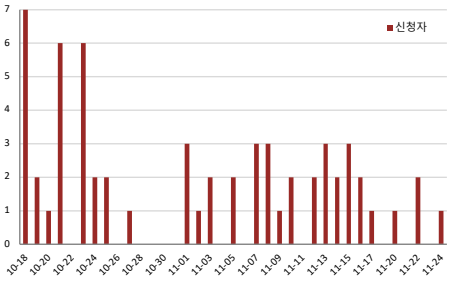
## 참가자 통계

□ 예선 참가자
- 63팀(126명)이 신청함
  - 4개 트랙중 제일 많이(34.81%) 신청함
- 대학(원)생 → 일반인 → 기업 → 기타 → 고등학생 → 연구기관 순으로 신청함

□ 본선 진출자
- 진출팀 중 상위 5개팀을 진출시킴
  - 진출팀 중 아래 조건의 팀들은 제외함
    - 제출팀 중 제출포맷이 제시한 포맷과 다를 경우
    - 기준 정확도보다 낮을 경우

| 유형 | 고등학생 | 대학(원)생 | 기업 | 연구기관 | 일반인 | 기타 | 총 합계 |
|---|---|---|---|---|---|---|---|
| 개인 | 1 | 15 | 4 | 1 | 12 | 2 | 35 |
| 팀 | 1(3) | 14(43) | 8(31) | 0(0) | 4(12) | 1(2) | 28(91) |
| **합계** | **2(4)** | **29(58)** | **12(35)** | **1(1)** | **16(24)** | **3(4)** | **63(126)** |

[소속별 신청건수]




[일자별 신청건수 그래프]


©2018, 해킹대응기술연구실


# 모바일 악성앱 탐지

## 데이터 수집 방법

□ 프로젝트 제공, 수집한 모바일 악성앱과 정상앱
- 연구실 내 소유하고 있는 모바일 악성앱과 정상앱으로 데이터셋을 구성함
  - 연구실 프로젝트에서 제공받은 악성앱, 정상앱
  - 연구실에서 수집(악성앱 공유 사이트, 구글 플레이스토어)한 악성앱, 정상앱
  - 기간: 2011년 ~ 2015년

- 본 챌린지 문제에 기초가 된 참고문헌
  - Jae-wook Jang, Hyunjae Kang, Jiyoung Woo, Aziz Mohaisen, and Huy Kang Kim, *"Andro-AutoPsy: Anti-malware system based on similarity matching of malware and malware creator-centric information,"* Digital Investigation, vol. 14, pp. 17–35, 2015.

- 정보보호 R&D 데이터 챌린지 예선, 본선에서 활용한 데이터셋은 공유됨
  - 공유된 데이터셋을 이용하여 예선, 본선 데이터셋을 랜덤하게 구성함
  - 키사 정보보호 R&D 데이터셋: https://www.kisis.or.kr/kisis/subIndex/283.do
  - 해킹대응기술연구실: http://ocslab.hksecurity.net/Datasets/ku-cisc2017-otids


©2018, 해킹대응기술연구실

# 모바일 악성앱 탐지

## 데이터셋 구성

□ KU-CISC2017-AutoPsy 1st ~ 5th

- 모바일 악성앱, 정상앱을 혼합한 데이터셋
  - 예선: 패밀리 유형 10개
    - 패밀리 분류 시 유형 및 패밀리명 통일을 위하여 정답지가 포함된 분석용 데이터셋을 추가로 제공함
    - 제출시에는 정답지가 없는 제출용 데이터셋을 사용한 결과를 제출해야함
  - 본선: 1차(패밀리 유형 2종 추가), 2차(패밀리 유형 3종 추가)
    - 새로운 패밀리가 제공되기 때문에 각 패밀리마다 30개씩 분석용 데이터셋을 제공함

| 구분 | 사용용도 | 데이터셋 KU-CISC2017-AutoPsy | 정상앱 | 악성앱 | 패밀리수 | 패밀리 분배 | 총개수 |
|---|---|---|---|---|---|---|---|
| 예선 | 분석용 | 1st | 1,500 | 500 | 10 | 50 | 2,000 |
| | 제출용 | 2nd | 1,500 | 500 | 10 | 50 | 2,000 |
| 본선 | 1차 분석용 | 3rd-sample | - | 60 | 2 | 30 | 60 |
| | 1차 제출용 | 3rd | 750 | 250 | 12 | 랜덤 | 1,000 |
| | 2차 분석용 | 4th-sample | - | 90 | 3 | 30 | 90 |
| | 2차 제출용 | 4th | 750 | 250 | 15 | 랜덤 | 1,000 |
| | 예비용 | 5th | 600 | 200 | 15 | 랜덤 | 800 |

[데이터셋 구성표]

| 구분 | | No. | 패밀리명 |
|---|---|---|---|
| 예선 | | 1 | AdWo |
| | | 2 | AirPush |
| | | 3 | Boxer |
| | | 4 | Counterclank |
| | | 5 | Dowgin |
| | | 6 | Gappusin |
| | | 7 | OpFake |
| | | 8 | SMSAgent |
| | | 9 | SMStado |
| | | 10 | Wapsx |
| 본선 | 1차 | 11 | Kuguo |
| | | 12 | Ropin |
| | 2차 | 13 | Kmin |
| | | 14 | SmsPay |
| | | 15 | Youmi |

[챌린지에서 사용한 패밀리명]

©2018, 해킹대응기술연구실


# 모바일 악성앱 탐지

## 챌린지

### 안드로이드 악성앱 탐지 및 분류를 위한 알고리즘 개발

**사례**

최근 최신형 안드로이드 모바일 폰을 구매한 K씨는 안드로이드 마켓에서 한 브라우저 앱을 다운 받았습니다.
그로부터 며칠 후 **K씨는 본인이 알지 못하는 휴대전화 결제 요금이 청구**된 것을 알게 되었습니다.

알고보니 예전에 다운로드 받았던 브라우저 앱은 '프리미엄 SMS'로 불리는 악성코드로, 특정 사이트에 휴대폰 결제 SMS를 전송하여 프리미엄 요금이 부과된 것이었습니다.
위 상황과 같이 **정상 안드로이드 앱으로 위장한 악성 앱은 구글 안드로이드 마켓, 서드파티 마켓, 블랙 마켓 등의 다양한 경로로 배포되고 있어, 악성 앱을 효율적으로 탐지하는 방안이 필요한 실정입니다.**

**문제**

제공된 대용량의 안드로이드 앱 데이터셋을 기반으로 아래 사항을 탐지 및 분류할 수 있는 알고리즘 및 프로그램을 제시하시기 바랍니다.

- **정상 앱과 악성 앱 구분**
- **악성 앱에 한하여 유형(패밀리) 분류**

**제출물**

- **프로그램**
  - GitHub 링크 제출 (Public 링크)
- **결과파일**
- **알고리즘 설명 문서**

http://datachallenge.kr/challenge17/andro/challenge/

©2018, 해킹대응기술연구실

# 모바일 악성앱 탐지

## 평가방법 (정확도)

□ Accuracy

| 카테고리 | | 실제결과 | |
|---|---|---|---|
| | | Malware | Benign |
| 실험결과 | Malware | *True Positive(TP)* | *False Positive(FP)* |
| | Benign | *False Negative(FN)* | *True Negative(TN)* |

$$\text{악성앱 탐지 } Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- True Positive는 실제 Malware(True)를 Malware(True)로 정확하게 예측한 상황을 의미함
- True Negative는 실제 Benign(False)를 Benign(False)로 정확하게 예측한 상황을 의미함
- False Positive는 실제 Benign(False)을 Malware(True)로 예측한 상황을 의미함 (오탐)
- False Negative는 실제 Malware(True)를 Benign(False)로 예측한 상황을 의미함 (미탐)

| 카테고리 | 패밀리 | 패밀리수 | 실제결과 | |
|---|---|---|---|---|
| | | | 일치 | 비일치 |
| 실험결과 | Family 1 | $T_1$ | $A_1$ | $B_1$ |
| | Family 2 | $T_2$ | $A_2$ | $B_2$ |
| | ... | ... | ... | ... |
| | Family n | $T_n$ | $A_n$ | $B_n$ |

$$\text{패밀리 분류 } Accuracy = \frac{A_1 + A_2 + \cdots + A_n}{T_1 + T_2 + \cdots + T_n}$$


©2018, 해킹대응기술연구실


# 모바일 악성앱 탐지

## 평가결과

□ 본선 정확도 순위는 예선 정확도 순위와 동일함

**예선**

신청건수: • 63팀(126명) 지원

본선 진출팀 정확도

| 순위 | 팀명 | 팀 유형 | Accuracy |
|---|---|---|---|
| 1위 | ESTsoft | 팀(2명) | 96.34 |
| 2위 | 고려대&연세대 | 팀(2명) | 94.38 |
| 3위 | ASAP (Android Static Analysis Platform) | 팀(2명) | 90.46 |
| 4위 | 시큐베이스 | 팀(2명) | 78.16 |
| 5위 | 대만간 기사님 | 팀(4명) | 53.82 |

**본선**

진출팀수: • 5팀(12명) 진출
• ESTsoft팀은 불참함

정확도

오전 세션

| 순위 | 팀명 | 팀 유형 | Accuracy |
|---|---|---|---|
| 1위 | 고려대&연세대 | 팀(2명) | 91.08 |
| 2위 | ASAP | 팀(2명) | 88.88 |
| 3위 | 시큐베이스 | 팀(2명) | 87.68 |
| 4위 | 대만간 기사님 | 팀(4명) | 0 |
| 5위 | ESTsoft | 팀(2명) | 불참 |

오후 세션

| 순위 | 팀명 | 팀 유형 | Accuracy |
|---|---|---|---|
| 1위 | 고려대&연세대 | 팀(2명) | 91.76 |
| 2위 | ASAP | 팀(2명) | 88.52 |
| 3위 | 시큐베이스 | 팀(2명) | 87.86 |
| 4위 | 대만간 기사님 | 팀(4명) | 51.36 |
| 5위 | ESTsoft | 팀(2명) | 불참 |


©2018, 해킹대응기술연구실

# 모바일 악성앱 탐지

## 본선 최종 순위

□ 평가요소
- 예선 정확도는 포함되지 않음
- 정확도와 발표점수는 7:3비율로 계산
  - 각 세션별 정확도는 5:5 비율로 계산

□ 수상팀
- 1위 고려대&연세대 팀
  - 정보보호학회 회장상
  - 상금(300만원), 상품(카카오 후디 라이언 1개)
- 2위 ASAP 팀
  - 장려상 수상
  - 상금(200만원), 상품(카카오 대형 얼굴 쿠션 1개, 보안 프로젝트 저자 사인도서 1권)

[수상자 수상 모습]

| 구분 | 고려대&연세대 | ASAP | 시큐베이스 | 대만간 기사님 | ESTsoft |
|---|---|---|---|---|---|
| 1차 정확도 | 91.08 | 88.88 | 87.68 | 0 | - |
| 2차 정확도 | 91.76 | 88.52 | 87.86 | 51.36 | - |
| 최종 정확도 점수 | 91.42 | 88.70 | 87.77 | 25.68 | - |
| 발표점수 | 77.5 | 68.25 | 69.75 | 37 | - |
| **최종점수** | **87.24** | **82.57** | **82.36** | **29.08** | **-** |

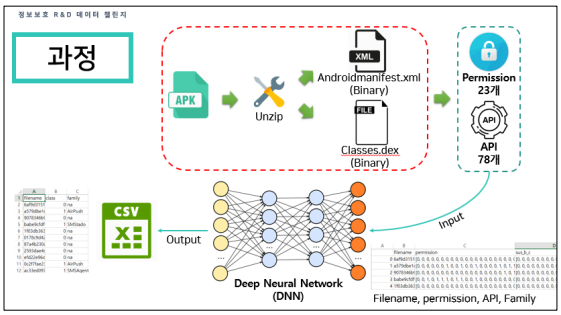
[최종 점수 정리표]


©2018, 해킹대응기술연구실

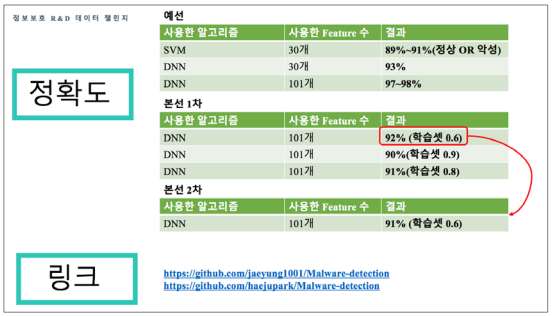

# 모바일 악성앱 탐지

## 1위: 고려대&연세대

□ 방법론(Deep Learning)
- 데이터셋 분석 후 AndroidManifest.xml 파일에서 Permission, 소스코드에서 API 정보가 유의미할 것이라 판단
- 자체 제작한 파싱 프로그램을 이용하여 API, Permission 정보를 추출
- API 78개, Permission 23개 feature를 선택한 후 DNN(Deep Neural Network)을 이용하여 악성앱을 탐지함



[방법론(수상자 발표자료)]



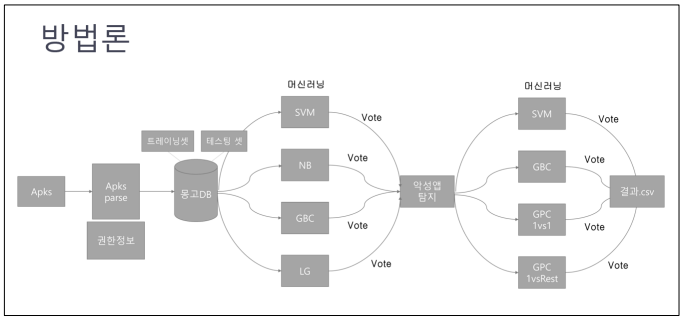
[정확도(수상자 발표자료)]


©2018, 해킹대응기술연구실

## 모바일 악성앱 탐지

### 2위: ASAP(Android Static Analysis Platform)

- 방법론(Machine Learning)
  - APK parse를 이용하여 정보를 파싱한 후 json 형태로 몽고DB에 적재
    - AndroidManifest.xml 정보를 파싱하여 위험한 권한이 있는지 확인함
    - Classes.dek에서 Class와 method를 추출하여 Permission과 연관된 API가 사용되었는지 확인함
  - 악성앱에서 악용될 수 있는 위험한 Permission 138개를 feature로 선택
  - 4개의 Machine Learning 알고리즘(SVM, NB, GBC, LG)의 결과를 도출하여 악생앱 탐지
  - 탐지한 악성앱들 중 위험한 Permission들을 그룹화 하여 악성앱 패밀리 분류




[방법론]



## Lesson learned

### 국내 data-driven security 의 준비도를 높여나가야 함

- 정보보안 + AI/Machine Learning 교육

### Dataset 공유 문화

- Project, 논문 등에 1회성으로 쓰이고 사장되는 데이터가 없도록
- 모든 기술논문은 "재현가능" 해야 함을 전제로 데이터 공유에 적극 나서야 함

### Citation + motivation + compensation

- Dataset 을 제작하고 공유하는 것에 대한 가치 인정

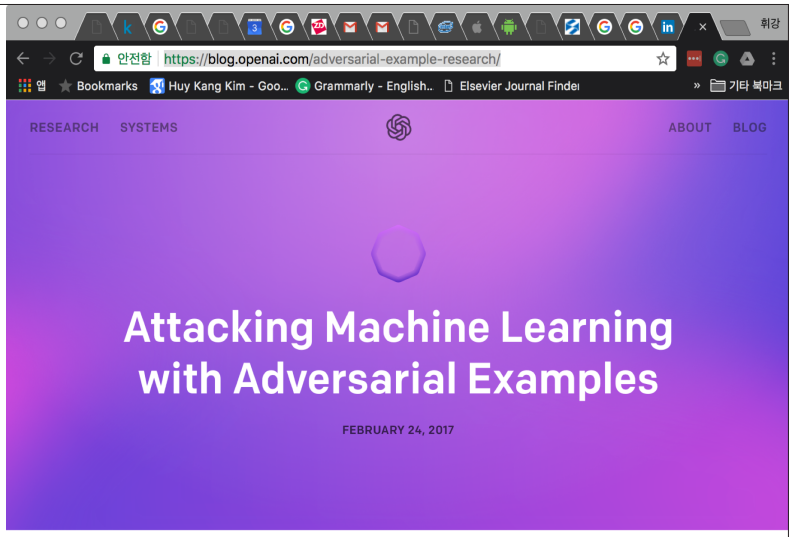
### Kaggle 과 같이 대회에 활용된 데이터셋의 상시 운영

- 교육과 연계

## Lesson learned

**Adversarial machine learning 등으로 data challenge 확대 필요**

- Black box 를 black box 로 공격
- https://blog.openai.com/adversarial-example-research/




Adversarial examples are inputs to machine learning models that an attacker has intentionally designed to cause the model to make a mistake; they're like optical illusions for machines. In this post we'll show how adversarial examples work across different mediums, and will

HCRL ©2018, 해킹대응기술연구실

# Thank You

KOREA UNIVERSITY

HCRL Hacking and Countermeasure Research Lab

# [참고] 차량 이상징후 탐지 – 평가방법 및 예외사항 정리

## 채점 기준

□ True Positive (정상 탐지)
- 정상 탐지 기준은 실제 공격이 시작되고 1초 이내에 해당 공격을 타입까지 탐지하는 경우를 의미함
- 정답지에 있는 각 공격 시작 포인트를 모두 1초 이내에 탐지했을 경우 True Positive의 개수를 최대로 획득할 수 있으며, 정상 탐지 개수의 범위는 0 ≤ True Positive ≤ '실제 공격 횟수'로 정의할 수 있음
- 예외 상황: 한 번의 공격 안에서 여러 개(N개)의 탐지 포인트가 있을 경우
  - 첫 번째 탐지는 True Positive (정상 탐지)로 판단하며, 나머지 탐지 포인트는 실제 공격 시작 1초 이내에 있어도 False Positive를 증가시킴
  - 모든 탐지 포인트를 True Positive로 판단할 경우 정상 탐지의 개수가 증가하므로 부정 행위로 간주함
    - True Positive = 1, False Positive = N-1, False Negative = 0

□ False Positive (오탐지)
- 오탐지의 기준은 참가자가 탐지한 공격 포인트가 각 공격이 시작된 후 1초 이내에 없는 경우를 의미함
- 탐지한 공격의 타입을 정확히 분류하지 못할 경우 역시 오탐지로 판단함
- 오탐지는 참가자의 탐지 포인트 마다 평가가 이루어지기 때문에, 개수의 범위는 0 ≤ False Positive ≤ '공격 탐지 횟수'로 정의할 수 있음
- 예외 상황: 실제 공격 동안 탐지가 이루어졌지만 1초 이내에 탐지 못 했을 경우
  - 오 탐지로 판단되지만, 해당 공격을 지나친 경우는 아니기 때문에 미 탐지의 숫자를 증가시키지는 않음₩
    - True Positive = 0, False Positive = 1, False Negative = 0

□ False Negative (미 탐지)
- 미 탐지의 기준은 실제 공격 동안 한 번의 탐지도 이루어지지 않고 지나칠 경우를 의미함
- 미 탐지는 정답지에 존재하는 각 공격마다 평가가 이루어지기 때문에, 개수의 범위는 0 ≤ False Negative ≤ '실제 공격 횟수'로 정의할 수 있음


©2018, 해킹대응기술연구실


# [참고] 차량 이상징후 탐지 – 평가방법 및 예외사항 정리

## 채점 예시

| No. | 구분 | 결과 |
|---|---|---|
| 1 | 13번째 Submit row가 13번째 Answer row의 구간에서 벗어난 경우 | False Positive = 1, False Negative = 1 |
| 2 | Row가 정렬된 데이터셋이 아닐 경우 | F1-Score = 0 |
| 3 | 모두 정답 값 안에 들 경우 | F1-Score = 1 |
| 4 | 3번 Submit파일을 기반으로 타입 중 DoS와 Fuzzy 혹은 Replay 값이 아닌 다른 값이 있을 경우 | False Positive =1 |
| 5 | 3번 Submit파일을 기반으로 타입의 대소문자 구분을 하지 않은 경우 | F1-Score = 1 |
| 6 | 동일한 시간과 타입을 가진 Row를 여러줄 추가 (부정 행위) | 추가 열 만큼 False Positive 추가 |
| 7 | True Positive 시간대 내에 Submit row를 중복 값을 넣은 경우 | 중복값은 False Positive로 판단 |
| 8 | 공격구간 내와 공격구간 후에 1초 간격으로 값을 넣은 경우 | 중복값은 False Positive로 판단 |
| 9 | 동일한 Row 100개를 넣었을 때 (부정 행위) | False Positive = 100 |
| 10 | 시간을 1초 간격으로 모두 입력하였을 때 (부정 행위) | False Positive → 입력 값 만큼 증가 |

## 동점자 발생 시

□ 동점자의 탐지 반응 시간의 평균을 통해서 탐지 시간이 빠른 참가자에게 순위를 높게 판단


©2018, 해킹대응기술연구실

# 블랙마켓 CC Crawling 결과 및 시사점

**신동휘** 스틸리언 이사

### 학력 및 경력사항

| | |
|---|---|
| 2007 ~ 2010 | 한국인터넷진흥원 |
| 2010 ~ 2011 | SAMSUNG SDS |
| 2011 ~ 2011 | SOFTFORUM |
| 2012 ~ 2015 | RAONSECURE |
| 2014 ~ 현재 | 성신여자대학교 융합보안공학과 겸임교수 |
| 2015 ~ 현재 | STEALIEN |
| 2015 ~ 현재 | 서강대학교 정보통신대학원 겸임교수 |
| 2017 ~ 현재 | 아주대학교 사이버보안학과 겸임교수 |

### 강연요약

정보보호 분야에서 작년부터 Darknet, DeepWeb, OSINT 등의 표현등을 이용하며 Underground Market 또는 Blackmarket에 대한 내용을 담은 언론 기사 및 발표들을 볼 수 있다.

