



순천향대학교
SOON CHUN HYANG
UNIVERSITY



LISA 순천향대학교 시스템보안연구실
LAB. OF INFORMATION SYSTEMS SECURITY ASSURANCE

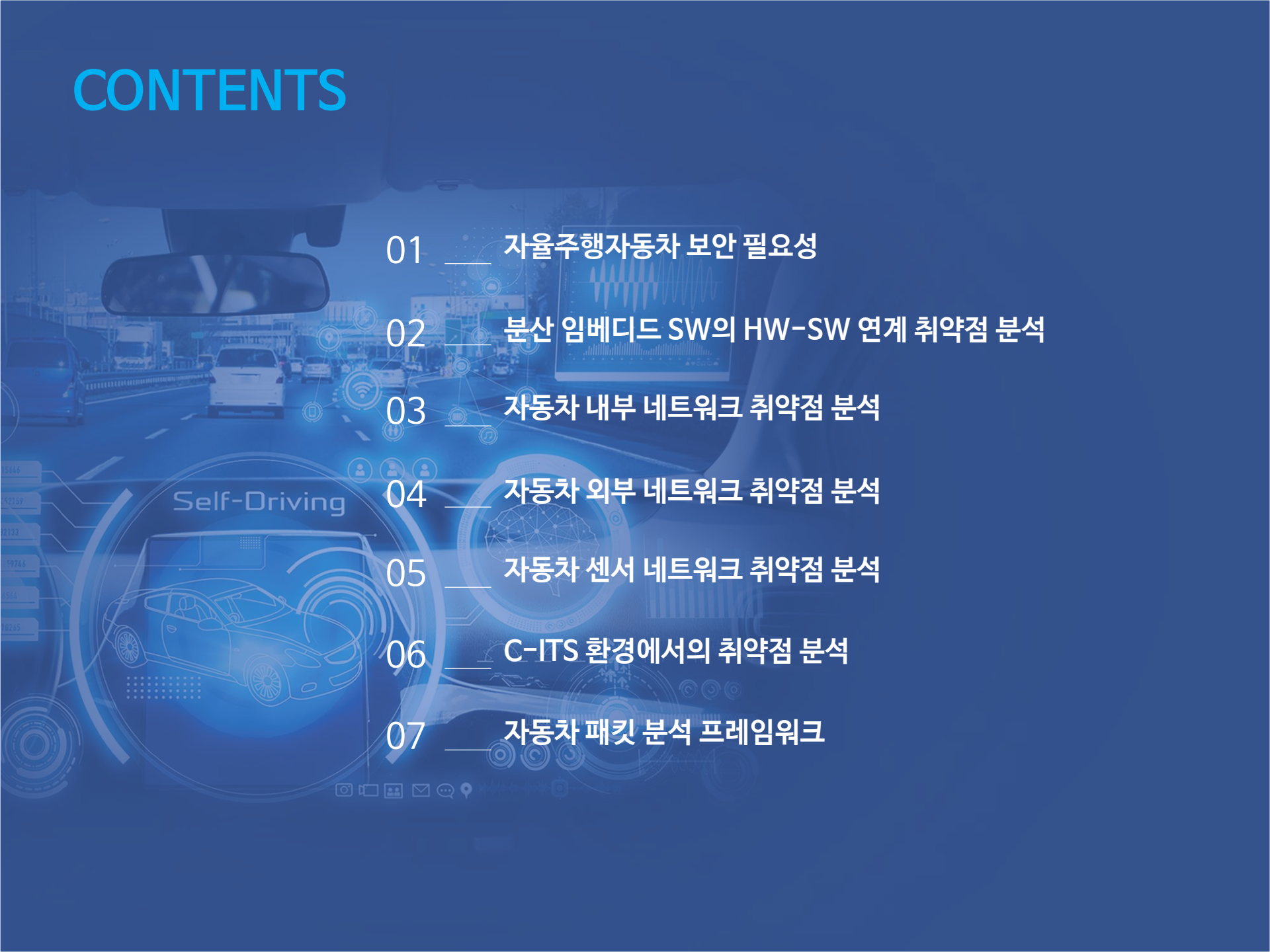
2020 NetSec-KR

자율주행자동차 보안

분산 임베디드 SW의
HW-SW 연계 취약점 분석을 통한
자동차 주행 데이터셋 수집 및 검증

순천향대학교 정보보호학과
임강빈 교수

CONTENTS

- 
- 01 — 자율주행자동차 보안 필요성
 - 02 — 분산 임베디드 SW의 HW-SW 연계 취약점 분석
 - 03 — 자동차 내부 네트워크 취약점 분석
 - 04 — 자동차 외부 네트워크 취약점 분석
 - 05 — 자동차 센서 네트워크 취약점 분석
 - 06 — C-ITS 환경에서의 취약점 분석
 - 07 — 자동차 패킷 분석 프레임워크



01

자율주행자동차 보안 필요성

자동차 발전 현황

과거 시스템

Radio

점화 (Battery, Coil, Spark Plug)

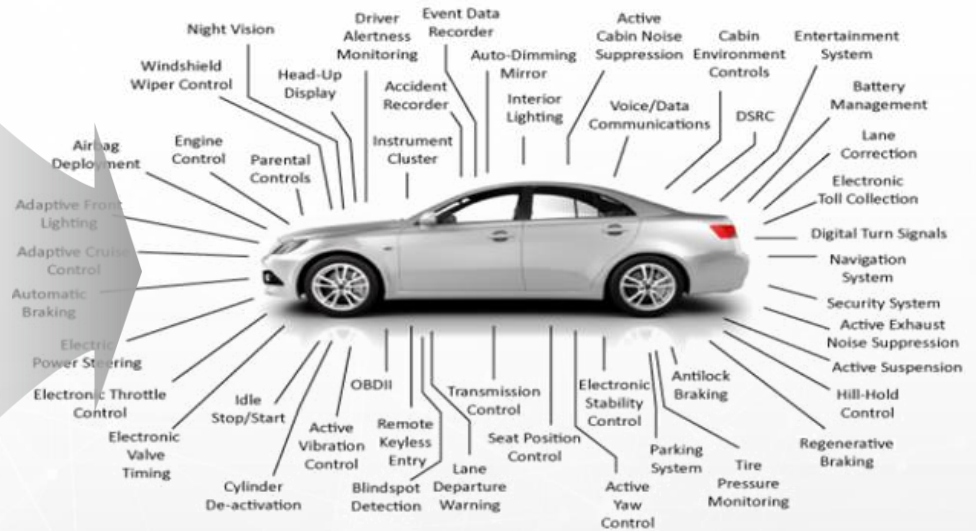


Head Lamp

Starter

주행을 위한 **최소한의 시스템**

현재 시스템



운전자 편의와 안전성 확보를 위해
자동차의 거의 모든 부분이 **전자화**

자율주행 기술의 발전

- Tesla에서 자율주행 전기자동차 Model S/X/3 출시
 - Autopilot (자율 주행) : 앞차와 간격 조절/ 차선 유지 및 변경
 - Telematics (이동 통신): 무선 소프트웨어 업데이트/ 차량 호출 / 자동 주차
- 현재 국내 차량제조사는 레벨 2~3단계의 조건부 자율주행차를 생산하고 있음
 - Level 0 : 전방 충돌방지 보조 (FCA), 후/측방 충돌경고 (BCW)
 - Level 1 : 차로 이탈 경고 (LDW), 자동 긴급 제동 (AEB), 사각 지대 경고 (BSD), 크루즈 컨트롤 (CC)
 - Level 2 : 차로 유지 보조 (LFA), 스마트 크루즈 컨트롤 (SCC), 자동 주차 보조 (SPAS)
 - Level 3 : 고속도로 주행 보조 (HAD), 특정 주행 모드에서 시스템이 차량 제어 전부 수행
- 차량에 장착되는 외부 센서의 증가 외에도 다양한 네트워킹 기능이 확대 될 것으로 전망



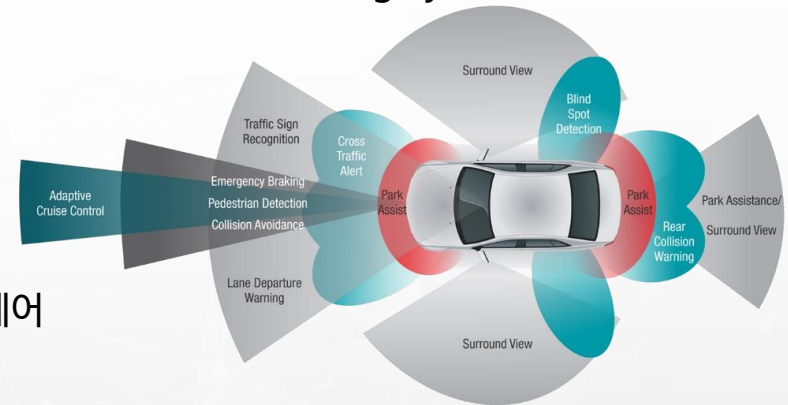
자율주행 단계

	Driver Only	Assisted	Partial Automation	Conditional Automation	High Automation	Full Automation
SAE 기준	Lv. 0	Lv. 1	Lv. 2	Lv. 3	Lv. 4	Lv. 5
NHTSA 기준	Lv. 0	Lv. 1	Lv. 2	Lv. 3	Lv. 4	
특징						
적용 기술		- ADAS 사용, BSD, FCWS, AEB, LDW 등	- SPAS(Parking) - ACC(Crusing) - Traffic Jam Assistant	- Highway Driving - City Road Driving - Country road Driving	- Fully autonomous with driver controls - V2X, Real time map	- Fully autonomous without driver controls - V2X, Real time map

자율주행 레벨4 이상에서 차량통신 필요 (출처: SAE, NHTSA)

외부 센서 기술

- 첨단 감지 센서, GPS, 지능형 카메라, 통신 모듈 등을 이용하여 주행 중 일부 상황을 차량 스스로 인지하기 위한 지능형 운전자 보조 시스템의 필수 요소
- 초음파 센서
 - 주차 보조 (Parking Assist System) / 충돌 방지 보조 (Collision Warning System)
- LIDER
 - 자동차 주변의 3D 정보 수집 및 구성
 - 빛을 이용한 레이더로 장애물의 심도 측정
- GPS
 - 위치정보 제공 / 어린이보호구역 등 구간별 속도 제어
- 지능형 카메라
 - 스마트 크루즈 컨트롤 보조
 - 차선 이탈 경고 / 차로 이탈방지 보조 (Lane Departure Warning / Lane Keeping Assist)
- 통신 모듈
 - 차량 원격제어, 차량 간 주행 정보 공유, 차량과 인프라 간의 소통



커넥티드카 보안 위협 사례

- 커넥티드카에 대한 해킹 사례가 지속적으로 보고되고 보안 위협 및 대응 연구가 전 세계적으로 진행중에 있음
- 해커가 차량을 점령하게 되면 원격으로 차량의 엔진, 브레이크, 핸들, 계기판, 가속 페달 등을 제어할 수 있게 되며 이는 심각한 차량 사고로 이어질 수 있음
- 차량 해킹을 사전에 예방하고 데이터를 검증하기 위한 차량 테스트 프레임워크 및 데이터셋의 사전 확보가 필요

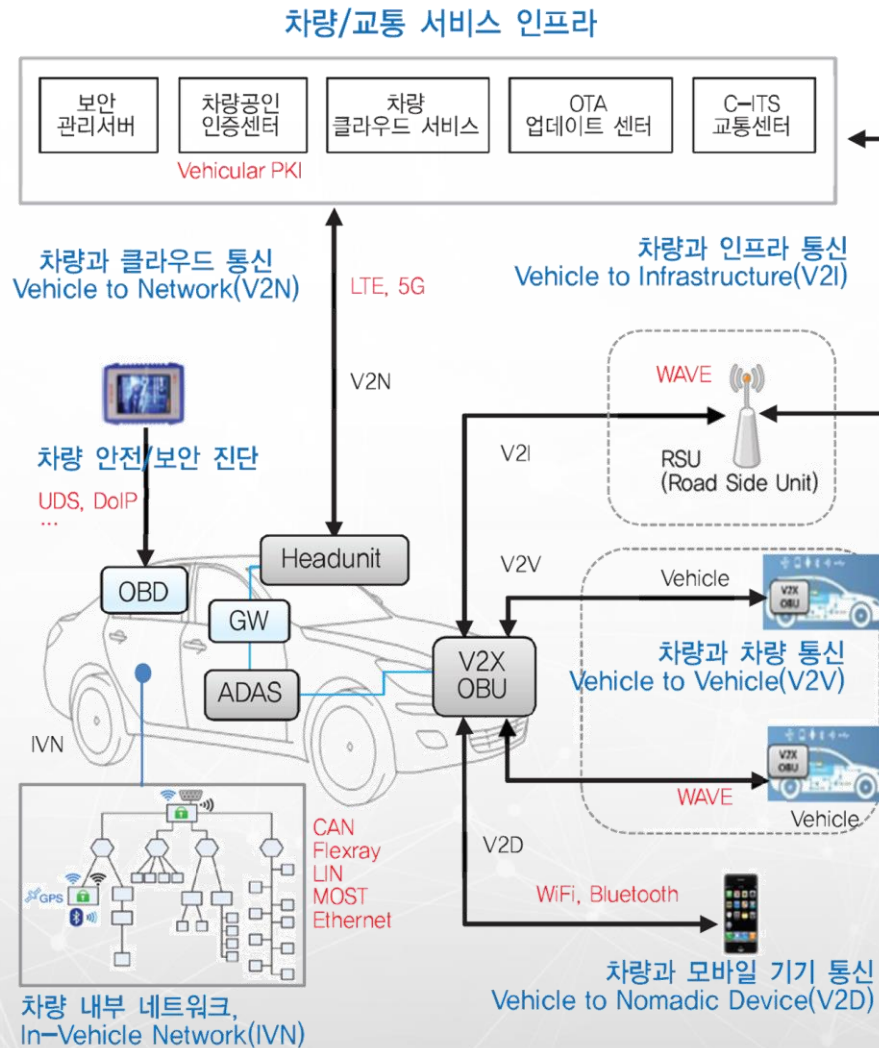
연도	주요 사고	관련 사진
2012	• 영국에서 신형 BMW 차량이 해킹에 의하여 탈취되는 사건 발생 • 3명의 절도범이 3분 내에 도난방지 기능이 탑재된 차량의 탈취에 성공 • 진단포트에 컴퓨터를 연결해 스마트키를 복제하여 차량을 탈취	
2013	• Defcon21에 자동차 해킹 내용 발표 • 도요타 프리우스와 포드 이스케이프를 노트북으로 해킹 • 자동차의 운전대, 브레이크, 계기판, 가속페달, 엔진, 전조등, 경적 등이 원격 제어가 가능함을 시연	
2015	• BlackHat에 자동차 해킹 내용 발표 • 에 연결된 인터넷을 통해 주행 중인 Jeep 'Cherokee'에 침입, 와이퍼, 가속 페달, 운전대 임의 조작 수행 • 해킹 발표 후 Cherokee 자동차 140만대 규모 리콜	
2016	• 중국 인터넷 보안 업체가 Tesla 자동차 모델 S를 해킹 • 모델 S의 스마트폰용 모바일 앱 6자리 코드를 해킹해 차량 원격 제어 • 주행 중인 Model S의 급제동, 트렁크 개방 등의 조작을 시연	

Remote Exploitation of an Unaltered Passenger Vehicle (2015)

- 외부와의 셀룰러 통신을 담당하는 Uconnect 시스템을 통해 차량의 네트워크에 침입
- 차량의 엔터테인먼트 시스템 및 네비게이션을 제어
- IVI와 연결되어 있는 Renesas V850 CAN 컨트롤러의 펌웨어 업데이트를 통해 악의적 CAN 메시지 전달
- 셀룰러 망을 통해 연결된 IVI를 해킹하여 차량에 CAN 메시지를 전송함으로써 차량의 물리적 제어에 성공
- 차량 주행 중 클러스터, 엔진, 라디오, 브레이크, 스티어링 휠, 트랜스미션 컨트롤 등을 제어 가능



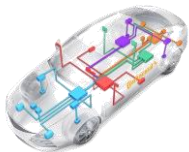
자율주행자동차 공격표면



출처 : 한국전자통신연구원 (ETRI) - 자율주행 자동차 보안기술 동향 (2018)

현제까지의 자율주행자동차 공격표면에 대한 분석 결과

내부 네트워크 취약점



- CAN 메시지 전송 채널을 통한 메시지 재전송 및 Fuzzing 공격
- 진단 CAN 메시지를 이용한 차량 ECU 펌웨어 업데이트 공격
- 진단 CAN 메시지를 이용한 차량 제어 공격

텔레매틱스 취약점



- 텔레매틱스 제공 서버 및 클라이언트 단말기 공격을 통한 차량 제어 공격
- OTA(Over The Air) 채널을 통한 펌웨어 업데이트시 업데이트 프로토콜 공격을 통한 악성 펌웨어 교체 공격

