2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 2-2

의료사물인터넷(IoMT) 보안

권혁찬 책임 (한국전자통신연구원)

[요약문]

대규모 병원에서는 수만개의 커넥티드 디바이스 들이 있다. Irdeto의 보고서에서는 작년 한 해 동안 사이버 공격을 당한 의료 기관의 IoT 장치가 전체의 82%에 달한다고 보고한다. 실제로 최근 Ryuk, Phobos, Sodinokibi 등 랜섬웨어로 인한 의료기관의 피해가 속출하고 있으며, 특히 보안 시스템을 우회하며 보안에 취약한 의료기기를 장악해 Backdoor, Botnet 등을 구축하며 병원 네트워크 깊은 곳까지 침투하는 등 공격도 계속 진화되고 지능화되고 있다. 원격의료, 정밀의료 등 의료서비스가 확대되면서 의료사물인터넷 (IoMT: Internet of Medical Thing)환경에서는 더욱 다양하고 복잡한 보안 위협이 존재할 것으로 예상된다.

본 강연에서는 의료사물인터넷 환경의 특징을 분석하고, 이에 따른 보안 위협, 국내외 기술 현황/수준, 관련 원천기술 및 이슈를 소개한다.

[발표자 약력]

2018.04 ~ 현재　연세대학교 의과대학 의생명시스템정보학 조교수
2016.01 ~ 2018.03 서울아산병원 헬스이노베이션빅데이터센터 연구개발 담당교수
2015.09 ~ 2018.03 서울아산병원 임상의학연구소, 의생명정보학과 연구조교수
2013.11 ~ 2015.08 서울아산병원 임상의학연구소 특수전문학자
2013.05 ~ 2013.10 삼성 SDS 플랫폼 개발팀 책임연구원

관심분야 : 디지털 치료제, 보건의료 자료 표준화, 분산형 컴퓨팅

의료사물인터넷(IoMT) 보안

Security in the age of the Internet of Medical Things
Enabling smart Hospitals

ETRI 정보보호연구본부 권혁찬
hckwon@etri.re.kr

2020. 9. 24

목 차

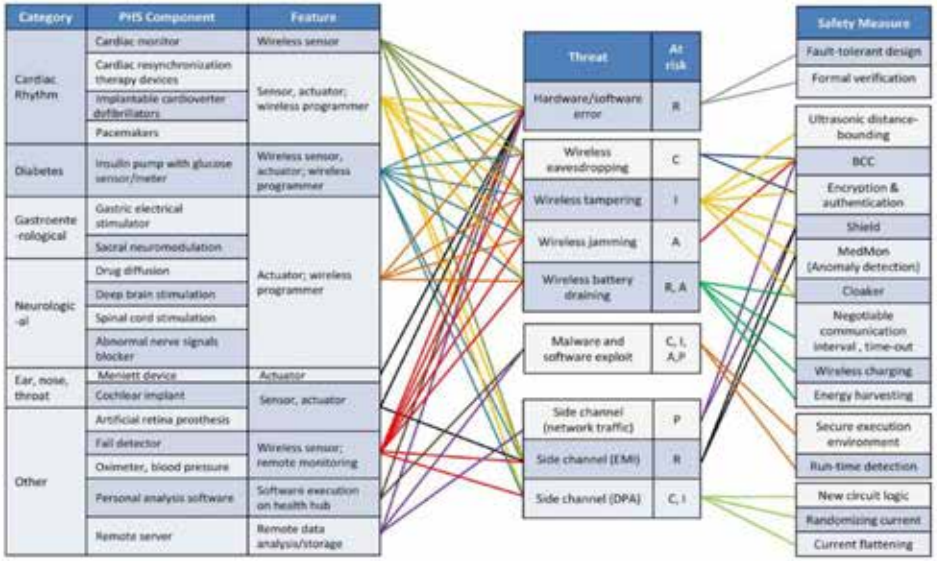
- 배경
- IoMT medical device 보안
- IoMT Implantable medical device 보안

20.8.18	2

배경 : IoMT (Internet of Medical Things)

◆Healthcare/Medical device의 IoT 化

- 연결성 확대 (유선, 무선), 원격의료, 정밀의료, 클라우드, 공유, 원격 모니터링 (환자, 기기), 원격 진단/유지보수(기기), 약/캡슐, Post-COVID
  → IoMT Security vulnerability ↑, IoT 보안 이슈 증가



Abilify MyCite

PillCamTM

IWMD(implantable and wearable medical devices) threats and countermeasures

20.8.18	3

IoMT medical device 보안

20.8.18	4

배경 : IoMT 사이버 공격 (통계)

89% of healthcare organizations have suffered from a security breach of the IoMT

82% of the IoMT have been targeted in the past year

Ransomware attacks on healthcare are predicted to grow 5X **by 2021**

Common types of IoMT attacks include: side channel, tag cloning, tampering, sensor tracking, eavesdropping, replay, man-in-the-middle, rogue access, denial of service, cross-site request forgery, session hijacking, cross-site scripting, SQL injection, account hijacking, ransomware, and brute force attacks

$408 per patient is the average cost-per-capita for a data breach in healthcare (the highest in any industry)

Hospitals spend 64% more annually on advertising after a breach 2 years following

출처: 802secure 보고서

95% of medical devices have **no endpoint security**

HEALTHCARE SECURITY CONCERNS

Most attacked industry since 2015

90% of hospitals are cyberthreat victims

75% of network traffic in a hospital is unmonitored

73% of hospitals do not have a security strategy for medical devices

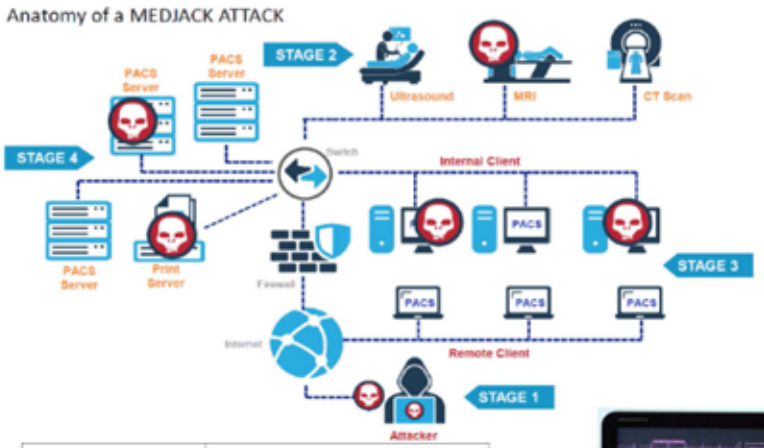
17% of confirmed attacks originate from connected medical endpoints

출처: Zingbox 보고서, 2018

20.8.18	5

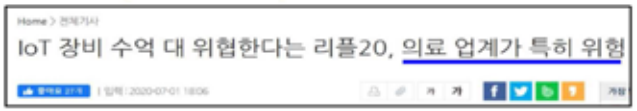
배경 : IoMT 사이버 공격 (사례)

MEDJACK:
X레이, MRI 등 의료 기기를 통해 네트워크에 침투하는 공격 발견 (2015~)