Underground Market에서 주로 거래되는 내용을 살펴보면 개인 정보를 비롯한 기업 정보들이 거래되고 있다.

이렇게 거래되는 정보 중, Underground Market에서 판매한다고 하는 신용카드 정보들을 수집해보고 그 내용과 의미에 대해 파악해본다.

이와 더불어 Underground Market에 대한 접근과 활용 방안에 대해 논의해보고자 한다.

# 블랙마켓 CC Crawling 결과 및 시사점

(주) 스틸리언

2018.04

we STEAL ALIEN technology

STEALIEN

## 목차

01

블랙마켓 CC Crawling 결과 및 시사점

1. 개요
가. CC
나. Stolen CC
다. Underground Shopping
라. Carding

2. CC Crawling
가. Crawling
나. BE EVIL
다. Result

02

# 1. 개요

가. CC
나. Stolen CC
다. Underground Shopping
라. Carding

## 가. CC

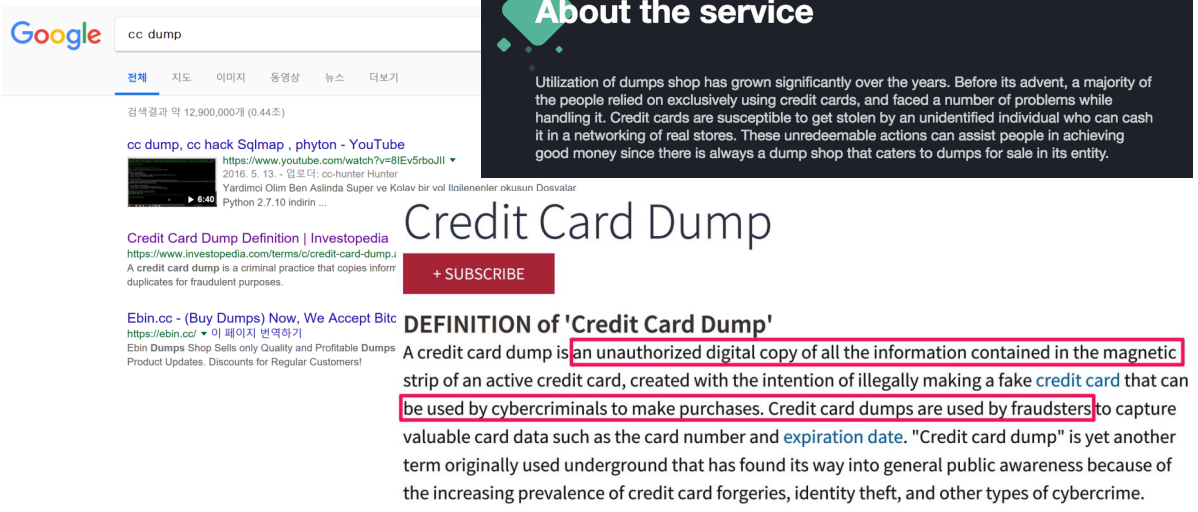


### CC

**Introduction**

· CC = Credit Card

· CC DUMP in Google



## 나. Stolen CC

04

1. 개요

### Stolen

**Introduction**

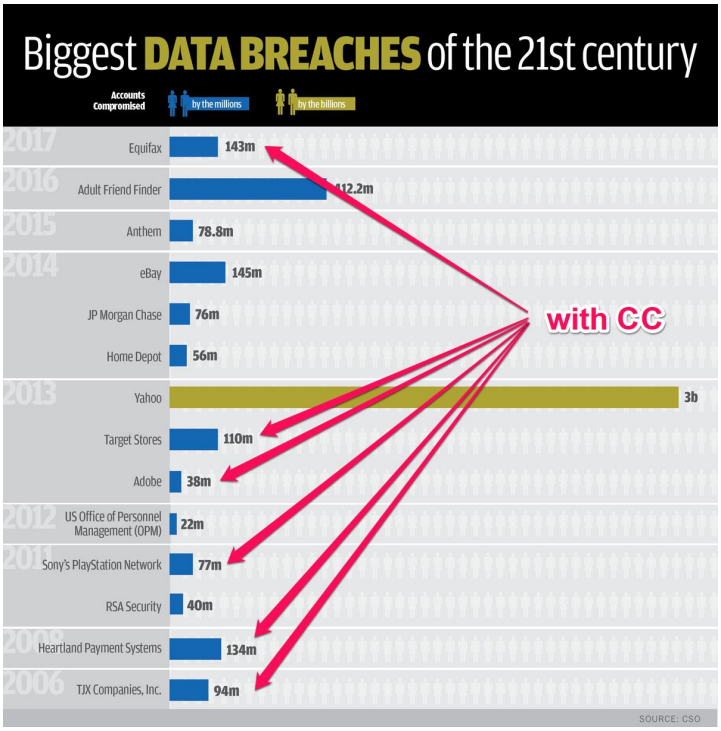
· Source of CC

**Data breaches cases**

→ 596M

Scarping malware

Skimmer




https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

## 나. Stolen CC

05

1. 개요

### Stolen

**Introduction**

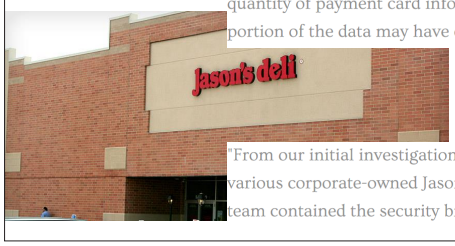
· Source of CC

Data breaches cases

**Scarping or Capture or Keylogging malware**

Skimmer

Although the company did not yet specify the total number of its customers affected by the breach, it did confirm that malware was installed on some point of sale (POS) systems in stores across the U.S. at varying times between April 3, 2017, and November 18, 2017.




"On December 22, 2017, Jason's Deli was notified by payment processors that credit card security personnel had informed it that a large quantity of payment card information had appeared for sale on the 'dark web,' and that an analysis of the data indicated that at least a portion of the data may have come from various Jason's Deli locations," the company says in its breach notification.

"From our initial investigation findings, criminals deployed RAM-scraping malware on a number of our point-of-sales (POS) terminals at various corporate-owned Jason's Deli restaurants ... starting on June 8, 2017," it adds. "During the course of the investigation, our response team contained the security breach and has also disabled the malware in all of the locations where it was discovered."

# 나. Stolen CC

06

1. 개요

## Stolen

### Introduction

· Source of CC

Data breaches cases

Scarping or Capture or Keylogging malware

**Skimmer**

Main » TERM » C »

card skimming

Like 1 Tweet G+

By Vangie Beal

(card skim'ming) (n.) The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is

Related Terms

- identity
- phishing (email)
- medical identity theft
- subscriber identity module
- smishing
- Windows CardSpace
- vishing
- spear phishing
- virtual identity
- network identity

Skimming works by replacing a card reader like an ATM with a camouflaged counterfeit card reader. The counterfeit reader records all of the data on a credit, debit or ATM card as it passes through the skimmer. In addition to ATMs, other locations where

these instances, the thief has fitted the card reader with a skimmer, or uses a hand-held skimmer hidden in a pocket.

# 나. Stolen CC

07

1. 개요

## Stolen

### Introduction

· Source of CC(KOREA CASE)

The biggest case with USB

### 3. 유출 과정 [편집]

**개인정보**를 유출한 **범인**은 아이핀을 관리하는 신용평가 업체인 코리아크레딧뷰로(KCB)에 근무하는 직원인 박모 차장으로 밝혀졌다. 박씨는 각 카드사의 분실·위변조 탐지 시스템 개발 프로젝트(FDS) 책임자로 각 카드사에 파견돼 일하면서 시스템을 테스트하기 위해 받은 개인 정보를 USB에 담아 빼냈다. 여기에는 카드사의 안일한 대처도 한몫했는데 테스트를 할 땐 진짜 고객 정보가 아니라 가짜 더미 데이터를 사용해야 되는 게 상식인데도 외부 용역에게 진짜 개인정보에 접근하도록 했다. 인가되지 않은 USB를 차단하는 시스템 따위도 없었다. 그야말로 총체적 난국.

### 4. 피해규모 [편집]

3사에서 유출된 개인정보는 사망자와 중복 포함 1억 580만 건이며 대한민국에서 일어난 개인정보 유출사태 중 가장 큰 규모다. 3사에서 유출된 개인정보 건수는 KB국민카드는 약 4000만 건, 롯데카드와 NH농협카드가 약 2,000만 건이다. 유출된 개인정보도 상당히 방대하다. 3사 모두 개인 신상정보와 결제계좌가 유출되었고 KB국민카드는 타사 카드 정보, 롯데카드와 NH농협카드에서는 카드번호와 카드유효기간이 유출되었다. 게다가 개인 신상정보는 이름, 주민등록번호, 연락처, **집 주소** 같은 기본적인 개인정보 뿐만 아니라 연봉, 결혼 여부, 자동차 소유 여부와 같은 세부 개인정보와 결제일, 신용한도 금액, 신용등급과 같은 민감한 금융정보까지 유출되었다. 더욱이 KB국민카드는 같은 계열사인 국민은행 사용자 정보까지 유출된 것으로 드러났다. 이러다보니 NH농협은행 개인정보도 유출되었을 가능성이 높다.[4]

우리나라 경제인구의 약 75%가 피해자로 추정된다는 보도가 나왔다.

## 다. Underground Shopping 08

1. 개요

### Underground CC Mall

**Introduction**

· U can find AMAP

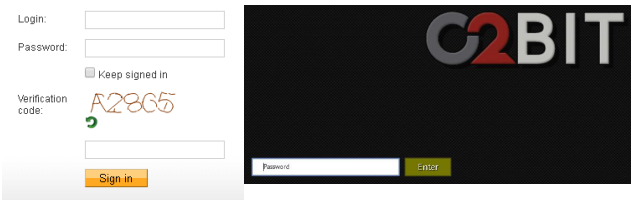
## 다. Underground Shopping 09

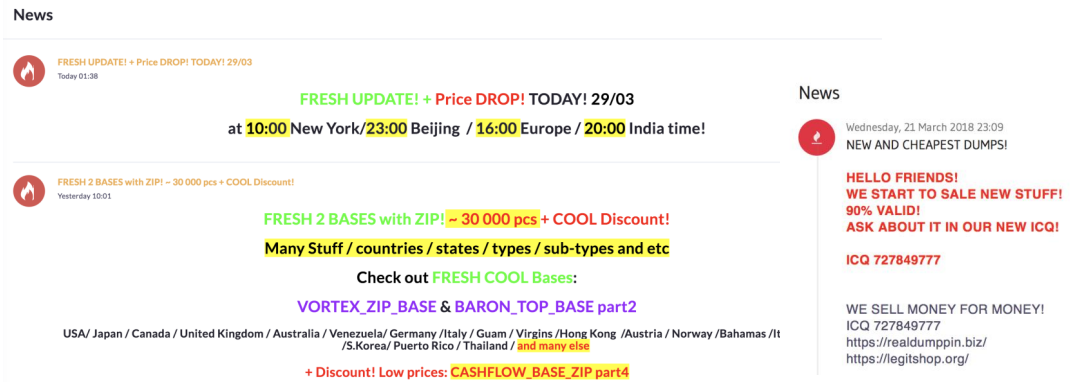
1. 개요

### Underground CC Mall

**Introduction**

· Login, News



# 다. Underground Shopping 10

1. 개요

## Underground CC Mall

### Introduction

· Tutorial

**Guide**

Whatsup guys! This guide is for newbies in the world of card dumps. HoneyMoney Team take care about all sorts of our clients and future clients, so here are some information, advises and tips, that would probably interest you. So get your cup of tea, with honey, of course, and enjoy!

##1 What the hell Dump is?

Card Dump is nothing but the information written on the magnetic strip of a credit card. This data is kept on the tracks and we are interested only in the Track 1 and 2 (In Track 2 only in most cases)

This data looks smtng like this:

B4000001234567890^THEBLADE/BORIS^03101011123400567000000;;4000001234567890=03101011123495679991.

This is Track 1: B4000001234567890^THEBLADE/BORIS^03101011123400567000000;

This is Track 2: 4000001234567890=03101011123495679991

Track 2 is considered to be the main one and if you own it, you can obtain the information from Track 1.

Lets have a detailed look at this Tracks.

- format code =B ,mean that is a bank card (in formula B)
- primary account number or PAN= which is the number embossed on the card (in formula PAN)
- field separator =usual ^ (in formula ^)
- card holder name=between 2 and 20 alphabets (in formula name/last name)
- field separator=usual ^ (in formula ^)
- expiration date of card=in format YYMM year aand month (in formula YYMM)
- service code=three digits which can be replaced with their meaning and know where and for which kind of . transaction can be the card used (in formula 101)
- discretionary data=which can be Pin Verification Key Indicator (1 digit),Pin Verification Value (4 digits) or . Card Verification Value or the well known CVV (in formula CVV)

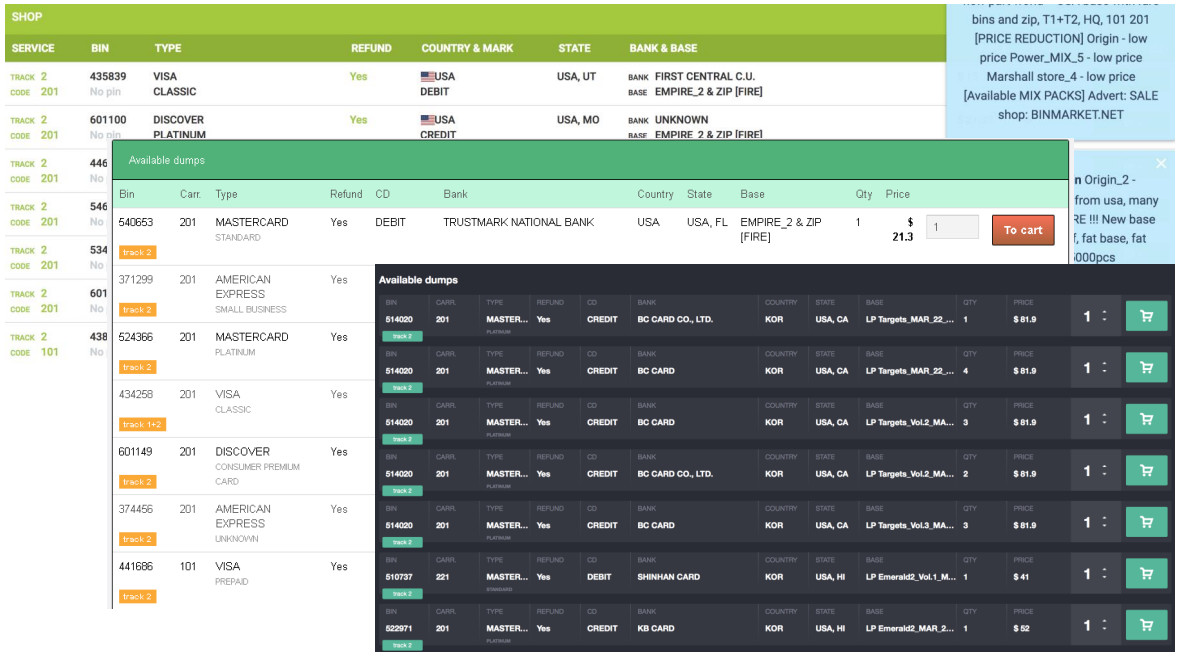
# 다. Underground Shopping 11

1. 개요

## Underground CC Mall

### Introduction

· Product



## 라. Carding

12

1. 개요

### Make a money with CC or Dumps

**Carding**

· Carding

Online Carding with CC(CVV)

In Store Carding with DUMP

## 라. Carding

13

1. 개요

### Make a money with CC or Dumps

**Carding**

· In Store Carding with DUMP

## 라. Carding 14

1. 개요

### Make a money with CC or Dumps

**Carding**

· In Store Carding with DUMP

Dressing the part:

This should come natural to most people out there. To buy something expensive you need to make it look like you can buy these items along with acting like you can (below). For your first operation i suggest should include you going into any of the clothing stores listed below and buy a decent amount of quality clothes. I cannot stress enough how quality plays a part in dressing up. Buying a sweater in Walmart and a sweater in banana republic could determine the difference between getting out with your goods or running out of the store. Along with clothing you might want to buy some jewelry or a very high priced watch. If a cashier suspects something is up, seeing some classy jewelry or a watch could also help reduce the suspicion.

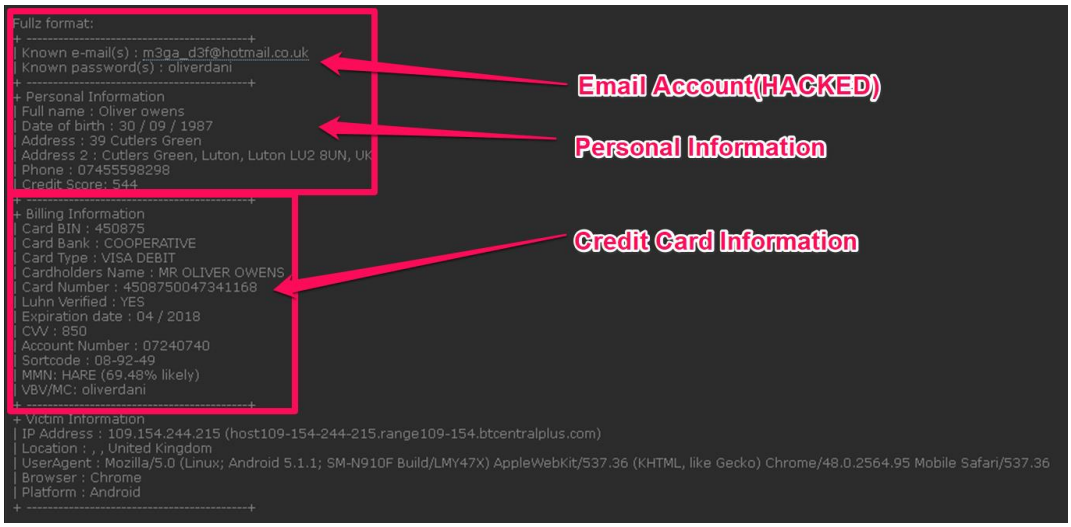
## 라. Carding 15

1. 개요

### Make a money with CC or Dumps

**Order**

· Information for valid transaction



# 라. Carding

16

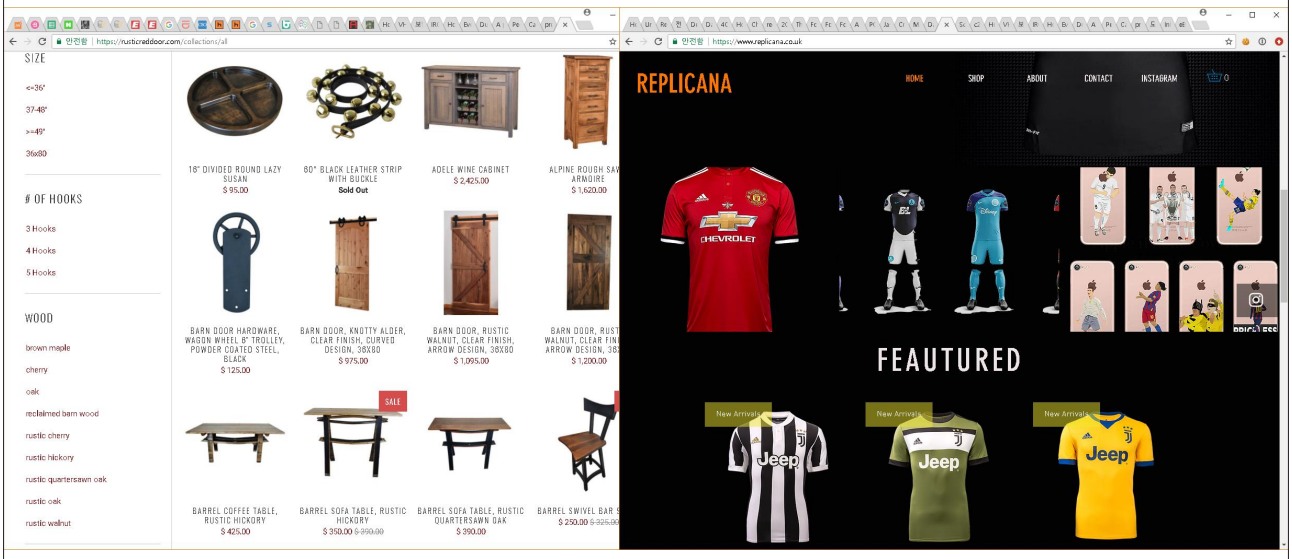
1. 개요

## Make a money with CC or Dumps

### Order

· Online Carding with CC(CVV)