공격방향

외부 네트워크 취약점



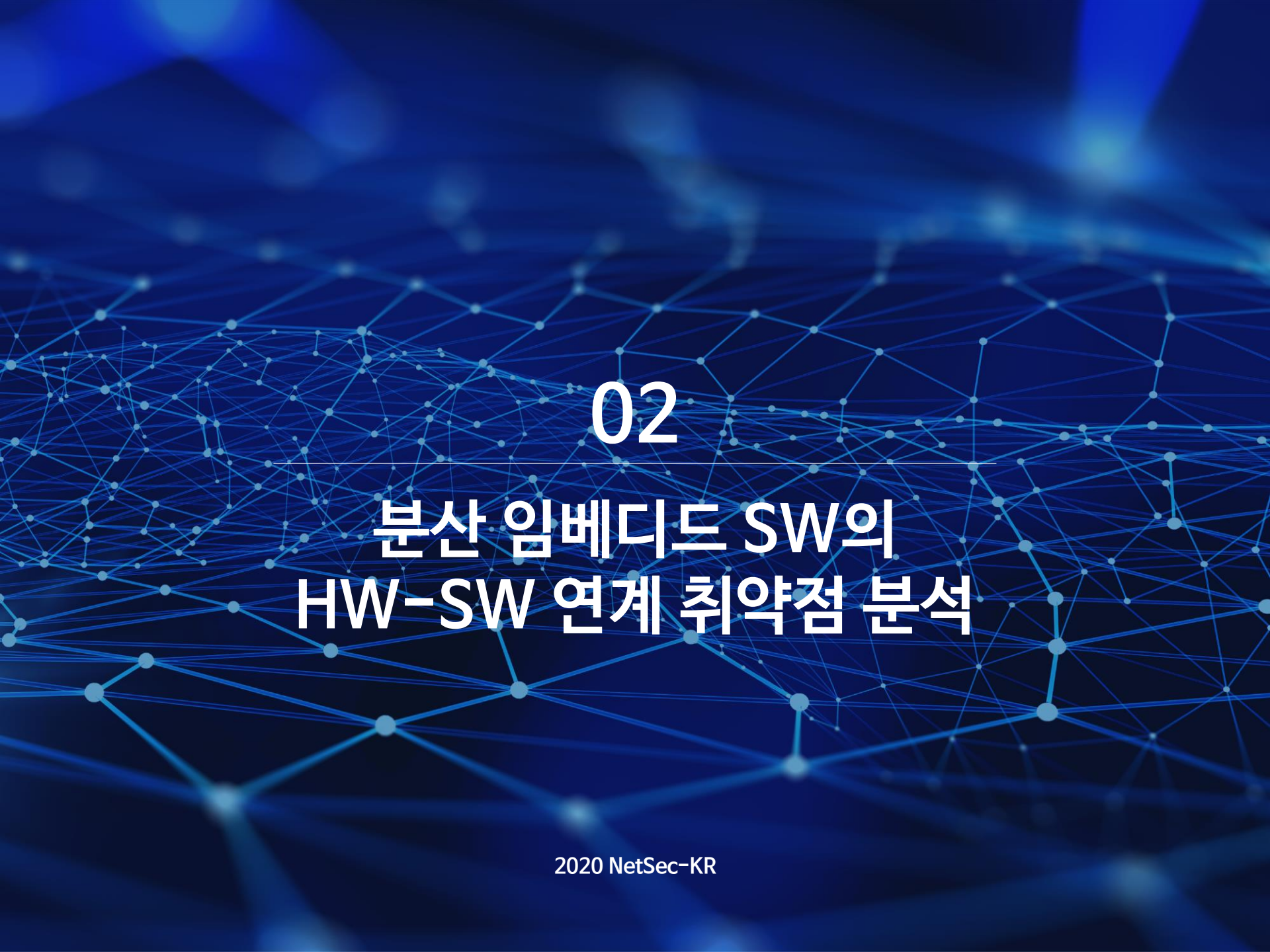
- 블루투스 연결 시 발생할 수 있는 버퍼 오버플로우 및 PIN 전사 공격
- 통신 모듈 및 이동통신 인증 과정에서 발생할 수 있는 취약점 유도 공격
- V2X OBU 권한 탈취 및 메시지 스니핑/스푸핑

센서 네트워크 취약점



- 자율주행에 필요한 전방카메라에 대한 블라인드/적대적 공격에 대한 카메라 인식 오류 유도 공격
- 자율주행 센서 / GPS 센서의 스푸핑/재밍을 통한 센서 및 네비게이터의 오작동 공격

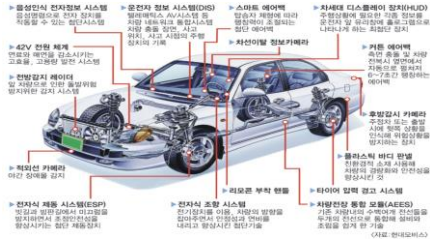
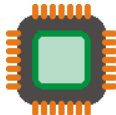
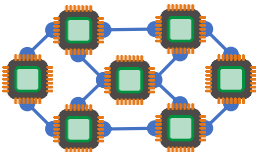




02

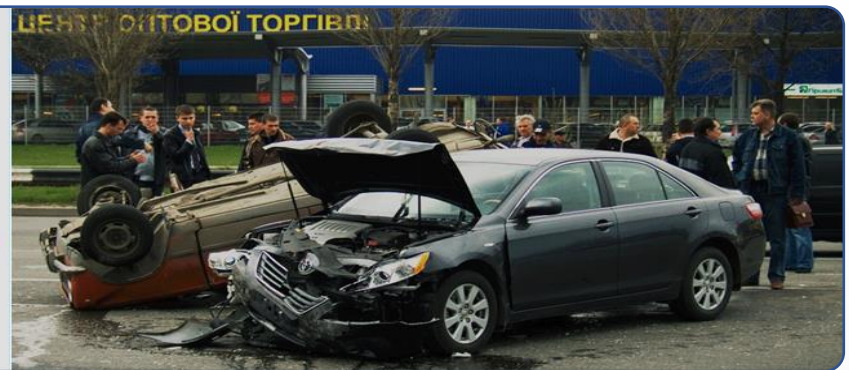
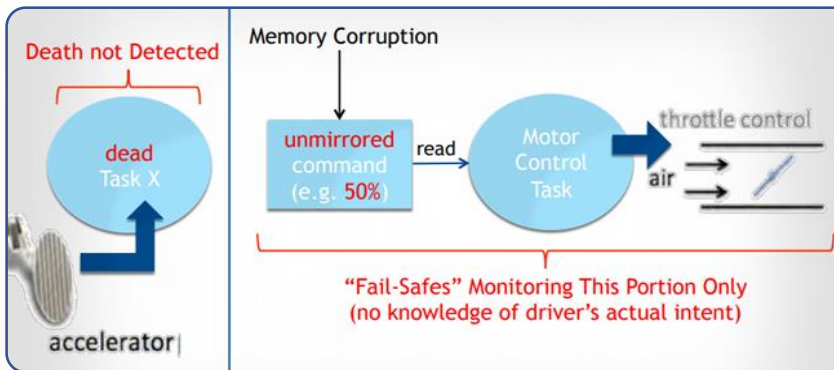
분산 임베디드 SW의 HW-SW 연계 취약점 분석

분석 대상 시스템의 변화

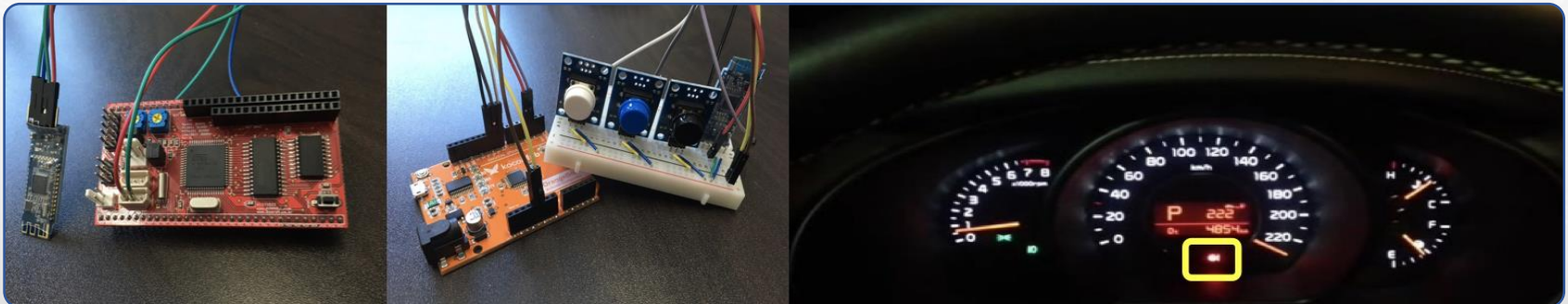
시스템	과거 (1800~)	근래 (1900~)	현재 (2000~)
HW			
SW	 단순 하드웨어	 단일 프로세서	 분산 프로세서
평가	기계식 로직	순차실행	상호작용
현황	내구성 분석	코드 분석	데이터 분석
코드 경량화 + 분산 노드화 → SW융합소재부품 네트워크			

분석 대상 시스템의 변화

도요타 급발진 현상

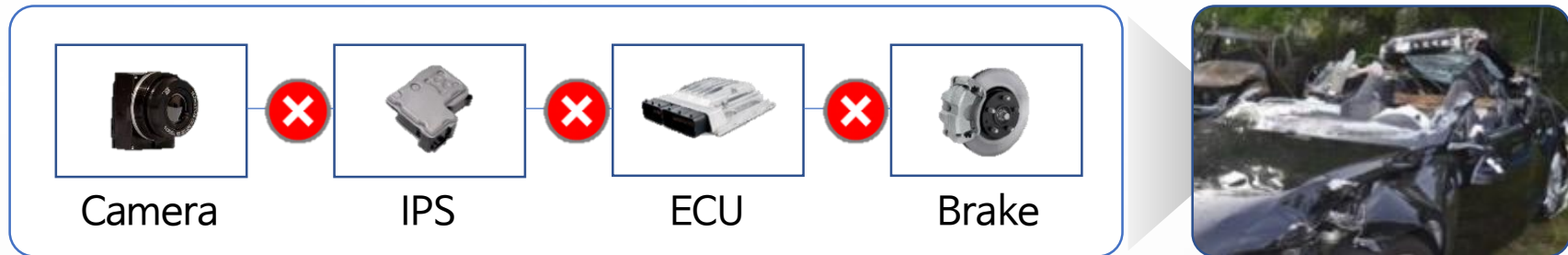


현대/기아 스티어링 락 현상

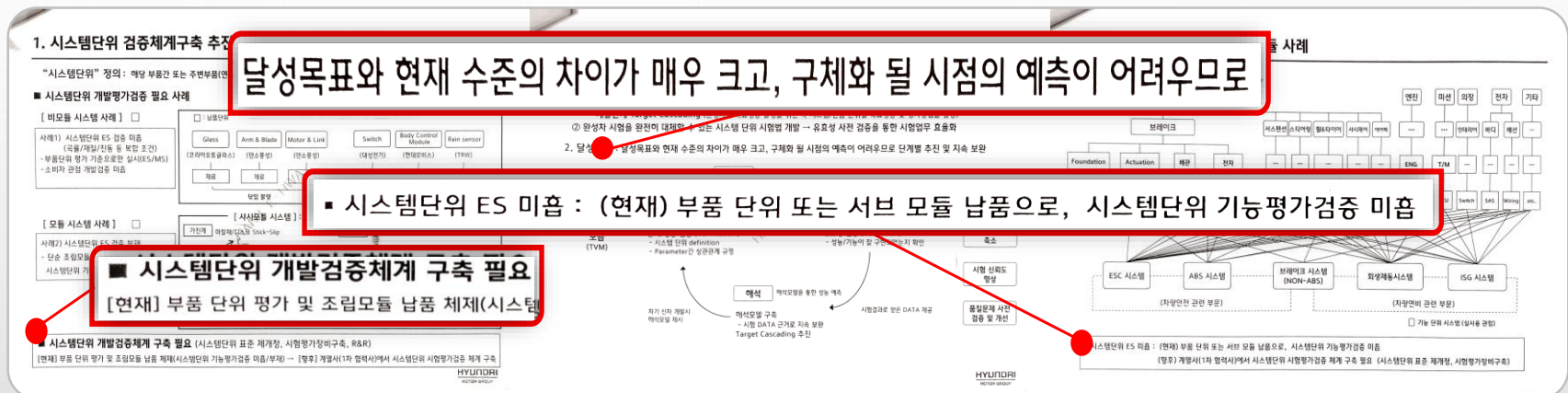


비상 환경에서의 입력벡터 영향 평가 부재

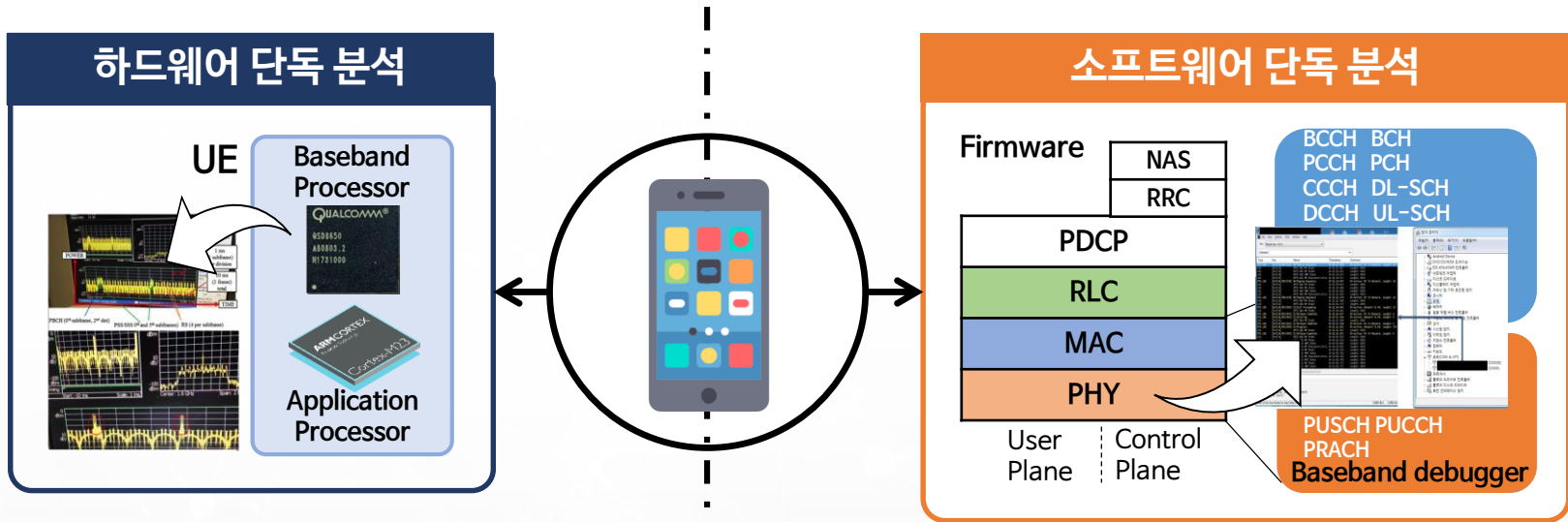
테슬라 자율주행 자동차 사고 사례



자동차 생산기업에서의 해결 과제 (2014~)



기존 취약점 분석 방법의 오류



기본 방법의 문제점

- 단순 기능적 요소에 대한 독립적이고 단편적인 분석 검증 평가 수행
- 비상 상황 입력에 대한 SW 반응특성 분석 부재 → Live Deadblock 방치
- 전파특성 파악 불가 → RAS 관련 사고 발생 후 재현 및 원인 규명 불가

문제해결을 위한 요구 사항

- H/W와 S/W 연계 분석 → 위협과 입력벡터와의 상관관계 파악
- 분석 및 진단 방법 정규화 → 분석 검증 자동화 핵심기술 확보
- 고수준 공통 분석 및 검증 시스템 확보 → 시스템 안전성 내재화

HW-SW 연계분석 실례 #1

HW 기반 분석

플래시 메모리 추출 및 덤프

메모리 덤프 파일

SW 기반 분석

제조사 웹사이트

펌웨어 다운로드

알고리즘	설명
패리티 체크	수신 비트군의 1 또는 0의 수를 카운트하여 짝수 또는 홀수 인지를 체크하여 에러 검출, 낮은 오류 탐지 검출
모듈러 연산	n 비트 워드 값을 모두 더해 나머지 연산을 하는 과정을 통해 체크섬을 생성하는 알고리즘
암호화 해시	의도적인 데이터 변형을 감지. MD5, SHA 등을 주로 사용