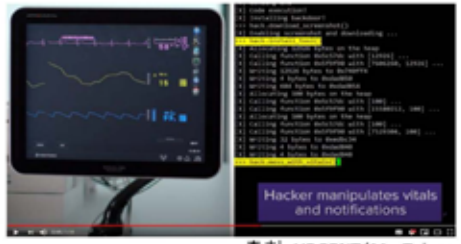


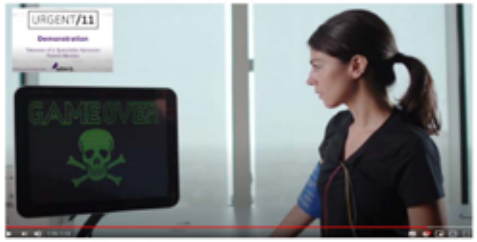
Medjack 1 ('15년)	의료기기 백도어
Medjack 2 ('16년)	의료기기 봇넷 공격, 내부망 침투
Medjack 3 ('17년)	패치되지 않는 구형OS 저사양 의료기기 공격, 탐지 시스템 우회

Ripple20 vulnerabilities (19 CVEs)
→ TCP/IP sw library 취약점
→ 19 zero day vulnerability



Urgent/11 vulnerabilities (11 CVEs)
→ VxWorks RTOS의 TCP/IP (Ipnet) 관련 취약점





출처: URGENT/11 - Takeover of a Spacelabs Xprezzon patient monitor (ARMIS), Youtube

배경 : IoMT 사이버 공격 (Ransomware)

◆ 의료 타겟의 랜섬웨어 증가, 공격의 지능화/고도화

Ransomware	Exploit	Spreading (malware)
Ryuk Phobos Dharma SamSam	Bluekeep (RDP…)	Emotet, Trickbot, PowerGhost …..
WannaCry NotPetya BadRabbit	EternalBlue (SMB) DoublePulsar	

EternalChampion,
EternalRomance….

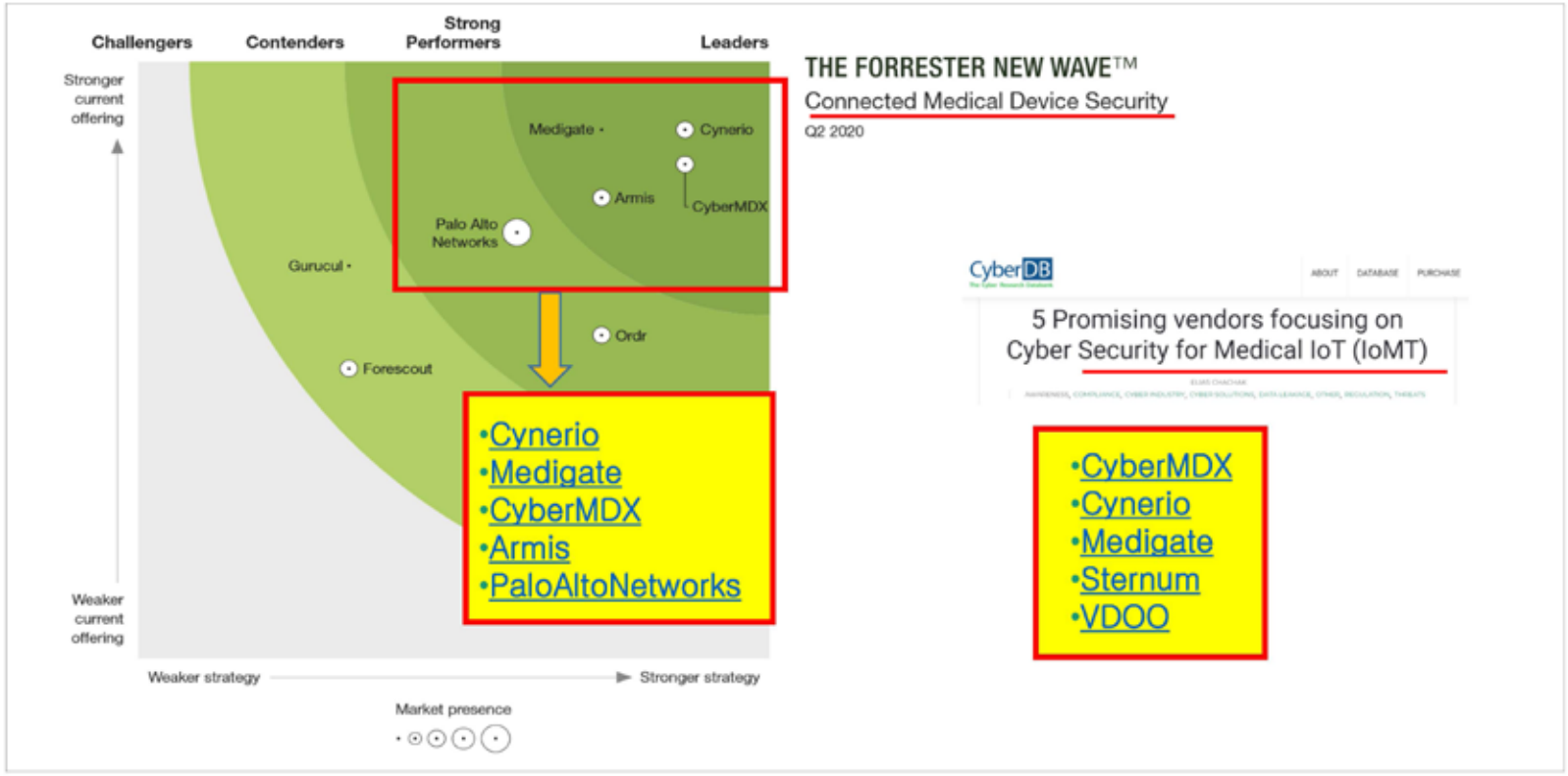
✚ Numerous variants

EternalBlue – Developed by NSA, 2017
Leaked by the Shadow Brokers hacker group, 2017

- RDP (Remote Desktop Protocol)
- SMB (Server Message Block, port# 445)

RDP exploit

해외: PROMISING VENDORS



20.8.18	8

이슈 1 – 비침습적 해킹 대응

백신도 못 까는 의료기기…보안성 강화 시급

OS버전, 상당수 업데이트 지원 끊긴 윈도7 이하

◆ 병원 커넥티드 의료기기의 특성

병원 커넥티드 의료기기 특성

보안이 고려되지 않은 설계

- 오래된 SW (구형 OS)
- 보안 패치/업데이트 불가
- 고가장비 – 10년 이상 사용
- PW하드코딩, 암호/인증/접근제어(인가) X

엔터프라이즈 보안 솔루션 적용 어려움

- SW 변경 불가
- 의료기기 가용성 우선
- 외산 의료기기 90% 이상
- 특수목적의 제한된 플랫폼 (BusyBox, Tizen, RTOS, Windows)

무선/네트워크 연결 의료기기 급증

- 약 2.4억대/2020년
- IoMT 化
- 최근 출시 의료기기는 대부분 네트워크 연결

취약점 공격

ARP poisoning , 멀웨어 /랜섬웨어, Botnet
insecure remote access, 무선 Radio 역공학,
settings 불법 변경, 배터리 소모공격(DoS), 스푸핑,
Replay, 버퍼 오버플로우, 오작동 공격 등

Medical Device Cyber Security - Best Practices Guide (2015,IHE, PCD-MEM)

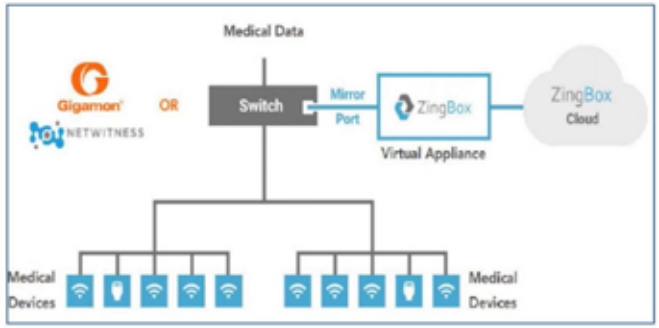
의료기기 가용성을 보장하는
비침습적 해킹 대응기술

➔ 비침습적 랜섬웨어 대응?