Cardable Website




# 라. Carding

17

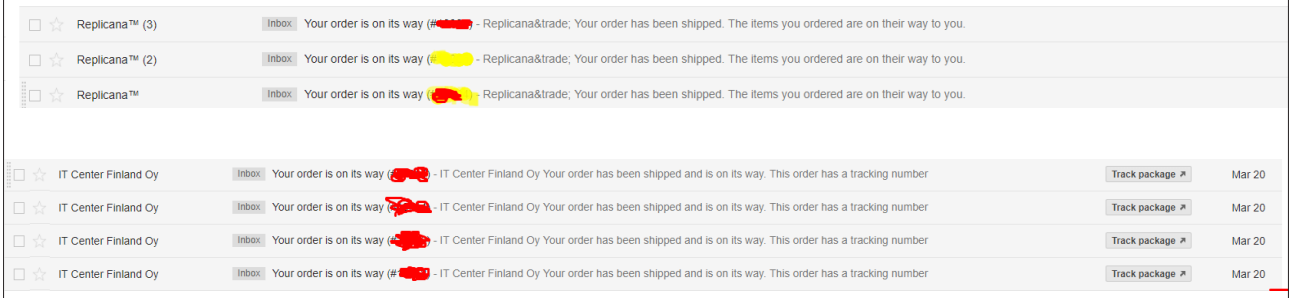
1. 개요

## Make a money with CC or Dumps

### Order

· Online Carding with CC(CVV)

Cardable Website(PROOF)



18

# 2. CC Crawling

가. Crawling
나. BE EVIL
다. Result

## 가. Crawling



### CC Crawling

**Introduction**

· CC Crawler = Selenium + PhantomJS + MySQL + Python

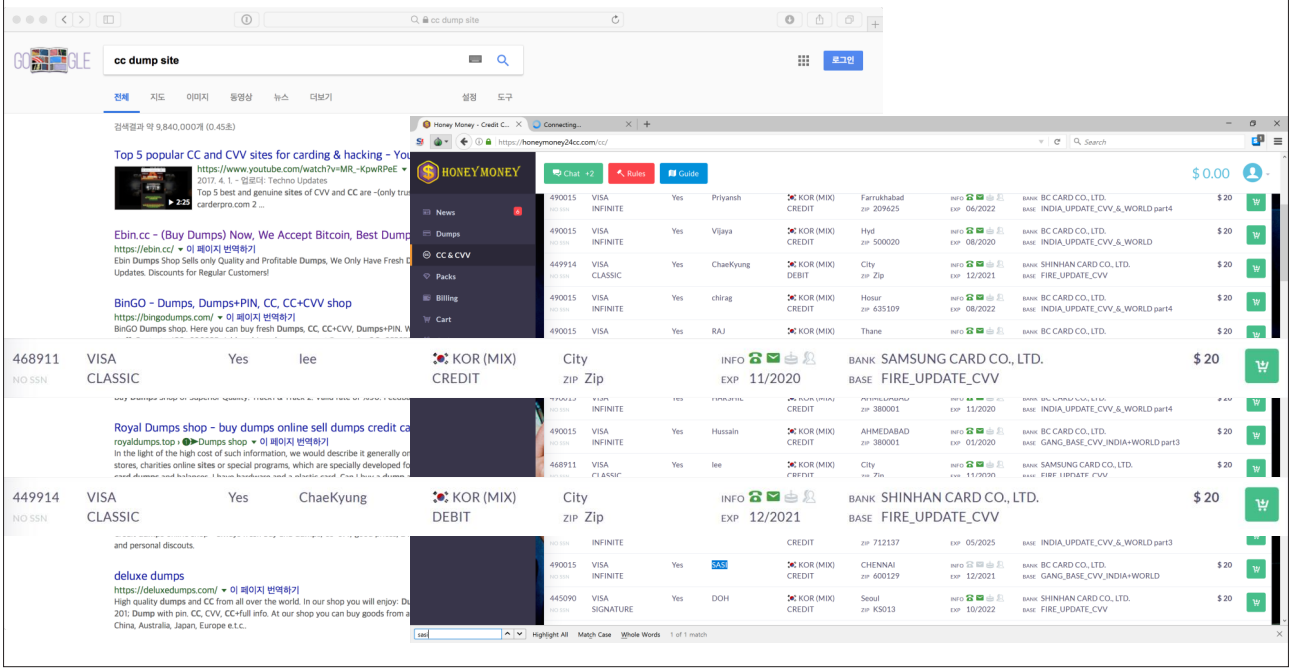
# 가. Crawling



## CC Crawling

### Introduction

· It's too easy to find information




# 가. Crawling

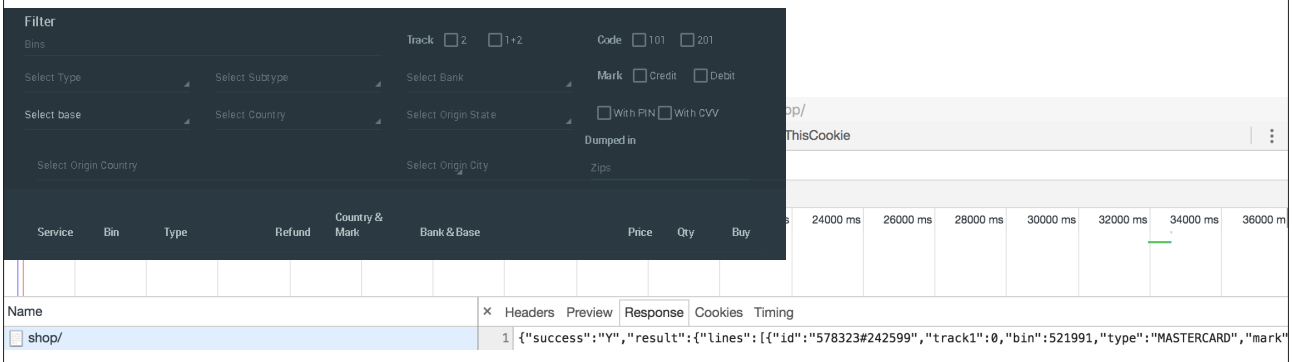


## CC Crawling

### Introduction

· Fetch CC information from CC or DUMPS menu

JSON Information



# 가. Crawling 22

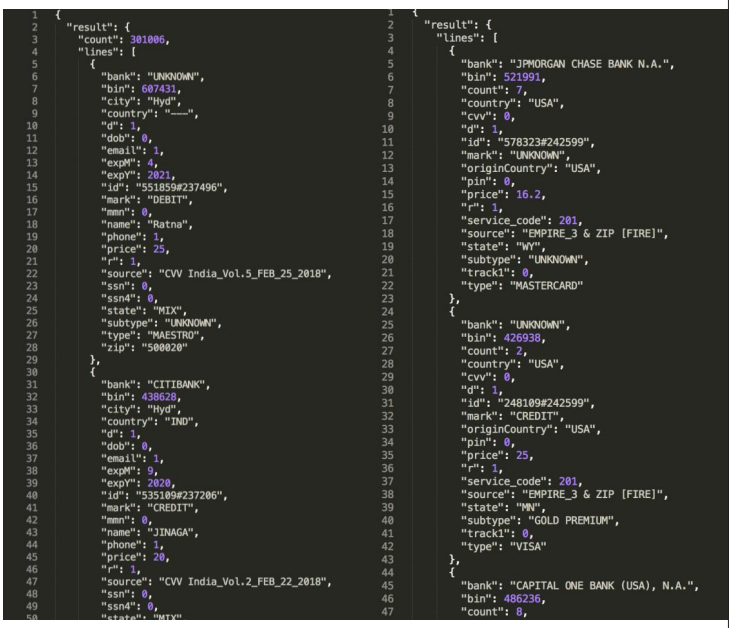


## CC Crawling

### Introduction

· Fetch CC information CC or DUMPS menu


"bank": "CITIBANK",
"bin": 438628,
"country": "IND",
"expM": 9,
"expY": 2020,
"id": "535109#237206",
"mark": "CREDIT",
"name": "JINAGA",
"source": "CVV India_Vol.2_FEB_22_2018",
"subtype": "PLATINUM",
"type": "VISA",
"zip": "500020"


# 가. Crawling 23



## CC Crawling

### Introduction

· Fetch CC information CC or DUMPS menu → Just simple information

| | | | | | | |
|---|---|---|---|---|---|---|
| STL_2276 | 552377 | MASTERCARD | WORLD | CREDIT | 01/19 | 2018.03.16 |
| STL_2277 | 402596 | VISA | CORPORATE T&E | CREDIT | 11/19 | 2018.03.16 |
| STL_2278 | 552377 | MASTERCARD | WORLD | CREDIT | 04/20 | 2018.03.16 |
| STL_2279 | 402596 | VISA | CORPORATE T&E | CREDIT | 04/19 | 2018.03.16 |
| STL_2280 | 433028 | VISA | PLATINUM | CREDIT | 05/19 | 2018.03.22 |
| STL_2281 | 433028 | VISA | PLATINUM | CREDIT | 12/19 | 2018.03.22 |
| STL_2282 | 433028 | VISA | PLATINUM | CREDIT | 08/20 | 2018.03.22 |
| STL_2283 | 433028 | VISA | PLATINUM | CREDIT | 08/18 | 2018.03.22 |
| STL_2284 | 547227 | MASTERCARD | BUSINESS | CREDIT | 06/19 | 2018.03.22 |
| STL_2285 | 552377 | MASTERCARD | WORLD | CREDIT | 12/18 | 2018.03.22 |
| STL_2286 | 552377 | MASTERCARD | WORLD | CREDIT | 01/19 | 2018.03.22 |
| STL_2287 | 402596 | VISA | CORPORATE T&E | CREDIT | 11/19 | 2018.03.22 |
| STL_2288 | 552377 | MASTERCARD | WORLD | CREDIT | 04/20 | 2018.03.22 |
| STL_2289 | 402596 | VISA | CORPORATE T&E | CREDIT | 04/19 | 2018.03.22 |
| STL_2290 | 433028 | VISA | PLATINUM | CREDIT | 05/19 | 2018.03.23 |
| STL_2291 | 433028 | VISA | PLATINUM | CREDIT | 12/19 | 2018.03.23 |
| STL_2292 | 433028 | VISA | PLATINUM | CREDIT | 08/20 | 2018.03.23 |
| STL_2293 | 433028 | VISA | PLATINUM | CREDIT | 08/18 | 2018.03.23 |
| STL_2294 | 547227 | MASTERCARD | BUSINESS | CREDIT | 06/19 | 2018.03.23 |
| STL_2295 | 552377 | MASTERCARD | WORLD | CREDIT | 12/18 | 2018.03.23 |
| STL_2296 | 552377 | MASTERCARD | WORLD | CREDIT | 01/19 | 2018.03.23 |
| STL_2297 | 402596 | VISA | CORPORATE T&E | CREDIT | 11/19 | 2018.03.23 |
| STL_2298 | 552377 | MASTERCARD | WORLD | CREDIT | 04/20 | 2018.03.23 |
| STL_2299 | 402596 | VISA | CORPORATE T&E | CREDIT | 04/19 | 2018.03.23 |

1,017,480EA
(about 1M)

## 가. Crawling 24

2. CC Crawling

### CC Crawling

**Introduction**

· 1,017,480/95,640,000(Korea CC # in 2016) from "휴면신용카드 - KDI 경제정보센터"

About 1% = 1/100

□ (신용카드 발급현황) '16년말 현재 **국민 1인당*** 보유하고 있는 **신용카드는 평균 3.6개**(총 발급 카드수 9,564만개)로

## 나. BE EVIL 25

2. CC Crawling

### BE EVIL

**Disclosed Information**

· Just with crawling, we can **NOT** do anything

Counting → "count": 301006,

Trace with holder name + expM/Y + Name + Address

| BIN | TYPE | REFUND | NAME | COUNTRY & MARK | CITY & ZIP | INFO & EXP | BANK & BASE |
|---|---|---|---|---|---|---|---|
| 512652 | MASTERCARD<br>STANDARD | Yes | ANKIT | IND (MIX)<br>CREDIT | kangra<br>177117 | INFO<br>EXP 09/2018 | BANK PUNJAB NATIONAL BANK<br>BASE INDIA cvv Base 13k_3 |
| 607431 | MAESTRO<br>UNKNOWN | Yes | SONAL | --- (MIX)<br>DEBIT | Uttar Pradesh<br>231304 | INFO<br>EXP 08/2022 | BANK UNKNOWN<br>BASE INDIA cvv Base 13k_9 |
| 489377 | VISA<br>PLATINUM | Yes | NAGARBHAI | IND (MIX)<br>CREDIT | AHMEDABAD<br>380001 | INFO<br>EXP 06/2019 | BANK HDFC BANK, LTD.<br>BASE INDIA cvv Base 13k_8 |
| 452055 | VISA<br>UNKNOWN | No | Vikram | IND (MIX)<br>DEBIT | delhi<br>110086 | INFO<br>EXP 02/2021 | BANK TORONTO-DOMINION BANK INDIA<br>BASE INDIA + WORLD CVV part 2 |

# 나. BE EVIL



## BE EVIL

### Disclosed Information

· Sometimes wrong information

"bank": "CITIBANK",

"bin": 438628,

cf. https://www.bincodes.com/bin-checker/

BIN Validation Result

You did not provide the correct captcha information. Try again!


```
{
  "result": {
    "count": 301006,
    "lines": [
      {
        "bank": "UNKNOWN",
        "bin": 607431,
        "city": "Hyd",
        "country": "----",
        "d": 1,
        "dob": 0,
        "email": 1,
        "expM": 4,
        "expY": 2021,
        "id": "551859#237496",
        "mark": "DEBIT",
        "mmn": 0,
        "name": "Ratna",
        "phone": 1,
        "price": 25,
        "r": 1,
        "source": "CVV India_Vol.5_FEB_25_2018",
        "ssn": 0,
        "ssn4": 0,
        "state": "MIX",
        "subtype": "UNKNOWN",
        "type": "MAESTRO",
        "zip": "500020"
      },
      {
        "bank": "CITIBANK",
        "bin": 438628,
        "city": "Hyd",
        "country": "IND",
        "d": 1,
        "dob": 0,
        "email": 1,
        "expM": 9,
        "expY": 2020,
        "id": "535109#237206",
        "mark": "CREDIT",
        "mmn": 0,
        "name": "JINAGA",
        "phone": 1,
        "price": 20,
        "r": 1,
        "source": "CVV India_Vol.2_FEB_22_2018",
        "ssn": 0,
        "ssn4": 0,
        "state": "MIX",
```

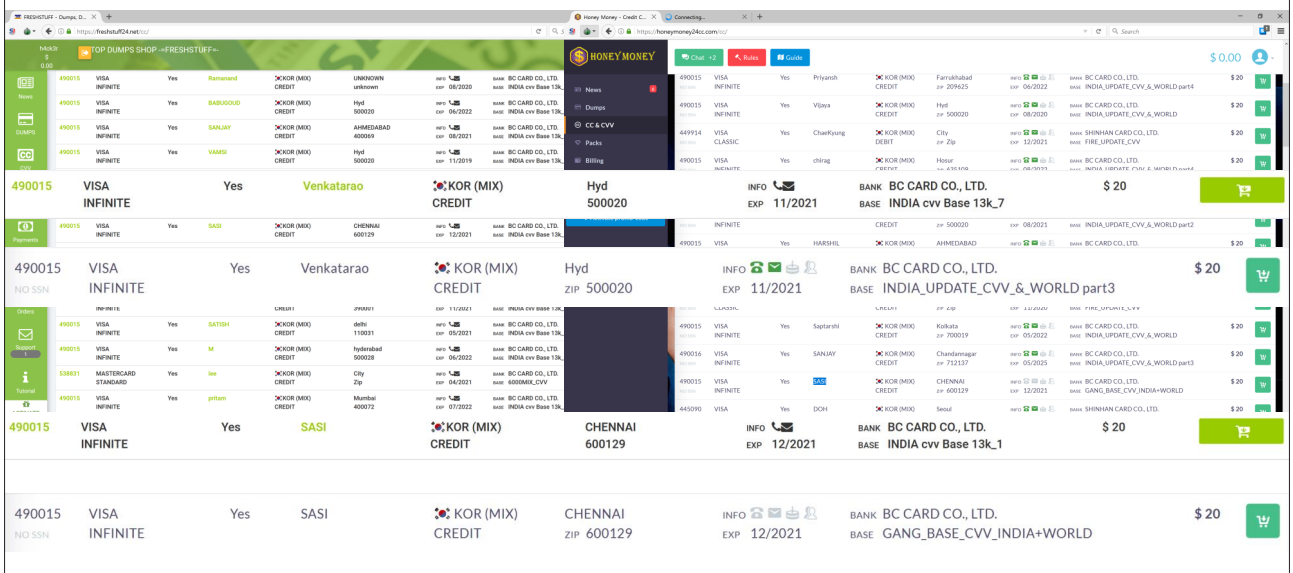

# 나. BE EVIL



## BE EVIL

### Disclosed Information

· Sometimes overlapping or wired



# 나. BE EVIL

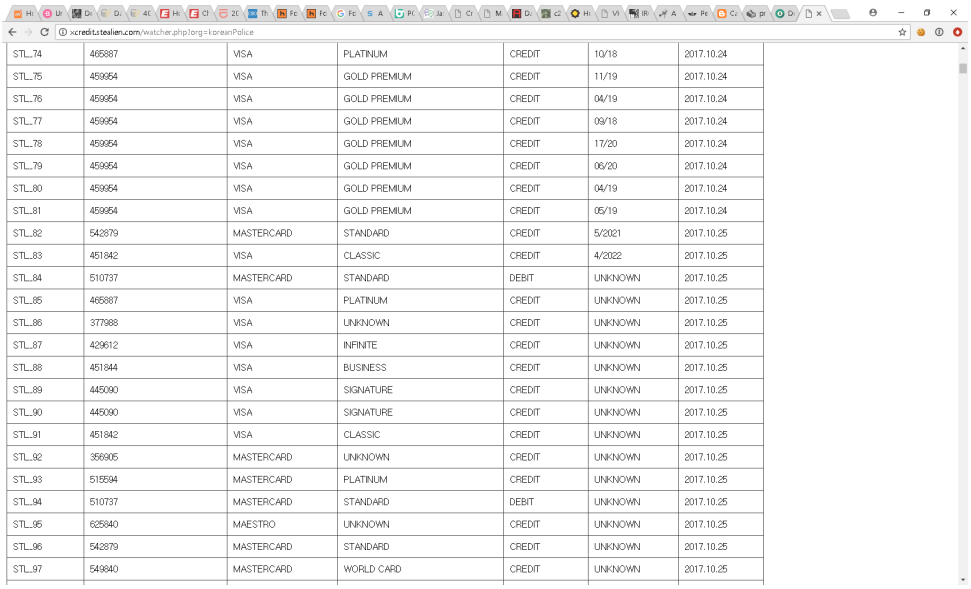
28

2. CC Crawling

## BE EVIL

### Disclosed Information

· Expired?