PCL 펌웨어 무결성 검증 분석

HW-SW 연계 분석

PLC 펌웨어 오류공격 신규 취약점 추가 발굴

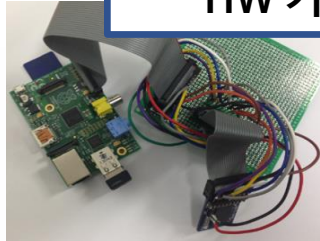
펌웨어 구조 분석

펌웨어 변조 및 업데이트

PLC Bricking

HW-SW 연계분석 실례 #3

HW 기반 분석



플래시 메모리 추출 및 덤프

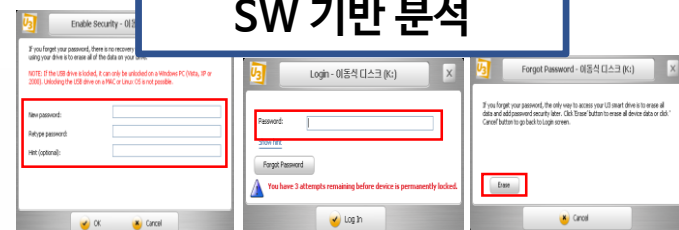


오실로스코프를 통한
신호 파형 및 패턴 조사



Stimulator

SW 기반 분석



보안 USB 소프트웨어 분석



커맨드를 이용한 분석



감청을 이용한 취약점 분석

HW-SW 연계 분석

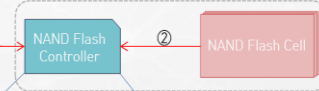
1. 올바른 사용자 인증 시 출력되는 파형



2. 음바라지



U3 Launchpad

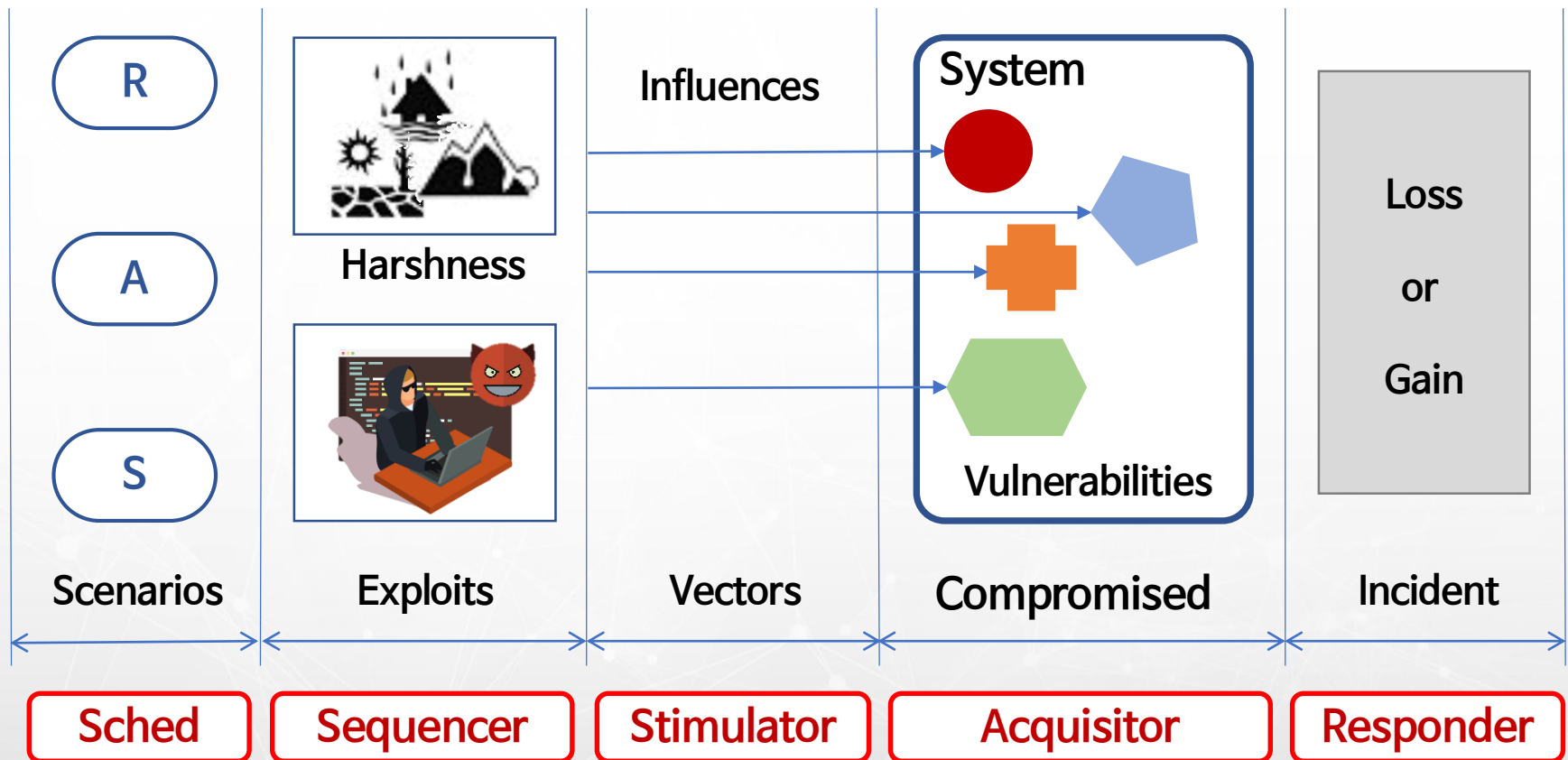


NAND 플래시 메모리

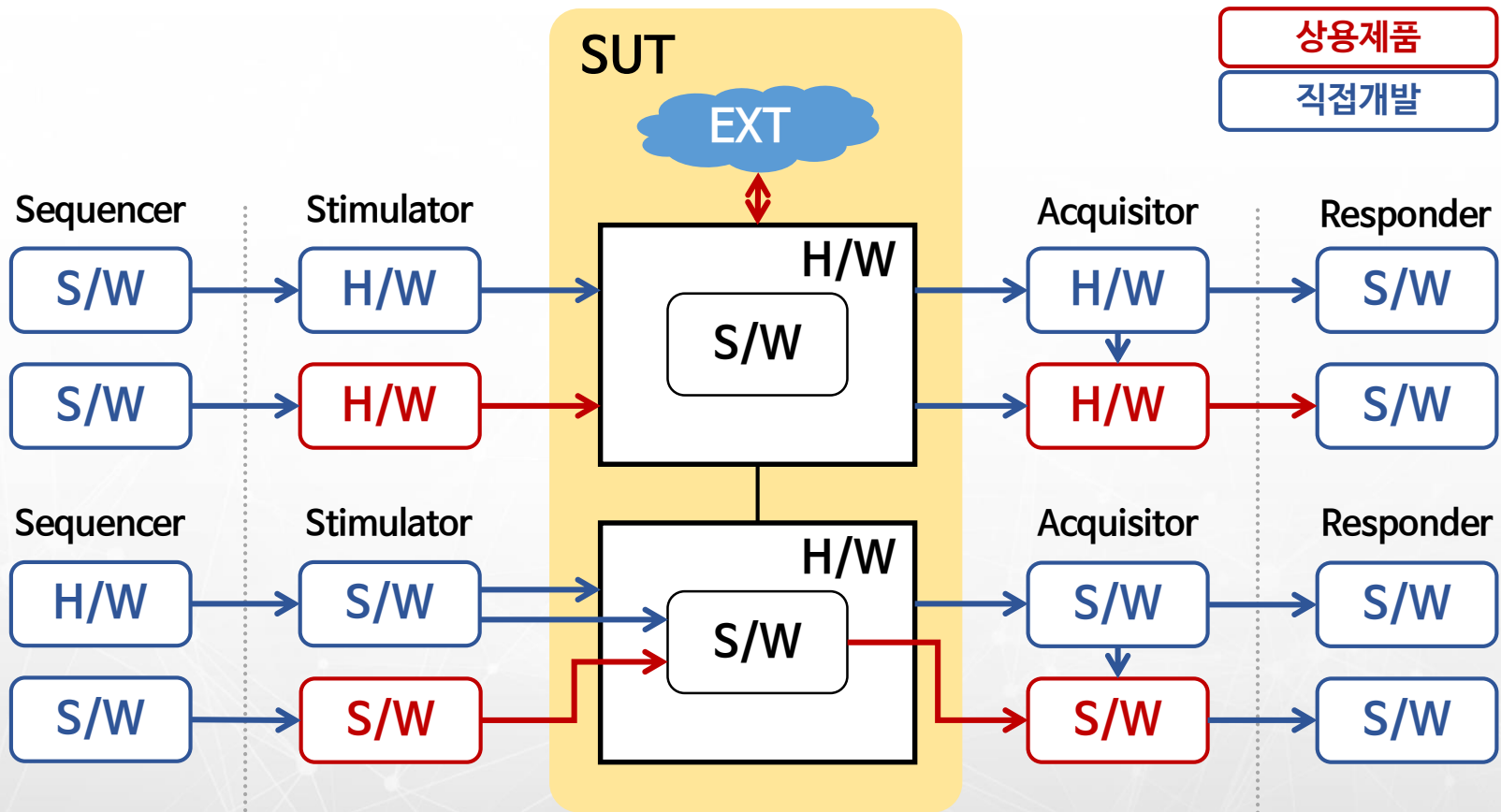
암호화 USB 메모리 신규 취약점 추가 발굴

NAND Flash Controller

HW-SW 연계분석을 위한 정규화 모델 개발 필요성

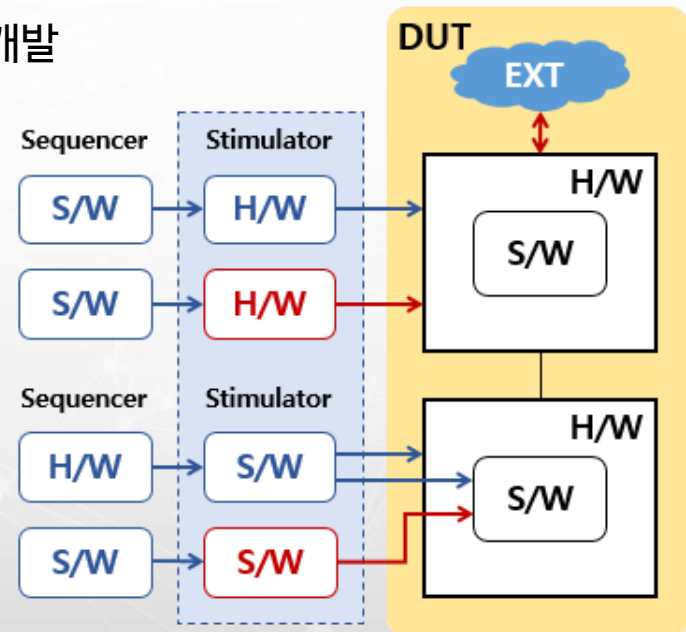


H/W-S/W 연계분석 프레임워크



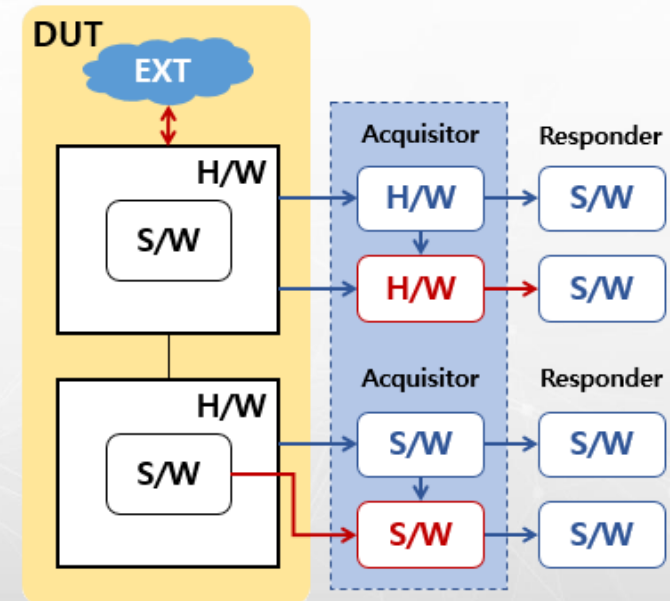
기존 발견 취약점에 대한 자극 입력 공격벡터 분류

- H/W Stimulator → H/W
 - 인터페이스 특성에 따라 사용 가능한 상용제품 섭외 또는 자체 개발
 - 하드웨어 인터페이스로의 시나리오 기반 자극 주입
 - 자동차 OBD를 통한 CAN 메시지 주입, GPS 교란, TPMS 교란, 카메라 오류주입 등
- S/W Stimulator → H/W
 - 하드웨어와 마찬가지로 상용제품 섭외 또는 자체 개발
 - 하드웨어 포트, 레지스터, 버퍼 직접 제어
 - 키보드 C/D 비트, RESEND 취약점 공격 등
 - MAC 주소, USB VID/PID, PCI 헤더 변경 등
- S/W Stimulator → S/W
 - 소프트웨어 변수, 메모리, 인자 주입
 - PC 환경의 대다수의 공격이 해당
 - 암호 키 변경, Buffer Overflow, Hooking 등



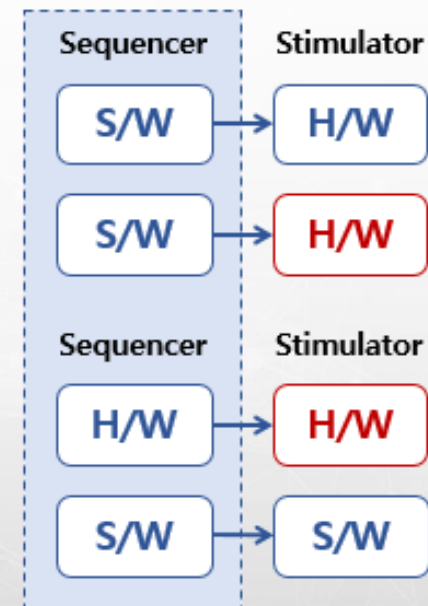
기존 발견 취약점에 대한 자극 입력 공격벡터 분류

- H/W → H/W Acquisitor
 - 인터페이스 특성에 따라 사용 가능한 상용제품 섭외 또는 자체 개발
 - 하드웨어 인터페이스로부터 출력되는 반응 수집
 - Video, Audio 등 외부 출력에 대한 신호 및 데이터 수집
 - 프로세서, 메모리 Tapping, Signal Sniffing 등
- H/W → S/W Acquisitor
 - 상용제품 섭외 또는 자체 개발
 - 하드웨어 포트, 레지스터, 버퍼 직접 판독
 - 키보드 버퍼, 프로세서 PSW 변화 추적 등
- S/W → S/W Acquisitor
 - 소프트웨어 변수, 메모리, 수행결과 수집
 - 인증결과 확인, 프로세서 리스트 목록화 등



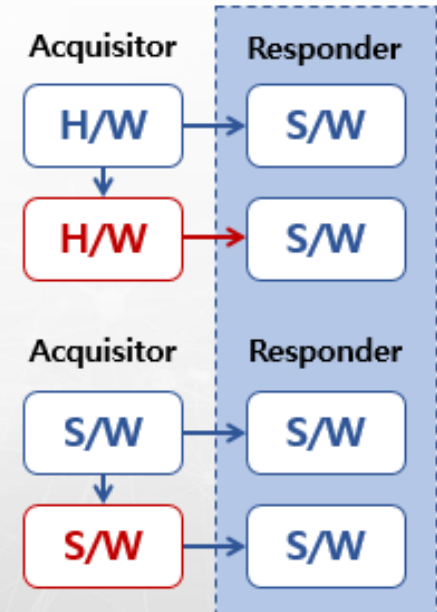
기존 발견 취약점에 대한 자극 입력 공격벡터 분류

- Stimulator에 대한 시나리오 기반 행위 수행 유도 (Exploits)
- 개념적 시나리오 설계 및 이를 기반으로 Sequencer의 프로세스 도출
- H/W Sequencer → H/W Stimulator
 - 기존의 H/W Stimulator에 새로운 H/W 모듈을 추가하여 변형된 공격벡터 유도
 - CAN Burst 주입, BT/WiFi 호핑 무력화 등
- S/W Sequencer → S/W Stimulator
 - 소프트웨어 적으로 생성된 대개의 Exploit
 - 자동, 수동 또는 스케줄링 기반 수행
 - Stimulator에 대한 설정 또는 절차 수행
- S/W Sequencer → H/W Stimulator
 - H/W Stimulator에 대한 이상행위 조작
 - Add-on 디바이스에 대한 강제 변형행위 유도



기존 발견 취약점에 대한 자극 입력 공격벡터 분류

- Acquisitor의 출력 값에 대한 시나리오 기반 처리
- Analog/Digital Signal, Video, Audio 등 수집정보의 의미 해석
- 처리 방식은 변환, 가시화, 전송 등이 가능하도록 설계
- 다중의 Responder를 기반으로 빅데이터 또는 인공지능 엔진과 연동 가능
- H/W Acquisitor → S/W Responder
 - 영상 및 음성 분석, 행위 분석, Firmware 이미지 분석 등
 - 상용 하드웨어 Acquisitor의 경우 제공 라이브러리 활용
 - R-Gog, 휴대폰 SW, 자동차 초음파센서 오류 진단 등
- S/W Acquisitor → S/W Responder
 - 암호 키 탐색 (엔트로피 계산), IDS 플러그인 등
 - 상용 Debugger, 대개의 개념증명도구 후처리기
 - Compromise Map, Function Call Graph, Taint Analysis 등



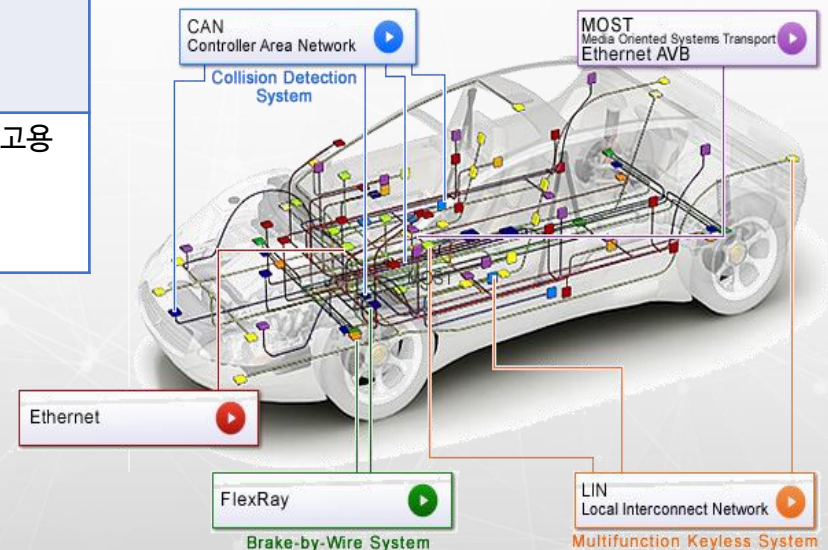


03

자동차 내부 네트워크 취약점 분석

커넥티드카 내부 네트워크

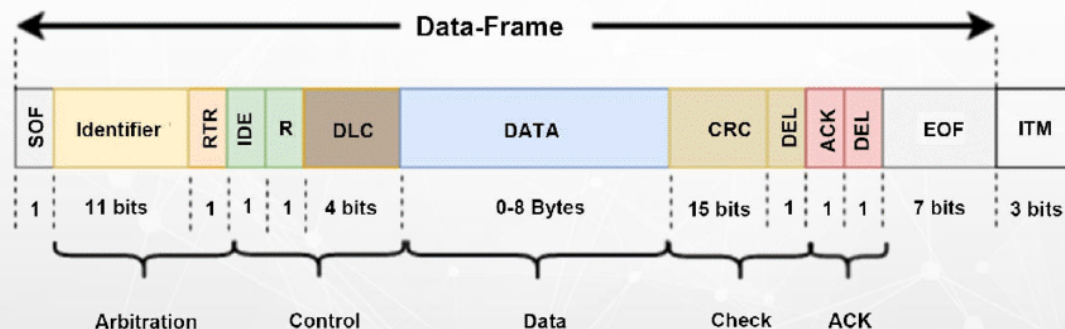
네트워크	특징
FlexRay	- 내고장성(fault-tolerant) 고속 버스 시스템 - X-by-wire를 위한 오류 허용성 및 시간 결정성 성능 조건을 제공 - 더 높은 대역폭 요건을 위한 CAN 대체 - 안전 관련 시스템
CAN	- Multi Master 통신 - 전기적인 노이즈에 강함 - 높은 신뢰성, 동력전달 시스템에 사용 - 탁월한 오류 처리와 오류 제한 기능 - 빠른 데이터 전송 속도 (1MBit/s)
LIN	- 분산된 전자 시스템을 위한 저비용, 직렬 통신 네트워크 - CAN 통신 말단부 시스템 분산화를 위해 사용 - 주로 사용자의 편의를 위한 시스템에 사용 - Single-Master/Multi-Slave 구성
MOST	- 인포테인먼트 및 멀티미디어 서비스를 제공하기 위한 고용량 데이터 네트워크 25, 50, 150Mbit/s baud rate 지원 - 동기 및 비동기 채널 사용