비침습적 해킹 대응 기술

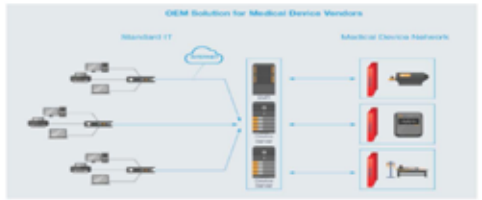
◆ 관련 연구 (vendor)

- **Medigate社 병원의료기기보안플랫폼: (이스라엘start-up)- (최초, 18.3.,HIMSS쇼케이스)**
  - ✓ 비침습적 이상징후를 원격 센싱/탐지, 공격 예측 및 대응
- **PaloAlto networks社 (zingbox)**
  - ✓ 디바이스 행위(network)에 대한 딥러닝 분석
- **ARMIS**
  - ✓ AgentLess 공격 탐지/대응
- **MediTechSafe社**
  - ✓ 사이버 공격 예측을 위한 AI 기반 분석



PaloAlto networks(zingbox)
– Machine learning 기반 이상징후 탐지
Network meta 데이터 → 클라우드 분석 기반

Armis
- Machine learning 기반 이상징후 탐지



병원-
MD network-level

제조사
-MD level

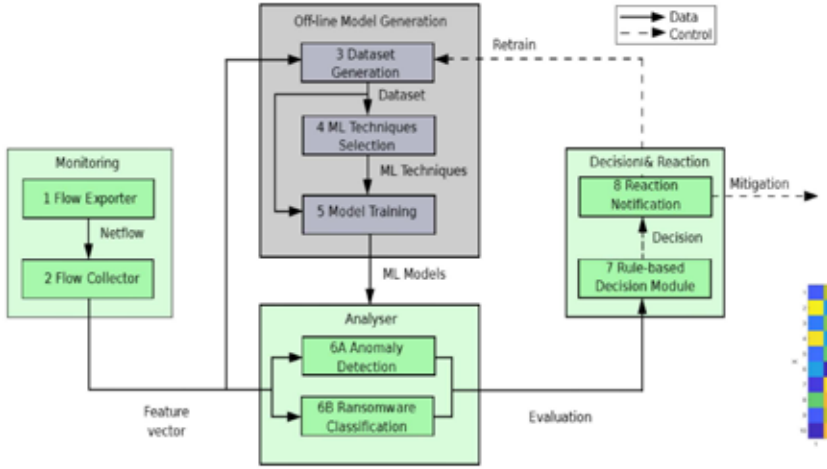
Medigate- agent 기반 의료기기 자동 식별,
공격탐지대응, 시각화

20.8.18	10

비침습적 해킹 대응 기술 – 네트워크 피노타이핑

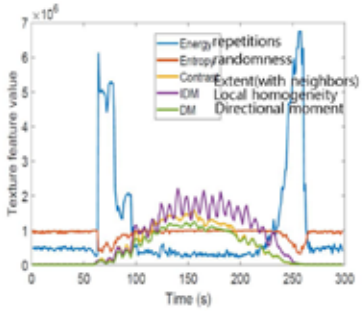
- **Murcia대, Pennsylvania 대 등: 머신러닝 기반 의료기기 Ransomware 탐지**
  - Spreading 단계에서 탐지 (wannacry, petya, badrabbit, powerghost)
  - ICE 프레임워크 통합

Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments, J. of sensors, 2019

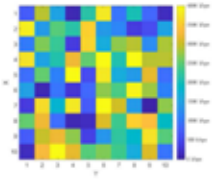


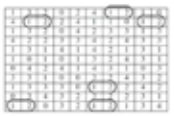
- **Georgia 공대, Chongqing 대 : 시공간/외형 행위적 특성 분석 기반 이상징후 탐지**
  - 시공간/외형 행위적 특성 : Resource usage, 통신관계/볼륨/속도/지연시간, 통신주기, 동작시간 빈도, 시계열 유사성 등

Network Phenotyping for Network Traffic Classification and Anomaly Detection, Chongqing대, Georgia 공대, IEEE (submitted)



Time-series Trends





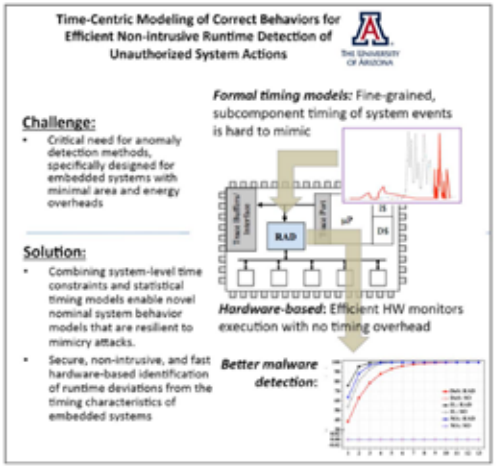
A. **Spatial** analysis of the communication image
B. **Temporal** analysis of **GLCM** texture features
C. **Classification** of the communication patterns
D. **Anomaly** detection

디바이스 피노타이핑

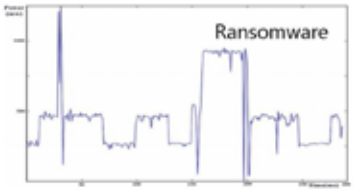
- 미국 Umass/UW/미시건대 : 비침습적 에너지소모분석-멀웨어탐지
  - SHARPS 보안 프로젝트 @메사추세츠 대학
- Georgia공대 : CPS 블랙박스 특성 핑거프린팅 기술
- Univ. of Arizona: 비침습적 비인가행위 실시간탐지 모델
  - 심박기에 적용할 런타임 이상 감지 (멀웨어, 오작동)

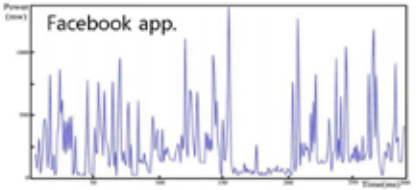
Protecting Implantable Medical Devices From Malware, Side-Channel Attacks (UA, 2017.03) @UA`` (16-19년, 45.3만불)