| | | | | | | |
|---|---|---|---|---|---|---|
| STL_74 | 465887 | VISA | PLATINUM | CREDIT | 10/18 | 2017.10.24 |
| STL_75 | 459954 | VISA | GOLD PREMIUM | CREDIT | 11/19 | 2017.10.24 |
| STL_76 | 459954 | VISA | GOLD PREMIUM | CREDIT | 04/19 | 2017.10.24 |
| STL_77 | 459954 | VISA | GOLD PREMIUM | CREDIT | 09/18 | 2017.10.24 |
| STL_78 | 459954 | VISA | GOLD PREMIUM | CREDIT | 17/20 | 2017.10.24 |
| STL_79 | 459954 | VISA | GOLD PREMIUM | CREDIT | 06/20 | 2017.10.24 |
| STL_80 | 459954 | VISA | GOLD PREMIUM | CREDIT | 04/19 | 2017.10.24 |
| STL_81 | 459954 | VISA | GOLD PREMIUM | CREDIT | 05/19 | 2017.10.24 |
| STL_82 | 542879 | MASTERCARD | STANDARD | CREDIT | 5/2021 | 2017.10.25 |
| STL_83 | 451842 | VISA | CLASSIC | CREDIT | 4/2022 | 2017.10.25 |
| STL_84 | 510737 | MASTERCARD | STANDARD | DEBIT | UNKNOWN | 2017.10.25 |
| STL_85 | 465887 | VISA | PLATINUM | CREDIT | UNKNOWN | 2017.10.25 |
| STL_86 | 377988 | VISA | UNKNOWN | CREDIT | UNKNOWN | 2017.10.25 |
| STL_87 | 429612 | VISA | INFINITE | CREDIT | UNKNOWN | 2017.10.25 |
| STL_88 | 451844 | VISA | BUSINESS | CREDIT | UNKNOWN | 2017.10.25 |
| STL_89 | 445090 | VISA | SIGNATURE | CREDIT | UNKNOWN | 2017.10.25 |
| STL_90 | 445090 | VISA | SIGNATURE | CREDIT | UNKNOWN | 2017.10.25 |
| STL_91 | 451842 | VISA | CLASSIC | CREDIT | UNKNOWN | 2017.10.25 |
| STL_92 | 356905 | MASTERCARD | UNKNOWN | CREDIT | UNKNOWN | 2017.10.25 |
| STL_93 | 515594 | MASTERCARD | PLATINUM | CREDIT | UNKNOWN | 2017.10.25 |
| STL_94 | 510737 | MASTERCARD | STANDARD | DEBIT | UNKNOWN | 2017.10.25 |
| STL_95 | 625840 | MAESTRO | UNKNOWN | CREDIT | UNKNOWN | 2017.10.25 |
| STL_96 | 542879 | MASTERCARD | STANDARD | CREDIT | UNKNOWN | 2017.10.25 |
| STL_97 | 549840 | MASTERCARD | WORLD CARD | CREDIT | UNKNOWN | 2017.10.25 |

# 나. BE EVIL

29

2. CC Crawling

## BE EVIL

### Paid Information

· Fetch CC information CC or DUMPS menu

After shopping

(ONLINE) CC/CCV

5546370226887914|02|2017|918|Bhamini|Pattabhiraman||Old 43/2, New 52/2, 11th Avenue,|Chennai|600083|+91 9500032305|INDIA

[CC#][MM][YYYY][CVV][NAME][ADDRESS][ZIPCODE][PHONE#][COUNTRY]

# 나. BE EVIL

30

2. CC Crawling

## BE EVIL

### Paid Information

· Fetch CC information CC or DUMPS menu

After shopping

(OFFLINE) DUMP

+ ----------+

- Billing Information
| Card BIN : 446272
| Card Type : VISA DEBIT PLATINUM
| Cardholders Name : CHRIS READ
| Card Number : 4462 7212 5405 7510
| Luhn Verified : YES
| Expiration date : 07 / 17
| Start date : 08 / 14
| CVV : 186
| Account Number : 00425612
| Sort Code : 309389
| Carard Bank : LLOYDS TSB BANK PLC

+ ----------+

- Security Question : Mothers Maiden Name
- Security Answer : Clark
- Account Takeover Information
| Confirmed name : Christopher James Read
| Confirmed address : YES
| Confirmed age : 40-44

+ ----------+

BIN Details

| Details for BIN 446272 | |
|---|---|
| BIN | 446272 |
| Issuing Bank | LLOYDS BANK PLC |
| Card Brand | VISA |
| Card Type | DEBIT |
| Card Level | PLATINUM |
| ISO Country Name | UNITED KINGDOM |
| ISO Country A2 | GB |
| ISO Country A3 | GBR |
| ISO Country Number | 826 |
| Issuers Website | http://www.lloydsbankinggroup.com/ |
| Issuers Contact | (0871) 384-2990 |

# 나. BE EVIL

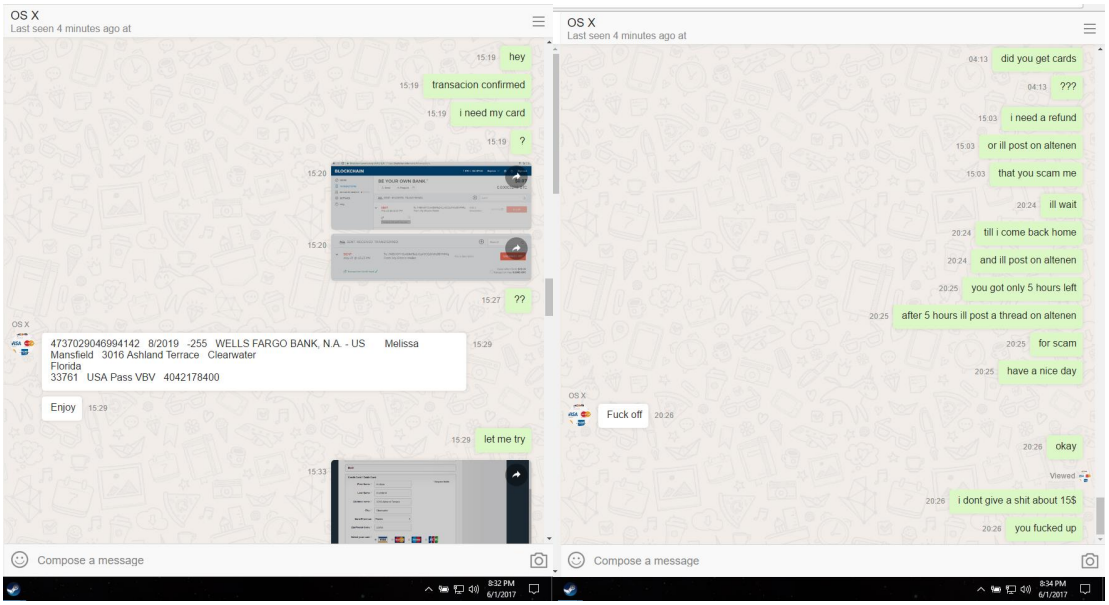
31

2. CC Crawling

## BE EVIL

### Paid Information

· Sometimes SCAM!



## 나. BE EVIL

32

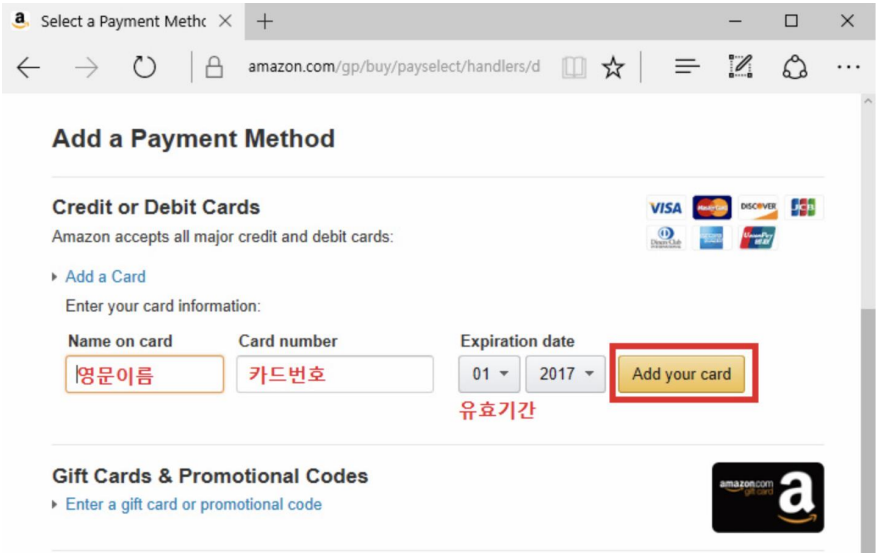
2. CC Crawling

### BE EVIL

**Payment System**

· Global service

Payment system with CC




## 나. BE EVIL

33

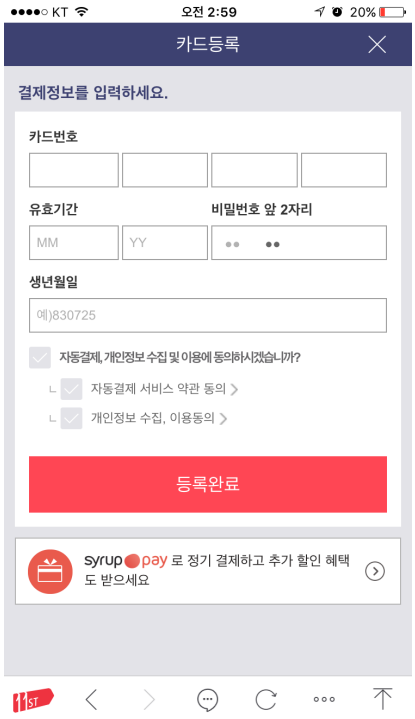
2. CC Crawling

### BE EVIL

**Payment System**

· Korean service

Payment system with CC



## 다. RESULT

34

2. CC Crawling

### RESULT

**Something we can do or can't do with CC**

· Global

Online Carding

In store Carding

· Korea

In store Carding

But, the CC based on the IC chip

· Exactly

Only leaked CC information : Reliable, SCAM, ...

With just disclosed information, we can't be evil

After CC/DUMP shopping, we only can do 'In store Carding' in Korea

But, we can be evil with the global service

# 감사합니다.

(주) 스틸리언

The 24th Network Security Conference -Korea

# CDR 기술 기반의 모바일 웹 콘텐츠 보안 구현

**이상준** 지란지교시큐리티 연구소장

### 학력 및 경력사항

現 (주)지란지교시큐리티 연구소장
前 삼성그룹, 유넷시스템
고려대학교 정보보호대학원

### 강연요약

보안 위협의 지능화와 함께 보안 기술과 대응 트렌드가 변화하고 있다. 특히 예방적 관점의 보안인 CDR(Content Disarm & Reconstruction)은 기존 보안 환경을 이루는 정적/동적 보안 솔루션을 우회하는 지능화된 보안 위협의 대응 방안으로 다양한 영역에서 주목받고 있는 대표적인 기술이다. CDR은 시그니처 기반의 필터링이나 행위 분석을 통한 탐지 관점이 아닌 최종 엔드유저에게 전달되는 콘텐츠 관점에서 콘텐츠의 구조를 분석하고 시스템 정책을 기반으로 승인되지 않은 모든 구성 요소를 제거한 후 안전한 콘텐츠로 재조합하여 전달하는 기술로 콘텐츠에 포함될 수 있는 의심스러운 요소를 사전에 차단한다. 본 강연에서는 대표적인 엔드포인트 위협 요소인 웹 콘텐츠에 대한 보안으로 CDR 기반의 Remote Browser Isolation 기술을 통한 엔드포인트 보안을 구현하는 방안에 대하여 소개하고자 한다.

*원격 브라우저 격리(Remote Browser Isolation) : 웹 콘텐츠에 대하여 컨테이너 같은 가상 환경에서 로컬 장치와 완전히 격리하는 기술로 2017년 보안 분야 10대 기술로 가트너가 선정함.

[NETSEC-KR 2018]

# CDR 기술 기반의 모바일 웹 콘텐츠 보안 구현

2018. 4. 13

이상준 이사
지란지교시큐리티



## 목차

Ⅰ. 증가하는 모바일 위협
Ⅱ. 예방적 콘텐츠 보안 기술, CDR
Ⅲ. 원격 브라우저 격리 기술
Ⅳ. 모바일 웹 콘텐츠 보안 제안
Ⅴ. 결론

# 증가하는 모바일 위협

지란지교시큐리티

## 공격 대상의 확대

PC Mobile

*모바일 위협 증가*

***1. 사용자와 밀접한 디바이스***

*- 사용자정보를 노린 공격부터, 공격 벡터로 이용 가능한 디바이스*

***2. 모바일 디바이스 보급 증가***

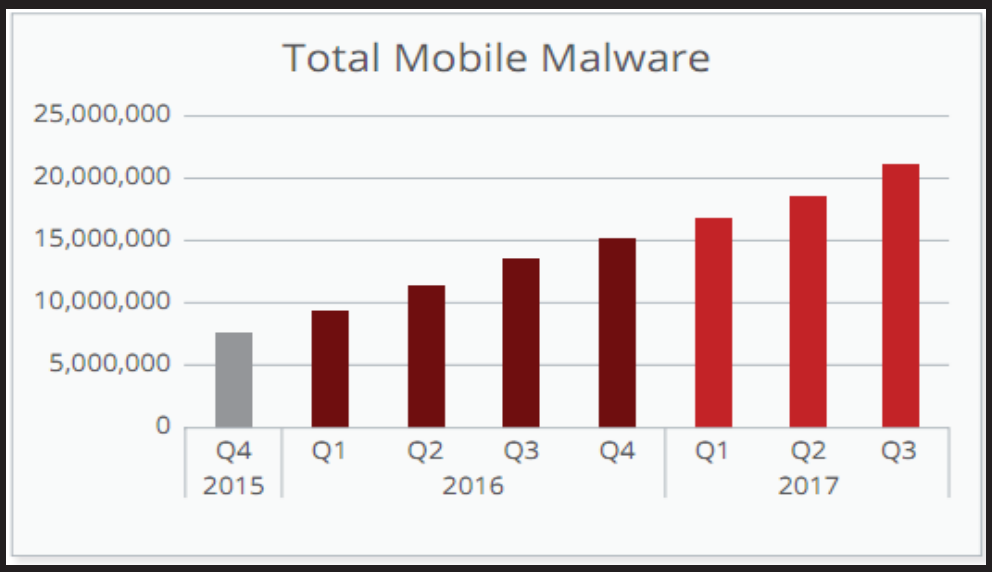
*- 모바일 오피스 확대, 개인, 기업 등 다양한 영역에서 디바이스 의존 및 활용 증가*

**PC → Mobile로 보안 위협의 확대**

지란지교시큐리티

# 증가하는 모바일 악성코드

*2015 – 2017 전체 악성코드 샘플*




* 출처 : McAfee

**모바일 악성코드 지속적으로 증가 추세**

지란지교시큐리티

# 주요 모바일 위협 유형

*데이터 유출*

*피싱(사회공학)*

*악성 Wi-Fi*

*오래된 디바이스, OS*

*물리적 침해*

* 출처 : CSO Online

**디지털 자산부터 물리적 침해까지**

지란지교시큐리티

## 주요 모바일 공격 요소, App

악성 어플리케이션 기반 디바이스 장악

지란지교시큐리티

## 웹으로 유도되는 위협

플랫폼 보안 강화

취약점 및 사회공학

웹 기반 악성코드 다운 유도 및 피싱 증가

지란지교시큐리티

# 웹 기반 모바일 위협 및 특징

피싱 공격 | 웹 사이트 | 파일 다운로드

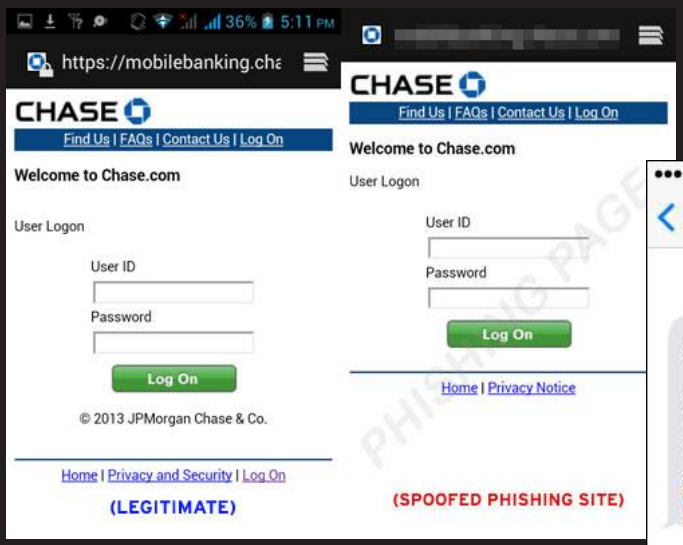
*1. 스크린 사이즈의 제약으로 브라우저 URL 전체를 확인하기 어려움*
*2. 모바일 디바이스는 끊임없이 인터넷에 연결되어 있음*
*3. 개인 디바이스에 대한 사용자의 높은 신뢰성*

* 출처 : EUROPOL

## 디바이스의 제약 및 개인 소유에 따른 위협

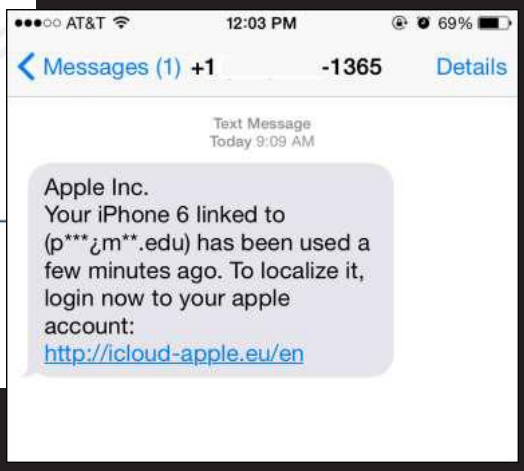
지란지교시큐리티

# 모바일 웹 위협 사례




모바일 피싱 공격

악성 URL 포함 메시지




* 출처 : Trend Micro, Tutorials Point

## 사용자 행위 유도 측면에서 피해 증가

지란지교시큐리티

# 웹 콘텐츠 관점의 보안, CDR

*CDR :*
*콘텐츠 악성코드 무해화*

*웹 콘텐츠를 이용하는데 필요한 요소만 사용자에게 전달*

**예방적 관점에서 의심요소를 제거한다면?**

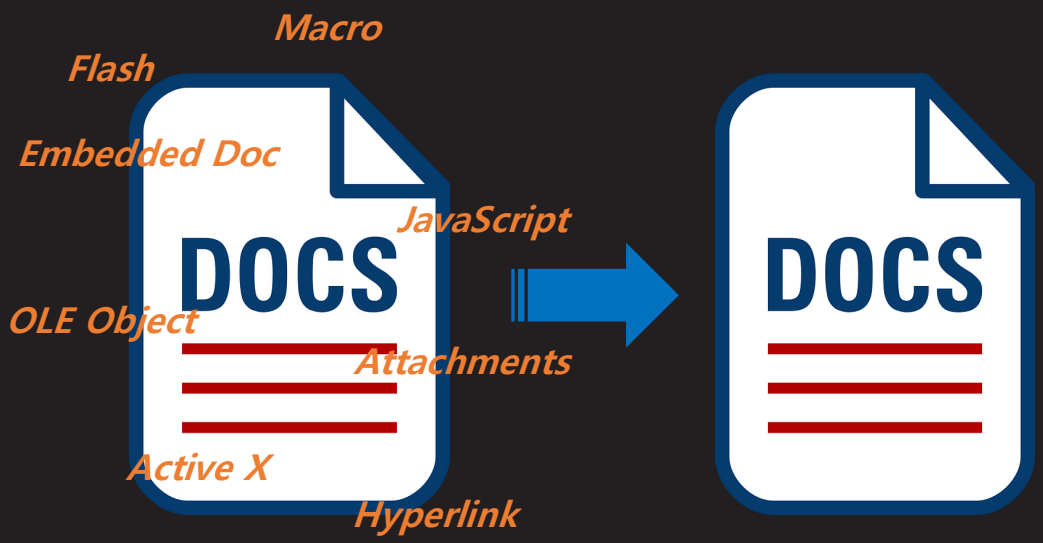
지란지교시큐리티

# 예방적 콘텐츠 보안 기술, CDR

지란지교시큐리티

# CDR 개념

*Content Disarm & Reconstruction*




의심스러운 요소 제거 후 사용자에게 전달

지란지교시큐리티

# 표적형 공격 대응 기술

* 출처 : Trend Micro

이메일 스피어피싱 주요 첨부파일, 문서 포맷

지란지교시큐리티

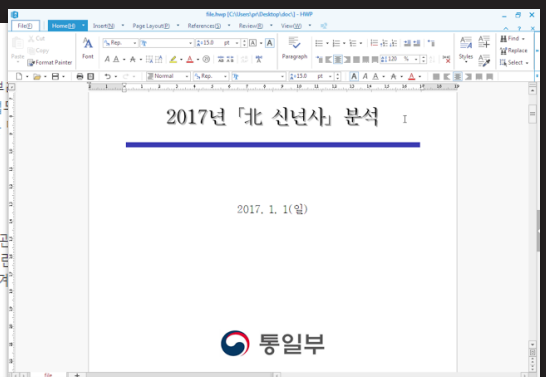
# Malicious HWP 공격 사례

[긴급] '북한 2018년 신년사 분석' 제목의 악성파일 유포 - 보안뉴스
www.boannews.com/media/view.asp?idx=65847
2018. 1. 2. - 통일부를 사칭한 악성파일은 '북한 2018년 신년사 분석'이란 제목으로 2일 새벽 5시쯤 뿌
진 것으로 분석됐다. 유포된 악성 ... 이는 공격자가 정부를 사칭한 만큼 정부부처나 공공기관, 관련 업
관계자 등을 타깃으로 하고 있으며, 악성코드 감염 유도를 위해 많은 사람들이 관심 갖는 최대 이슈를
고 있다. 더욱이 ...

北 신년사 분석 문서 열었다간 '악성코드 감염' - 전자신문
www.etnews.com/20180103000179
2018. 1. 3. - 통일부를 사칭해 북한 신년사를 분석한 내용의 사이버 공격이 발생했다. 탈북자와 북한 관
업무 담당자를 노린 것으로 추정된다. 3일 보안 업계는 통일부를 사칭해 '북한 2018년 신년사 분석'이란
제목의 한글 문서에 악성코드가 숨겨진 것을 발견했다. 김정은 북한 노동당 위원장은 실제로 평창 동계
림픽 참가 의사 ...