CAN(Controller Area Network)

- Twist Pair Wire (CAN_H/CAN_L)
- Message-Oriented Protocol
- Multi-Master Network
- CSMA/CD+AMP

CAN 메시지 구조

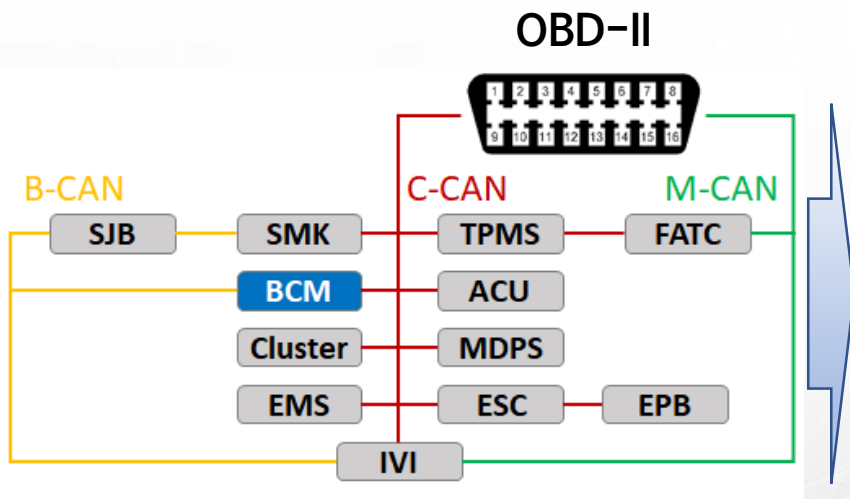


수집한 실제 CAN 메시지

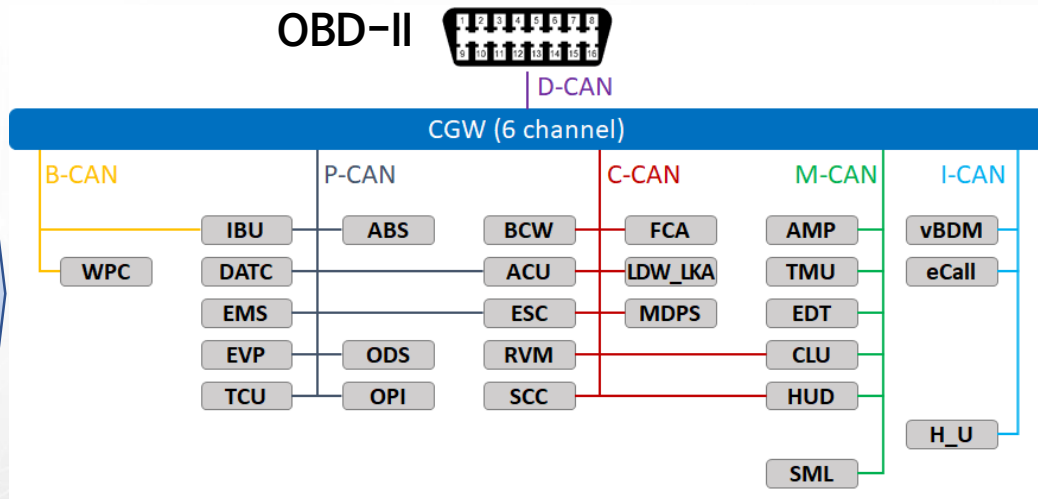
Time (rel.)	Bus	Type	ID	DLC	Data
20.4629	1	Rx	545h	8	C8 18 00 87 F9 FF FD FF
20.4649	1	Rx	4B0h	8	00 40 00 00 00 40 00 80
20.4651	1	Rx	164h	8	00 08 00 00 00 00 04 0C
20.4654	1	Rx	370h	8	FF 20 00 80 FF 00 00 28
20.4656	1	Rx	43Fh	8	00 40 60 FF 67 B8 09 00
20.4658	1	Rx	440h	8	FF A0 00 00 FF B8 09 00
20.4662	1	Rx	4F2h	8	20 00 30 38 00 00 00 C3
20.4665	1	Rx	4F0h	8	00 00 86 00 00 11 CD 06
20.4674	1	Rx	510h	8	00 00 00 00 00 00 00 00
20.4684	1	Rx	350h	8	30 2B 94 90 A2 00 00 BD
20.4698	1	Rx	153h	8	00 80 10 FF 00 FF 20 AE
20.4701	1	Rx	220h	8	F6 23 07 34 0C 00 FF 0F
20.4706	1	Rx	316h	8	45 32 54 0A 32 33 00 7F
20.4708	1	Rx	18Fh	8	FE 5D 32 00 00 43 00 00
20.4710	1	Rx	260h	8	05 32 00 30 04 89 5B 0E
20.4713	1	Rx	080h	8	00 17 54 0A 32 33 32 D8
20.4715	1	Rx	081h	8	40 84 88 00 00 00 00 88
20.4718	1	Rx	165h	8	08 F8 7F 00 00 00 06 89
20.4720	1	Rx	2A0h	8	02 00 88 98 95 12 9D 04
20.4721	1	Rx	2B0h	5	56 00 00 07 26
20.4724	1	Rx	329h	8	40 B4 7E 8C 11 2F 00 10
20.4726	1	Rx	545h	8	C8 18 00 87 F1 FF F6 FF
20.4748	1	Rx	4B1h	8	00 00 00 00 00 00 00 00
20.4751	1	Rx	164h	8	00 08 00 00 00 00 05 0D
20.4753	1	Rx	370h	8	FF 20 00 80 FF 00 00 EC
20.4756	1	Rx	43Fh	8	00 40 60 FF 67 B8 09 00
20.4758	1	Rx	440h	8	FF F0 00 00 FF BC 09 00
20.4798	1	Rx	153h	8	00 80 10 FF 00 FF 30 BE
20.4801	1	Rx	1F1h	8	00 00 00 00 00 00 00 00
20.4803	1	Rx	220h	8	F6 2B 02 14 0C 00 FF 0F
20.4807	1	Rx	316h	8	45 32 54 0A 32 33 00 7F
20.4809	1	Rx	260h	8	05 32 00 30 04 89 5B 1D
20.4812	1	Rx	165h	8	08 F8 7F 00 00 00 07 88
20.4814	1	Rx	080h	8	00 17 54 0A 32 33 32 C9
20.4816	1	Rx	081h	8	40 84 88 00 00 00 00 79
20.4819	1	Rx	18Fh	8	FE 5D 32 00 00 43 00 00
20.4821	1	Rx	2A0h	8	A2 00 88 98 95 12 9D 04
20.4823	1	Rx	2B0h	5	56 00 00 07 37
20.4825	1	Rx	329h	8	40 B4 7E 8C 11 2F 00 10
20.4828	1	Rx	382h	8	40 FE 0F 00 00 00 00 04
20.4830	1	Rx	545h	8	C8 18 00 87 F2 FF F7 FF
20.4849	1	Rx	4B0h	8	00 80 00 00 00 40 00 80
20.4851	1	Rx	164h	8	00 08 00 00 00 00 06 0E

CAN 네트워크 구조

- 자동차에서 가장 많이 사용되고 있는 통신 네트워크이며 ECU간의 정보 공유 가능
- 단순한 형태에서 다양한 외부 센서 기능들이 추가되며 복잡하게 변화
- 기존의 OBD-II 에는 다양한 CAN이 연결되어 있지만 최근에는 진단에 관련된 채널만 포함
- CAN 데이터 수집을 위해서는 모든 CAN을 포함하고 있는 Gateway 접근 필요



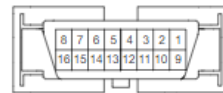
구형 CAN 네트워크 구조



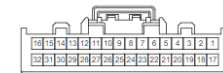
신형 CAN 네트워크 구조

- OBD-II (On-Board Diagnostics) 포트를 통해 차량의 상태 등 주요 상태 진단 가능
- 게이트웨이 역할을 하는 ICU 모듈에 접근하면 모든 CAN 채널의 메시지 수집 가능

ICU를 통한 CAN 채널 확보



- | | | | |
|-------|----------------------|---------|--|
| 1. - | - | 10. - | |
| 2. - | - | 11. Y | D-CAN (Low) |
| 3. W | D-CAN (High) | 12. - | |
| 4. B | 신호 연결 (GE02) | 13. L/B | 반대 K-라인 : VDC 모듈,
오프 모듈 또는 K4이 모듈을
대기할 때 제거 가능 |
| 5. B | 제어 연결 (GE02) | | |
| 6. Gr | ICU 전원 모듈 (부속 - 모듈5) | 14. - | |
| 7. - | - | 15. - | |
| 8. - | - | 16. - | |
| 9. R | ICU 전원 모듈 (부속 - 모듈1) | | |

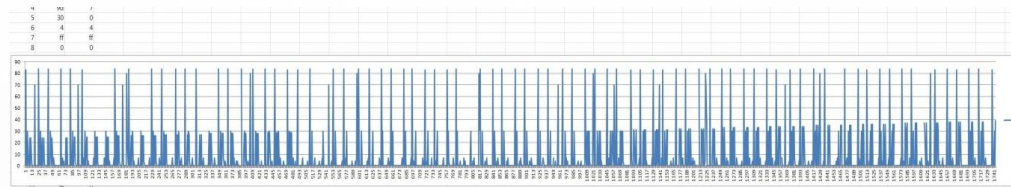


- | | | | |
|--------|--|--------|---------------------------------------|
| 1. - | - | 22. G | IPS 전방엽 연결
(표어 인접 구조): |
| 2. - | - | | (표어 인접 구조): |
| 3. Br | IPS 전방엽 연결
(표어 인접 구조)
(표어 인접 구조) | 23. Gr | 표어 전방엽 연결
(표어 인접 구조)
(표어 인접 구조) |
| 4. - | - | | (표어 인접 구조) |
| 5. W | I-CAN (Low) | 24. O | IPS 전방엽 연결
(표어 인접 구조) |
| 6. Br | I-CAN (High) | 25. - | 표어 인접 구조 (표어) |
| 7. M | M-CAN (High) | 26. Gr | IPS 전방엽 연결
(표어 인접 구조) |
| 8. B | M-CAN (Low) | | (표어 인접 구조) |
| 9. W | C-CAN (High) | | (표어 인접 구조) |
| 10. Br | C-CAN (Low) | | (표어 인접 구조) |
| 11. G | P-CAN (High) | 27. L | (표어 인접 구조) |
| 12. O | P-CAN (High) | | (표어 인접 구조) |
| 13. P | D-CAN (High) | | (표어 인접 구조) |
| 14. Gr | D-CAN (Low) | 28. G | IPS 전방엽 연결
(표어 인접 구조) |
| 15. L | B-CAN (Low) | | (표어 인접 구조) |
| 16. R | B-CAN (High) | | (표어 인접 구조) |
| 17. - | - | 29. - | (표어 인접 구조) |
| 18. - | - | 30. W | IPS 전방엽 연결
(표어 인접 구조) |

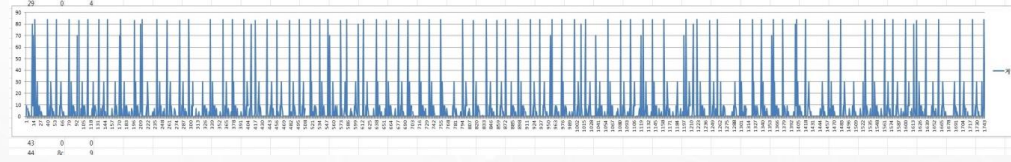
CAN 메시지 분석

- 자동차 제조사는 CAN 메시지에 대한 정보를 제공하고 있지 않음
- 포맷은 표준으로 정의되어 있지만 각 CAN 메시지들에 대한 연관된 기능 파악이 필요
- 특정 기능들을 동작 시키면서 CAN 메시지를 수집하고 변화 관찰/통계로 의미 파악 가능

가속 상태



정상시 상태



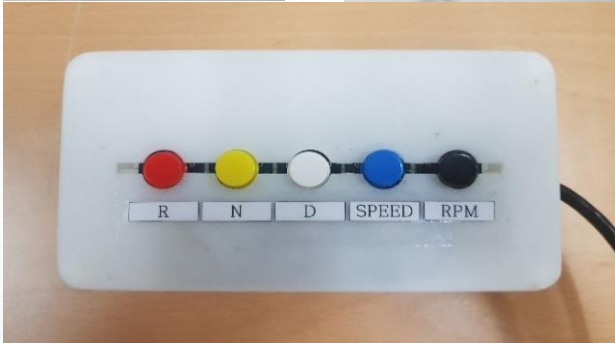
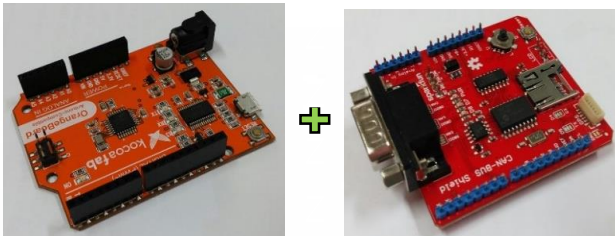
가속 상태에서의 RPM 관련 패킷 비교

종류	ID	Data
Speed	440	00 00 FE 00 00 00 00 00
RPM	316	00 00 00 50 00 00 00 00
Gear	43F	00 06 00 00 00 00 00 00

모듈별 CAN ID LIST

모듈명	CAN 네트워크	CAN ID
AVN	I-CAN	587
	M-CAN	8~A, D~F, 70, FA, 100, 10E, 115, 11E, 122, 123, 171, 173, 196, 197, 1C0, 1CA, 1CB, 1E5, 1E7, 440, 504, 571
ICU	B-CAN	168~16A, 188~18A, 416, 588, 589
	C-CAN	7F, 356, 366~368, 410, 428, 436, 453, 470, 4A9, 4C9, 4CB, 50E, 520, 533~537, 541, 544, 553, 559, 568, 572, 57F, 5A4, 5BE, 5C7
	D-CAN	7E8
	I-CAN	7F, 410, 436, 541, 553, 559
	M-CAN	126, 131~135, 150, 158, 15D~15F, 166, 167, 169, 16A, 17A, 17B, 17F, 455, 531, 56E
	P-CAN	436, 450, 471, 50E, 520, 541, 553, 559, 569, 578, 5D9, 5D3
IBU	B-CAN	100 ~ 107, 10F~113, 400, 510
	P-CAN	593
SCC (RADAR)	C-CAN	38D, 483, 4A2
	Local-CAN	X
DATC	P-CAN	40, 42~44, 383
MDPS	C-CAN	251, 2B0, 381

CAN 메시지 삽입 공격



RPM

Index	ID	Ext	RTR	Data
0	316	0	0	00 00 00 50 00 00 00 00
1	440	0	0	00 00 fe 00 00 00 00 00
2	43f	0	0	00 06 00 00 00 00 00 00

Speed

Index	ID	Ext	RTR	Data
0	316	0	0	00 00 00 50 00 00 00 00
1	440	0	0	00 00 fe 00 00 00 00 00
2	43f	0	0	00 06 00 00 00 00 00 00

Gear

Index	ID	Ext	RTR	Data
0	316	0	0	00 00 00 50 00 00 00 00
1	440	0	0	00 00 fe 00 00 00 00 00
2	43f	0	0	00 06 00 00 00 00 00 00



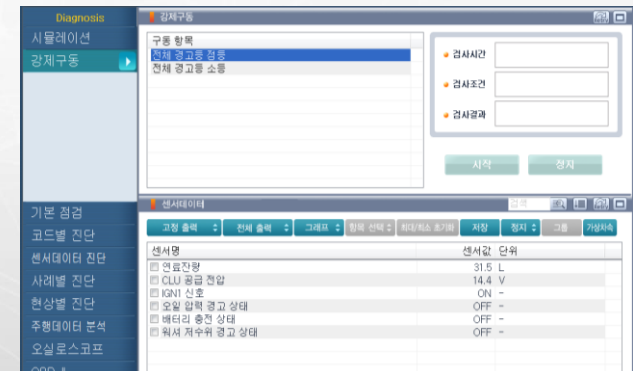
진단 점검 메시지 삽입 공격

- UDS(Unified Diagnostic Services) : 차량의 진단을 위한 통신 프로토콜(ISO 14229)
- 자동차 제조사에서 제공하는 표준 진단 및 업데이트시 진단 도구 활용
- 진단 세션 연결을 수행하고 고정된 데이터 및 메시지를 이용하여 통신
- 진단 도구 없이 진단 요청 CAN 메시지만 추출하여 재전송 시 강제 구동 가능