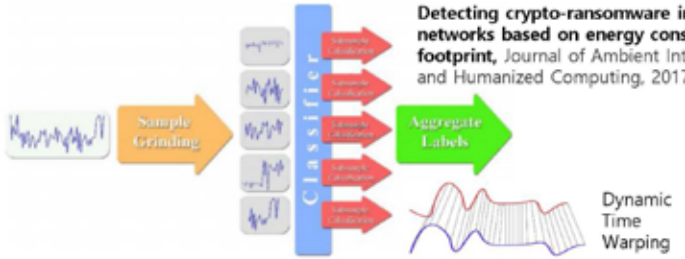
TWC: Small: Time-Centric Modeling of Correct Behaviors for Efficient Non-intrusive Runtime Detection of Unauthorized System Actions (@UA, NSF지원 2016.10-19.9)



- 워터루 대: CPU 전력소비 footprint기반 Crypto-ransomware 탐지 (android 장치 대상)
  - CPU전력 소비패턴 추출/분석 (신호처리, spectral분석, impulse response계산, 시계열파장 유사성분석(DWT) 등) → 기계학습 → 비침습적 프로세스 추적 및 이상징후탐지







Detecting crypto-ransomware in IoT networks based on energy consumption footprint, Journal of Ambient Intelligence and Humanized Computing, 2017.7

- Purdue, Princeton: Physical/ behavioral anomaly 탐지
  - 무선 신호 분석, DPI 기반 이상징후 탐지 기술

20.8.18	12

이슈 2 – 의료기기 데이터 셋

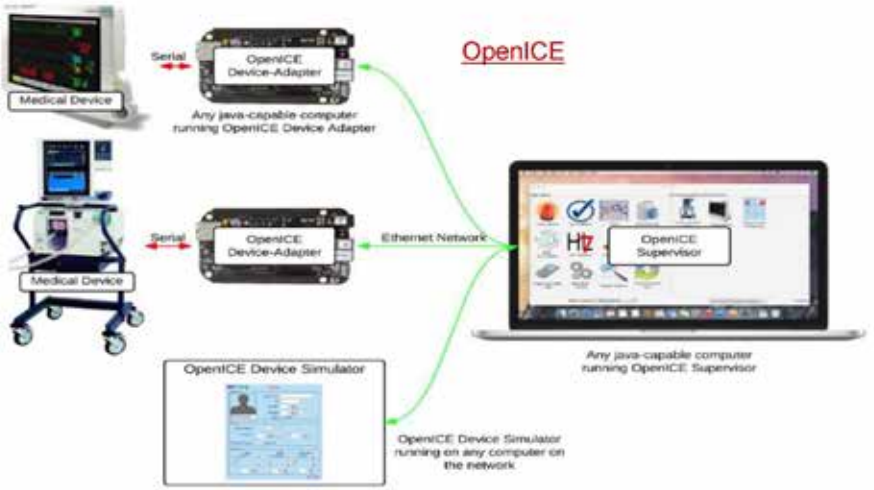
◆ 학습, 분석 용 데이터 확보 이슈

- ➔ 병원 데이터?
- ➔ 정상 데이터, 비정상 데이터?
- ➔ 가상 의료기기, 가상네트워크? (OpenICE)
- ➔ open dataset?
- ➔ 공격 dataset

MALWARE bazaar by ABUSE

数据堂 Datatang

PacketTotal
Simple, free, high-quality PCAP analysis



Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol
2020-07-15 1607723 Z	A Network Trojan was detected	ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray	1	[redacted]	53218	[redacted]	445	TCP
2020-07-15 1607725 Z	A Network Trojan was detected	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	1	[redacted]	445	[redacted]	53218	TCP
2020-07-15 1607726 Z	A Network Trojan was detected	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response	1	[redacted]	445	[redacted]	53218	TCP
2020-07-15 1607737 Z	Attempted Administrator Privilege Gain	ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010	1	[redacted]	53218	[redacted]	445	TCP
2020-07-15 1607740 Z	A Network Trojan was detected	ET EXPLOIT Possible DOUBLEPULSAR Beacon Response	1	[redacted]	445	[redacted]	55221	TCP
2020-07-15 1607743 Z	A Network Trojan was detected	ET EXPLOIT Possible DOUBLEPULSAR Beacon Response	1	[redacted]	445	[redacted]	55571	TCP
2020-07-15 1607743 Z	A Network Trojan was detected	ET EXPLOIT Possible DOUBLEPULSAR Beacon Response	1	[redacted]	445	[redacted]	55572	TCP
2020-07-15 1607743 Z	A Network Trojan was detected	ET EXPLOIT Possible DOUBLEPULSAR Beacon Response	1	[redacted]	445	[redacted]	55572	TCP

20.8.18	13

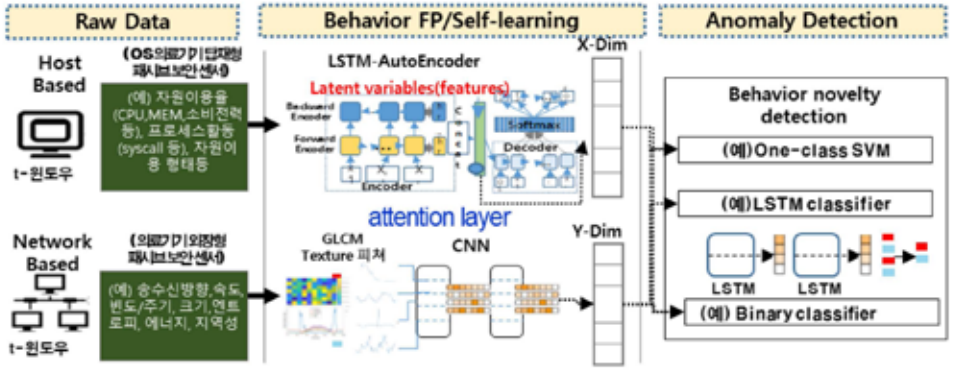
이슈 3 – 학습 모델, FEATURE ENGINEERING

◆ 학습 모델 설계? Feature?

➔ Per packet? Flow?
➔ 1-class classifier? 2-class classifier?
➔ normal? Abnormal?
➔ feature vector?

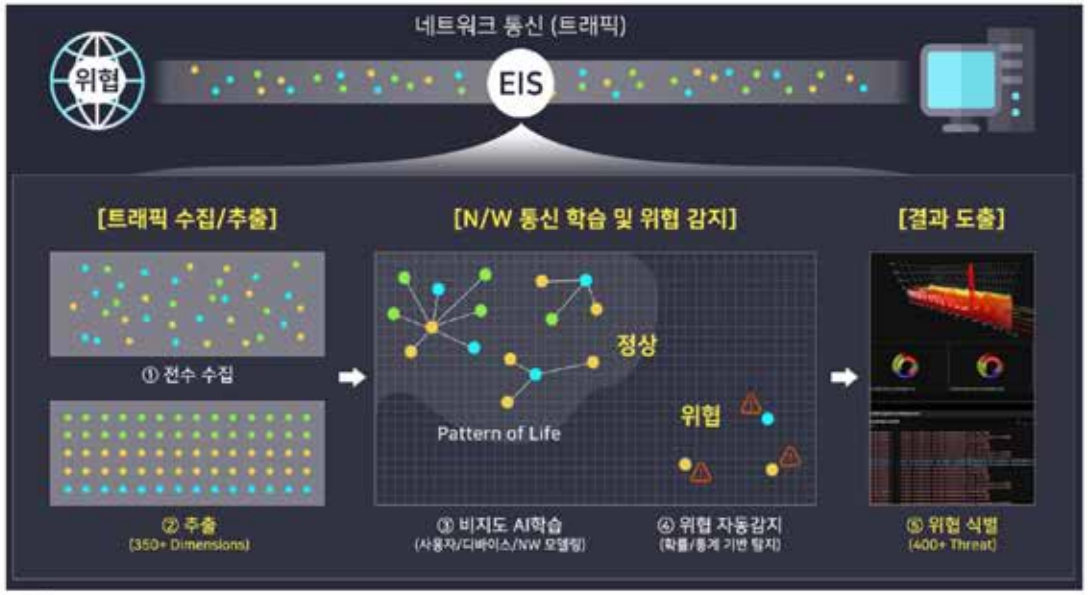
➔ anomaly detection technique
- 1-class Support Vector Machine (OC-SVM)
- Local Outlier Factor (LOF) ….