"정부로펌 서버 장악 北해커, 신년사관련 악성코드 유포" - 데일리NK
www.dailynk.com/korean/read.php?num=110033&cataId=nk00100
2017. 1. 2. - 2017년 김정은 신년사(1일 발표)를 두고 정부 기관 및 국내외 북한 전문가들의 관심이 집
된 가운데, 북한 해커가 악성코드가 담긴 맞춤형 메일을 유포해 해킹공격을 시도하고 있는 것으로 확
다. 특히 북한 해커는 국가관련 소송을 맡고 있는 '정부법무공단'의 서버를 장악, 해킹 공격명령을 내
'명령제어서버' ...

"군·북한·정치"...HWP 악성코드 단골소재 - 지디넷코리아
www.zdnet.co.kr/news/news_view.asp?artice_id=20170129102123
2017. 1. 30. - HWP 파일엔 감염PC 정보와 화면캡쳐 이미지 파일을 국내 한 쇼핑몰 서버로 보내고,
악성코드 다운로드를 수행하는 악성코드가 담겼다. . 지난 25일 경찰청 사이버안전국은 지난해 11월
된 '우려되는 대한민국.hwp', 지난 3일 유포된 '2017년 북한 신년사 분석.hwp' 파일 관련 수사결과를
했다. 문제의 ...



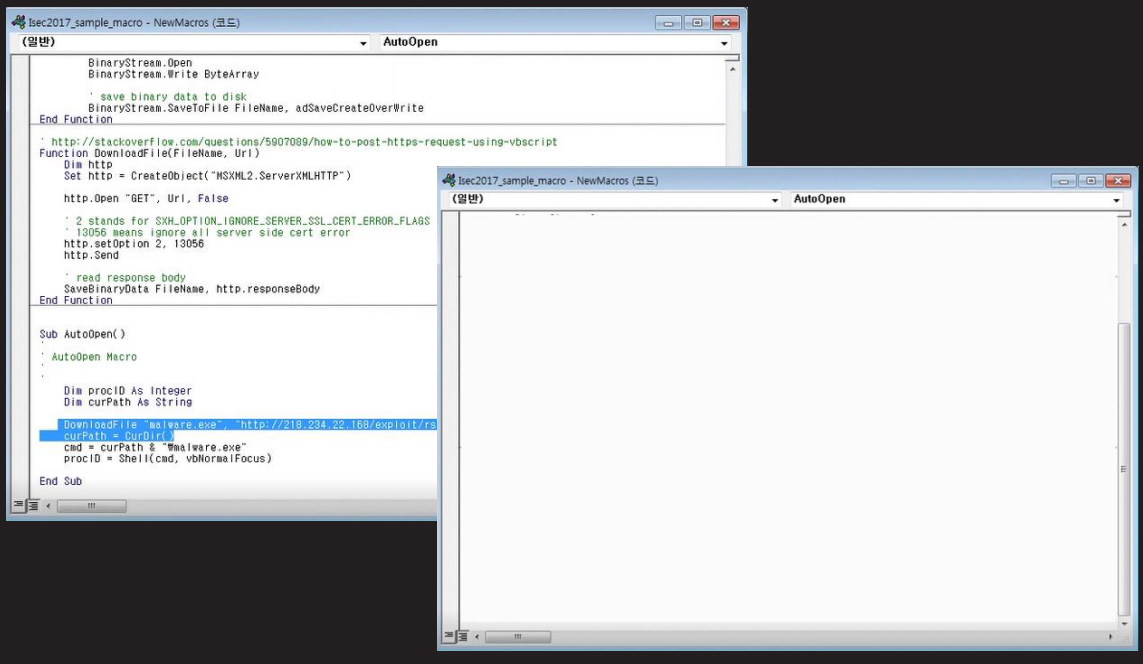

붙임 ① '16년 및 '17년 주요과업 비교
* 더블클릭 하시면 한글문서로 보실 수 있습니다.
② '16년 및 '17년 대남분야 비교
*악성 URL 더블 클릭 유도, 파일 내 OLE 실행*
끝

* 출처 : 주요 매체, Cisco

## 공공기관을 사칭한 표적형 공격

지란지교시큐리티

# 매크로 무해화 사례

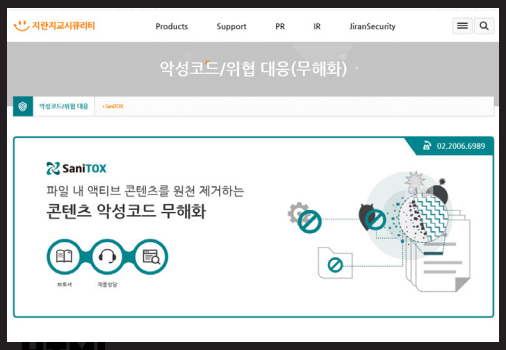



## 액티브 콘텐트 제거&재조합, 잠재적 위협 예방

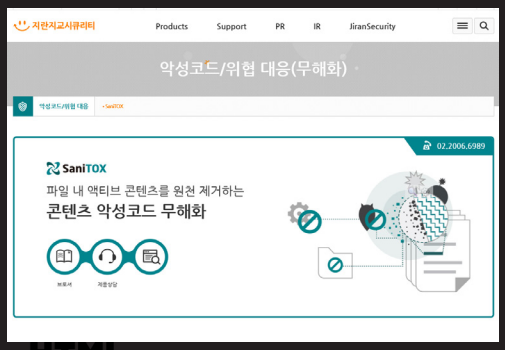
지란지교시큐리티

# 웹 콘텐츠 무해화 적용

*웹 사이트 구조 분석*



*사이트 동작 외 불필요한 요소 제거*



**불필요한 동적 요소들을 제거 후 전달**

지란지교시큐리티

# 웹 콘텐츠 무해화 한계

*불필요한 동적 요소 판단 기준*

*사용자 경험 보존 필수*

*웹 구성 요소 변화 민감*

*높은 웹 콘텐츠 분석 난이도 및 의존성*

**무해화 외 예방적 보안 요소 필요**

지란지교시큐리티

# 원격 브라우저 격리 기술

지란지교시큐리티

# 원격 브라우저 격리 기술

2017년 가트너 선정, 보안 분야 최고 기술 Top 10

## Gartner Identifies the Top Technologies for Security in 2017

Gartner, Inc. today highlighted the top technologies for information security and their implications for security organizations in 2017. Analysts presented their findings during the Gartner Security & Risk Management Summit, being held here through Thursday.

**Remote Browser**

Almost all successful attacks originate from the public internet, and browser-based attacks are the leading source of attacks on users. Information security architects can't stop attacks, but can contain damage by isolating end-user internet browsing sessions from enterprise endpoints and networks. By isolating the browsing function, malware is kept off of the end-user's system and the enterprise has significantly reduced the surface area for attack by shifting the risk of attack to the server sessions, which can be reset to a known good state on every new browsing session, tab opened or URL accessed.

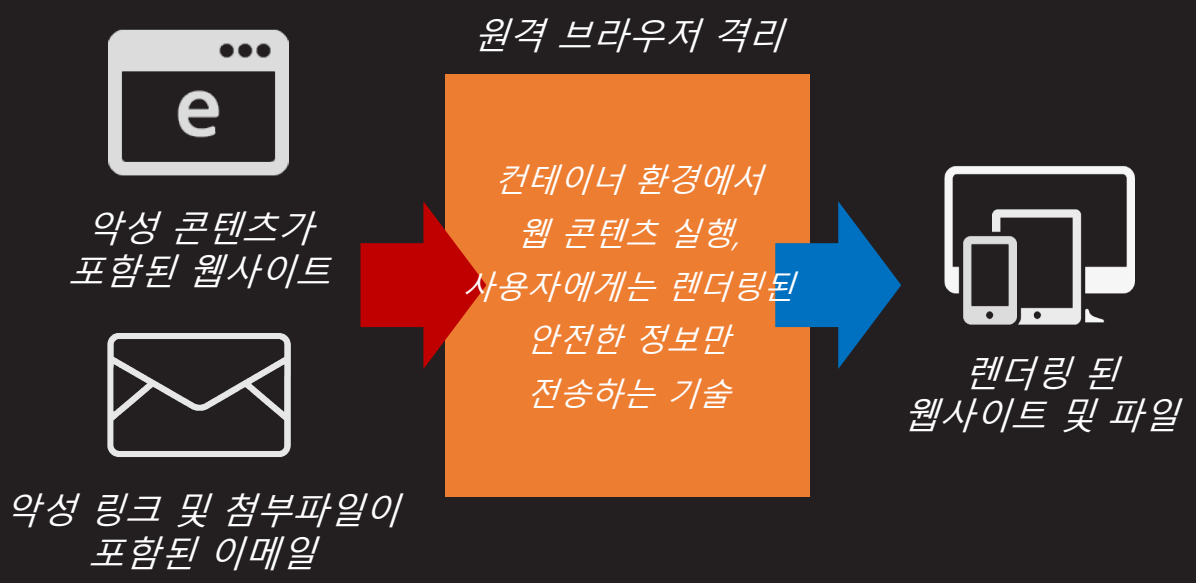
Gartner

*원격 브라우저 격리는 엔터프라이즈 엔드 포인트 및 네트워크에서 최종 사용자의 인터넷 탐색 세션을 격리하는 형태로 브라우징 기능을 분리함으로써 최종 사용자의 시스템 유입을 사전에 예방할 수 있는 기술임.*

## RBI: Remote Browser Isolation

지란지교시큐리티

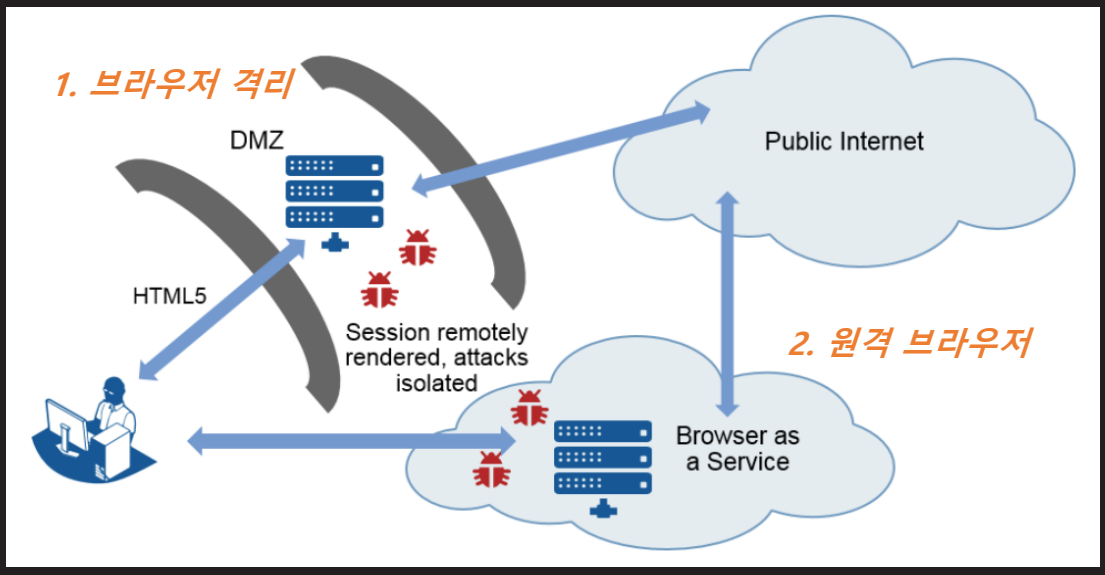
# 원격 브라우저 격리 개요




**사용자 디바이스에서의 실행 원천 차단**

지란지교시큐리티

# 원격 브라우저 격리 기술

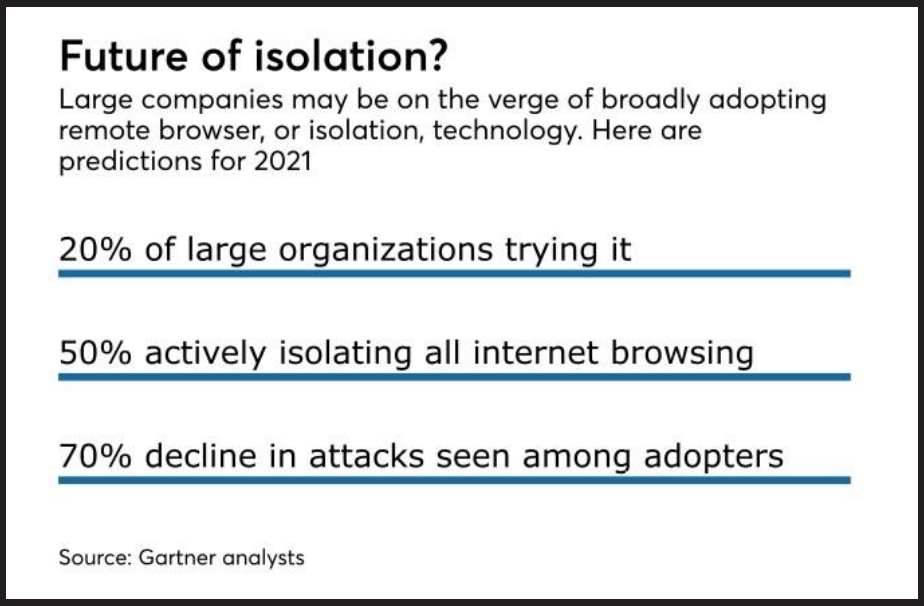



* 출처 : Gartner

**안전한 파일로 재조합 하는 기술**

지란지교시큐리티

# 원격 브라우저 격리 기술 전망




* 출처 : Gartner

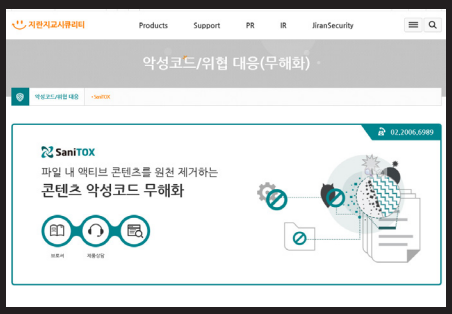
## 액티브 콘텐트 제거&재조합, 잠재적 위협 예방

지란지교시큐리티

# 모바일 웹 콘텐츠 보안 제안

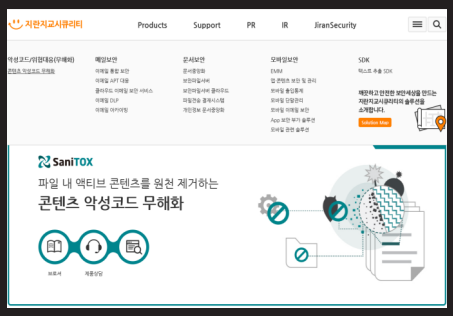
# 웹 콘텐츠 보안 기술 변화

*이미지 변환 및 전달*




*모든 동적 콘텐츠 비활성화, 사용자는 읽기만 가능(인터랙션 불가)*

*웹 콘텐츠 무해화 및 격리*

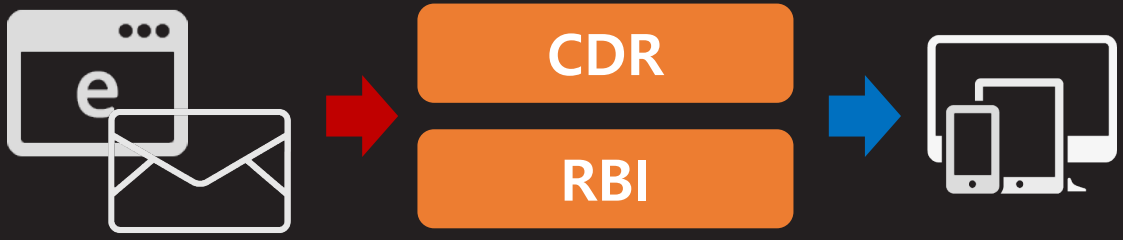



*모든 콘텐츠를 격리, 재가공(무해화) 후 전달, 사용자 경험 보존(인터랙션 가능)*

**이미지 변환 및 전달 → 사용자 경험 보존**

지란지교시큐리티

# CDR + RBI로 구현하는 웹 보안




*웹사이트 및 악성 링크*

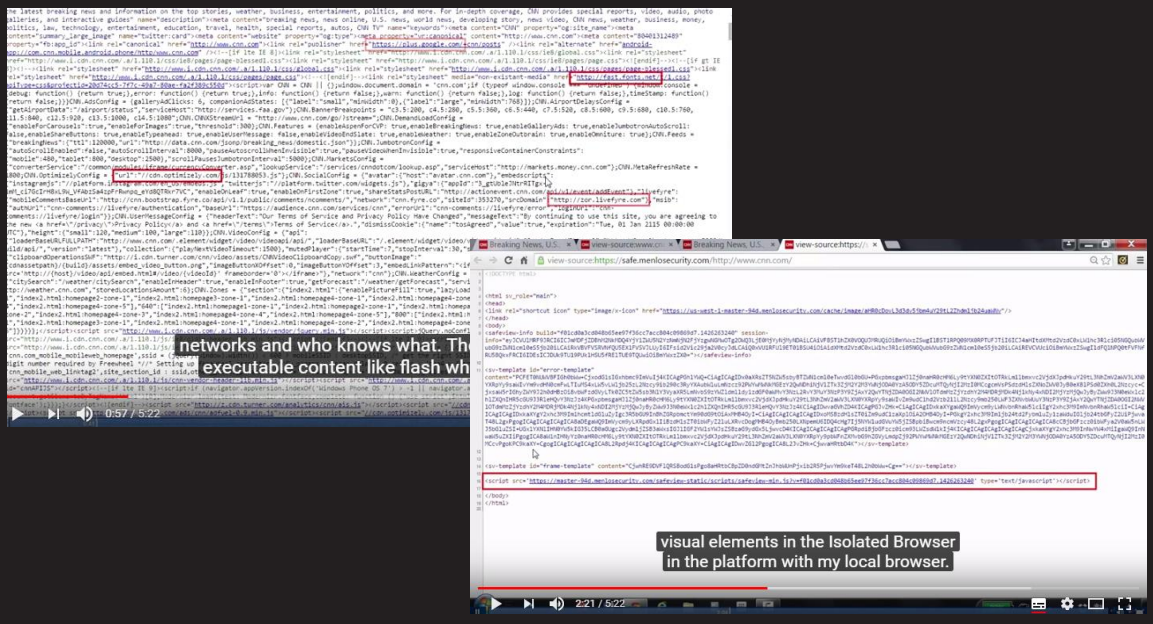
*1차 CDR + 2차 RBI*

*사용자에게 전달(렌더링)*

**발생할 수 있는 위협에 대하여 사전 예방 수행**

지란지교시큐리티

# 웹 콘텐츠 CDR + RBI 적용 예시




엔드 유저에게는 렌더링 코드만 전달

지란지교시큐리티

# CDR + RBI의 기대효과

*브라우저 격리를 통해 위협 요소의 유입을 원천적으로 차단*

*동적 콘텐츠 무해화를 바탕으로 안전한 콘텐츠 제공*

*디바이스, OS 종속성 탈피를 통한 사용자 경험 보존*

디바이스 및 OS 의존성 탈피, 웹 보안 구축

지란지교시큐리티

# 결론

보안 위협의 진화 및 변화에 대응하기 위한 방안으로

**방어**
(악성 유무 판단)

**예방**
(CDR + RBI)

**예방 측면의 모바일 웹 콘텐츠 보안 제시**

지란지교시큐리티

진화하는 사이버위협 '방어'에서
'예방'으로 변화가 필요합니다.

지란지교시큐리티

# 감사합니다.

지란지교시큐리티

The 24th Network Security Conference -Korea

# 5G 이동통신 인증프레임워크

**유일선** 순천향대 교수

### 학력 및 경력사항

| | |
|---|---|
| 2002.02 | 이학박사, 단국대학교 |
| 2012.03 | 공학박사, 큐슈대학교 |
| 2015.09 ~ 현재 | 부교수, 순천향대학교 |
| 2017.01 ~ 현재 | 학과장, 순천향대학교 정보보호학과 |
| 2012.01 ~ 현재 | 한국정보보호학회 이사 |
| 2010.03 ~ 현재 | 편집장, JoWUA 저널 (Scopus) |
| 2016.01 ~ 현재 | 편집위원, Information Sciences (IF: 4.832) |
| 2016.01 ~ 현재 | 편집위원, JNCA (IF: 3.5) |
| 2017.01 ~ 현재 | 사물인터넷포럼 정보보호분과 위원 |
| 2014.09 ~ 현재 | IFIP WG8.4 member |
| 2014.04 ~ 현재 | IET Fellow |
| 2014.01 ~ 현재 | IEEE Senior Member |

### 강연요약

본 강연에서는 3GPP SA3 워킹그룹에서 제안되었던 5G 보안에 관한 기술문서 3GPP TR 33.899 V1.3.0을 중심으로 차세대 5G 네트워크를 위한 독립적인 보안앵커(Security Anchor) 기반의 인증프레임워크 구조와 키계층, 그리고 인증 및 키교환을 다룰 예정이다. 또한, 집계서명을 활용한 대규모 사물인터넷 장치의 인증 프로토콜에 대해서 소개할 예정이다.