강제 구동 메시지 주입

2870)	6513.1	Rx	07DF	8	02	10	81	00	00	00	00	00
2906)	6579.1	Rx	07DF	8	01	20	00	00	00	00	00	00
2943)	6649.1	Rx	07C6	8	02	10	03	00	00	00	00	00
2958)	6676.7	Rx	07C6	8	02	3E	00	00	00	00	00	00
2973)	6698.7	Rx	07C6	8	02	3E	00	00	00	00	00	00
2984)	6724.6	Rx	07C6	8	02	3E	00	00	00	00	00	00
3217)	7246.5	Rx	07C6	8	03	22	B0	02	00	00	00	00
3228)	7275.0	Rx	07C6	8	30	08	02	00	00	00	00	00
3233)	7278.1	Rx	07C6	8	03	22	B0	03	00	00	00	00
3247)	7296.7	Rx	07C6	8	30	08	02	00	00	00	00	00

강제 구동 기능의 예



04

자동차 외부 네트워크 취약점 분석

IVI(In-Vehicle Infotainment system)

- 차량 내 오디오, 멀티미디어 장치 및 내비게이션 등이 통합되어 구현된 시스템
- 최근 IVI의 경우 차량진단, 원격 제어, 차량위치 전송 등을 위해 차량의 내부네트워크(CAN)와 연결되어 있음
- 여러 편의 기능을 제어하기 위해 마이크, 후방카메라, 블루투스, Wi-Fi 등 다양한 차량내의 입출력 장치들이 연결되어 있음

차량 AVN 시스템



IVI 보드



IVI하단 보드



WIFI를 통한 악성 어플리케이션 설치



System.img

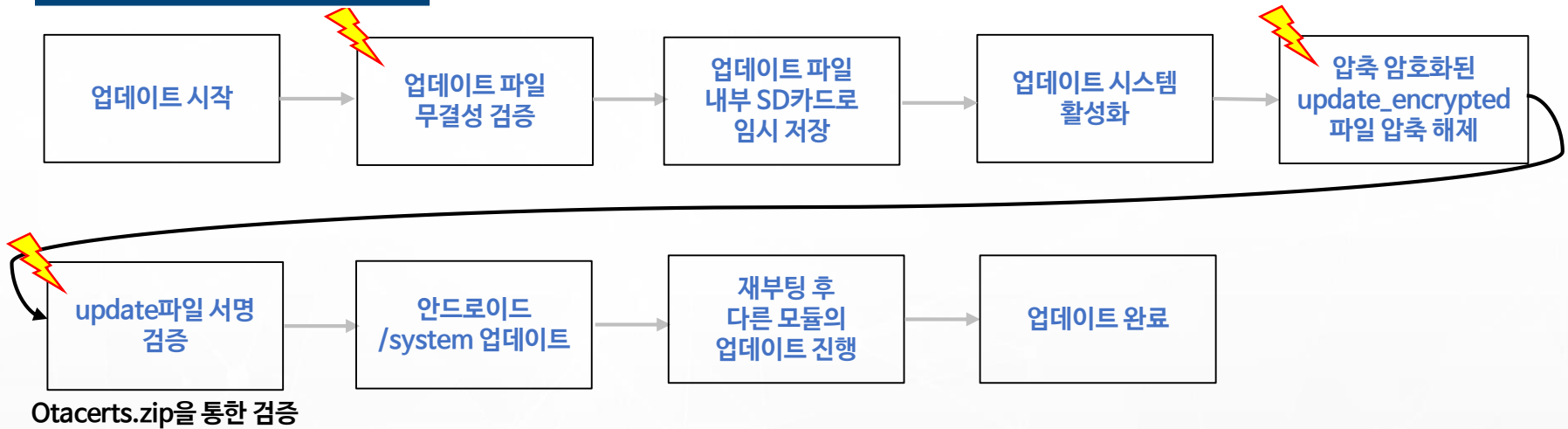
app	2015. 12. 22. 오...	파일 폴더
bin	2015. 12. 22. 오...	파일 폴더
etc	2015. 12. 22. 오...	파일 폴더
fonts	2015. 12. 22. 오...	파일 폴더
framework	2015. 12. 22. 오...	파일 폴더
lib	2015. 12. 23. 오...	파일 폴더
media	2015. 12. 22. 오...	파일 폴더
usr	2015. 12. 22. 오...	파일 폴더
vendor	2015. 12. 22. 오...	파일 폴더
xbin	2015. 12. 22. 오...	파일 폴더
.DS_Store	2015. 12. 23. 오...	DS_STORE 파일
build.prop	2015. 12. 22. 오...	PROP 파일
default.prop	2015. 12. 22. 오...	PROP 파일

변조된 부트 로그

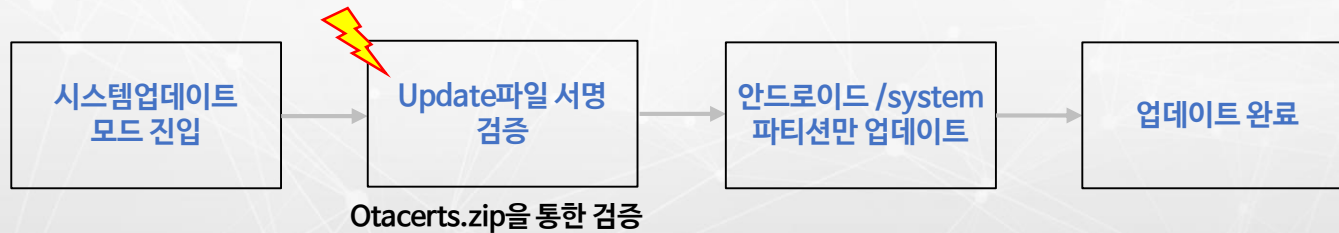


IVI 업데이트 수행 절차

일반 업데이트 (정상 절차)



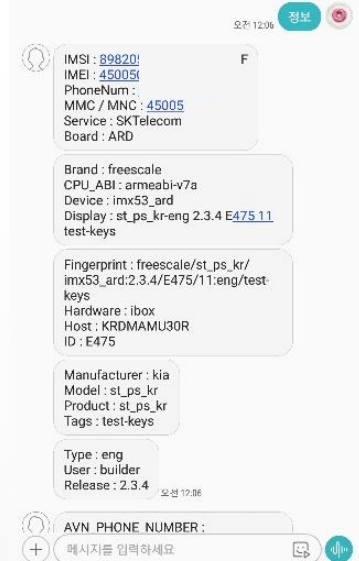
시스템 업데이트 (공장 업데이트)



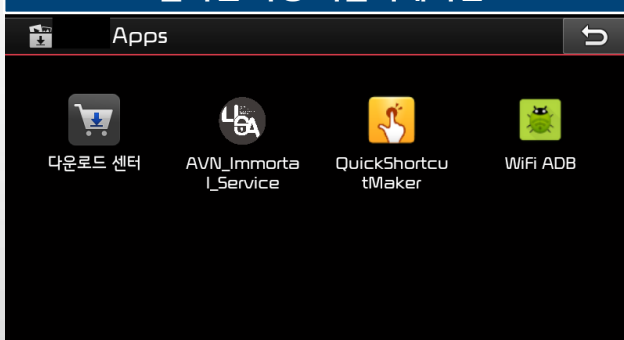
악성 어플리케이션을 통한 보안 위협

- IVI의 경우, 시스템 앱을 제외한 앱은 백그라운드에서 동작 불가
- 보드의 플랫폼키 확보 후 서명하여 시스템 권한 및 백그라운드 동작 가능
- 셸 명령 실행 및 제조사 화이트리스트 앱 보안 설정 무력화 가능
- 지속적인 서비스를 통해 메시지 수신 시 특정 명령어 조작 가능
- 특정 명령어를 통해 문열림/닫힘, 시동 제어 가능

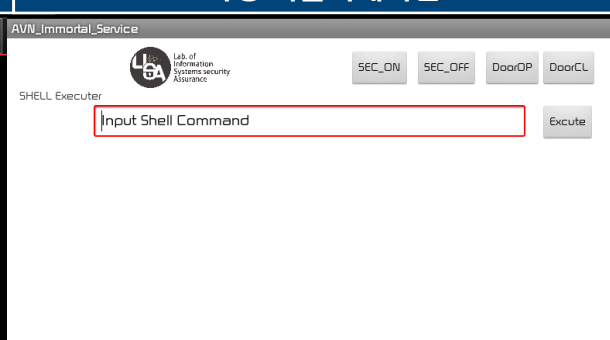
문자를 통한 IVI 정보 탈취



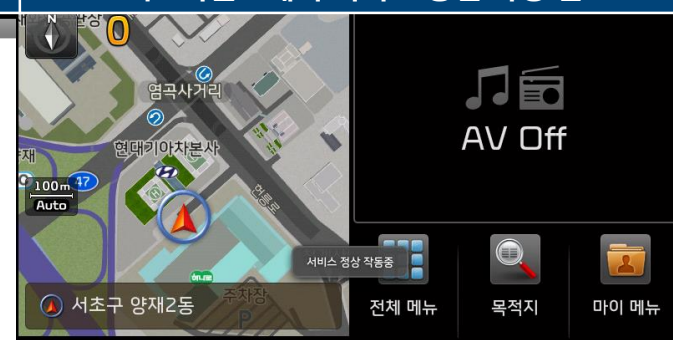
설치된 악성 어플리케이션



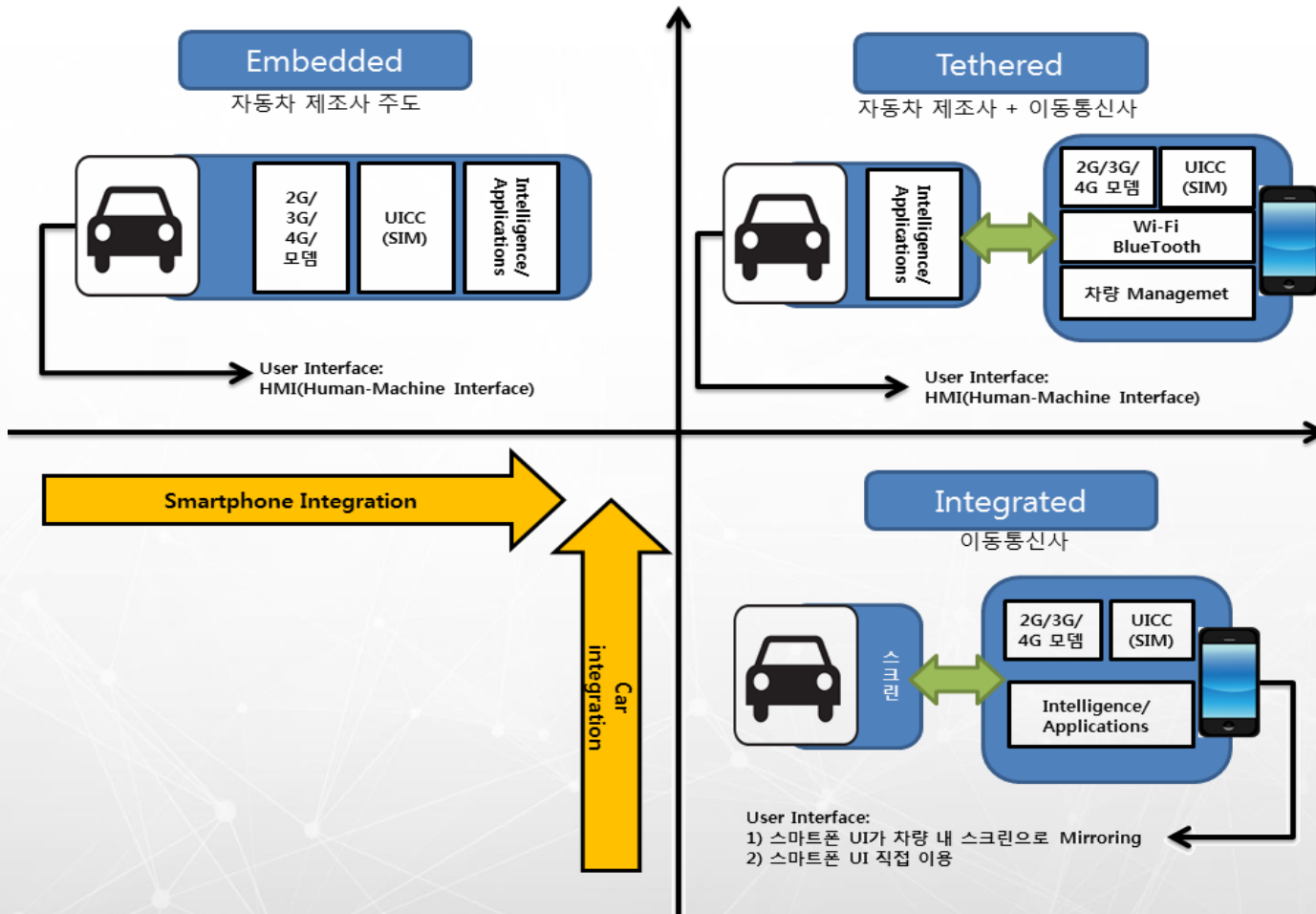
악성 어플리케이션



백그라운드에서 서비스 중인 악성 앱



텔레메틱스 시스템



텔레매틱스 전송 메시지 분석

- 구형 AVN의 경우 신형과 달리 모뎀이 노출되어 있어 USIM 추출 가능
- IMEI 인증으로 인해 USIM 독립적으로 분석 힘들며 IMEI 스푸핑을 통하여 분석 가능하지만 법적문제로 인해 수행 불가
- 내부 펌웨어 번조를 통한 분석 환경 구축
- 문 열림 및 닫힘, 제어 명령 등을 SMS 기반으로 송/수신
- 메시지 데이터 로그를 통해 데이터셋 수집

LogCat Logs

```

I/Engine [T1::RecvVpFIFO] FIFO Read Version = 1404220111
VIT-TPEG MosenNoticeFileSave() BufferSize is 577
BroadcastUtils... AA 0E 89 FF 01 20 08 E0 F1 00 00 00 02 01 3C
TimePolicyService.onLocationChanged
TimePolicyService.onStatusChanged: gps, status = 1
BroadcastUtils... AA 07 EF 18 01 0E 00 4A 00 14
RadioService => Micom(FMI(0x81), REQ_RADIOSTATUS(0x49))
Micom c => m: 16 1F 81 01 49 db
NaviHeapWorker... com.ansoft.nevi(181) HeapWorker (183) CPU usage = 0%
I/Engine [T1::RecvVpFIFO] FIFO Read Version = 1404220111
VIT-TPEG MosenNoticeFileSave() BufferSize is 577
BroadcastUtils... AA 07 EF 18 01 00 00 4E 00 17
RadioService => Micom(FMI(0x81), REQ_RADIOSTATUS(0x49))
  
```

LogCat Code

```

Log.i(str2, "android.os.Environment.getExternalStorageState()");
if (action.equals("android.intent.action.BOOT_COMPLETED")) {
    str3 = SDCardMonitorService.TAG;
    Log.v(str2, "on BOOT_COMPLETED");
    if (Environment.getExternalStorageState().equals("mounted")) {
        str3 = SDCardMonitorService.TAG;
        Log.v(str2, "ExtSD MEDIA_MOUNTED");
        SDCardMonitorService.this.setIgnoreMounted(SDCardMonitorService.DBG);
        return;
    }
}
  
```

안드로이드 메시지 전송 로그

```

I/telephonyManager( 696): [jeoni] getSmsType mSmsType= 1
I/System.out( 111): [CMM]Received Center SMS Msg.
I/System.out( 111): [MofGen2Receiver]centerMsgReceiver
I/System.out( 111): [CMM]Add Wakeup Thread:23
I/System.out( 481): [MOF] 2020-01-07 18:46:27.102 INFO [Thread-23] root (SmsCodec.assembly:215)
SMS : msgID = 1578390386, totalCount = 9, seq = 1
I/System.out( 111): [MofGen2Receiver]Received SMS Size: 76
I/System.out( 111): [MofGen2Receiver]Wakeup Received Center -> I-BOX ] -> FAIL : Request is null
D/libc ( 1447): fork handler start
D/libc ( 1447): fork handler end
I/Java_Layer( 191): [772]proc handler entered. mode = 2
D/libgps ( 111): :gps_hippo_poll(305):[0x32-01]: 32 01 cf 07 08 16 00 0a 24 10 00 00 00 00 00 02 00 00
D/libgps ( 111): :gps_hippo_poll(309):[UTC]: 8/22/1999 0:10:36, 935280636000 ms(System clock)
V/Location_Manager( 481): iBox|GPS lat:37.46386944|GPS lon:127.0429888|GPS alt:-18.0|GPS head:0|GPS speed:0|G
:20200107184631
  
```

Dmsg Logs

```

usb 1-1: New USB device found, idVendor=1d74, idProduct=2100
usb 1-1: New USB device strings: Mfr=3, Product=2, SerialNumber=0
usb 1-1: Product: LG Innatek HSDPA Modem
usb 1-1: Manufacturer: LG Innatek, Incorporated
PM: Adding info for usb:1-1
  