➔ Probablistic classification techniques
- Neural Network (NN)
- Naïve Bayes (NB)
- Random Forest (RF) ….

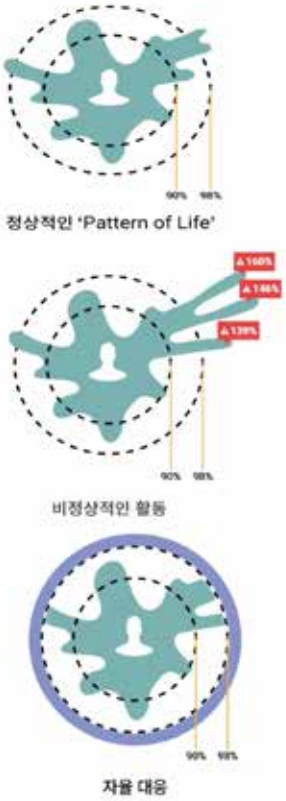


➢ 참고: DARKTRACE Cyber AI 면역 시스템 (Enterprise Immune System)

- 비지도 학습기반 (비지도 * 비지도 * 비지도 * 지도)
- 이상행위 분석 + 딥 패킷 분석



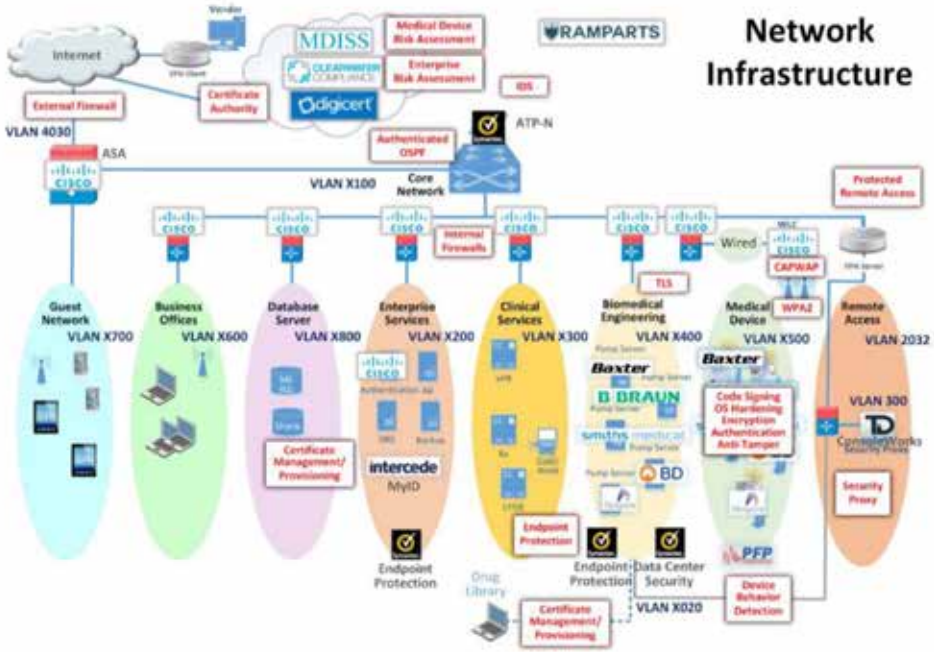
출처: DarkTrace



20.8.18	15

이슈 4 – MEDICAL NETWORK RE-DESIGN, 의료기기 식별

◆ 보안이 고려된 병원네트워크 재설계 이슈



"병원, 로그분석 등 모니터링과 의료기기 보안대책 세워야"

NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps
In Healthcare Delivery Organizations

20.8.18	16

◆ 의료기기 식별/관리 이슈

Cisco 솔루션 – Medical NAC (Network Access Control)

- **Identifying, Classifying, and Segmenting Clinical Healthcare Devices**
- **802.1x, MAC 기반 인증, Radius, Profiling**

Cisco Identity Service Engine

Cisco ISE supports various probes, each capable of capturing different endpoint data. Raw data for a given endpoint is parsed and stored in the ISE internal endpoint database. Relevant endpoint attributes are then analyzed against a library of fingerprinting rules known as Profiler policies.

The Cisco ISE Profiler includes the following probes and context sources for collecting endpoint attributes used to classify medical devices:

- RADIUS
- SNMP
- DHCP
- HTTP
- DNS
- Network scan (Nmap)
- NetFlow
- AnyConnect® Identity Extensions (ACIDEX)
- Device Sensor