The 24th Network Security Conference-Korea

# NetSec-KR 2018

## 5G 이동통신 인증프레임워크

순천향대학교 정보보호학과
모바일인터넷보안연구실
유일선 교수
isyou@sch.ac.kr

SCH 순천향대학교 정보보호학과

## INDEX

- 5G 혁명
- 5G 보안 표준화 현황
- 5G 보안 프레임워크
- 5G 환경에서 대규모 IoT 기기 인증
- Q & A

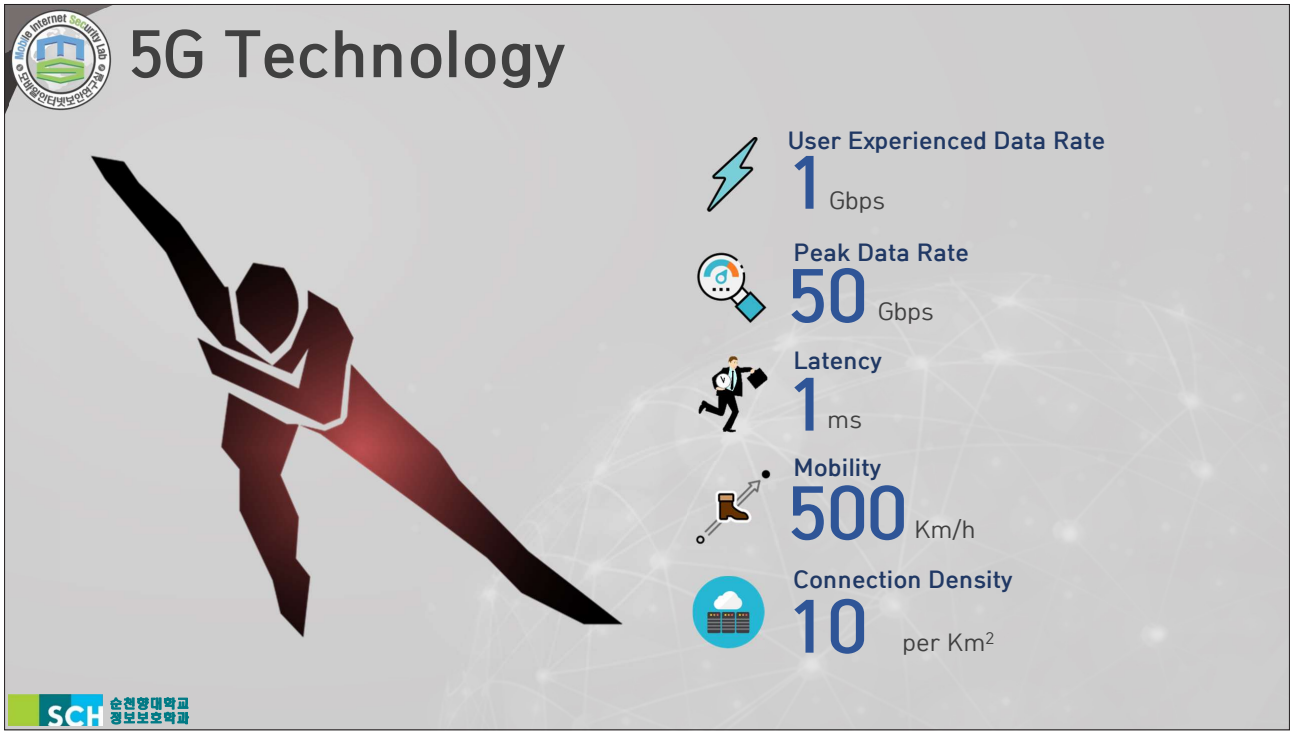
SCH 순천향대학교 정보보호학과

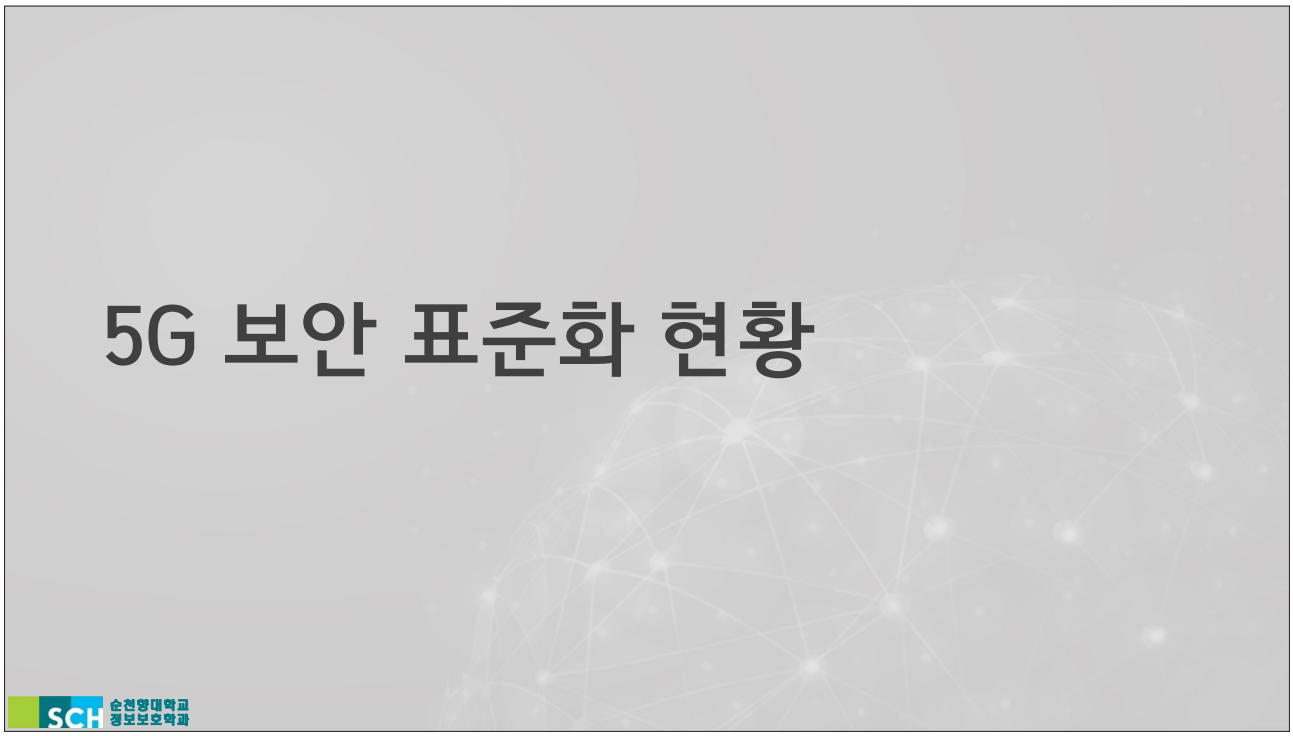
# 5G 혁명

SCH 순천향대학교 정보보호학과

# 5G Revolution

SCH 순천향대학교 정보보호학과


5G Technology
User Experienced Data Rate
1 Gbps
Peak Data Rate
50 Gbps
Latency
1 ms
Mobility
500 Km/h
Connection Density
10 per Km2
SCH 순천향대학교 정보보호학과


5G 보안 표준화 현황
SCH 순천향대학교 정보보호학과

# 5G Security Standard

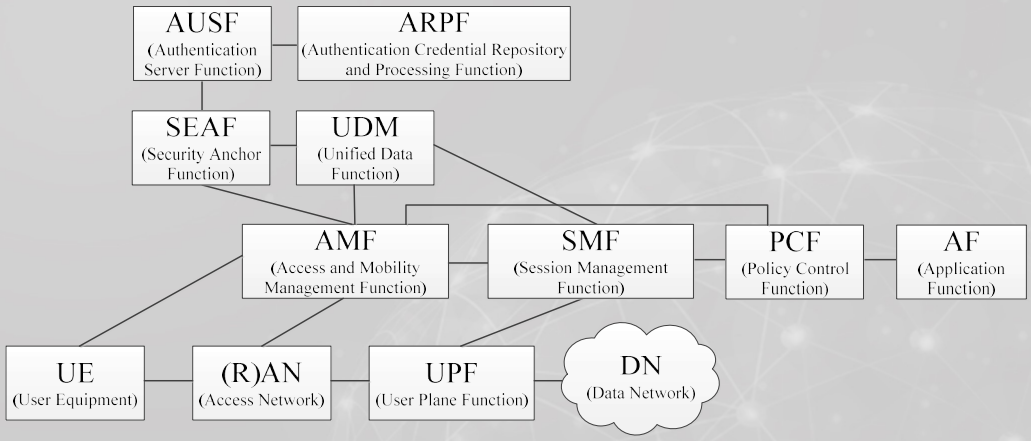
- 3GPP TR 33.899 v1.3.0 (Release 14)
  - 2017년 8월 배포
  - 차세대 시스템의 보안 측면 연구에 관한 기술 보고서
  - 2017년 9월 Withdrawn
- 3GPP TS 33.501 v1.0.0 (Release 15)
  - 2018년 3월 배포
  - 5G 시스템의 보안 구조 및 절차에 관한 기술 사양 문서
- 3GPP TS 28.530 v0.5.1 (Release 15)
  - 2018년 3월 배포
  - 통신 관리, 5G 네트워크, 네트워크 슬라이스 관리의 개념, 사용사례 및 요구사항에 관한 기술 사양 문서



# 5G 보안 프레임워크

# 5G 네트워크 구조

- 3GPP TS 33.501 v1.0.0






# 5G 네트워크 구성요소의 기능 및 역할

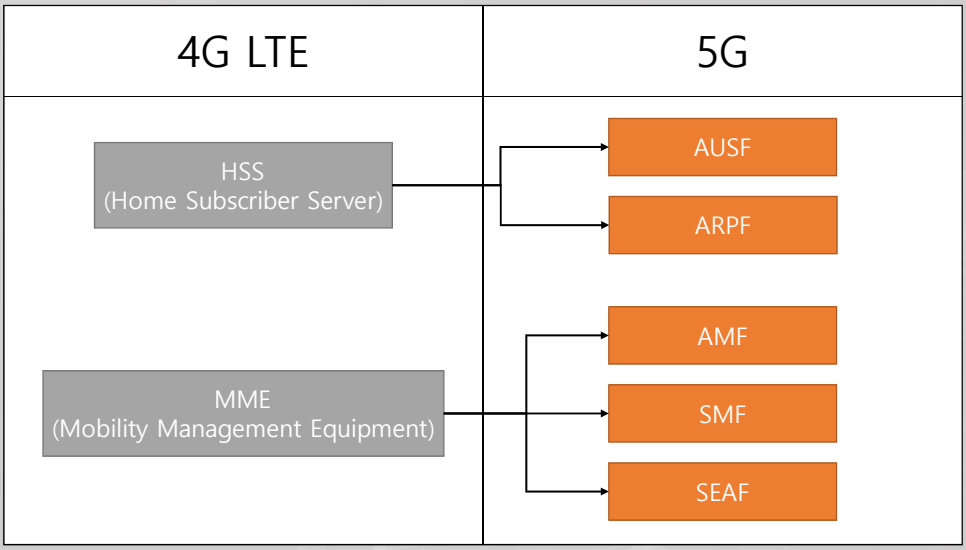
| 엔티티 | 기능 및 역할 |
|---|---|
| UE (User Equipment) | 네트워크 사용자의 장비 |
| RAN (Radio Access Network) | 새로운 무선 액세스 기술을 사용하는 기지국 |
| AN (Access Network) | Non-3GPP 접속 기술을 포함한 일반적인 기지국 |
| UPF (User Plane Function) | User Plane 데이터 처리를 담당 |
| DN (Data Network) | 네트워크 운영자의 서비스 또는 인터넷 액세스 서비스 |
| AMF (Access and Mobility management Function) | UE의 등록 및 연결 관리<br>UE의 접근 및 이동성 관리<br>UE의 접근 인증 및 인가<br>UE와 SMF 간의 세션 관리 메시지 전달<br>보안 문맥 관리 (SCM; Security Context Management) |
| SMF (Session Management Function) | 세션 설정의 수정 및 해제 관리<br>UE의 IP 주소 할당 및 관리<br>로밍 기능<br>UPF에서의 과금 데이터 수집의 제어 및 조정 |
| PCF (Policy Control Function) | 네트워크 동작을 제어하기 위한 통합 정책 프레임워크 지원 |

# 5G 네트워크 구성요소의 기능 및 역할

| 엔티티 | 기능 및 역할 |
|---|---|
| AF (Application Function) | 트래픽 라우팅에 대한 Application Influence<br>Network Exposure 기능 접근<br>정책 통제를 위한 정책 프레임워크와의 상호작용 |
| UDM (Unified Data Function) | 3GPP AKA 인증 자격 증명의 생성<br>사용자 식별 처리<br>Subscription Data를 기반으로 액세스 권한 부여<br>UE의 Serving NF 등록 관리 |
| SEAF (SEcurity Anchor Function) | 초기 인증 처리<br>UE의 보안 기능을 기준으로 보안 매개 변수 결정<br>5G 보안의 핵심 중추 역할 |
| AUSF (AUthentication Server Function) | 5G의 인증 절차에서 EAP의 Authenticator 역할 수행 |
| ARPF (Authentication Credential Repository and Processing Function) | UE의 인증정보를 저장<br>EAP의 인증 서버 역할 수행 |



# 5G 네트워크 구조 변화

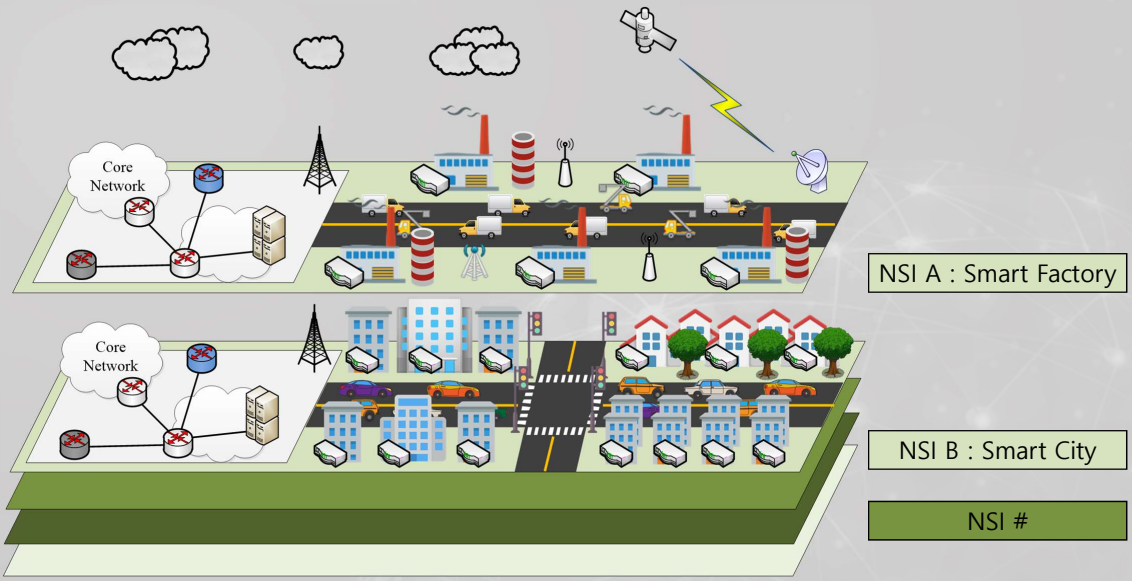


# 네트워크 슬라이스

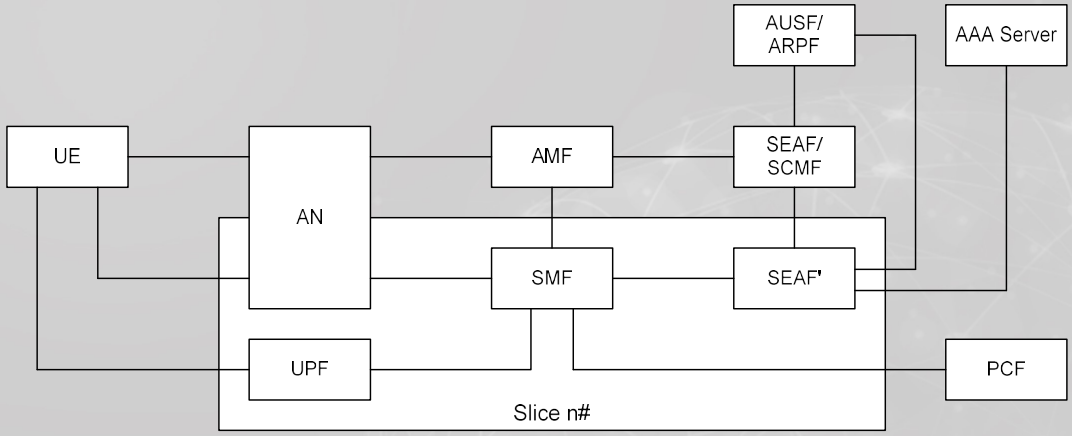
- 네트워크 슬라이스란 네트워크의 자원과 기능을 개별 서비스에 맞춰 하나의 독립적인 슬라이스(Slice)로 제공하는 것
- 네트워크 슬라이스의 특징은 다음과 같음
  - 맞춤형(Customization)
  - 자원의 분리(Isolation)
  - 독립적인 관리(Independent Management and Orchestration)
- 사용자, 서비스, 비즈니스 모델 등의 기준에 따라 네트워크 기능들을 선택 및 조합하여 **독립적이고 유연한 서비스**의 제공 가능



# 네트워크 슬라이스 구조

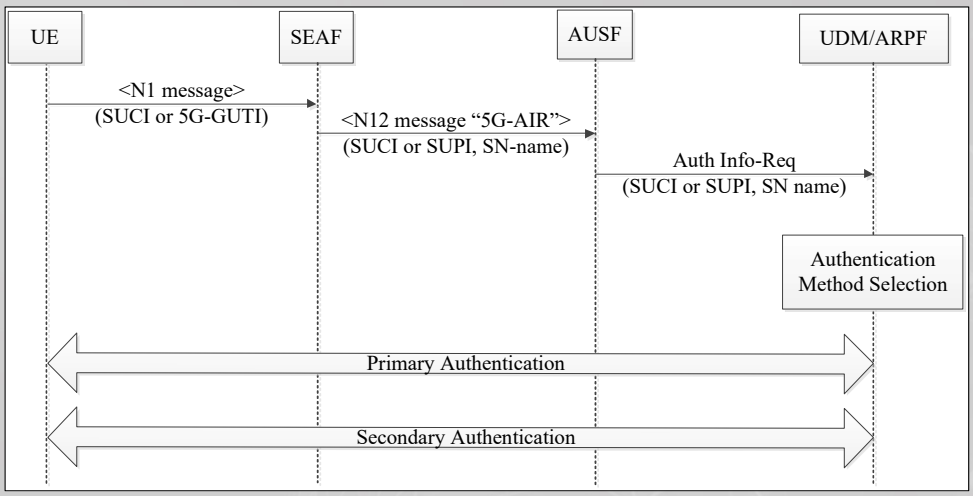


# 네트워크 슬라이스 구조






# 5G 인증 절차



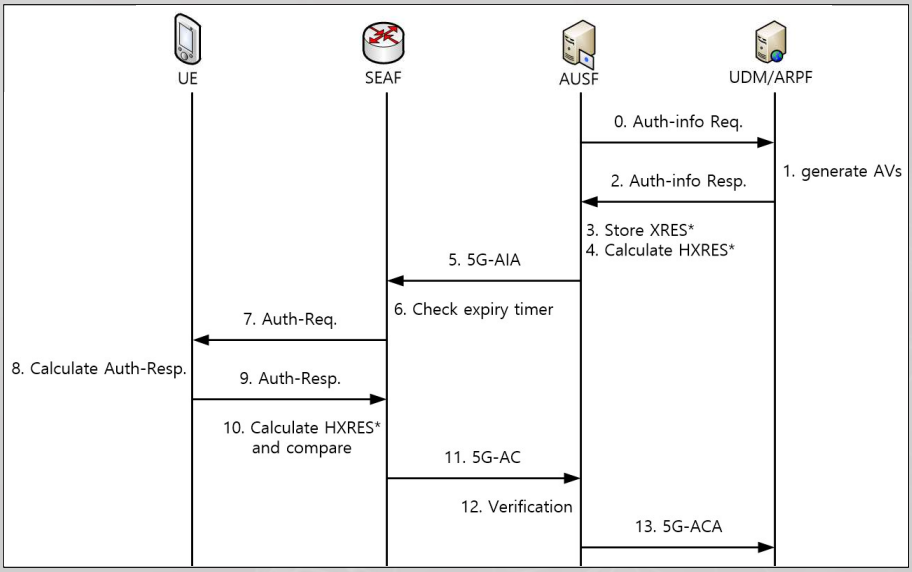
# 5G 인증 프레임워크

- 5G의 인증은 크게 **Primary Authentication**과 **Secondary Authentication**으로 분류됨
- Primary Authentication은 Core Network 접근 시에 활용되며
- Secondary Authentication은 각 기능에 특화된 네트워크 슬라이스의 접근에서 활용됨

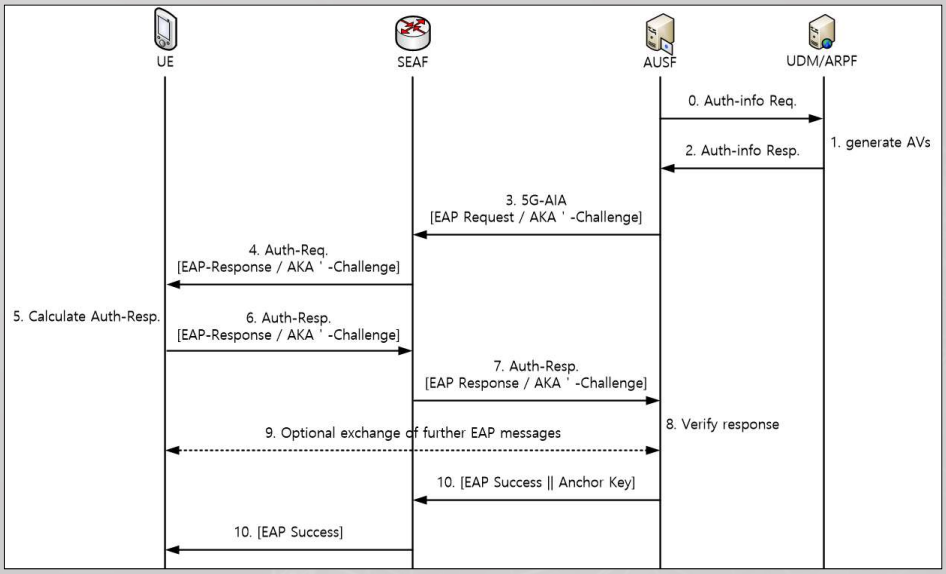
- 5G 인증에서 활용될 것으로 예상되는 유망한 인증 기법으로 **EAP-AKA'**과 **5G-AKA**가 있음
- 해당 기법들은 기존의 4G에서의 AKA와는 다르게 **2개의 인증 벡터**를 사용함
- 2개의 인증 벡터를 활용하여 UE와 SEAF간의 인증을 AUSF에게 **증명**할 수 있음



# 5G-AKA

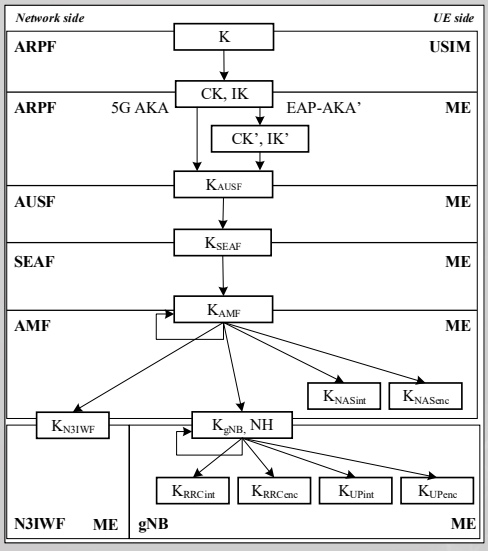


# EAP-AKA′





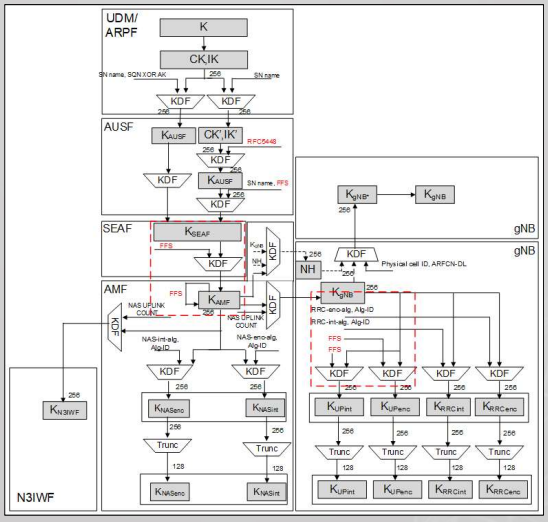

# 5G 키 계층



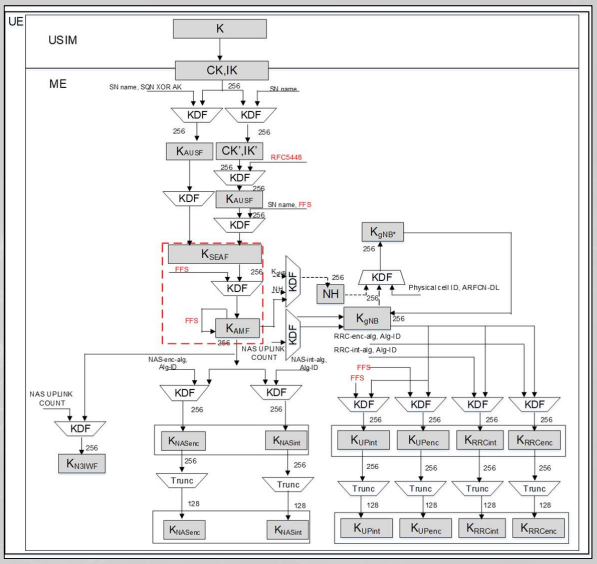

- AMF에서 활용되는 키
  - $K_{AMF}$
- NAS 신호를 위한 키
  - $-K_{NASint}$
  - $-K_{NASenc}$
- gNB에서 활용되는 키
  - $-K_{gNB}$
- U-Plane 트래픽을 위한 키
  - $K_{UPenc}$
  - $K_{UPint}$
- RRC 신호를 위한 키
  - $K_{RRCenc}$
  - $K_{RRCint}$
- 중간 키
  - NH
  - $K_{gNB}^{*}$
  - $K'_{AMP}$

# 5G 키 계층

- for Network Nodes




- for UE




순천향대학교 정보보호학과

# 5G와 IoT

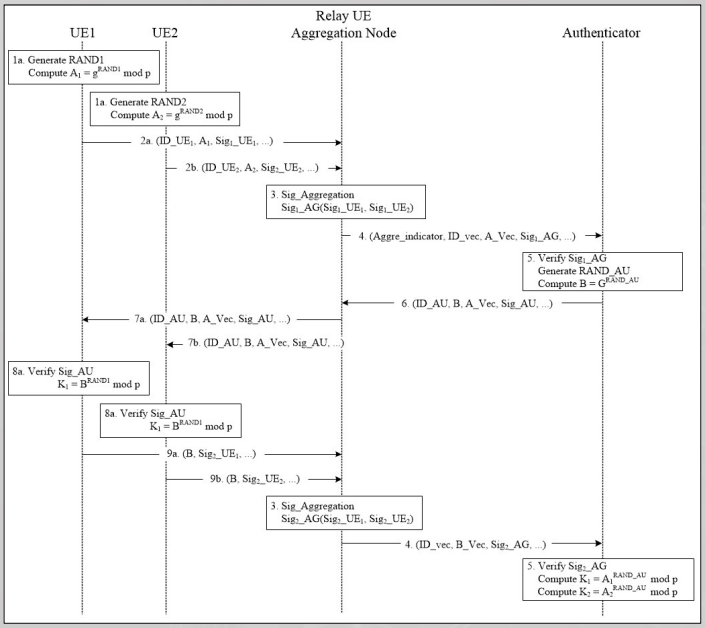
순천향대학교 정보보호학과

# AA-mIoT

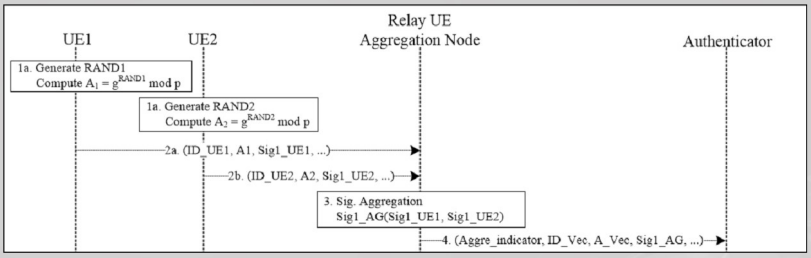
- 3GPP TR 33.899 v1.3.0에서 AA-mIoT가 제안됨
- AA-mIoT (Aggregation Authentication for massive IoT) 프로토콜은 대규모의 IoT 환경에서 발생할 수 있는 **시그널 과부화(Signaling Storm)**를 막기위해 제안됨
- Aggregation Node가 각각의 UE로부터 전송 받은 서명을 결합하여 집계 서명을 생성하고 Authenticator가 집계 서명을 인증함
- 다수의 서명을 하나의 집계서명으로 압축하기 때문에 **시그널 과부하를 예방**할 수 있음



# AA-mIoT



# AA-mIoT 절차




(1a) UE들은 DH 개인키 RAND값을 생성하고 DH 공개키 A를 계산함

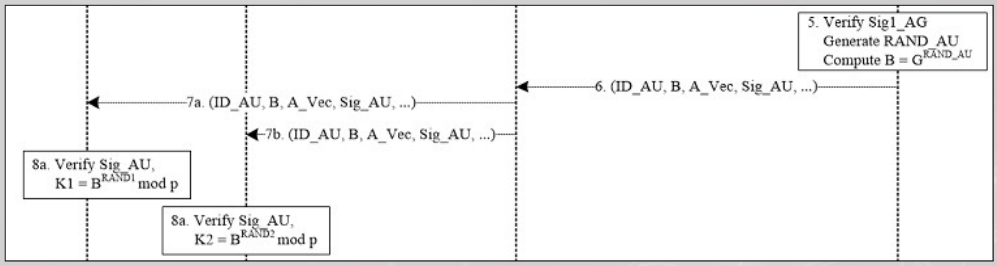
(2a)-(2b) UE들은 인증메시지($ID_{UE}$, $A_n$)를 생성하고 IBS 개인키로 전자서명($Sig_n$)을 생성하여 Aggregation Node로 전송함

(3) UE들로부터 수신한 서명을 집계하여 전자서명($Sig_1$_AG)을 생성함

(4) Aggregation Node는 집계된 인증메시지를 Authenticator에게 전송함



# AA-mIoT 절차



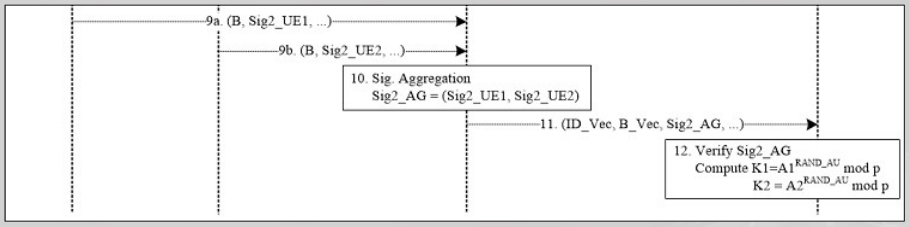

(5) Authenticator는 $Sig_1$_AG를 우선 검증하고, DH 개인키 RAND_AU를 생성하고 DH 공개키 B를 계산함

(6) Authenticator는 응답 메시지(ID_AU, B, A_Vec)와 전자서명(Sig_AU)를 Aggregation Node에게 전송함

(7a)-(7b) Aggregation Node는 수신한 응답 메시지를 UE들에게 전송함

(8a) UE들은 Sig_AU를 우선 검증하고, DH 공개키 B를 활용하여 세션키 $K_n$을 생성함

# AA-mIoT 절차




(9a)-(9b) UE들은 Authenticator의 DH 공개키 B와 이를 자신의 IBS 개인키로 전자서명(Sig2_$UE_n$)하여 Aggregation Node에게 전송함

(10) Aggregation Node는 서명을 집계하여 Sig2_AG를 생성함

(11) Aggregation은 Sig2_AG를 Authenticator에게 전송함

(12) Authenticator는 Sig2_AG를 우선 검증하고, 세션키 $K_n$를 생성함



# AA-mIoT를 위한 연구

- Massive-IoT를 효과적으로 인증하기 위한 방법으로 **IBAS(Identity-Based Aggregate Signature)**가 핵심 기술로 떠오르고 있음
  - Cheon et al. IBAS
  - Herranz et al. IBAS
  - Hohenberger et al. IBAS
  - S. Deva Selvi et al. IBAS
  - Yuan et al. IBAS
  - Gentry et al. IBAS

# AA-mIoT를 위한 연구

| IBAS | ST(ms) - 서명시간 | | AL(bits) | | VT(ms) - 검증시간 | |
|---|---|---|---|---|---|---|
| | 80/SS2 | 128/BN | 80/SS2 | 128/BN | 80/SS2 | 128/BN |
| Cheon et al. | 0.38 | 0.22 | 379,379 | 256,256 | 1561.56 | 2542.32 |
| Herranz et al. | 1.14 | 0.66 | 379,379 | 256,256 | 2321.56 | 2983.32 |
| Hohenberger et al. | 1180 | 2320 | 379 | 256 | 1532821.18 | 3013682.32 |
| S. Deva Selvi et al. | 0.38 | 0.22 | 635,256 | 515,128 | 2280.76 | 1320.44 |
| Yuan et al. | 0.38 | 0.22 | 1137 | 768 | 384.72 | 229.28 |
| Gentry et al. | 2.28 | 1.32 | 886 | 640 | 383.54 | 226.96 |

- MIRACL에서 제공하는 Benchmark를 기반으로 각 IBAS에 요구되는 연산량을 계산함



# AA-mIoT 분석

- 3GPP TR 33.899-130에서 제안된 AA-mIoT 프로토콜은 초기단계의 연구에 있지만 5G 네트워크 환경에서 대규모 IoT를 지원하기 위한 프로토콜로서의 의미가 있음
- AA-mIoT를 위한 연구 진행 상황
  - 지금까지 제안된 IBAS들의 구체적인 집계 서명 크기와 서명 검증 시간을 고려해보면 **Gentry et al.의 기법이 가장 적합함**
  - 그러나, Gentry et al.의 기법은 서명 시간이 상대적으로 길어 이에 대한 **개선이 필요**

# 감사합니다

KISA 한국인터넷진흥원

# 2018 인터넷 10대 이슈
# INTERNET 10 ISSUES

01

환상에서 현실로…실생활 적용 시작한
**인공지능**

02

시범사업으로 날개다는
**블록체인**

03

상용화 시동 거는
**자율주행차**

04

규제 샌드박스에서 성장의 싹이 트는
**4차 산업혁명 규제 혁신**

05

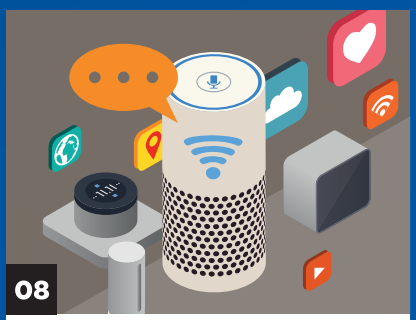
생활 속 반려자로 자리 잡을
**로봇**

06

평창 동계올림픽과 함께 눈앞에 펼쳐질
**5G**

07

내가 쇼트트랙 국가대표가 되는
**가상현실·증강현실**



08

음성 혁명의 촛불이 될
**대화형 서비스**

09

건강체크를 넘어 진단으로,
**디지털 헬스케어**

10

디지털 신도시 설계가 본격화 될
**스마트시티**

KONA CARD

매 달 혜 택 이 **업 데 이 트**

# 코나카드

## 4 월 의 업 데 이 트 혜 택

스타벅스 **30%**, 커피빈 **20%**, 버거킹 **10%**, GS25 **10%**

코나카드

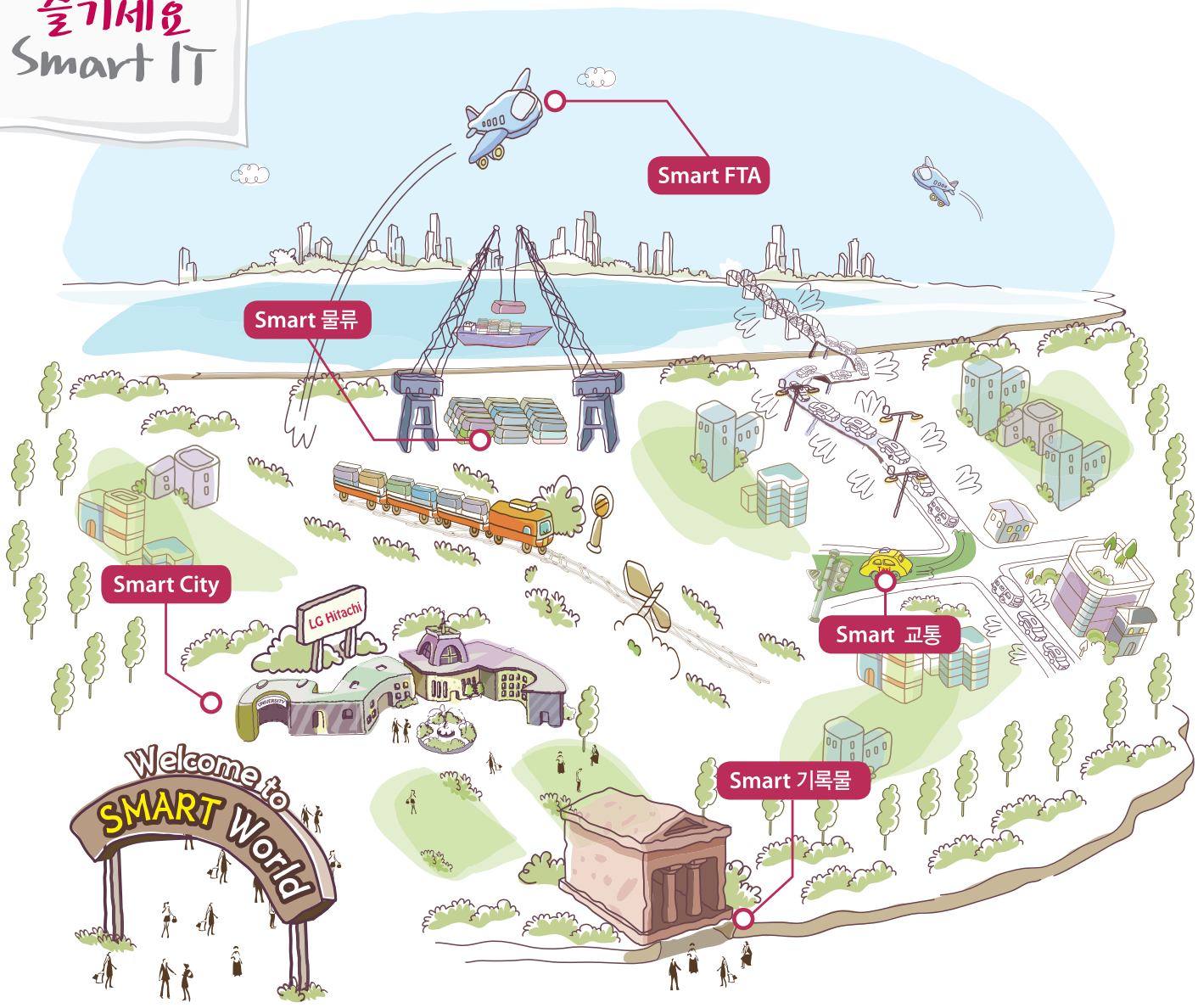
Download on the App Store

Download on the Google Play

LG히다찌

http://www.lghitachi.co.kr

즐기세요
Smart IT




# LG히다찌가
# Smart 세상을 만들어 갑니다

# SecuSign 모바일 생체수기서명 인증

SecuSign(시큐사인)은 사용자의 모바일 단말기에 손가락 또는 터치펜으로 서명을 하면 사용자의 서명행위 과정의 동적인 행위특징정보를 인식하여 서명자를 인증하는 기술로 기존 서명 결과 이미지를 비교하는 방식을 넘어선 최첨단 핀테크 인증 솔루션 입니다.

## 생체수기서명 인증의 강점

| 항목 | 생체수기서명 (행위적 특징 기반 바이오 인증) |
|---|---|
| 인증 방식 | 사용자 행위적 특징 기반 인증 |
| 생체 정보 유출 대응 | 유출 대응 가능 (유출되었을 경우, 서명 변경을 통해 대응 가능) |
| 타인에 의한도용 가능성 (수면, 음주 등 무의식 상태) | 무의식 상태에서 인증 불가 (본인의 의식과 의지가 있어야만 인증 가능) |
| 복제 가능성 | 인증 당시 동적인 데이터를 입력해야하므로 복제 불가능 |
| 외부 환경 영향 | 외부환경에 대한 영향 없음 |
| 추가적인 인식 센서 | 추가적인 장치 필요 없음 (모든 스마트폰 지원 가능) |
| 응용/활용성 | 다양한 응용 방안<br>- 필기인식과 연동 (요구되는 OTP 암호 등을 입력)<br>- 겹쳐 쓰는 암호 입력<br>- 조건(결제 금액 등)에 따라 다른 서명 입력 |

## 시큐사인(SecuSign)활용분야

핀테크 서비스 | 본인확인 (인증)서비스 | Outdoor Sales | O2O | 공공기관 | 공인인증서 대체효과

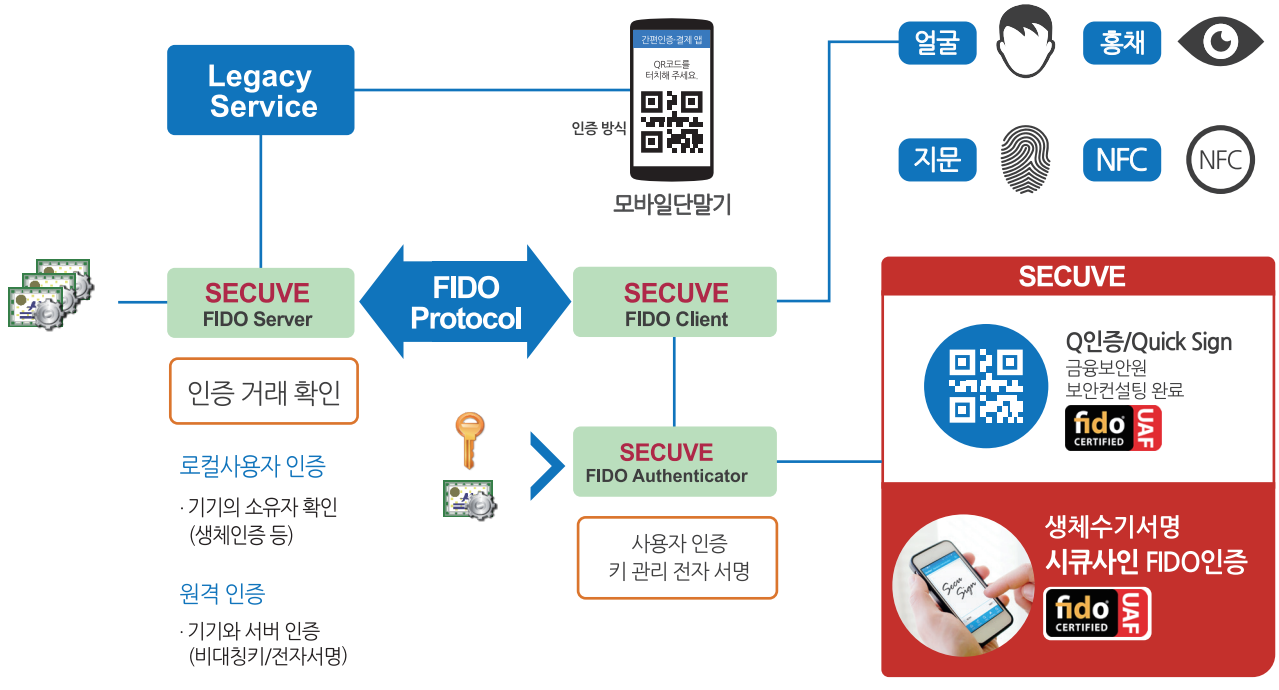
### 시큐사인(SecuSign) 지원 플랫폼

안드로이드 | 아이폰(iOS) | 모바일 웹

## FIDO(Fast Identity Online)인증 통합 플랫폼

퀵사인(QuickSign) 플랫폼과의 연동 구성

- SecuSign FIDO Authenticator for Android 1.0
- SecuSign FIDO Authenticator for iOS 1.0




· FIDO 인증 취득 (2016.03)

SECUVE 시큐브
www.secuve.com
주소:서울특별시 구로구 디지털로 26길 111 JnK디지털타워 801호 (우:08390)
대표전화:02) 6261-9300 | 팩스:02) 6261-9309 | E-mail:webmaster@secuve.com
KOSDAQ 코스닥상장법인

fido ALLIANCE MEMBER

# 암호화폐 거래소 보안

# II

# 라온시큐어

## 해킹으로부터 안전한 비즈니스 환경,
## 금융권 수준 보안체계를 구축하고 싶다면!

라온시큐어는 다수의 금융 및 공공 레퍼런스를 보유한 통합 ICT 보안 선도기업입니다.

라온시큐어 7대 모바일 보안 기술

ONEGuard

MDM 단말관리 MAM App관리 MTM 위협관리 MIM 계정관리

모바일 전자서명 (PKI)

모바일 백신

모바일 구간 암호화

모바일 보안 키패드

모바일 OTP

앱 위변조 및 디컴파일 방지

iOS MDM 공식지원

삼성전자 엔터프라이즈 얼라이언스 프로그램 S.E.A.P. Gold 파트너

삼성패스, 삼성 녹스(KNOX) 공식파트너

LG전자 MDM 공식 파트너

Intel Software Partner 선임

RAONSECURE 모바일 솔루션에 대해 더 알고 싶으신가요?
Email : mkt@raonsecure.com Tel : 070-8240-3406 www.raonsecure.com

# POWER OF VISIBILITY

## 가시성, 대응의 차원을 바꾸다

AhnLab MDS는 지능형 위협(APT), 타깃 공격 및
다양한 경로를 이용한 고도화된 공격에 효과적으로 대응합니다.

## AhnLab MDS

### AhnLab MDS에게만 허용된 4가지 특별함

No 1. 직관적인 UI로 위협의 흐름 및 행위에 대한 상세한 정보 제공
No 2. 악성코드 자동 • 수동 삭제 및 실행 보류를 통한 랜섬웨어 대응
No 3. 이메일 기반의 다양한 공격 탐지 및 대응(MTA)
No 4. 머신러닝 기반의 의심파일 수집을 통한 잠재 위협 탐지 및 대응

대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 팩스 : 031-722-8901 | 경기도 성남시 분당구 판교역로 220 (우)13493

www.ahnlab.com

지란지교시큐리티

문서 기반 악성위협에 톡! 톡! 톡!

# 이제 SaniTOX 하세요!

사회공학적 기법의
메일 첨부파일 공격

문서 형태의
샌드박스 우회 공격

문서 취약점 악용한
표적 공격

서버간 자료 전송 시
악성코드 유입 공격

바이러스 검사 · 무해화 · 파일재조합

문서 기반 악성위협 대응을 위한 최적의 솔루션_콘텐츠 악성코드 무해화

## SaniTOX 어플라이언스 출시!

**SaniTOX**는 CDR 엔진을 적용한 **콘텐츠 악성코드 무해화 솔루션**으로 이메일, 웹·파일서버 등 다양한 채널을 통해 유입되는 파일 내 포함된 액티브 콘텐츠를 원천 제거한 후 안전한 파일로 재조합하여 제공함으로써 문서 형태로 유입되는 랜섬웨어, APT 등 잠재적인 보안 위협 실행을 사전에 예방합니다.
SaniTOX 어플라이언스는 **별도의 소프트웨어 설치나 설정이 필요없는 일체형 장비**로 간편한 구축 및 운영이 가능합니다.

* CDR : Contents Disarm&Reconstruction, 콘텐츠 무해화&재조합)

### 자체 개발 CDR 엔진 탑재

- 다년간의 R&D 투자를 통해 자체 개발한 CDR 엔진 보유

### Known/Unknown 위협 대응

- Content Prevention Engine (Anti-Virus+CDR) 으로 Known/ Unknown 위협에 전방위적 대응

### 다양한 네트워크 지원

- 단일 어플라이언스 장비에서 웹서버, 파일서버(FTP, SMB) 등 연동 지원

EVENT

### 방문상담 신청 이벤트

SaniTOX 무료 방문 상담을 신청하신 분들께 **샤오미 에어웨어(미세먼지 방지 마스크+리필필터)**를 선물로 드립니다.

기 간 2018년 3월 26일(월) - 2018년 4월 30일(월)

대 상 SaniTOX 방문상담 신청 고객

신 청 신기술융합사업부 02-2006-6989 /sanitox@jiran.com 신청

※1차 유선상담 후 방문상담 확정 고객에게 상담일에 전달드립니다.

제품 문의 신기술융합사업부 영업마케팅팀 | 02-2006-6989 | sanitox@jiran.com

지란지교시큐리티
KOSDAQ 코스닥상장법인
서울특별시 강남구 역삼로 542, 5층(대치동, 신사S&G) www.jiransecurity.com

# 차세대 보안을 디자인하다

## 더 강력해진 국가대표 침입방지시스템

*인텔리전트 보안 | 조직에서 가용한 모든 정보를 수집, 분석 후 조치 가능한 정보를 도출하는 것

네트워크기반의 위협 트래픽
**심층분석** 및 **상관분석기술**로
공격을 방어합니다.

차세대 침입방지시스템

# SNIPER ONE-i


(주)윈스

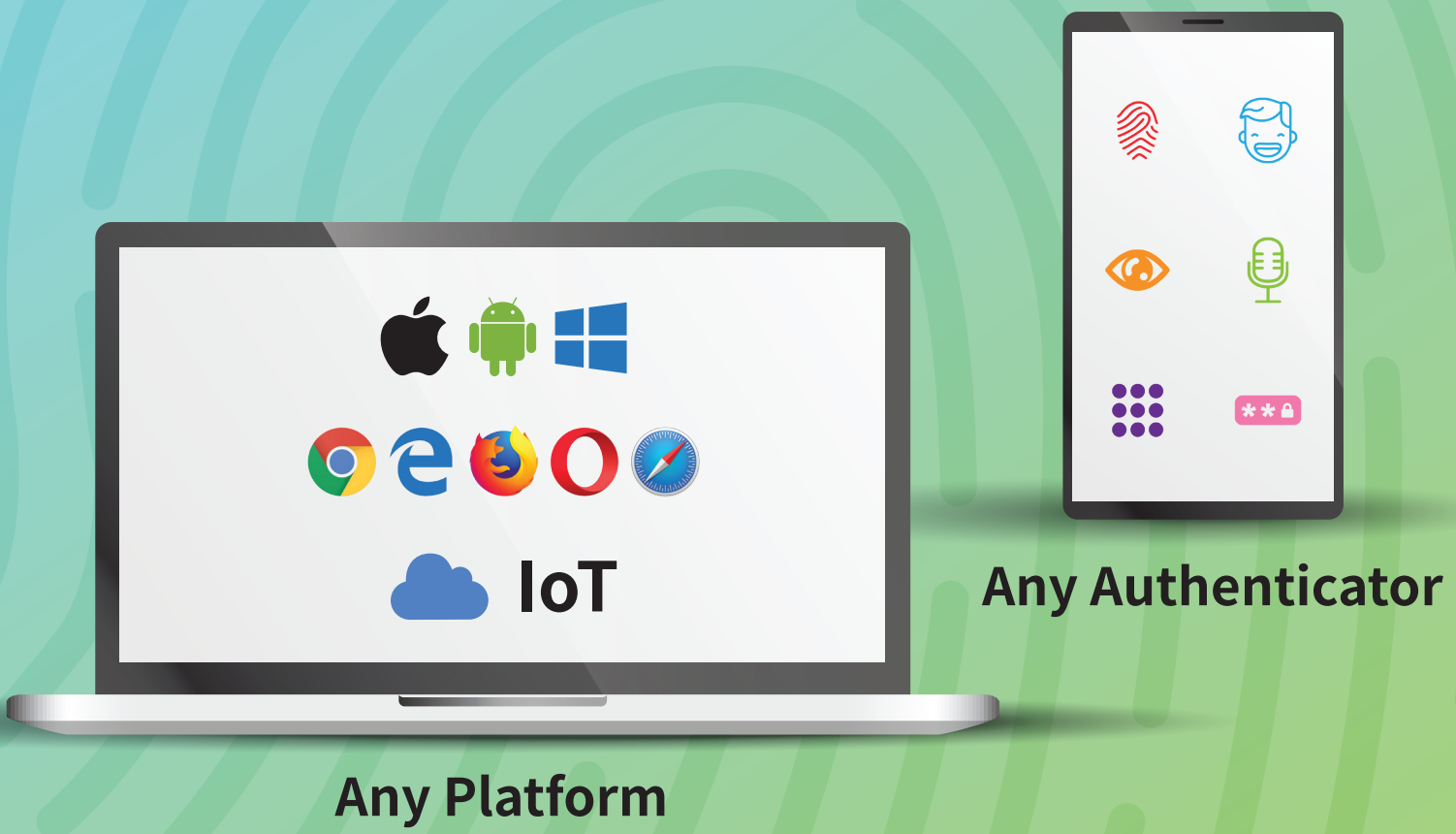
WORLD CLASS 300 선정기업

경기도 성남시 분당구 판교로 228-17 세븐벤처밸리 2단지 4, 7층 / 1단지 4층

Tel. 031-622-8600 I Fax. 031-622-8601 I www.wins21.co.kr

# 생체인증의 새로운 시작

# Magic FIDO 2.0




DREAM SECURITY Digital Trust

(주)드림시큐리티 | Dream Security Co., Ltd.
05833 서울특별시 송파구 중대로8길 8 서경빌딩 3~7층
Seokyoung Bldg. 3~7F, 8, Jungdae-ro 8-gil, Songpa-gu, Seoul, Korea 05833
Tel 82 2 2233 5533 Fax 82 2 402 3622 www.dreamsecurity.com

문의 : 02-2233-5533

# SentryAPT는

## 알려진 보안위협과 잠재적인 보안 위협까지 탐지/제거하는 **차세대 APT 보안 솔루션** 입니다.

**탐지(Detection)**
대응의 판단 근거를 제공하는 위협 이벤트 탐지

**대응(Response)**
탐지한 결과를 기반으로 한 대응 기능

**분석(Analysis)**
위협 탐지를 위한 방안 제공

**운영·관리**
시스템 관리 및 운영을 위한 제반 기능

| 비교항목 | 서버 운영체제 지원 | Windows PC 환경 지원 | 알려진 위협의 정적분석 지원 | 비정상 행위 탐지 기능 지원 | 가시성 확보 제공 | 실질적인 대응 / 조치기능 제공 |
|---|---|---|---|---|---|---|
| 기존 Sandbox | ○ | ○ | ◑ | ◑ | ◔ | ◔ |
| Post-Sandbox | ◔ | ⊖ | ◑ | ◔ | ◑ | ◔ |
| | ● | ● | ● | ● | ● | ● |
| | 대부분의 상용 Unix, Linux 및 Windows 서버 지원 | Windows PC 이외에 상용 Unix, Linux, Windows 서버 지원 | 알려진 위협 외에 비정상 행위 기반의 분석 기능 지원 | 비정상 행위 기반의 탐지 / 대응 / 분석 기능 지원 | APT 킬체인 매핑, 위협레벨링을 통한 가시성 지원 | 프로세스 Kill, 접근통제 등의 실질적인 대응기능을 지원 |

○ 미지원 ◔ 미흡 ◑ 보통 ◔ 양호 ● 지원

SGA Solutions Co., Ltd.
에스지에이솔루션즈(주)

**주소** : 05836 서울시 송파구 법원로11길 25, H비지니스파크 A동 901호
TEL : 02-574-6856 FAX : 02-6499-1814
**제품구입문의** : sales@sgacorp.kr URL : www.sgasol.kr

KOSDAQ LISTED COMPANY

IGLOO SECURITY

# 항상 지켜드리겠습니다.

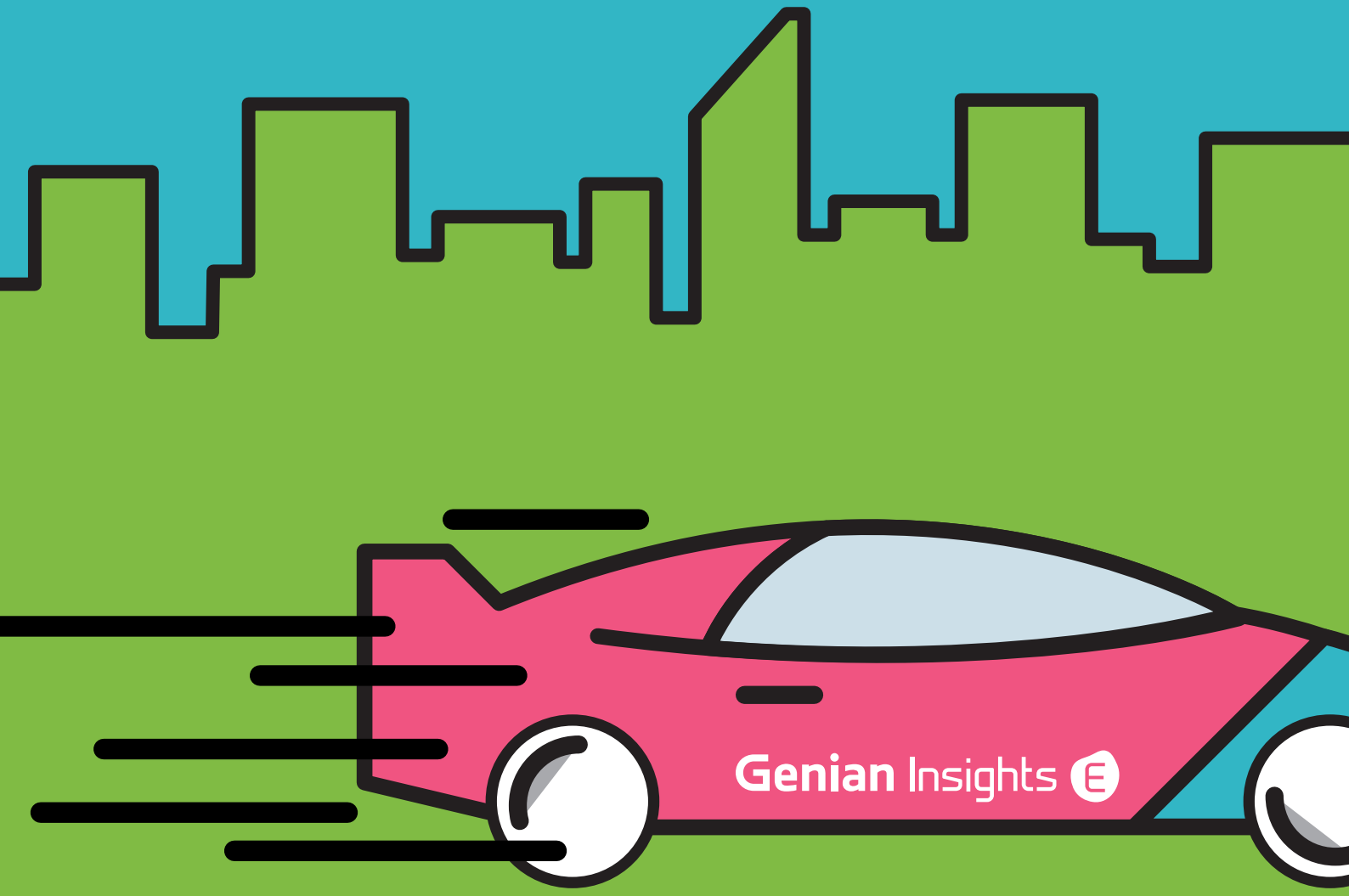
## 어려운 보안 때문에 고민하고 계시진 않습니까?

이글루시큐리티는 복잡한 사이버 세상에서 고객이 편안하게
보안위협정보를 관리하도록 최고의 제품과 서비스를 제공하고 있습니다.

신뢰할 수 있는 사이버 세상을 만드는 기업, **이글루시큐리티**입니다.

**(주)이글루시큐리티** 서울특별시 송파구 정의로8길 7 한스빌딩 6층 TEL : 02-3452-8814 www.igloosec.co.kr

Genians




# 실례합니다.
# 먼저 가겠습니다!

단말 기반 지능형 위협 탐지 및 대응(EDR)의 새로운 기준
지니안 인사이츠 E

지니언스 http://www.genians.com
Tel. 031-422-3823

(우 06648) 서울시 서초구 반포대로 110 산우빌딩 5층 (서초동 1543-11) TEL. 02 - 563 - 8763 | FAX. 02 - 563 - 8764 | E-MAIL. contact@formalworks.com

# FORMALWORKS

## 소프트웨어 개발 및 검증 전문 기업

## 주요 서비스

**SCADA 사이버보안** SCADA 장비/시스템에 대한 사이버 보안 위협 분석 및 대응 조치 수립 서비스

**소프트웨어 안전성 분석** 안전성 필수 소프트웨어 위험 요소 분석 및 안전성 평가 서비스

**소프트웨어 확인 및 검증** 규제 지침/국제 표준에 기반한 소프트웨어 V&V 및 시험 서비스

**내장형 소프트웨어 및 분석 솔루션 개발** 고품질/고신뢰 실시간 내장형 소프트웨어 및 분석 도구 개발 서비스