```

Sysdump Logs

```

[ 0.000000] p = 2000, size( 0, 0), size( 0, 0), mediaBinding=0, mediaDithering=0, invalidate=0, alpha=0,
name=cm.android.systemui.wallpaper.ColorWallpaper
(client=0x20000, identity=
[ mode=0, mediaBinding=0, queue=0 ] realClock=0x00000000, identity=0, status=
format=4, [media=0x0] [480x800-480], freeClock=0x0, hsync=0, dq-q-time=2000 us
Region transparentRegion (this=0x20000, count=1)
[ 0, 0, 0, 0 ]
Region transparentRegionScreen (this=0x2007ac, count=1)
[ 0, 0, 0, 0 ]
Region visibleRegionScreen (this=0x200780, count=1)
[ 0, 0, 0, 0 ]
  
```

텔레메틱스 서비스 계정 탈취



Remote App



텔레메틱스 서버

제어 메시지 전송

- 원격 시동 및 온도 조절
- 문잠김/문열림
- 비상등/경적울림
- 차량상태확인



IVI

pushVersion.do

통신을 위한 정보 교환

license.do

라이선스 정보 전송

~~auth.do~~

전화번호, 주민번호, 비밀번호 전송

smsNo.do

이용할 단말기의 번호 전송

smsAuth.do

SMS 인증번호 전송

session.do

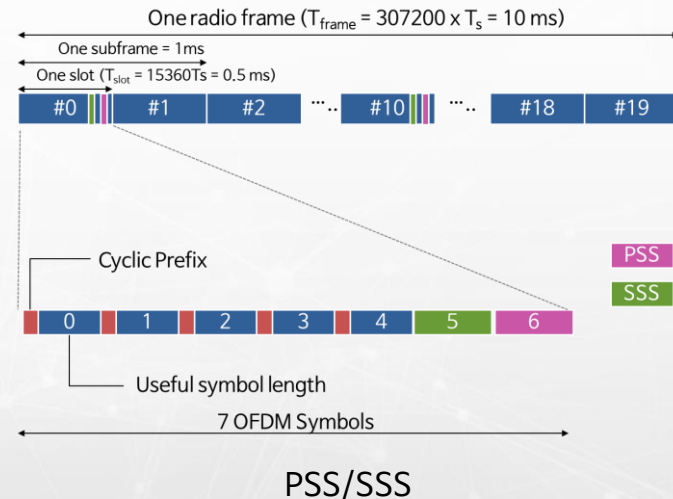
로그인 확인

계정 데이터 탈취

탈취된 계정을 통한 차량 제어

IVI 텔레메틱스 서비스 분석

- 내부 보드를 분석한 결과 LG USIM 내장형 LTE 모듈을 사용
- 모뎀 정보를 통해 전화번호와 IMSI, IMEI 등을 확인 가능
- 기존 이동통신망(LTE)에서 존재하는 PSS/SSS 교란을 통한 서비스 거부 공격 테스트 수행
- PSS/SSS는 초기 연결, 핸드 오버 시에 새로운 기지국과의 연결을 위한 기준 신호



텔레메틱스 서비스 신호 간섭 가능성

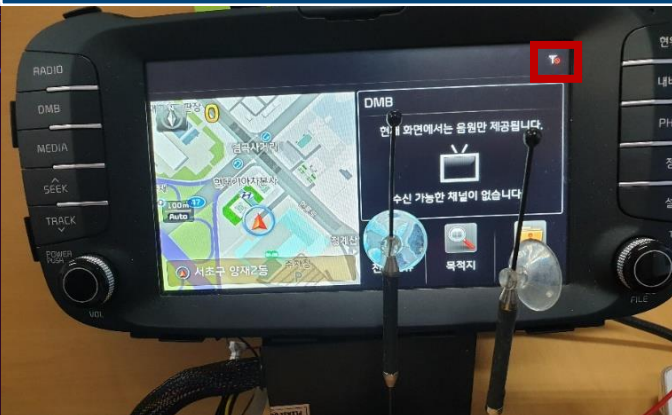
- 텔레메틱스 서비스는 이동통신사의 3G/LTE 망을 사용 (Downlink 2140~2150MHz 대역)
- SDR기반 srsLTE와 무선 주파수 발생기 USRP B210을 활용
- 시동을 걸 때, 이동 중 핸드오버 발생 시 등의 기지국과의 초기 연결이 필요한 상황
- 2145MHz의 PSS/SSS 신호 송출하여 신호 교란 (날짜와 시간 포함)

srsLTE를 통한 jamming 신호 송출

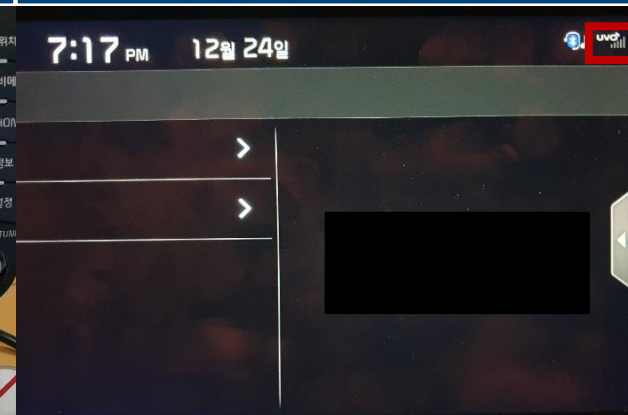
```

root@lisa-500R5K-501R5K-500R5Q:/home/lisa/Desktop/srsLTE/build/lib/
Opening RF device...
[INFO] [UHD] linux; GNU C++ version 7.4.0; Boost_106501; UHD_3.14.1.
[INFO] [LOGGING] Fastpath logging disabled at runtime.
Opening USRP with args: type=b200,master_clock_rate=30.72e6
[INFO] [B200] Detected Device: B210
[INFO] [B200] Operating over USB 3.
[INFO] [B200] Initialize CODEC control...
[INFO] [B200] Initialize Radio control...
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Asking for clock rate 30.720000 MHz...
[INFO] [B200] Actually got clock rate 30.720000 MHz...
[INFO] [B200] Asking for clock rate 11.520000 MHz...
[INFO] [B200] Actually got clock rate 11.520000 MHz.
Setting sampling rate 11.52 MHz
Set TX gain: 100.0 dB
Set TX freq: 2145.00 MHz
Cell Jamming Start...
  
```

IVI 텔레메틱스 서비스 신호 교란



신형 IVI 서비스 신호 교란





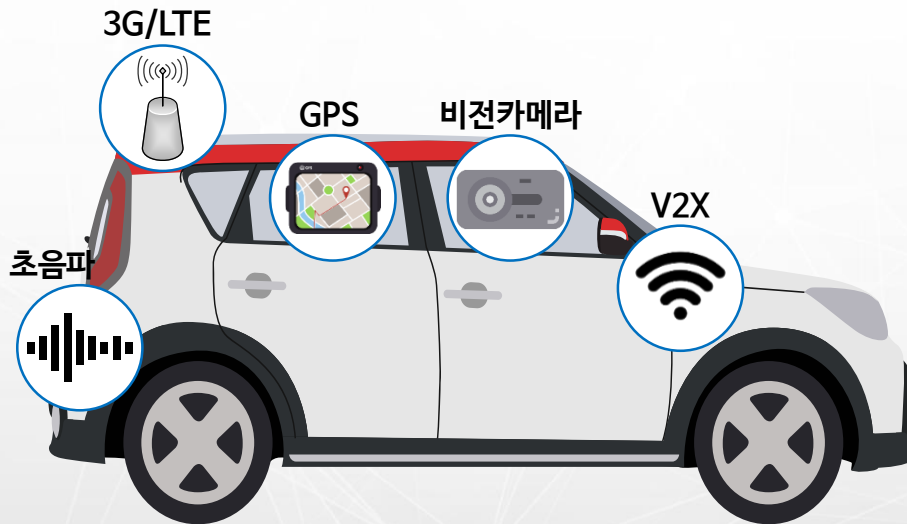
05

자동차 센서 네트워크 취약점 분석

외부 센서 네트워크

- 단위 모듈 및 센서에 대한 측정 값 교란 뿐만 아니라, 측정 값이 실제 차량 주행 시스템에 미치는 영향에 대해 분석함과 동시에 이에 대한 데이터 셋 확보

차량내 설치되어 있는 외부 접점

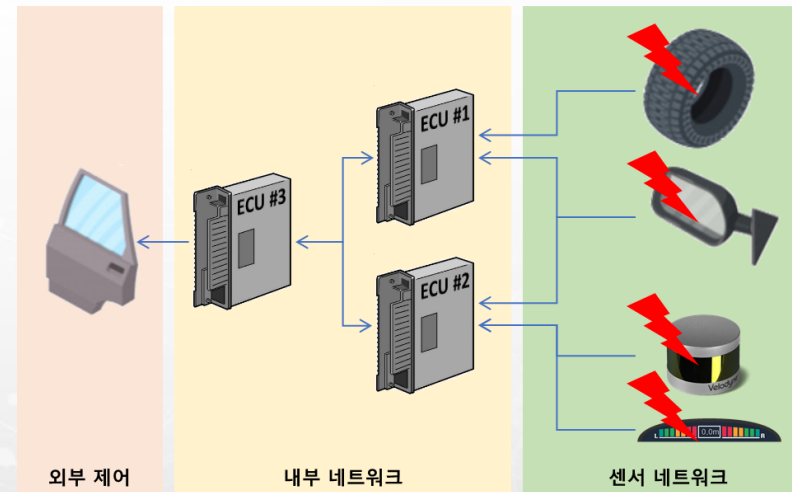


센서데이터로부터 변환된 CAN 데이터

3 센서오류에 의한 오작동 유발

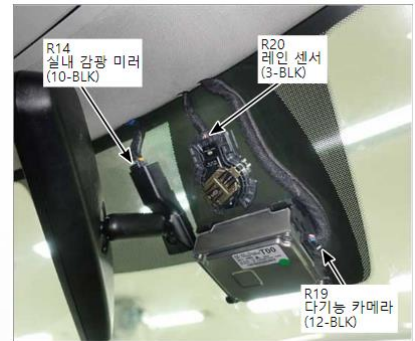
2 센서데이터 오류

1 센서 자극

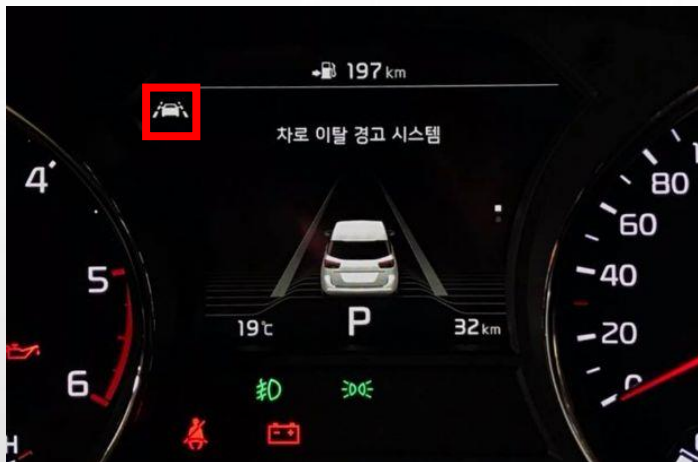


전방 카메라 센서 교란

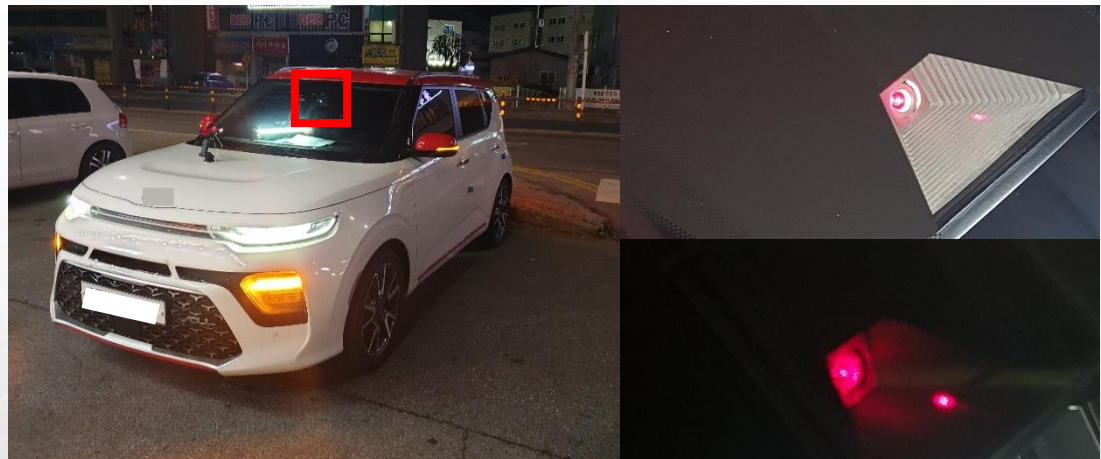
- ADAS 관련 차선 이탈방지보조, 전방추돌방지 시스템에 활용
- 아두이노 레이저 모듈을 통해서 카메라 렌즈에 직접 레이저 투사
- 차선 이탈 방지 기능이 작동중인 상태(60km/h 이상) 교란 시도
- 정상과 교란 상황에서의 P-CAN/C-CAN 데이터셋 확보
- 정상 작동 중인 ADAS 시스템의 작동 중단이 발생



전방 카메라 센서 모듈 구조



차선 이탈 방지 보조(LKA)



레이저 모듈을 통한 카메라 교란

초음파 센서 교란

- 드라이브(D)/리어(R)상태 에서 동작하는 전방/후방 초음파 센서를 대상(PDW)
- 초음파 발생기를 통해서 1에서 22000Hz 까지 다양한 범위의 주파수를 송출
- 일반적인 전방 및 후방 센서의 경우 130cm 까지 인식하나, 교란시에는 최대 300cm 거리에서도 교란 가능
- 정상적인 상태의 CAN 데이터 셋과 초음파 교란시의 CAN 데이터 셋 확보(C-CAN)



초음파 발생 모듈



전방 초음파 센서 테스트



후방 초음파 센서 테스트

카메라 센서 데이터셋

■ 초음파

Distance	Data
가까움	C0 00 03 09 / C0 18 00 09
덜 가까움	80 00 02 09 / 80 10 00 09 40 08 00 09 / C0 00 18 09 80 00 18 09 / 40 08 00 09

■ 카메라 센서

Function	CAN ID	Data
차로 이탈 방지	340	2C 40 01 2C AC 00 11 1A
후/측방 센서	58b	12 00 00 00 00 00 00 40
전방 충돌 방지	38d	00 00 48 00 68 00 00 BE
스마트 크루즈	4F1	C0 96 58 F1
ADAS 관련	130	7C 80 EF 7F 00 00 07 DB
비프음	52a	4B 00 00 00 02 00 4B 00
전조등 관련	541	03 04 81 80 C0 01 10 0D
와이퍼 관련	559	00 00 04 00 00 40 00 40

정상 데이터 셋

5.3745	1	Rx	436h	4	00 00 00 08
5.3972	1	Rx	436h	4	C0 00 03 09
5.4368	1	Rx	436h	4	C0 00 03 09
5.4772	1	Rx	436h	4	C0 00 03 09
5.5245	1	Rx	436h	4	C0 00 03 09
5.5745	1	Rx	436h	4	C0 00 03 09
5.6239	1	Rx	436h	4	C0 00 03 09
5.6739	1	Rx	436h	4	C0 00 03 09
5.7245	1	Rx	436h	4	C0 00 03 09
5.7745	1	Rx	436h	4	C0 00 03 09
5.8240	1	Rx	436h	4	C0 00 03 09
5.8743	1	Rx	436h	4	C0 00 03 09
5.9245	1	Rx	436h	4	C0 00 03 09
5.9745	1	Rx	436h	4	C0 00 03 09
6.0240	1	Rx	436h	4	C0 00 03 09
6.0742	1	Rx	436h	4	C0 00 03 09
6.1245	1	Rx	436h	4	C0 00 03 09
6.1745	1	Rx	436h	4	C0 00 03 09
6.2242	1	Rx	436h	4	C0 00 03 09
6.2743	1	Rx	436h	4	C0 00 03 09
6.3247	1	Rx	436h	4	C0 00 03 09
6.3745	1	Rx	436h	4	C0 00 03 09
6.4242	1	Rx	436h	4	C0 00 03 09
6.4741	1	Rx	436h	4	C0 00 03 09
6.5247	1	Rx	436h	4	C0 00 03 09
6.5744	1	Rx	436h	4	C0 00 03 09
6.6245	1	Rx	436h	4	C0 00 03 09
6.6742	1	Rx	436h	4	C0 00 03 09
6.7243	1	Rx	436h	4	C0 00 03 09
6.7745	1	Rx	436h	4	C0 00 03 09
6.8243	1	Rx	436h	4	C0 00 03 09
6.8742	1	Rx	436h	4	C0 00 03 09
6.9246	1	Rx	436h	4	C0 00 03 09
6.9745	1	Rx	436h	4	C0 00 03 09
7.0243	1	Rx	436h	4	C0 00 03 09
7.0742	1	Rx	436h	4	C0 00 03 09
7.1246	1	Rx	436h	4	C0 00 03 09
7.1748	1	Rx	436h	4	C0 00 03 09
7.2243	1	Rx	436h	4	C0 00 03 09
7.2744	1	Rx	436h	4	C0 00 03 09
7.2871	1	Rx	436h	4	C0 18 03 09
7.3271	1	Rx	436h	4	C0 18 03 09

비정상 데이터 셋

29.4023	1	Rx	436h	4	00 00 00 08
29.4507	1	Rx	436h	4	00 00 00 08
29.5018	1	Rx	436h	4	00 00 00 08
29.5508	1	Rx	436h	4	00 00 00 08
29.6018	1	Rx	436h	4	00 00 00 08
29.6507	1	Rx	436h	4	00 00 00 08
29.6740	1	Rx	436h	4	C0 00 18 09
29.7139	1	Rx	436h	4	C0 00 18 09
29.7540	1	Rx	436h	4	C0 00 18 09
29.8017	1	Rx	436h	4	C0 00 18 09
29.8508	1	Rx	436h	4	C0 00 18 09
29.9014	1	Rx	436h	4	C0 00 18 09
29.9508	1	Rx	436h	4	C0 00 18 09
30.0022	1	Rx	436h	4	C0 00 18 09
30.0507	1	Rx	436h	4	C0 00 18 09
30.1014	1	Rx	436h	4	C0 00 18 09
30.1509	1	Rx	436h	4	C0 00 18 09
30.2018	1	Rx	436h	4	C0 00 18 09
30.2507	1	Rx	436h	4	C0 00 18 09
30.3020	1	Rx	436h	4	C0 00 18 09
30.3508	1	Rx	436h	4	C0 00 18 09
30.4016	1	Rx	436h	4	C0 00 18 09
30.4506	1	Rx	436h	4	C0 00 18 09
30.5010	1	Rx	436h	4	C0 00 18 09
30.5509	1	Rx	436h	4	C0 00 18 09
30.6016	1	Rx	436h	4	C0 00 18 09
30.6506	1	Rx	436h	4	C0 00 18 09
30.7011	1	Rx	436h	4	C0 00 18 09
30.7508	1	Rx	436h	4	C0 00 18 09
30.8019	1	Rx	436h	4	C0 00 18 09
30.8506	1	Rx	436h	4	C0 00 18 09
30.9011	1	Rx	436h	4	C0 00 18 09
30.9041	1	Rx	436h	4	00 00 00 09
30.9438	1	Rx	436h	4	00 00 00 09
30.9836	1	Rx	436h	4	00 00 00 09
31.0021	1	Rx	436h	4	00 00 00 09
31.0506	1	Rx	436h	4	00 00 00 09



ADAS 교란 상태 및 경고등 점등

GPS 센서 - IVI 네비게이션, V2X

- 네비게이션과 지도는 GPS 데이터의 현재 위치를 기반으로 정보를 제공
- 스마트 크루즈 컨트롤은 현재 위치에 기반하여 과속 카메라의 제한 속도에 맞춰 속도 제어
- 자율주행 자동차의 경우 GPS를 기준으로 고정밀지도 데이터를 수신하여 주변 정보를 확보
- GPS 신호 교란 시 강제로 과속 카메라 위치로 이동하여 속도를 제한할 수 있는 가능성 존재



GPS 위성 (출처 : SK 브로드밴드 공식 블로그)

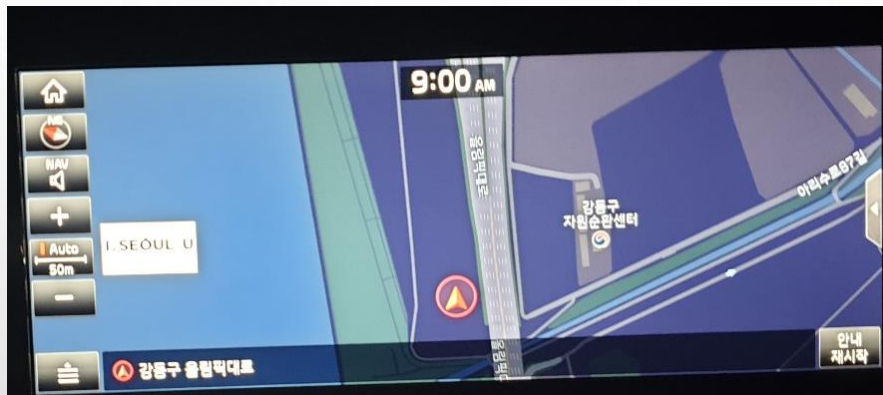


고정밀 지도 (출처 : 현대 엠엔소프트 공식 블로그)

GPS 센서 교란 - IVI 네비게이션

- GPS-SDR-SIM을 통한 GPS 신호 송출
- 송출력을 낮춰 주변에 영향을 최소화
- 초기 GPS 좌표를 기준으로 현재 위치 변화
- 위도/ 경도 37.5706933 / 127.1591379
- 단말기 내부 정상 GPS 데이터 확보

GPS 신호 발생 테스트



주행 중 조작된 GPS 좌표



조작된 GPS를 통한 길찾기

GPS 센서 교란 - OBU

- OBU 내부 모듈에 장착되어 있는 GPS 모듈을 대상으로 교란 시도
- 디버그 포트를 통해 “/dev/ttymx4”의 GPS 데이터를 수집함으로써 위치에 대한 교란 확인
- 현재 위치는 충남 아산시(3646.1357 N, 12655.9362 E)
- 교란 위치는 아프리카 부근(0001.8069 N, 07314.1091 E)



정상 데이터 셋

```
$GNGLL,3646.1357,N,12655.9362,E,165506.000,A,A*4A
$GPGSA,A,3,28,35,33,11,34,,,,,,,,,3.4,2.5,2.3*38
$BDGSA,A,3,07,20,,,,,,,,,3.4,2.5,2.3*27
$GPGSV,4,1,13,01,23,056,16,03,56,069,24,06,35,265,,09,05,147,*7C
$GPGSV,4,2,13,11,17,081,25,17,63,338,,19,45,316,,22,35,051,*71
$GPGSV,4,3,13,23,13,121,,28,62,209,32,33,44,148,27,34,20,182,24*79
$GPGSV,4,4,13,35,79,096,25*48
$BDGSV,1,1,03,07,49,195,31,19,,,22,20,50,133,32*61
$GNRMC,165506.000,A,3646.1357,N,12655.9362,E,0.00,94.77,070120,,,A*44
$GNVTG,94.77,T,,M,0.00,N,0.00,K,A*1E
$GNZDA,165506.000,07,01,2020,00,00*4F
$GPTXT,01,01,01,ANTENNA OK*35
$GNGGA,165507.000,3646.1360,N,12655.9360,E,1,07,2.5,15.3,M,0.0,M,,*4F
```

비정상 데이터 셋

```
$GNGLL,0001.8069,N,07314.1091,E,000335.000,A,A*4C
$GPGSA,A,3,12,25,31,20,14,10,24,19,32,06,,,1.8,1.7,0.7*33
$BDGSA,A,3,,,,,,,,,1.8,1.7,0.7*2B
$GPGSV,4,1,16,01,,,39,02,,,39,04,,,36,05,,,28*76
$GPGSV,4,2,16,06,42,017,44,07,,,30,08,,,30,09,,,29*43
$GPGSV,4,3,16,10,54,087,38,11,,,37,12,23,335,38,13,,,29*7C
$GPGSV,4,4,16,14,00,315,41,15,23,335,25,16,,,31,17,,,43*7A
$BDGSV,1,1,00*68
$GNRMC,000335.000,V,0001.8069,N,07314.1091,E,3.38,207.83,,,A*6A
$GNVTG,207.83,T,,M,3.38,N,6.25,K,A*24
$GNZDA,000335.000,11,01,2020,00,00*4C
$GPTXT,01,01,01,ANTENNA OK*35
$GNGGA,000336.000,0001.5695,N,07347.2007,E,1,10,1.7,-6378270.2,M,0.0,M,,*5F
```



06

C-ITS 환경에서의 취약점 분석

보안에 취약한 자동차는 도시 전체를 위협



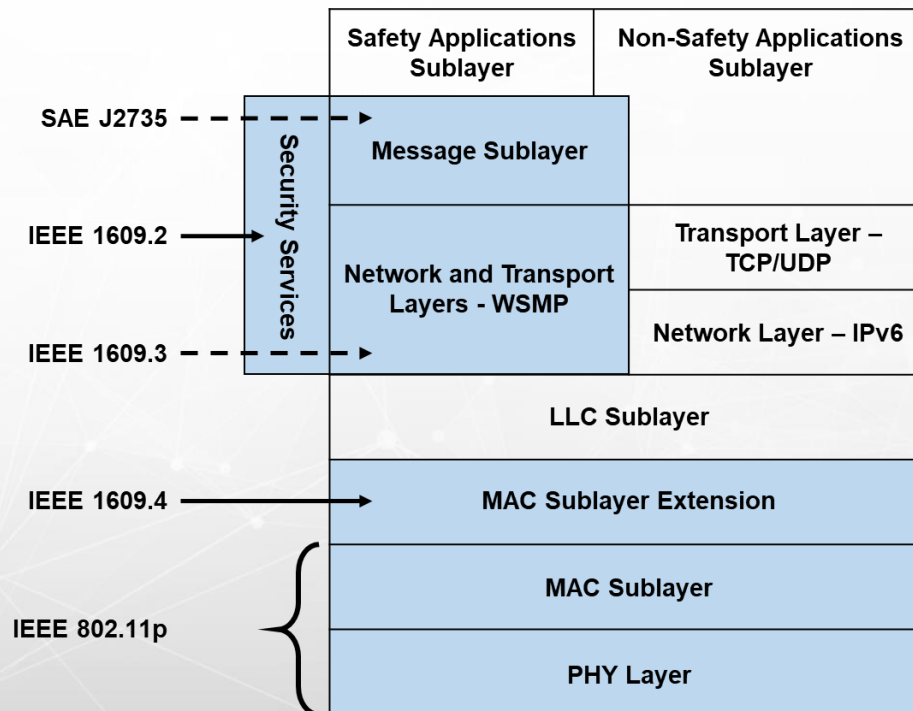
V2X 현황

- 센서 기반의 자율주행은 탐지거리 및 장애물 감지의 물리적 한계점 존재
- V2V(Vehicle to Vehicle), V2I(Vehicle to Infra) 등 상호 통신을 통해 차량간 데이터를 교환함으로써 보다 정밀한 데이터를 수신 받을 수 있는 형태로 발전
- 현재 DSRC(Dedicated Short-Range Communications) 방식의 WAVE와 셀룰러 방식의 C-V2X 두 종류의 표준 통신 기술이 존재

구분	WAVE	C-V2X
개요	무선랜 기술을 차량 통신에 적합하도록 커버리지 및 접속시간 개선	LTE를 차량 통신에 적합하도록 직접 통신 및 자원할당 방식 개선
이동성	최대 200km/h	최대 160km/h
필드 시험	2012년부터 유럽/미국/일본 주도	2015년부터 화웨이, 노키아 등 통신장비 업체 진행
대역폭	최대 27Mbps(10MHz 기준)	최대 100Mbps(10MHz 기준)
무선 지연	100ms 이내	100ms 이내
커버리지	별도 기지국 구축 최대 1km	LTE 기지국 1~5km
Echo system	교통 인프라, 무선랜 제조사	기존 LTE 통신장비, 단말 제조사, 이동통신사

WAVE(Wireless Access in Vehicular Environment)

- 고속으로 주행하는 차량환경에서 안전서비스를 제공하기 위하여 특화된 차세대 ITS 통신기술
- WLAN 기술(IEEE 802.11)을 자동차 환경에 맞도록 수정한 IEEE 802.11p를 기반으로 통신
- V2I(Vehicle-to-Infrastructure)와 V2V(Vehicle-to-Vehicle) 통신을 지원



WAVE 표준

▶ IEEE 1609.x

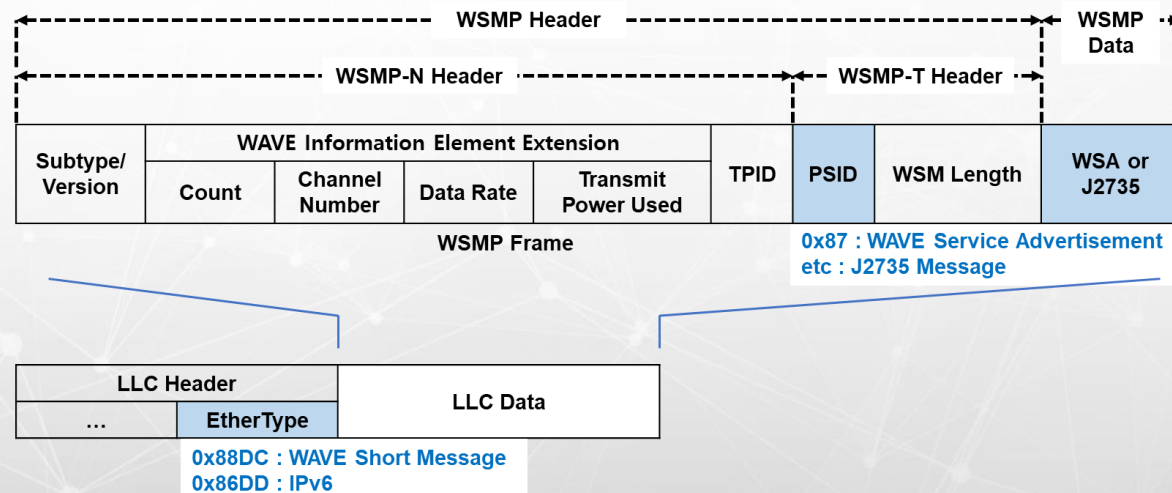
- WAVE를 통하여 고속의 차량환경에서 저 지연 통신을 수행하기 위한 시스템 구조, 통신 모델, 관리 구조, 보안 메커니즘, 물리계층 접근 등에 대하여 표준으로 정의함
 - IEEE 1609.0 : WAVE 시스템 구조 정의
 - IEEE 1609.2 - 2016 : WAVE 응용계층 및 관리메시지를 위한 보안 서비스 정의
 - IEEE 1609.3 - 2016 : WAVE 네트워킹 서비스 정의
 - IEEE 1609.4 - 2016 : WAVE 멀티채널 동작 정의
 - IEEE 1609.12 - 2016 : WAVE 식별자 할당 정의

▶ SAE J2735 DSRC

- DSRC(Dedicated Short-Range Communications) 메시지 셋을 정의한 규격
 - V2X 서비스에 필요한 차량 정보의 포맷을 정의
 - BSM(Basic Safety Message)
 - PVD(Probe Vehicle Data)
 - EVA(Emergency Vehicle Alert)
 - RSA(Road Side Alert)
 - TIM(Traveler Information Message)
 - SPaT(Signal Phase and Timing)

WAVE Short Message Protocol(WSMP) 구조

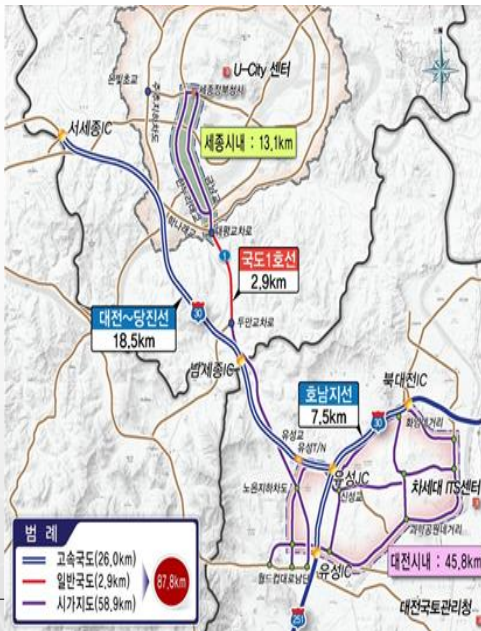
- WSA(WAVE Service Advertisement)와 WSM(WAVE Short Message)로 구분
 - WSA : 노변기지국(RSU)에서 제공하는 서비스유형(PSID)과 채널을 주변 OBU에게 알리기 위한 서비스 알림 메시지
 - WSM : 짧은 지연 시간이 요구되는 일반적인 통신과정에서 사용되는 메시지로 SAE J2735 메시지를 전송할 때 사용
- LLC Sublayer 헤더의 EtherType값이 0x88DC인 경우 WSMP, 0x86DD인 경우 IPv6 메시지
- WSMP의 헤더는 N-헤더와 T-헤더로 구분되며, T-헤더의 PSID 식별자는 IEEE 1609.12에 정의되어 있음
- PSID가 0x87일 경우 WSA 메시지로 구분되며, 이외의 메시지는 SAE J2735 또는 WSM로 구분됨



국내 V2X 시범 사업

- 국토교통부와 한국도로공사에서 스마트 하이웨이에 대한 실증 연구를 지속적으로 수행
 - 차세대 ITS(C-ITS) 센터
 - 스마트 자율협력주행(C-ARS) 센터

C-ITS 실증 구간

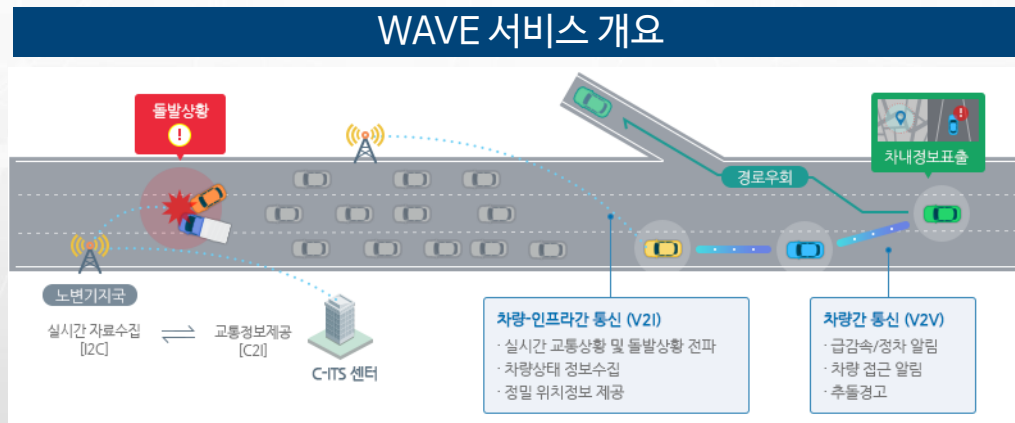
구분	도로명	구간(km)	구축 현황
고속도로 (26.0)	당진대전선	18.5	
	호남선지선	7.5	
국도 (2.9)	국도1호선	2.9	
대전시 (45.8)	유성대로	10.1	
	북유성대로	7.5	
	한밭대로	4.1	
	대덕대로	4.1	
	노은로	5.8	
	가정로	3.2	
	문지로	2.4	
	엑스포로	4.9	
세종시 (13.1)	대학로	3.7	
	한누리대로	5.0	
	갈매로	5.6	
	절재로	0.6	
	세종로	1.9	
계		87.8	