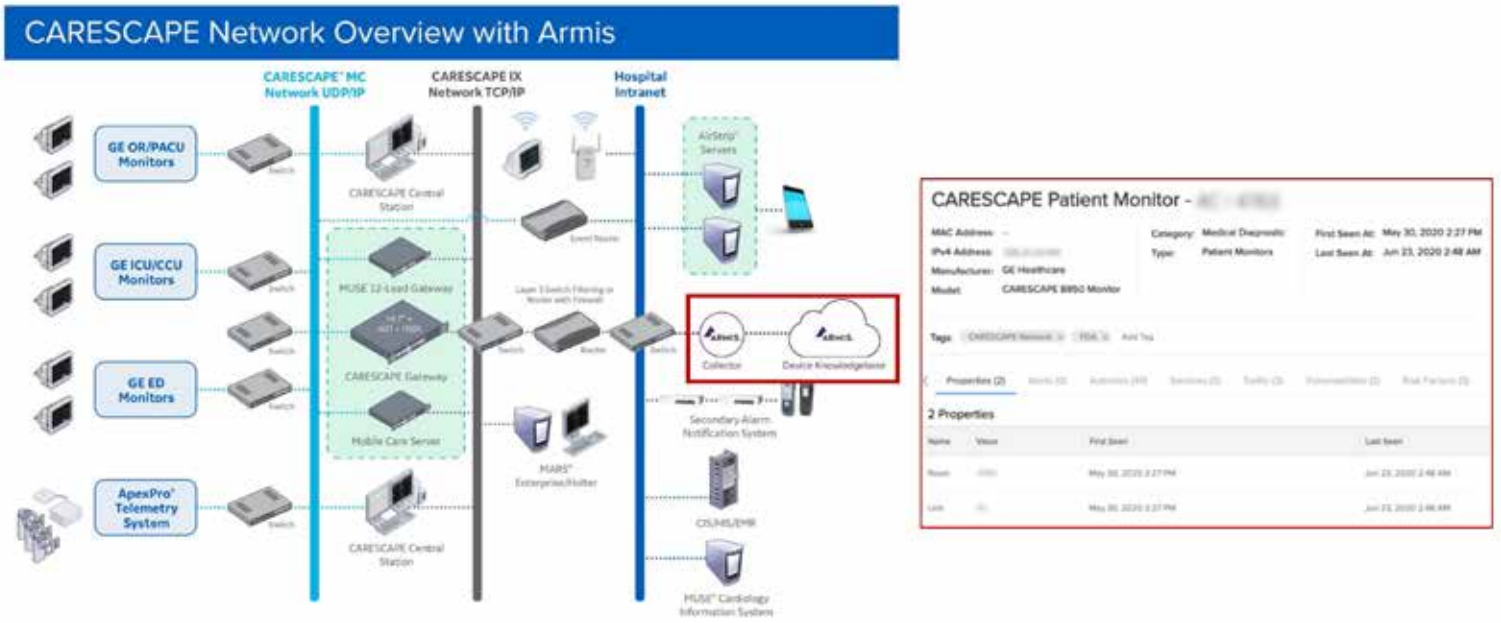
외부 서버 연동

- Cisco ISE internal endpoint database
- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Mobile device management (MDM)
- RADIUS

20.8.18	17

Armis solution

➢ GE Healthcare’ s CARESCAPE Network과 연동, 디바이스 식별, 위치추적, 관리



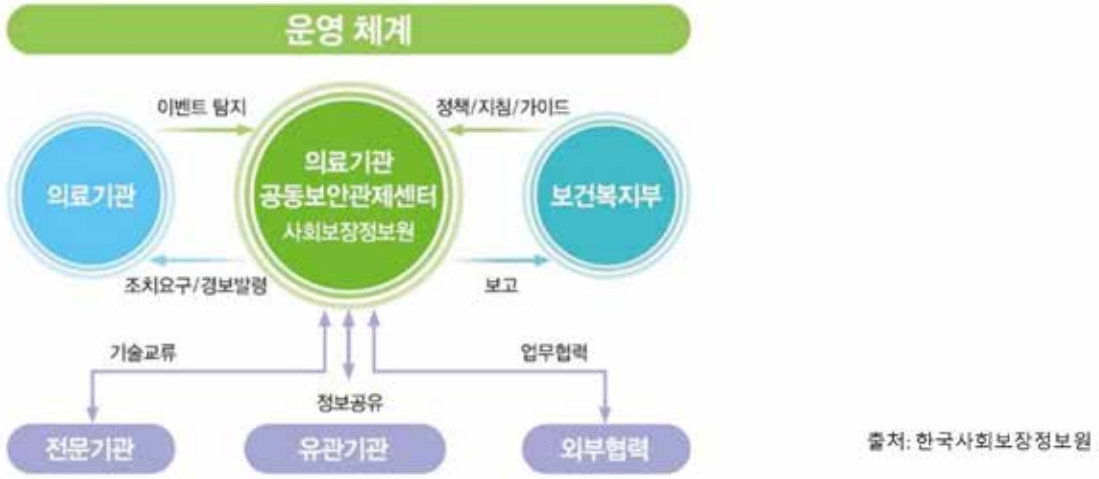
20.8.18	18

참고 – 의료 ISAC (의료기관 공동보안관제센터)

의료ISAC란?

「정보통신기반 보호법」 제16조(정보공유·분석센터)에 의해 설립된 의료분야 정보공유·분석센터의 명칭은 「**의료기관공동보안관제센터**」이며, 영문명은「Healthcare-Information Sharing and Analysis Center」, 약자는 **의료ISAC(H-ISAC)**라 합니다.

일반적으로 ISAC(Information Sharing & Analysis Center)이란, 동종 또는 유사 업무 분야별로 해킹, 악성코드 등 사이버위협에 효과적으로 대응하기 위한 공동 대응체계를 의미함



출처: 한국사회보장정보원

20.8.18	19

IoMT Implantable medical device 보안

20.8.18	20

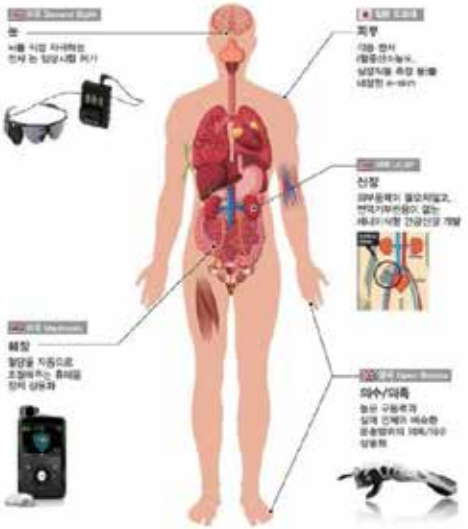
배경

◆ 의료기기 휴먼해킹 이슈 → 체내 이식 의료기기(전자 인공장기) 해킹으로 환자 생명 위협

➢ 보안이슈: (1) 보안 경량화, (2) 에너지 이슈, (3) 인증 및 키관리 이슈

Wireless Medical Implantable Device

Artificial Organs



IoMT device

Abilify MyCite
(센서내장 복용약),
PillCamTM
(캡슐-식도, 위, 소장, 결장 시각화)

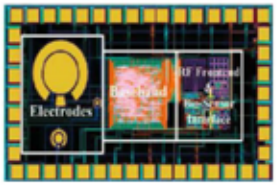
이슈 1 – 보안 경량화

Miniaturization

◆ 바이오센서 수준 제약 충족하는 miniaturized(28nm급), light-weighted 보안 issue

➢ 스트림/블록 사이퍼 암호, AES-OFB, PRESENT, HEGHT, CLEFIA… 경량화 (2,000 NAND gates 면적 ↓), 저전력(uW급) , 전파간섭, 생체의료안전성기준 충족 – 보안 SoC

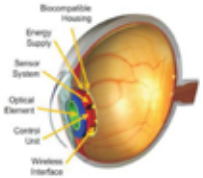
Insulin pump
- HummingBird Stream Cipher



Glucose sensor
(@푸단大, 2011)

S. Guan, Gu, J., Shen, Z., Wang, J., Huang, Y., and Mason, A., "Wireless powered implantable bio-sensor tag system-on-chip for continuous glucose monitoring", in Biomedical Circuits and Systems Conference (BioCAS), 2011 IEEE, 2011.

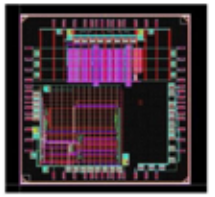
AES OFB stream Cipher mode



Ocular Implant
(@KIT, 카를스루에공대, 독일2011)

Beck, C.; Masny, D.; Geiselmann, W.; Bretthauer, G., Block Cipher Based Security for Severely Resource-constrained Implantable Medical Devices., ISABEL 2011

BiosensorCryptoHW
(TRNG, PUF, Hash, ENC 32nm CMOS)



Implantable Biosonsors
(@메사추세츠대학 , 2014)

http://sharps.org/clusters/telemedicine-cluster/securing-biosensors

20.8.18	22

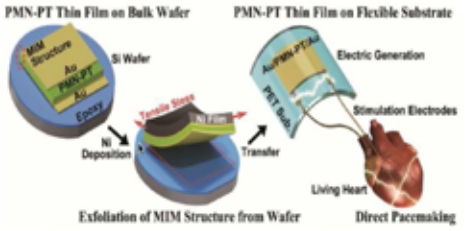
이슈 2 – 에너지 이슈

Energy issue

- 자가 충전 방식으로 인체 내장 배터리-DoS(방전) 공격 대응
- 수십 mW 급의 고소모전력이 요구되는 종래의 암호기술 적용 한계 극복 → 최소소비전력 암호

Energy harvesting

- 압전물질/나노발전기로 작동하는 자가발전 심장박동기 (글로벌프론티어사업, KAIST, 연대병원, 2014)
- 체액(나트륨, 칼륨, 칼슘, 염소 이온 등이 전극에 흡 · 탈착)으로 작동하는 생체이식형 슈퍼커패시터 (세라믹기술원, 인하대, 미래부, 2017)
- 체내 마찰전기를 이용하여 이식형 의료기기 충전기술 (외부 초음파가 체내에 삽입된 특정 소재의 변경을 발생 → 진동으로 유도되는 마찰전기 이용, 성균관대, 2019)



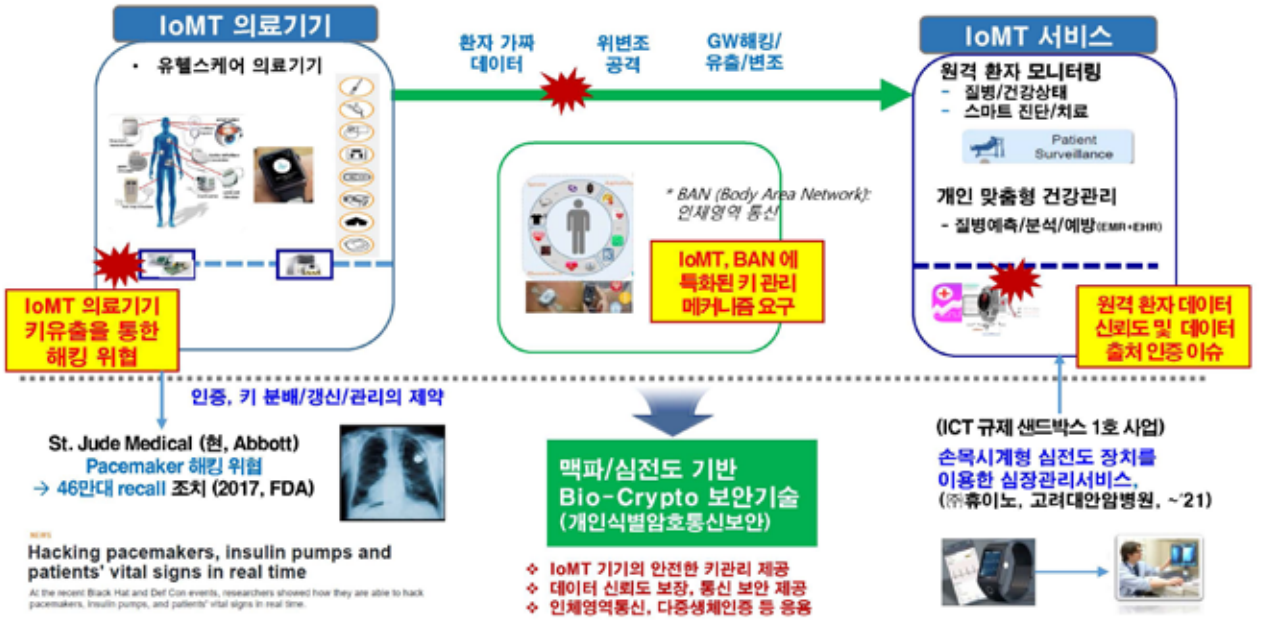
Piezoelectric self-powered pacemaker(2014.6) (KAIST, 연대병원)

Energy source	Classification	Power density
Solar power	Radiant energy	100 mW/cm^3
RF waves	Radiant energy	0.02 μW/cm^2 at 5 km
RF energy	Radiant energy	40 μW/cm^2 at 10 m
Body heat	Thermal energy	60 μW/cm^2 at 5 °C
External heat	Thermal energy	135 μW/cm^2 at 10 °C
Body motion	Mechanical energy	800 μW/cm^3
Blood flow	Mechanical energy	0.93 W at 100 mmHg
Air flow	Mechanical energy	177 μW/cm^3
Vibration	Mechanical ENERGY	4 μW/cm^3
Piezoelectric	Mechanical energy	50 μJ/N

이슈 3 – 인증 및 키관리 이슈

◆ 체내이식형 의료기기, 인공장기, IoMT 키관리 이슈

유헬스케어 의료기기 시스템
의료인이 진단 및 예방관리의 목적으로 활용하기 위해 의료기관 이외의 장소에서 개인의료정보 및 생체정보를 측정·수집하고 의료기관에 전송·저장하여 의사가 진단 가능하게 도와주는 일련의 모든 장치
(* 출처: 스마트의료 사이버보안 가이드, 과기정통부, KISA, 2018)

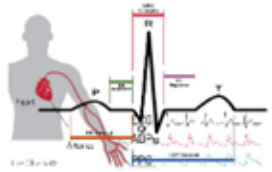


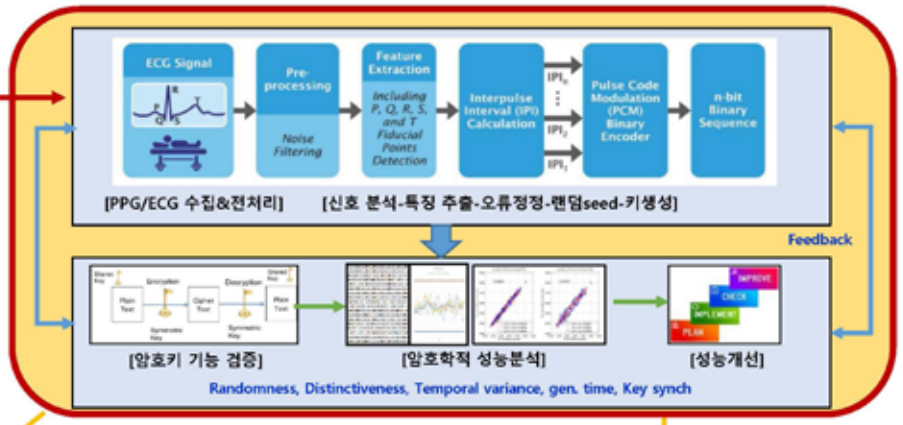
Bio-Crypto 개요

- ECG (Electrocardiogram)
- PPG (photoplethysmography)

◆ **가변적 생체신호로 부터 암호학적 특성 추출**
→ **BAN(Body area network) 보안 통신, 임플란터블 키 설정/업데이트 활용**