C-ARS 센터



WAVE 데이터 수집

- 한국도로공사에서는 OBU 지원을 통한 C-ITS 시범 사업 진행중



- Unex사의 RSU-101U/OBU-201U를 이용한 테스트망 구축
- WAVE 통신 패킷 확보, 인증서의 실제 사용 여부 검증 및 테스트베드 구축 등에 사용
- 통신 과정에서 인증 수단으로 사용될 수 있는 인증서 목록 등 수집
- 명령어를 통한 OBU 및 RSU간 테스트 메시지 송수신 구현

메시지 송/수신

```
dot3_wsm_send <handle> <psid> <radio number> <channel number> <data rate> <tx power>  
--dest_mac <size> <interval> <nnum>  
  
-- usage --  
  
<handle> handler id  
psid= psid of sending WSMV2 packets, 1 - 127  
radio number= radio number of the service, 1-2  
channel number= channel number of sending WSMV2 packets, 172 174 176 180 182  
184  
data rate= data rate of sending WSMV2 packets, 6 9 12 15 24 36 48 54  
tx power= tx power level of sending WSMV2 packets, 12- 25, unit:dBm  
--dest_mac peer mac address of sending WSMV2 packets, format: XXX:XXX:XX:XX:XX:XX  
XX  
--> <size> the size of sending packets, 0 - 1395, unit:byte  
--> interval= the interval of sending packets, 0 - 1000, unit:ms  
--> nnum= the number of sending packets, 1 - 10000  
  
-- example --  
dot3_wsm_send 1 123 1 172 6 18 FF:FF:FF:FF:FF:FF 1000 100 10  
  
[dot3_wsm_send 1 123 1 172 6 18 FF:FF:FF:FF:FF:FF 1000 100 10]  
[ate]>  
[info] [redacted]
```

```
[info] dot3_wsm_serv_create  
dot3_wsm_serv_create <handle> <psid>  
  
-- usage --  
  
<handle> handler id  
psid= psid of sending WSM packets, 1 - 127  
  
-- example --  
dot3_wsm_serv_create 1 123  
  
[info] dot3_wsm_serv_create 1 123  
[info] wsm_serv_create success, serv_index = 0  
[info] [redacted]
```

```
[info] recv pkt count = 1, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 2, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 3, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 4, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 5, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 6, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 7, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 8, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]  
[info] recv pkt count = 10, pld = 123, channel = 172, tx power = 18, data rate = 6, data len = 1000  
[info] [redacted]
```

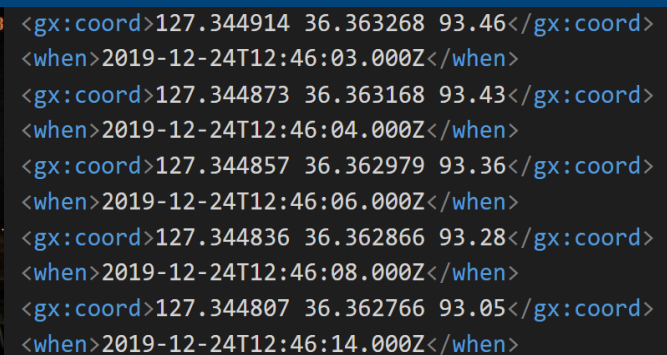
WAVE 통신 환경

- V2X 패킷의 경우 모든 패킷이 Broadcast 되므로 다중 포인트 연관성 분석 필요
- 외부 접점 교란에 대한 데이터를 확보하기 위해 타임스탬프를 포함한 총 6가지의 데이터셋을 수집
- 총 6종 22GB 분량의 주행 데이터셋 수집

③ 도로교통공사 운행 데이터

	A	B	C	D	E	F	G
1	ISSUE_DATE	OBJ_ID	RSU_ID	RCV_DATE	VEHICLE	VEHICL_X	
2	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331059
3	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330993
4	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330916
5	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330843
6	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330792
7	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330748
8	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.330663
9	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331121
10	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331129
11	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331132
12	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331135
13	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331158
14	2.01908E+13	7001F60B	C3999RSS00432	2.01908E+13	9220	4	127.331161

⑥ 주행 구간 GPS 데이터





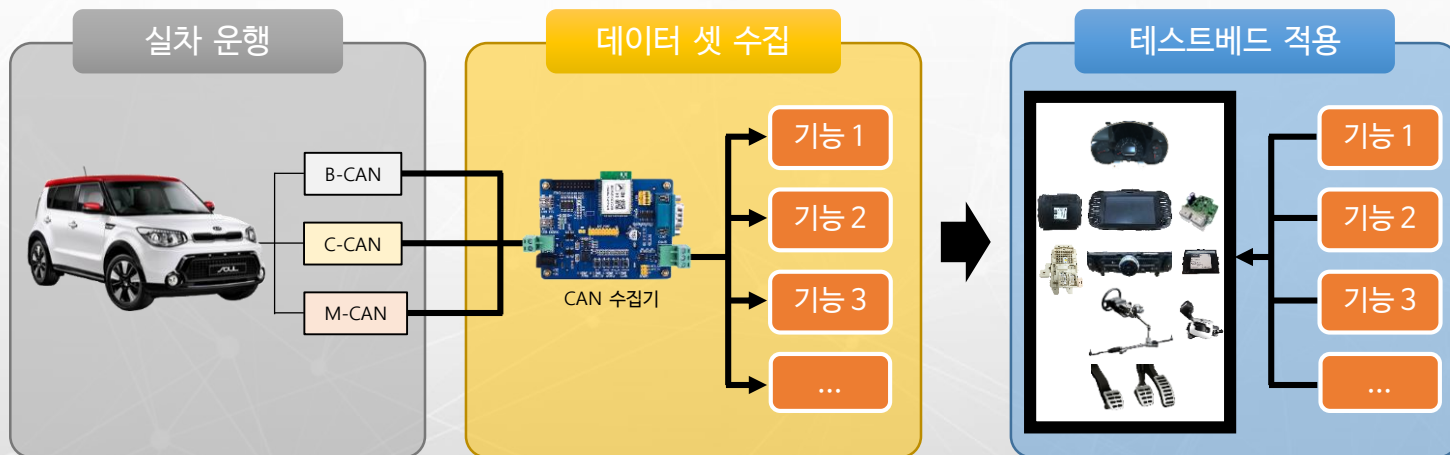
07

자동차 패킷 분석 프레임워크의 예

실제 ECU를 통한 침해사고 분석 프레임워크 개발 (LISA-TPCC-2017)

- 실제 차량에서 수집 가능한 데이터의 약 77% 수준 처리 가능 (CAN ID 기준)
 - 차량에서 수집 가능한 총 CAN ID 개수 : 95 개
 - 테스트베드에서 수집 가능한 총 CAN ID 개수 : 73 개
- CAN 네트워크와 관련 없는 엔진 등 동력 관련 기계 장비를 제외하고 구축
- 구현 기능
 - CAN 메시지 퍼징을 통한 공격 가능
 - 진단 메시지 전송을 통한 동작 유도 가능
 - 차량 수집 메시지 리플레이를 통한 재현 가능

CAN Network	실제 차량 CAN ID 개수	테스트베드 CAN ID 개수
B-CAN	16	16
C-CAN	45	37
M-CAN	34	20

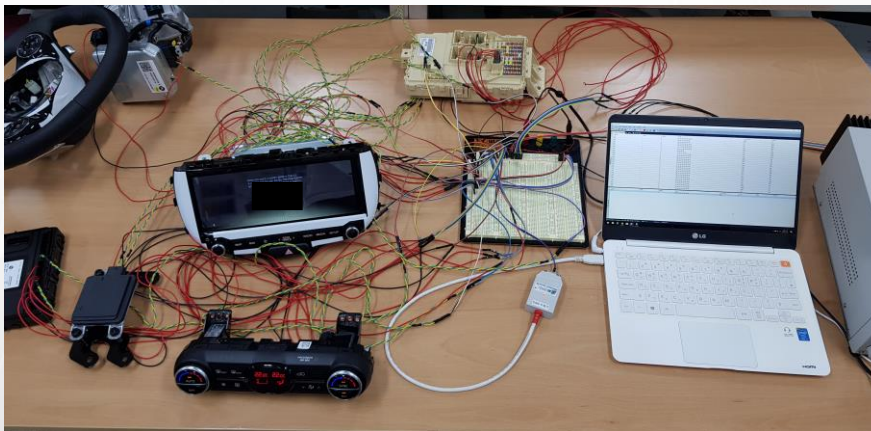


ECU 모듈간 연동 테스트

- 모듈 별 전원 공급 및 CAN 네트워크 식별
- 간이 테스트베드를 통한 모듈 별 CAN ID 파악
- 확보한 주행 데이터 리플레이 가능 여부 확인



구형 모듈 간이 테스트

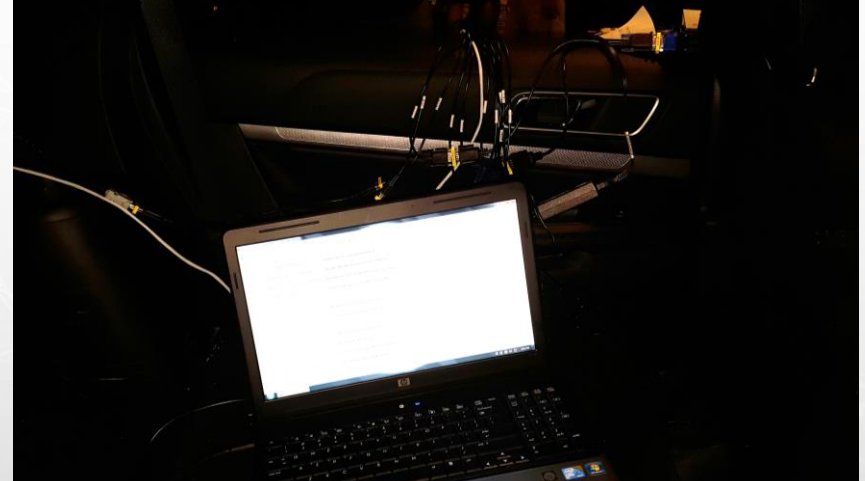
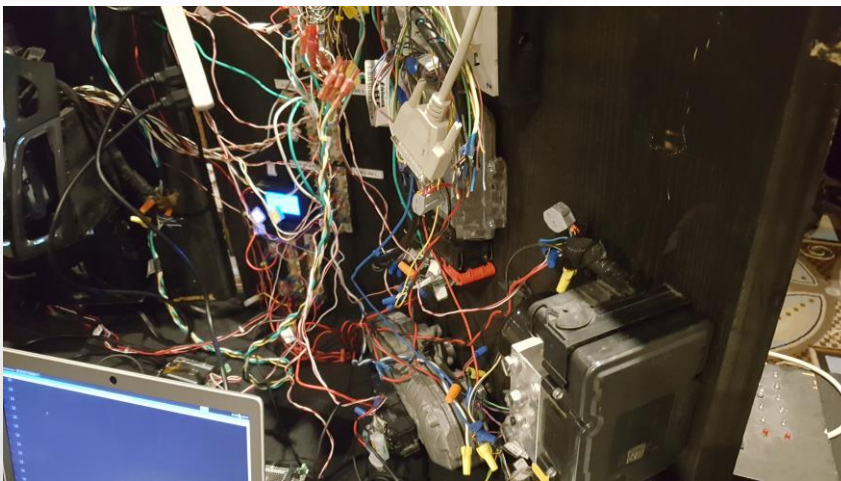
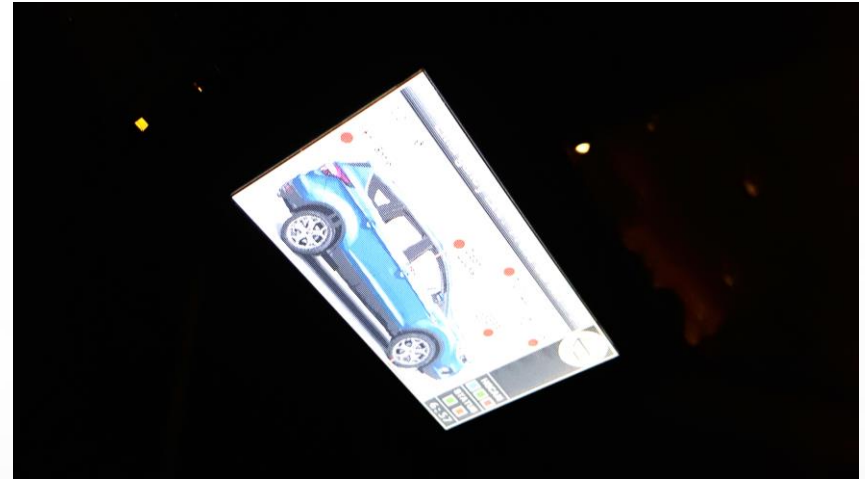


신형 모듈 간이 테스트



신형 모듈 연동 테스트

해외 프레임워크 현황



프레임워크 구성도

- Gear360을 통한 조작 데이터 확인
 - 차량 내부에서 설치하여 실제 운전자의 조작 확인
- 블랙박스를 통한 주행 환경 데이터 확보
 - 차량이 주행하고 있는 동안 발생하는 이벤트 확인
- CAN 수집기를 통한 CAN 메시지 확보
 - 차량에서 전송되는 모든 CAN 메시지 데이터 확인

운전자 조작 데이터



블랙박스 영상 (주행 환경)



주행 데이터 (CAN 메시지) 수집

Trace1 - PCAN-Trace [Playback]

File CAN Edit Trace Tools Help

Buffer: 9999/000 Messages (381.43 MB)

Message filter: ☒ Standard ☐ Extended

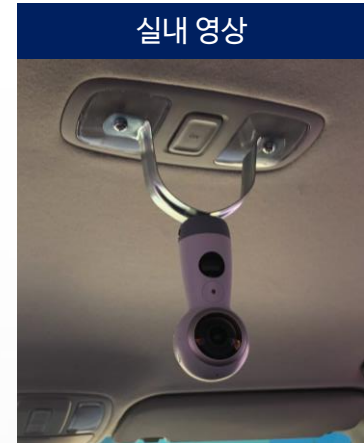
ID Range: 000 - 7FF

☐ Warnings ☐ Errors ☐ RTR

		Total	Current
Messages		2940683	729902
Errors		1	1
RTR		0	0
Time [sec]		1409.016	349.822

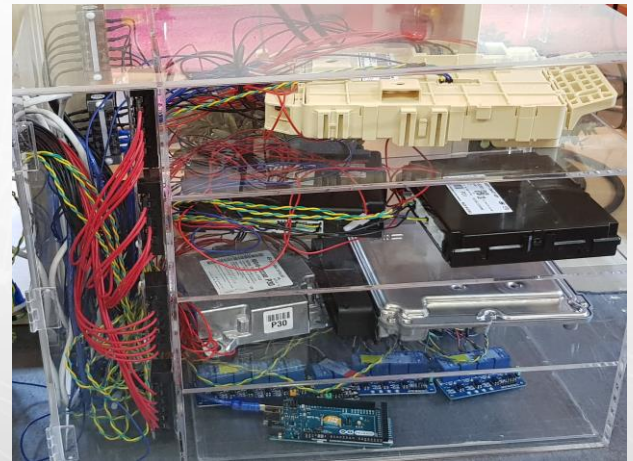
Time	Type	ID	DLC	Data
349.8162	Data	2B0	5	0C 00 01 07 4E
349.8164	Data	165	8	43 38 7F 00 00 00 0E 0A
349.8173	Data	4B0	8	7F C3 7F 43 7D 03 76 83
349.8176	Data	164	8	00 08 00 00 00 00 00 08
349.8180	Data	316	8	45 00 E4 12 0B 25 1D 7F
349.8182	Data	260	8	06 0B 00 30 FF A3 4D 1F
349.8185	Data	2A0	8	A2 00 93 1F 97 11 6E 04
349.8187	Data	080	8	00 17 E4 12 00 25 0B 4D
349.8190	Data	081	8	89 84 93 00 00 00 00 AD
349.8192	Data	18F	8	FE 50 0B 00 00 56 00 10
349.8194	Data	329	8	85 B0 7F 8C 12 2C 00 10
349.8197	Data	382	8	40 FE 0F 00 00 00 00 0C
349.8199	Data	4F2	8	A0 43 50 38 00 00 00 FD
349.8202	Data	545	8	D8 00 00 86 B0 FE 16 FF
349.8218	Data	43F	8	14 55 60 FF 7C F0 13 00
349.8220	Data	370	8	FF 1B 40 88 FF 00 00 8C
349.8223	Data	440	8	FF 34 1B 00 FF CC 13 7A
349.8225	Data	153	8	00 80 10 FF 00 FF 40 CE
349.8227	Data	220	8	04 04 63 23 9E 00 FA 0E
349.8240	Data	350	8	0F 2B 44 93 A4 00 00 57
349.8262	Data	2B0	5	0E 00 01 07 7F

실내 영상



테스트베드 기반 침해사고 분석 프레임워크 구축

- 각 ECU는 세 종류의 CAN 버스에 연결되어 있고, 이를 통해 진단 도구를 이용한 모듈 별 제어 및 실 차량에서 수집한 CAN 메시지 리플레이를 이용한 주행/공격 상황에 대한 재구성 가능



감사합니다



순천향대학교
SOON CHUN HYANG
UNIVERSITY



LISA 순천향대학교 시스템보안연구실
LAB. OF INFORMATION SYSTEMS SECURITY ASSURANCE