◆ **Crypto: (1) 암호학적 키생성 (2) 인증 (2) 인체영역통신보안, 생리신호기반 E2E**





measured ECG

PhysioNet
The Research Resource for Complex Physiologic Signals

PPG/ECG Bio-Crypto Library

end

PPG/ECG 기반
중단간 보안 프로토콜
(키동기화 등)

end

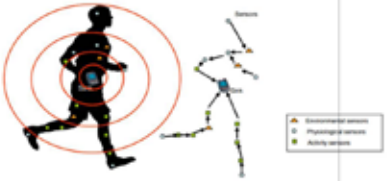
PPG/ECG Bio-Crypto Library

Known ECG

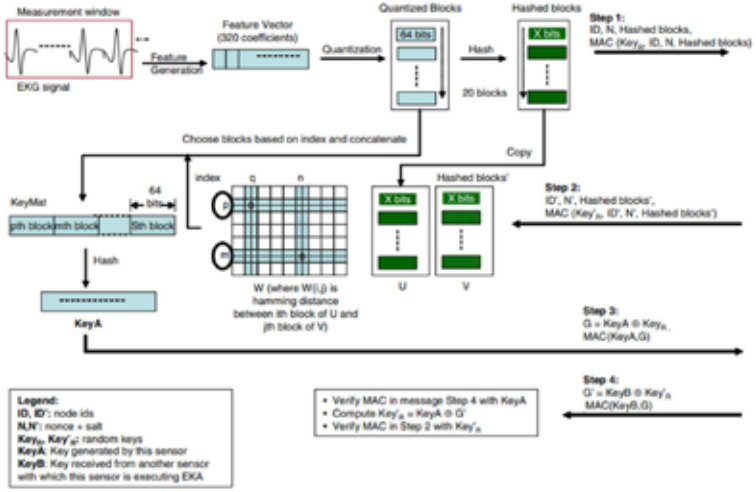
20.8.18	25

Bio-Crypto – Arizona 주립대

- **Arizona State University: EKG 기반의 Key agreement 기술**
  - 심전도 신호로부터 암호학적 키 생성 → 인체영역통신에 적용
  - 암호학적 성능 지표 : Randomness, Distinctiveness, Temporal variance 분석



EKG 기반 feature 생성 과정

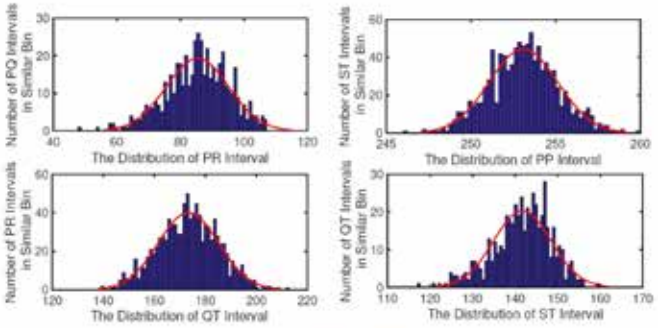


인체영역 통신을 위한 인체내 센서간 Key agreement 과정

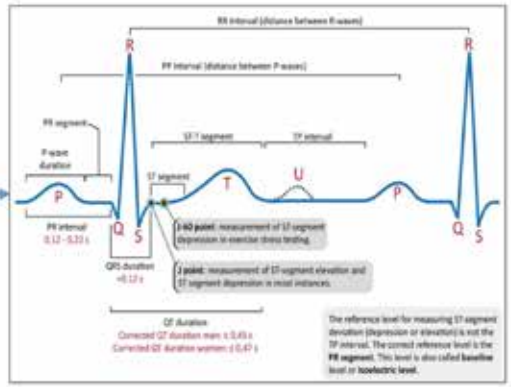
Bio-Crypto – Turfu 대

- **Turku 대: EKG 기반 암호학적 키 생성 기술** (IEEE Access, 2017)
  - 2가지 Feature set 구성 방식 적용
    - (1) Fiducial 방식 : P, Q, R, S, T 변곡점 특성 분석 기반
    - (2) Non-fiducial 방식 : 특정한 point가 아닌 frequency 특성을 분석

ECG 신호 분석 및 n-bit binary sequence 생성 과정



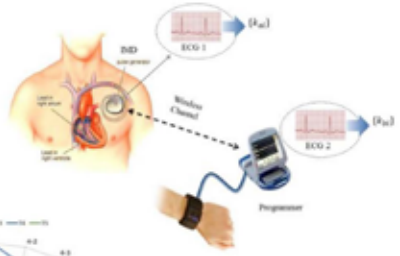
PR, PP, QT 및 ST 구간의 정규 분포



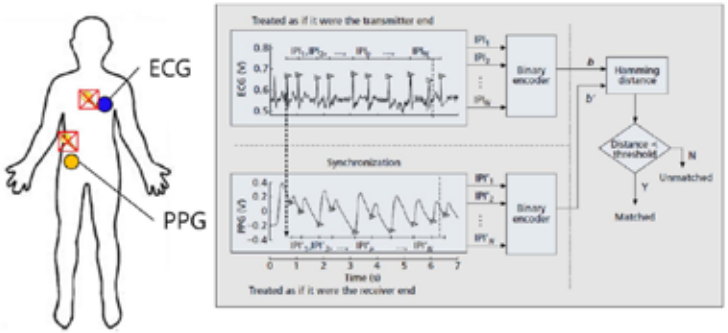
20.8.18	27

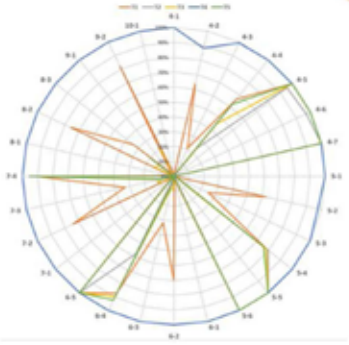
Bio-Crypto – Macquarie 대 등

- **Macquarie 대 (호주) : EKG 기반의 변형 OTP 생성 → 생체기반 암호 적용** (IEEE Access, 2015)
  - ECG 신호로 부터 생성한 random string 을 암호키로 바로 사용



- **Chinese university of Hong Kong : PPG, ECG 기반 인체영역 통신 보안** (IEEE comm. Magazine)
  - 맥파, 심전도의 IPI(inter-Pulse Interval) 분석 기반 인체영역통신 보안 기술





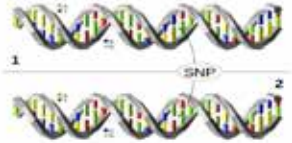
생체 비밀키의 엔트로피 테스트

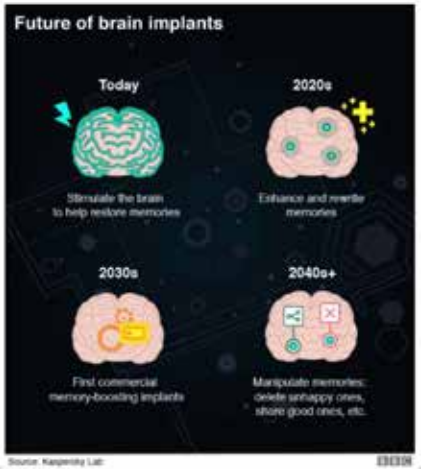
- **ETRI : PPG/ECG IPI 기반 암호학적 Seed 동기기법 연구**

기타 – 미래 IoMT 위협

이슈 1 – 디지털 DNA-유전체 해킹, 프라이버시 침해

이슈 2 – 휴먼 브레인 해킹





20.8.18	29

감사합니다
(Q&A)


ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute