Mobile & Embedded System Lab.

경희대학교 컴퓨터공학과
Mobile & Embedded System Lab.
http://mesl.khu.ac.kr

지도교수: 조 진 성 (chojs@khu.ac.kr)

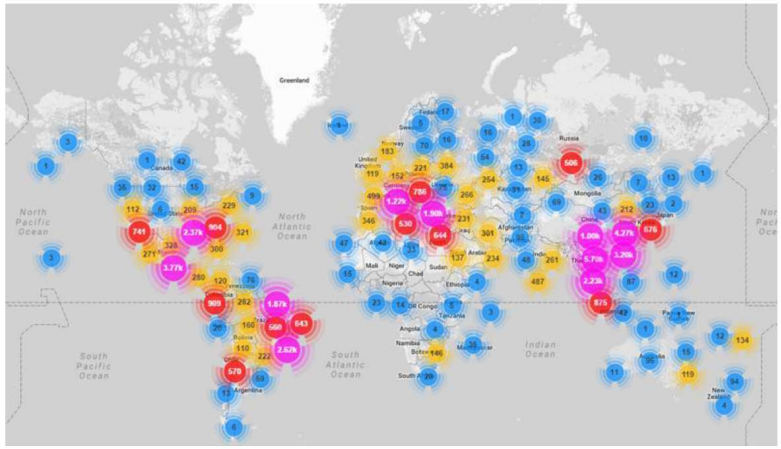
Contents

- IoT 디바이스 보안 취약성
- IoT 디바이스 보안 플랫폼
- IoT 디바이스 보안 플랫폼 응용
- 펌웨어 보안 (Firmware security)
- 드론 보안 (Drone security)
- 자동차 보안 (Automotive security)

IoT 디바이스 보안 취약성

IoT 보안 위협 사례

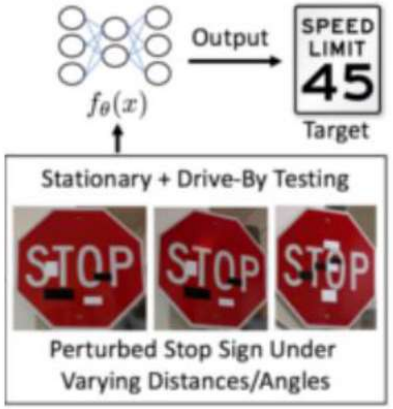
Mirai Botnet (2016)



[https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html]

Sensor Hacking (2016)

[https://youtu.be/IBDS4mD_WRE]



[Robust Physical-World Attacks on Deep Learning Models: https://arxiv.org/pdf/1707.08945.pdf]

Adversarial ML (2017)

[https://youtu.be/mxHWATXu3K0]

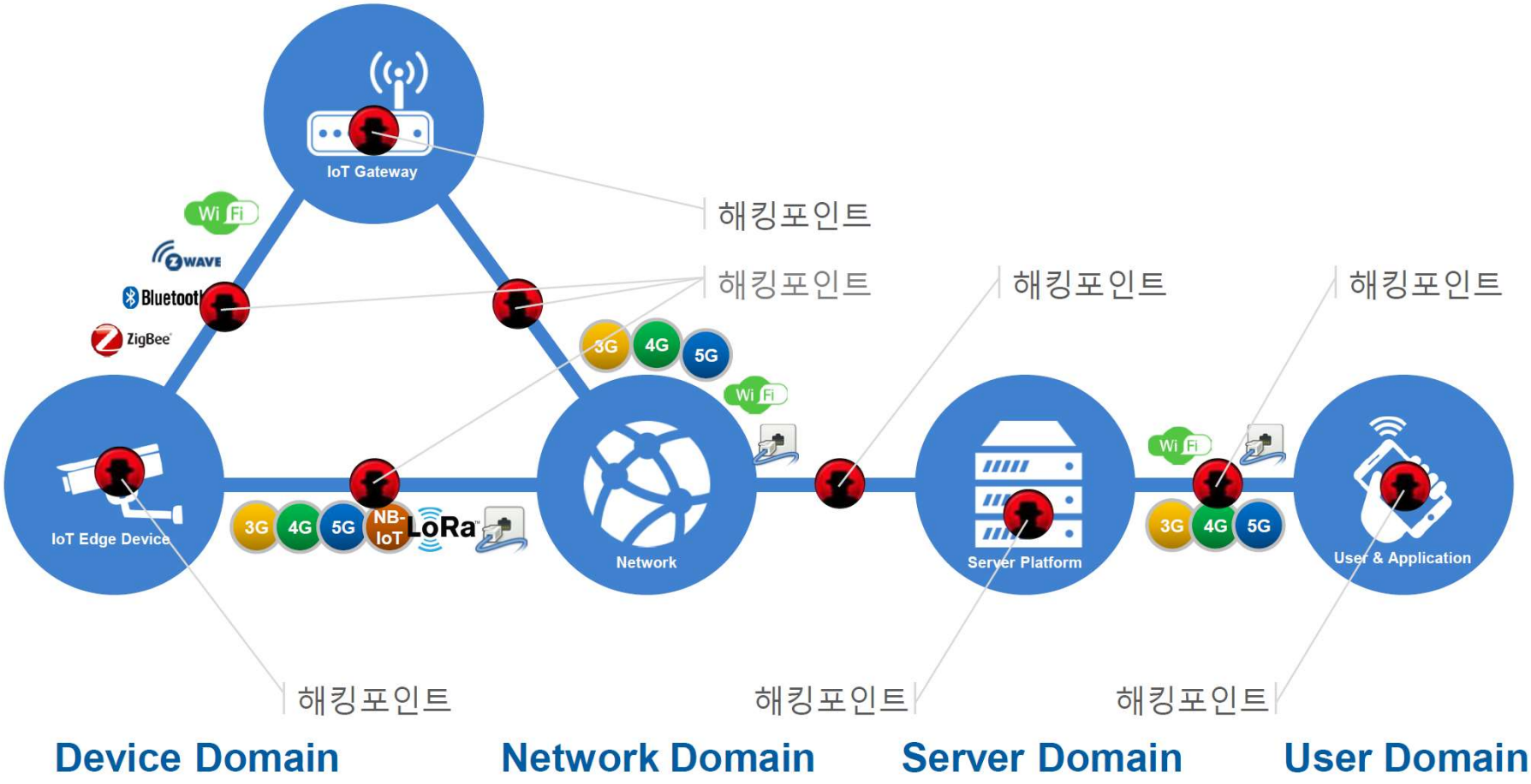
Drone Hacking (2015)

[https://youtu.be/c1XyhReNcHY]

Tesla Hacking (2017)

SAMSUNG Research
이충훈, KRnet 2018

IoT 보안 취약 지점

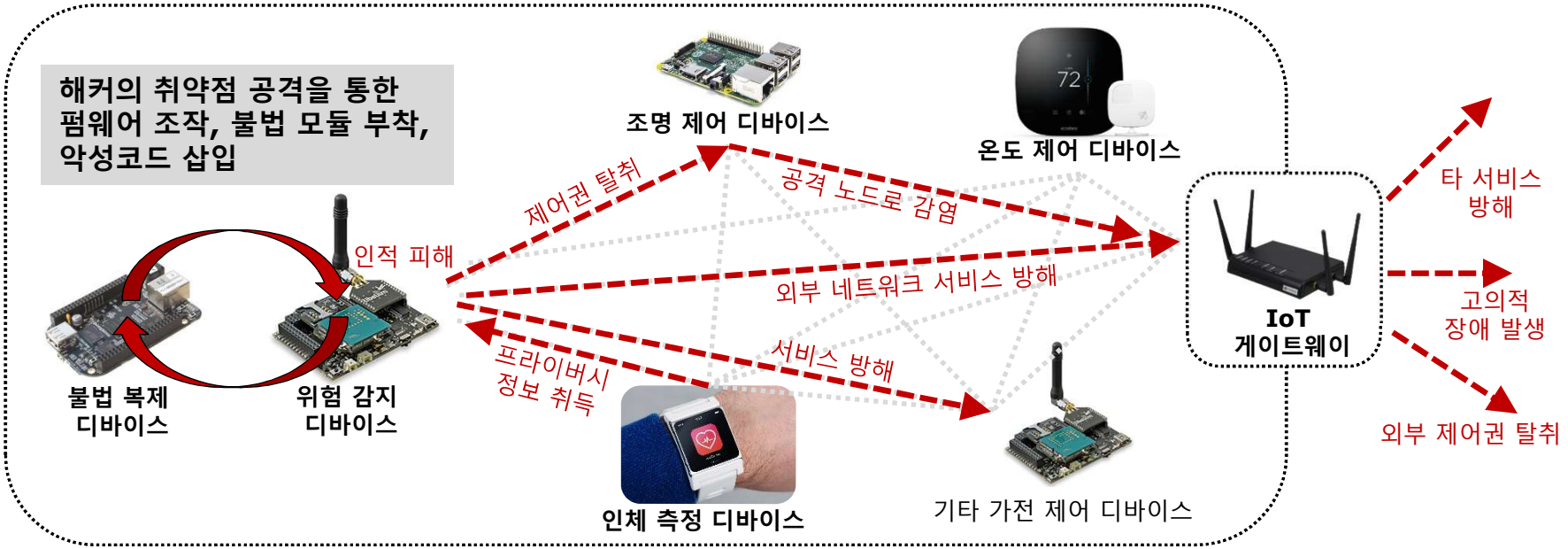


INITECH 이주화, KRnet 2017

IoT 디바이스 보안의 취약성

❖ IoT 보안 위협의 증가

- 경제적, 산업적, 또는 인명적 피해 유발
- 심각한 프라이버시 침해 야기



❖ Internet of Broken Things

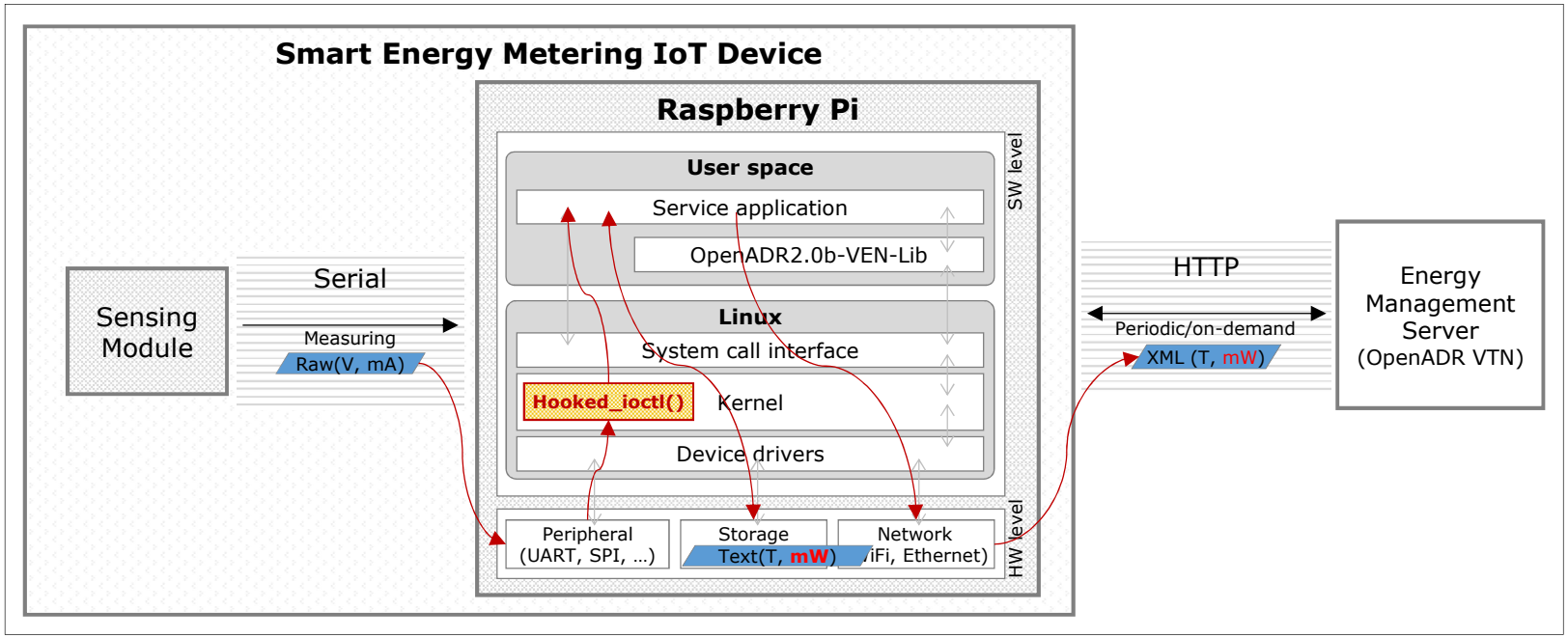
- Open source H/W 및 S/W 활용 가능성 증대
- 플랫폼/서비스의 상호 운용 증대

→ **많은 요소 기술들의 통합으로 보안 취약성이 높음**

IoT 디바이스 보안의 취약성

❖ 오픈소스 HW 고사양 IoT 디바이스 모의 해킹 (1)

- Raspberry Pi 기반 Smart Energy Meter 모의 해킹
  - 해킹된 smart metering 디바이스의 동작

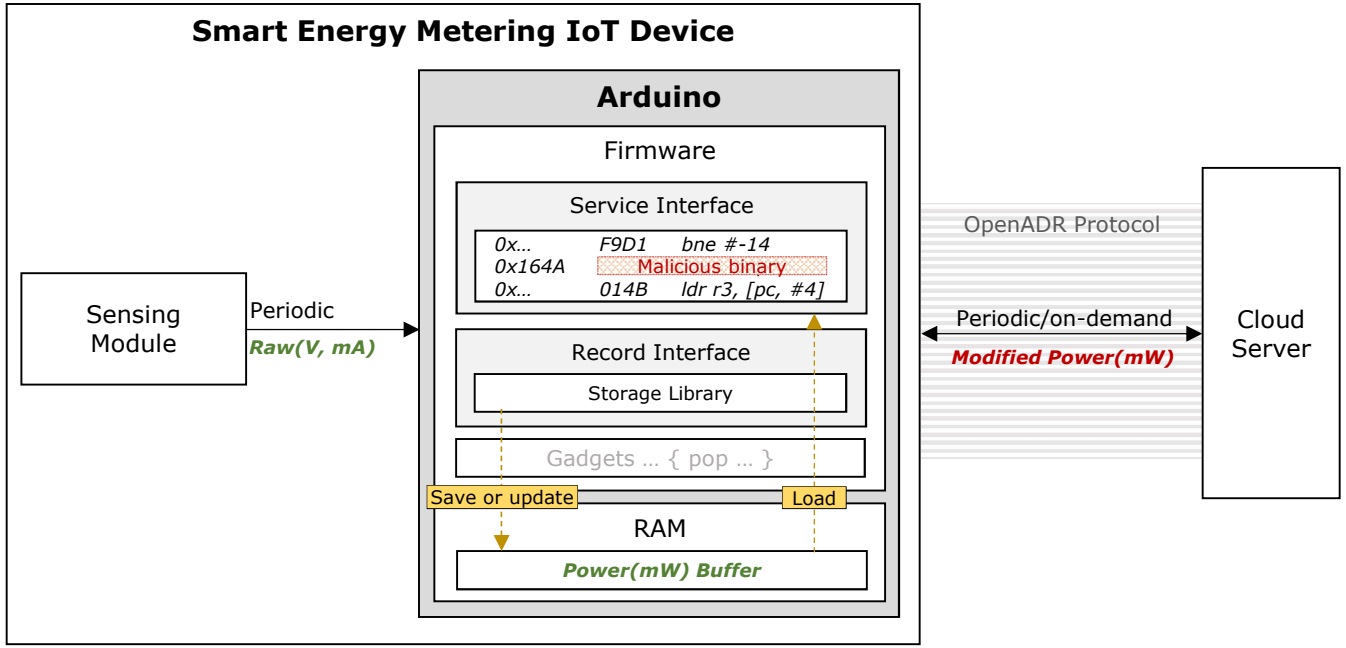


- 동영상 데모 (https://youtu.be/zmzIUV2CsLA)

IoT 디바이스 보안의 취약성

❖ 오픈소스 HW 저사양 IoT 디바이스 모의 해킹 (2)

- Arduino 기반 Smart Energy Meter 모의 해킹
  - 해킹된 smart metering 디바이스의 동작
    - 기존 대비 80% 감소된 평균 전력 소모량을 서버에 전송
    - 디바이스 Reset에도 변조된 펌웨어 바이너리는 지속적으로 존재



- 동영상 데모 (https://youtu.be/egZ9bOUYUcc)

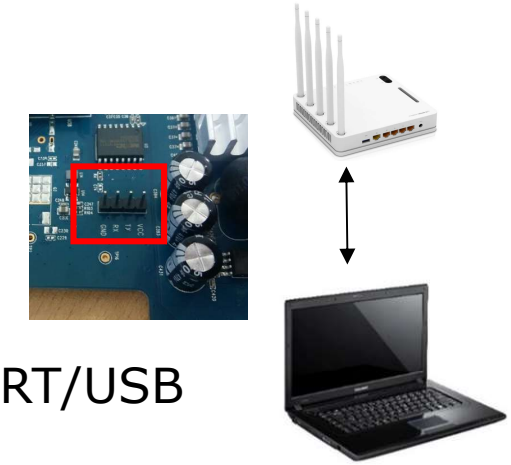
IoT 디바이스 취약점 분석 및 모의 해킹

❖ 상용 IoT 디바이스 취약점 분석 및 모의 해킹

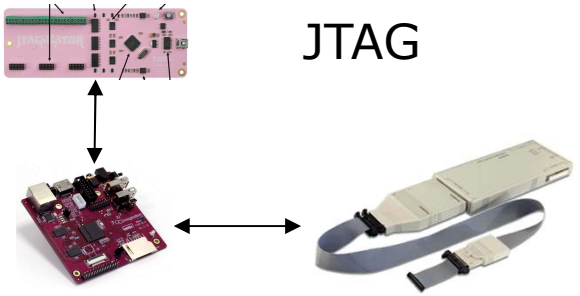
- 펌웨어 추출
- 펌웨어 정적 분석
- 펌웨어 동적 분석

IoT 디바이스 취약점 분석 및 모의 해킹

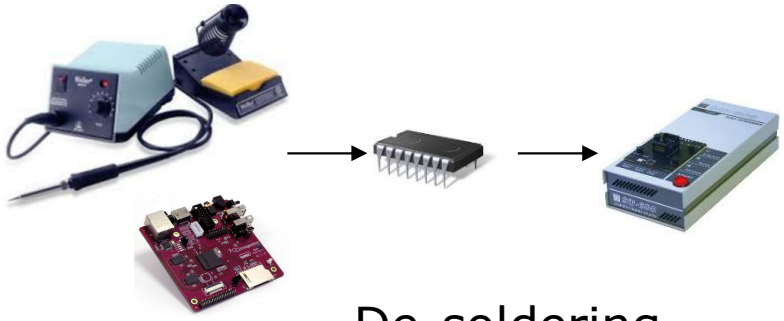
❖ IoT 디바이스 펌웨어 추출



UART/USB



JTAG

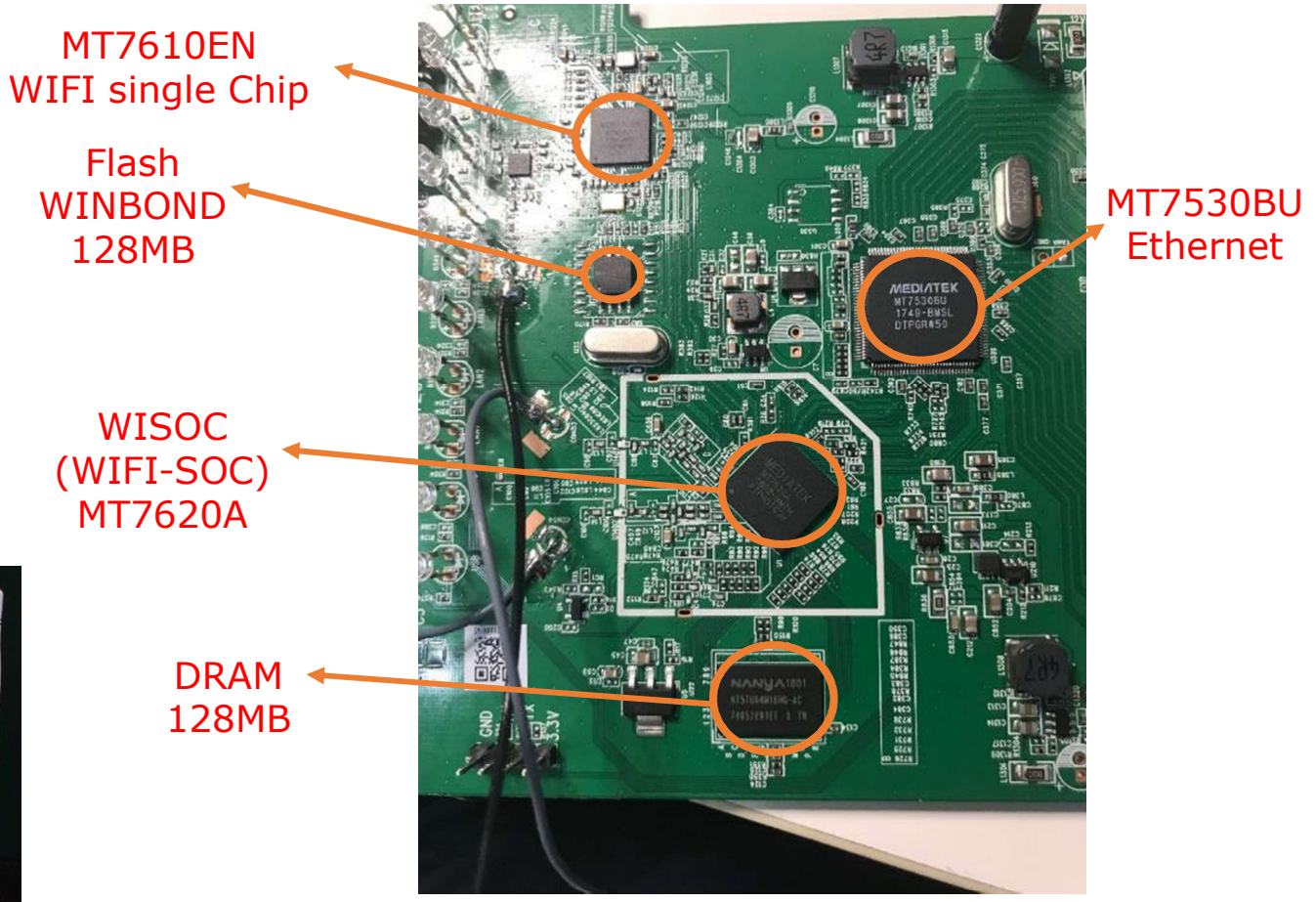


De-soldering

FW update file

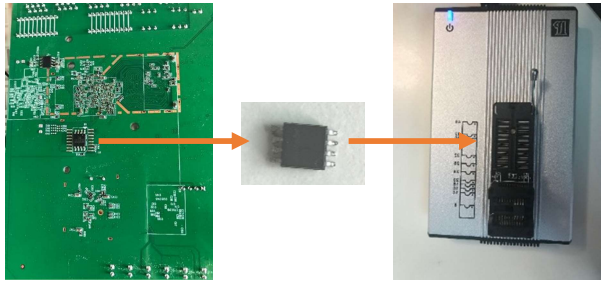
상용 IoT 디바이스 모의 해킹

- **ipTIME A1004ns**
  - MIPS

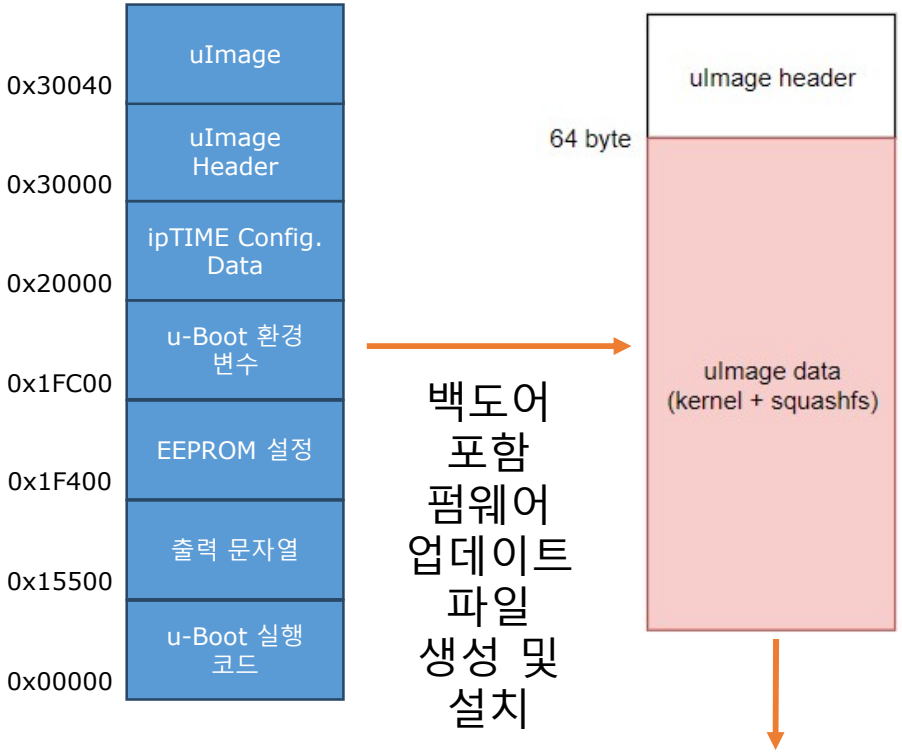


상용 IoT 디바이스 모의 해킹

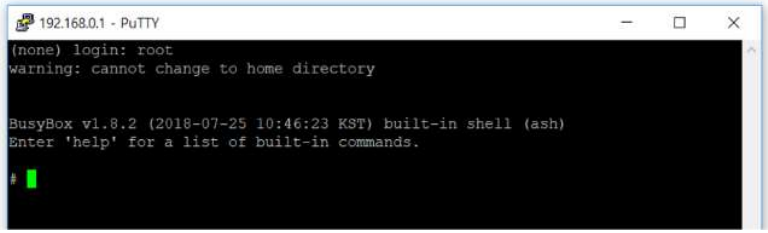
- **ipTIME A1004ns**
  - MIPS

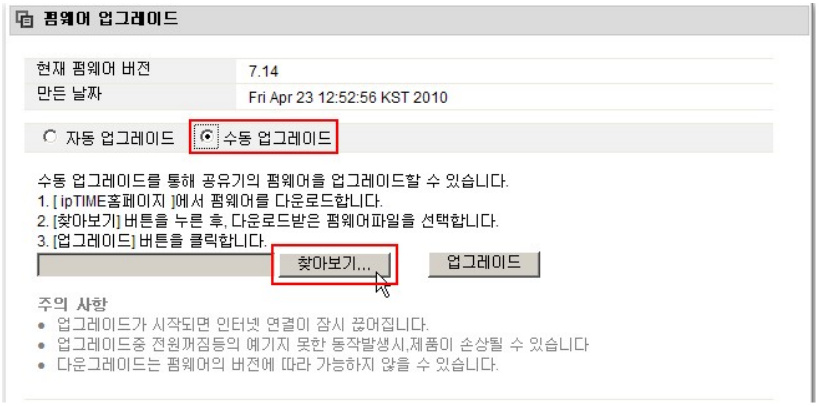


펌웨어 추출 및 분석



Root shell 획득





상용 IoT 디바이스 분석

❖ **22종 42개 상용 IoT 디바이스 분석**

Made In Wordcloud.kr

분석 대상 상용 IoT 디바이스

대분류	디바이스
IP 공유기	ASUS GT-A5300
	ipTime A1004ns
	LINKSYS WRT1900AC
	Netgear R6220
IP 카메라	EasyN ES100V
	FOSCAM
	Xiaomi Xiaofang
NAS	Synology DS218J
TV 셋톱박스	Xiaomi Mi Box S
로봇청소기	LG VR6341LVM
	Xiaomi Mi Roborock
스마트 TV	LG 47LM6690
	Samsung UN55NU8000FXKR
게임기	Nintendo Switch

대분류	디바이스
게임기	Sony PS4
	XBOX 360
공기청정기	브런트 에어젯S
도어락	Gateman 댄디s
드론	DJI Tello
	SYMA X5C-1
	SYMA X8W
블라인드 엔진	브런트 BEAKR1601
블랙박스	INAVI QXD1500MINI
	IROAD T8
	FINEDRIVE Solid 500
네비게이션	INAVI ST100
	SK LB-UH6CB
스마트 스위치	SK BDS301W

대분류	디바이스
센서	Xiaomi 미세먼지 측정기
	Xiaomi 온습도계
AI 스피커	SK 누구
	Xiaomi AI 스피커
	Amazon 에코닷 2세대
	Kakao MINI C
웨어러블 디바이스	Google 글라스
스마트폰	Samsung Galaxy S9+
프린터	EPSON M1120
	HP Oficejet 8600 Plus
	Samsung SL-C1454N
플러그	다원 PM-B540-W
게이트웨이	Broadlink RM-MINI3
	Xiaomi 미지아

상용 IoT 디바이스 분석

❖ **23개 상용 IoT 디바이스 펌웨어 추출**

HW 구조 및 운영체제 분석

대분류	CPU spec	메인메모리	플래시메모리	OS
AI 스피커	상	512MB	256MB	Android
NAS	상	512MB	16MB	Linux
TV 셋톱박스	상	8GB	2GB	Linux
게임기	상	8GB	HDD:500GB	Windows/FreeBSD
스마트폰	상	6GB	64GB	Android
스마트 TV	상	-	-	Linux
네비게이션	중	128MB	16GB	Windows
블랙박스	중	4GB	16GB	Linux/RTOS
빔 프로젝터	중	2GB	32MB	Linux
웨어러블 디바이스	중	512MB	16GB	Android
IP 공유기	중	128MB	128MB	Linux
IP 카메라	중	256MB	16MB	Linux
로봇청소기	중	1GB	2GB	Linux/Baremetal
프린터	중	128MB	16MB	Linux
게이트웨이	하	32KB	16MB	Baremetal
공기청정기	하	2MB	32KB	Baremetal
도어락	하	16KB	128KB	Baremetal
드론	하	4KB	32KB	Baremetal
블라인드엔진	하	20KB	2MB	Baremetal
센서	하	32KB	2MB	Baremetal
스마트스위치	하	50KB	2MB	Baremetal
플러그	하	50KB	4MB	Baremetal

펌웨어 업데이트 방법 비교 분석

대분류	디바이스	Update
IP 공유기	ASUS GT-A5300	O
	ipTime A1004ns	O
	LINKSYS WRT1900AC	O
	Netgear R6220	O
IP 카메라	EasyN ES100V	O
	FOSCAM	O
	Xiaomi Xiaofang	O
NAS	Synology DS218J	O
TV 셋톱박스	Xiaomi Mi Box S	O
로봇청소기	LG VR6341LVM	O
	Xiaomi Mi Roborock	O
스마트 TV	LG 47LM6690	O
	Samsung UN55NU8000FXKR	O
게임기	Nintendo Switch	O

대분류	디바이스	Update
게임기	Sony PS4	O
	XBOX 360	O
공기청정기	브런트 에어젯S	O
도어락	Gateman 댄디s	X
드론	DJI Tello	O
	SYMA X5C-1	O
	SYMA X8W	X
블라인드 엔진	브런트 BEAKR1601	O
블랙박스	INAVI QXD1500MINI	O
	IROAD T8	O
	FINEDRIVE Solid 500	O
네비게이션	INAVI ST100	O
	SK LB-UH6CB	O
스마트 스위치	SK BDS301W	X

대분류	디바이스	Update
센서	Xiaomi 미세먼지 측정기	X
	Xiaomi 온습도계	X
AI 스피커	SK 누구	O
	Xiaomi AI 스피커	O
	Amazon 에코닷 2세대	O
	Kakao MINI C	O
웨어러블 디바이스	Google 글라스	O
스마트폰	Samsung Galaxy S9+	O
프린터	EPSON M1120	O
	HP Oficejet 8600 Plus	O
	Samsung SL-C1454N	O
플러그	다원 PM-B540-W	O
게이트웨이	Broadlink RM-MINI3	O
	Xiaomi 미지아	O

펌웨어 업데이트 방법 및 파일 분석

대분류	디바이스	업데이트 방법	공식 업데이트 파일	Packing	Unpacking
IP 카메라	FOSCAM	수동	O	O	O
로봇청소기	LG VR6341LVM	자동, 수동	O	O	O
스마트 TV	LG 47LM6690	자동, 수동	O	O	O
블랙박스	FINEDRIVE Solid 500	수동	O	O	O
	INAVI QXD1500MINI	수동	O	O	△
네비게이션	INAVI ST100	수동	O	O	O
게임기	Sony PS4	자동, 수동	O	O	X
	XBOX 360	자동, 수동	O	O	X
스마트 TV	Samsung UN55NU8000FXKR	자동, 수동	O	O	X
프린터	Samsung SL-C1454N	수동	O	O	X
IP 공유기	ASUS GT-A5300	자동, 수동	O	X	-
	ipTime A1004ns	자동, 수동	O	X	-
	LINKSYS_WRT1900AC	자동, 수동	O	X	-
	Netgear_R6220	자동, 수동	O	X	-
IP 카메라	EasyN ES100V	수동	O	X	-
NAS	Synology DS218J	자동, 수동	O	X	-
블랙박스	IROAD T8	자동, 수동	O	X	-
웨어러블 디바이스	Google 글라스	자동, 수동	O	X	-
스마트폰	Samsung Galaxy S9+	자동	X	O	O
드론	DJI Tello	자동	X	X	O

펌웨어 추출

대분류	디바이스	Desoldering	Firmware 추출
AI 스피커	Kakao MINI C	O	X
IP 공유기	ipTime A1004ns	O	O
IP 카메라	EasyN ES100V	O	O
	FOSCAM	O	O
	Xiaomi Xiaofang	O	O
NAS	Synology DS218J	O	O
TV 셋톱박스	Xiaomi Mi Box S	O	X
게이트웨이	Xiaomi 미지아	O	O
	Broadlink RM-MINI3	O	O
공기청정기	브런트 에어젯S	O	O
도어락	Gateman 댄디s	O	X
드론	DJI Tello	O	O
	SYMA X8W	X	X
로봇청소기	LG VR6341LVM	O	X
	Xiaomi Mi Roborock	X	X
블라인드 엔진	브런트 BEAKR1601	O	O
블랙박스	INAVI QXD1500MINI	O	X
빔 프로젝터	SK LB-UH6CB	O	O
센서	Xiaomi 미세먼지 측정기	O	O
	Xiaomi 온습도계	X	X
스마트 스위치	SK BDS301W	O	O
프린터	EPSON M1120	O	O
플러그	다원 PM-B540-W	O	X

HSM 사용 여부

대분류	디바이스	HSM
IP 공유기	ASUS GT-A5300	X
	ipTime A1004ns	X
	LINKSYS WRT1900AC	X
	Netgear R6220	X
IP 카메라	EasyN ES100V	X
	FOSCAM	X
	Xiaomi Xiaofang	X
NAS	Synology DS218J	X
TV 셋톱박스	Xiaomi Mi Box S	X
로봇청소기	LG VR6341LVM	X
	Xiaomi Mi Roborock	X
스마트 TV	LG 47LM6690	O
	Samsung UN55NU8000FXKR	O
게임기	Nintendo Switch	X

대분류	디바이스	HSM
게임기	Sony PS4	X
	XBOX 360	X
공기청정기	브런트 에어젯S	X
도어락	Gateman 댄디s	X
드론	DJI Tello	X
	SYMA X5C-1	X
	SYMA X8W	X
블라인드 엔진	브런트 BEAKR1601	X
블랙박스	INAVI QXD1500MINI	X
	IROAD T8	X
네비게이션	INAVI ST100	X
	FINEDRIVE Solid 500	X
	SK LB-UH6CB	X
스마트 스위치	SK BDS301W	X

대분류	디바이스	HSM
센서	Xiaomi 미세먼지 측정기	X
	Xiaomi 온습도계	X
AI 스피커	SK 누구	X
	Xiaomi AI 스피커	X
	Amazon 에코닷 2세대	X
	Kakao MINI C	X
웨어러블 디바이스	Google 글라스	X
스마트폰	Samsung Galaxy S9+	O
프린터	EPSON M1120	X
	HP Oficejet 8600 Plus	X
	Samsung SL-C1454N	X
플러그	다원 PM-B540-W	X
게이트웨이	Broadlink RM-MINI3	X
	Xiaomi 미지아	X

보안성 분석

대분류	디비아스	Unexposed update file	Packed file	SoC	HSM	보안성 평가
AI 스피커	SK 누구	O	X	X	X	★
	Xiaomi AI 스피커	O	X	X	X	★
	Amazon 에코닷 2세대	O	X	X	X	★
	Kakao MINI C	O	X	X	X	★
IP 공유기	ASUS GT-A5300	X	X	X	X	
	ipTime A1004ns	X	X	X	X	
	LINKSYS_WRT1900AC	X	X	X	X	
	Netgear_R6220	X	X	X	X	
IP 카메라	EasyN ES100V	X	X	X	X	
	FOSCAM	X	O	X	X	★
	Xiaomi Xiaofang	O	X	X	X	★
NAS	Synology DS218J	X	X	X	X	
TV 셋톱박스	Xiaomi Mi Box S	O	X	X	X	★
게이트웨이	Broadlink RM-MINI3	O	X	X	X	★
	Xiaomi 미지아	O	X	X	X	★
게임기	Nintendo Switch	O	X	X	X	★
	Sony PS4	X	O	X	X	★
	XBOX 360	X	O	X	X	★
공기청정기	브런트 에어젯S	O	X	X	X	★
네비게이션	INAVI ST100	X	O	X	X	★
도어락	Gateman 댄디s	O	X	X	X	★
드론	DJI Tello	O	X	X	X	★
	SYMA X5C-1	O	X	X	X	★
	SYMA X8W	O	X	X	X	★
로봇청소기	LG VR6341LVM	X	O	O	X	★★
	Xiaomi Mi Roborock	O	X	X	X	★
블라인드 엔진	브런트 BEAKR1601	O	X	X	X	★
블랙박스	FINEDRIVE Solid 500	X	O	X	X	★
	INAVI QXD1500MINI	X	O	X	X	★
	IROAD T8	X	O	X	X	★
빔프로젝터	SK LB-UH6CB	O	X	X	X	★
센서	Xiaomi 미세먼지 측정기	O	X	X	X	★
	Xiaomi 온습도계	O	X	X	X	★
스마트 TV	LG 47LM6690	X	O	X	O	★★
	Samsung UN55NU8000FXKR	X	O	X	O	★★
스마트 스위치	SK BDS301W	O	X	O	X	★★
스마트폰	Samsung Galaxy S9+	O	O	X	O	★★★
웨어러블 디바이스	Google 글라스	X	X	X	X	
프린터	EPSON M1120	X	O	X	X	★
	HP Oficejet 8600 Plus	O	X	X	X	★
	Samsung SL-C1454N	O	O	X	X	★★
플러그	다원 PM-B540-W	O	X	X	X	★

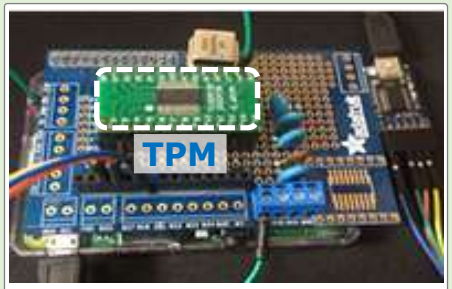
IoT 디바이스 보안 플랫폼의 필요성

IoT Service Application	IoT Service Application
Insecure HW & SW Platform	Secure HW & SW Platform

IoT 디바이스 보안 플랫폼

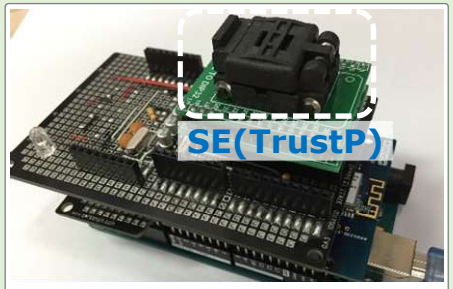
IoT 디바이스 보안 플랫폼 (MESL@KHU)

Secure Platforms for IoT Devices



Secure Pi
(Secure Raspberry Pi)

TPM



SArduino
(Secure Arduino)

SE

iS4IoT
(integrated Security for IoT device)

Security SoC

KHU-TEE
(ARM PSA TrustZone-m)

TEE

IoT 디바이스 보안 요소기술

SECURE
플랫폼

Insecure COTS IoT 디바이스 플랫폼

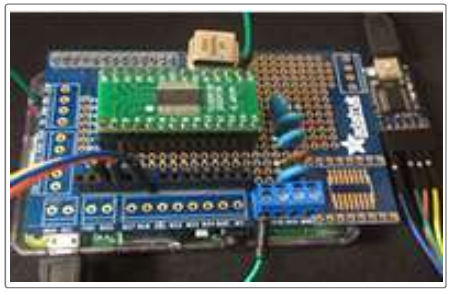
- **Secure Key Storage & Management**
- **Secure Boot**
- **Secure Firmware Update**
- **Remote Attestation**
- **Secure Communication**
- **Mandatory Access Control (MAC)**
- **File(system) Integrity**
- **File(system) Encryption**

Secure Pi: Secure Raspberry Pi

- **Linux 기반 고사양 COTS IoT 디바이스 신뢰 플랫폼**
  - Raspberry Pi + TPM
    - Secure Key Storage & Management
    - Secure Boot
    - Secure Firmware Update
    - Remote Attestation
    - Secure Communication
    - Mandatory Access Control (MAC)
    - File(system) Integrity
    - File(system) Encryption

Insecure Raspberry Pi

+

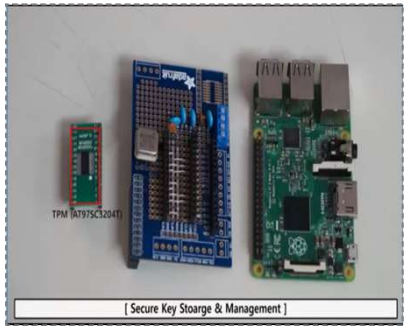


TPM

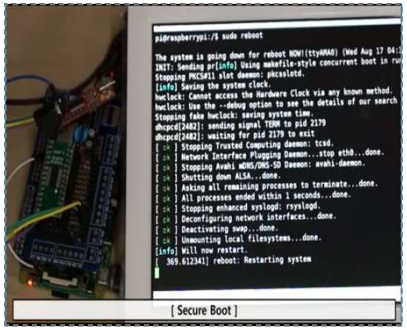
SECURE
플랫폼
(Secure Pi)

Secure Pi: Secure Raspberry Pi (계속)

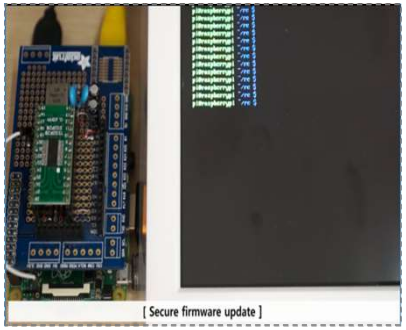
- **Linux 기반 고사양 COTS IoT 디바이스 신뢰 플랫폼**
  - 동영상 데모 (https://youtu.be/jgB5OKd6EME)



< Secure Key Storage & Management >

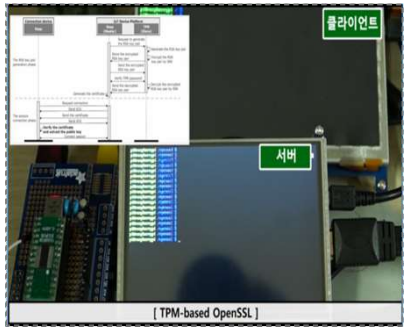


< Secure Boot >

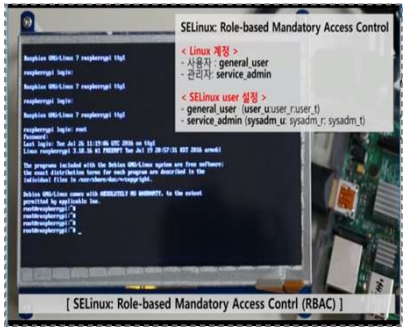


< Secure Firmware Update >

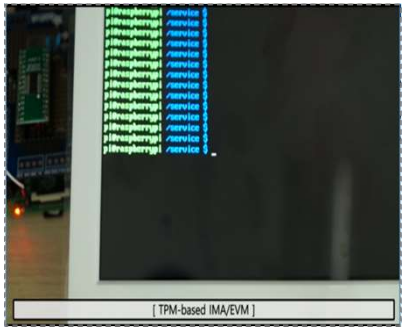
< Remote Attestation >



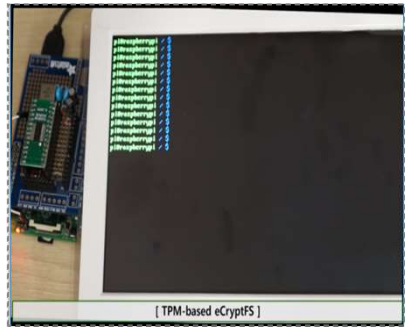
< Secure Communication >



< Mandatory Access Control >



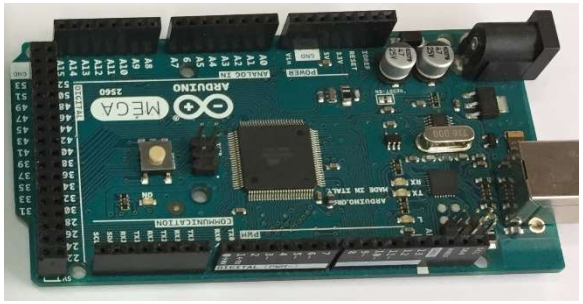
< File(system) Integrity >



< File(system) Encryption >

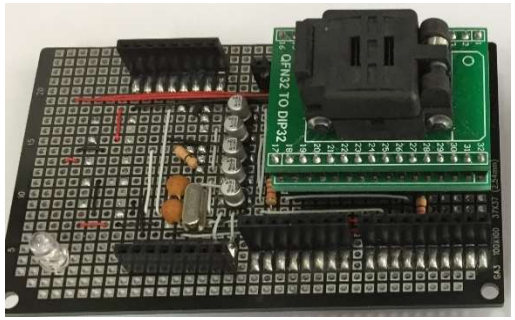
SArduino: Secure Arduino

- **RTOS/Firmware 기반 저사양 COTS IoT 디바이스 신뢰 플랫폼**
  - Arduino + SE
    - Secure Key Storage & Management
    - Secure Boot
    - Secure Firmware Update
    - Remote Attestation
    - Secure Communication

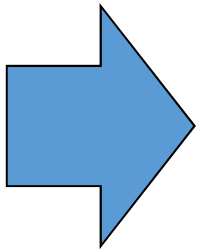


Insecure Arduino

+



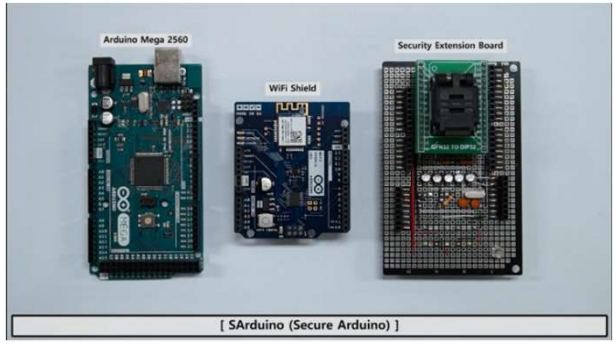
SE



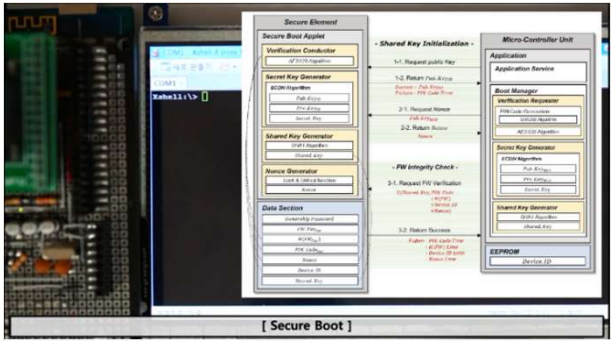
SECURE
플랫폼
(SArduino)

SArduino: Secure Arduino (계속)

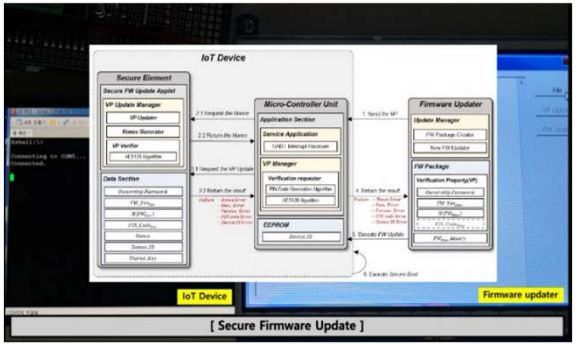
- **RTOS/펌웨어 기반 저사양 COTS IoT 디바이스 신뢰 플랫폼**
  - 동영상 데모 (https://youtu.be/9Tf9SKmWVKg)



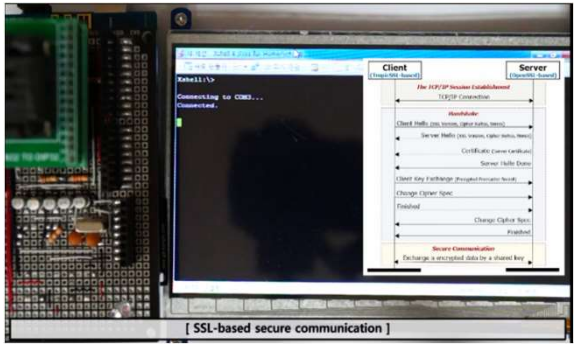
< Secure Key Storage & Management >



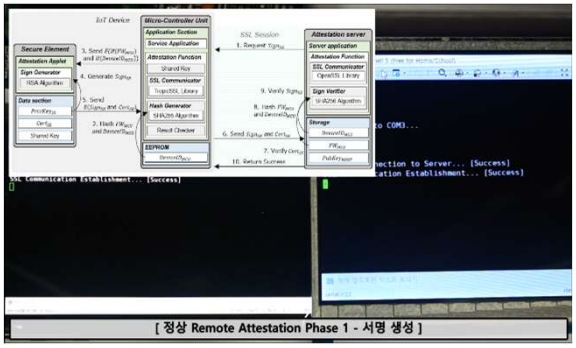
< Secure boot >



< Secure firmware update >



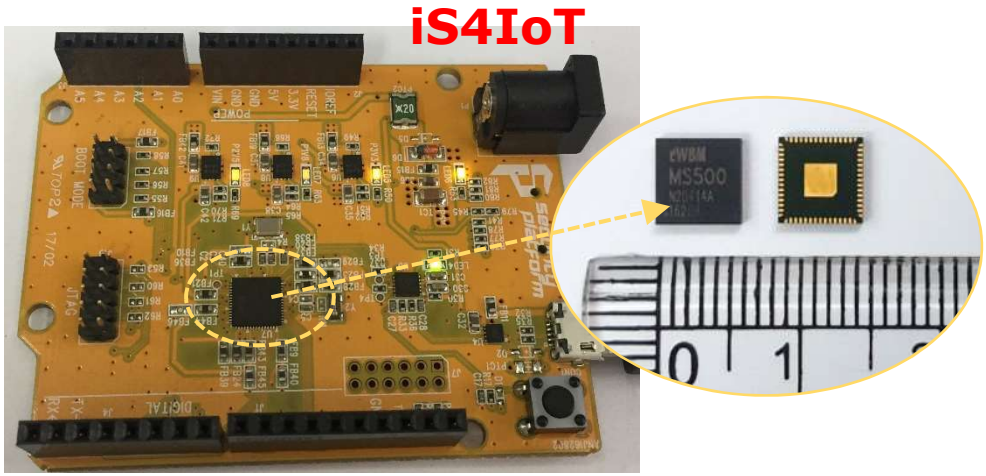
< Secure communication >



< Remote Attestation >

iS4IoT: integrated Security for IoT Device

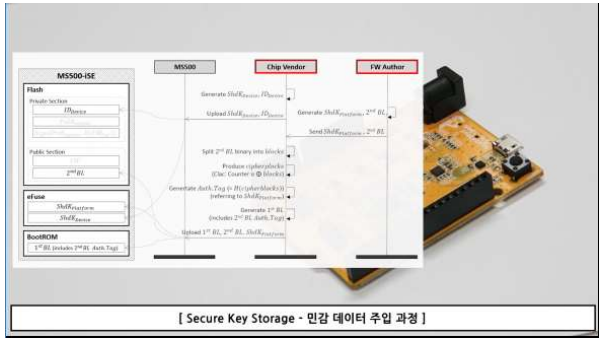
- **Integrated Security SoC 기반 저사양 COTS IoT 디바이스 신뢰 플랫폼**
  - eWBM MS500 기반 Axio Builder
    - Secure Key Storage & Management
    - Secure Boot
    - Secure Firmware Update
    - Remote Attestation
    - Secure Communication
    - Lightweight Security Services



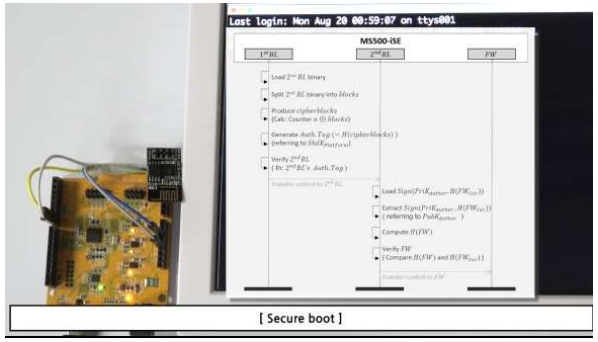
Integrated Secure SoC 기반 COTS IoT 디바이스 신뢰 플랫폼

iS4IoT: integrated Security for IoT Device

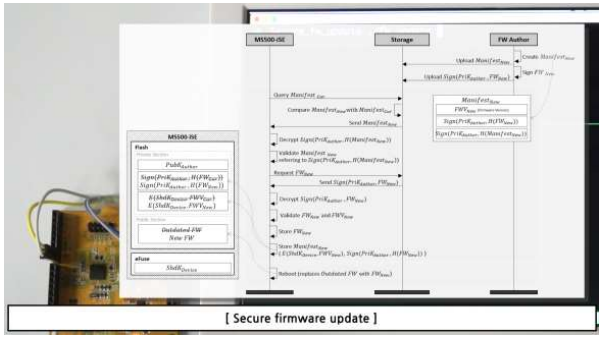
- **Integrated Security SoC 기반 저사양 COTS IoT 디바이스 보안 플랫폼**
  - 동영상 데모 (https://youtu.be/DvEIU1w1BE4)



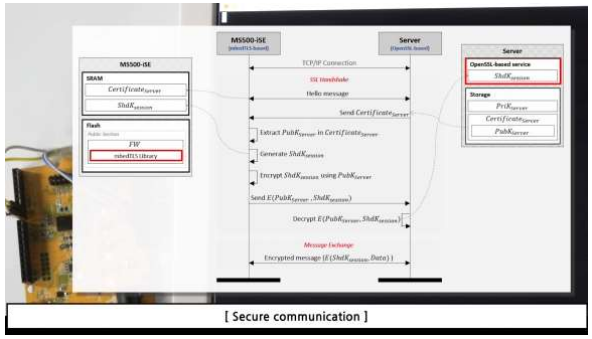
< Secure Key Storage & Management >



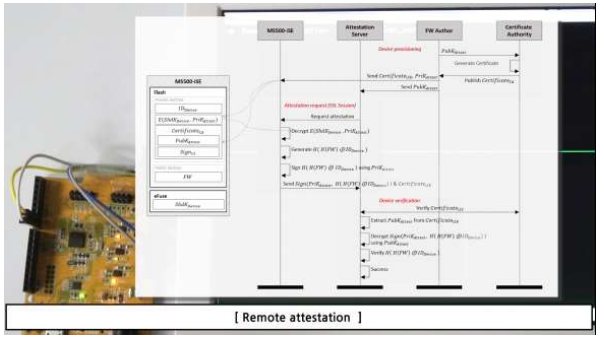
< Secure boot >



< Secure firmware update >



< Secure communication >

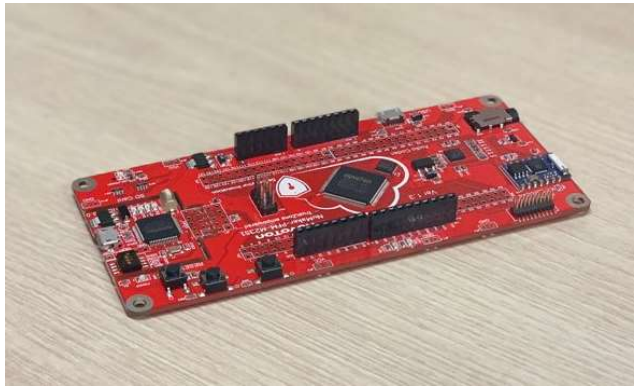


< Remote Attestation >

ARM PSA 기반 저사양 COTS IoT 디바이스 보안 플랫폼

- ARM MPS2+ FPGA Prototyping Board (& Nuvoton)
  - Secure Key Storage & Management
  - Secure Boot
  - Secure Firmware Update
  - Secure Communication
  - Remote Attestation
  - Secure Storage & Crypto. Function

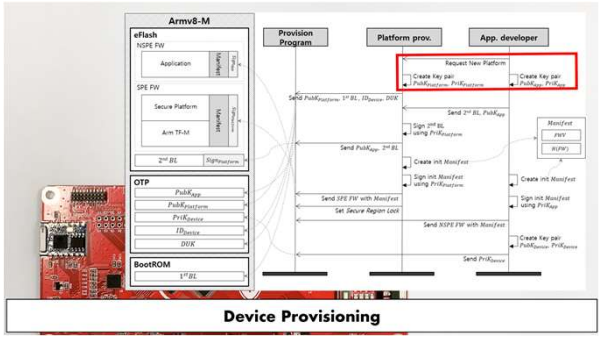
[ARM MPS2+FPGA Prototyping Board]



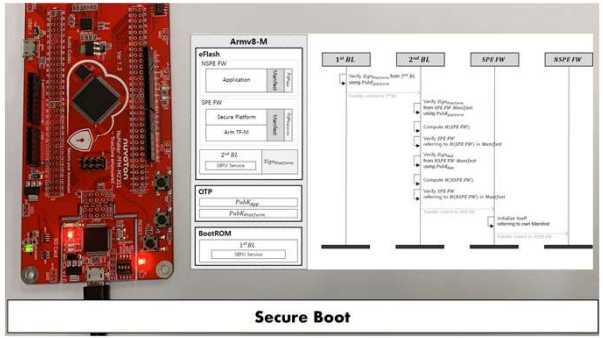
[Nuvoton]

❖ ARM PSA 기반 저사양 COTS IoT 디바이스 보안 플랫폼

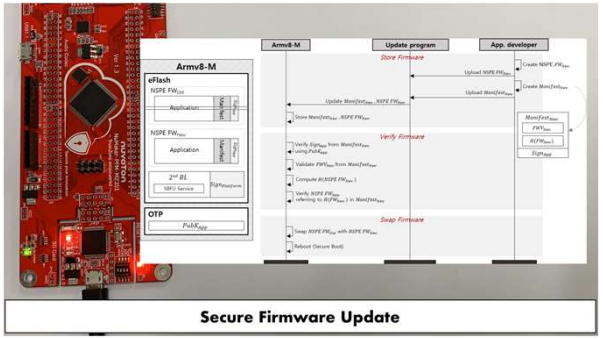
- 동영상 데모 (https://youtu.be/V5UhR4eV7x0)



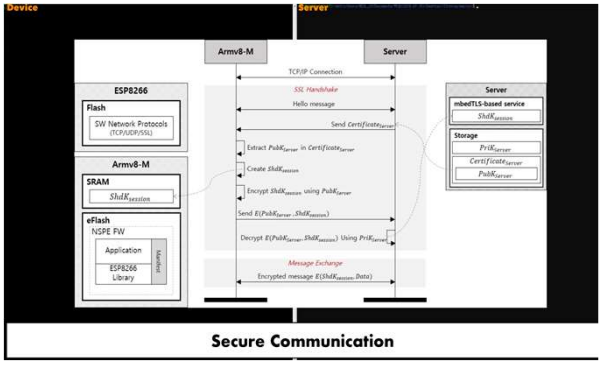
< Secure Key Storage & Management >



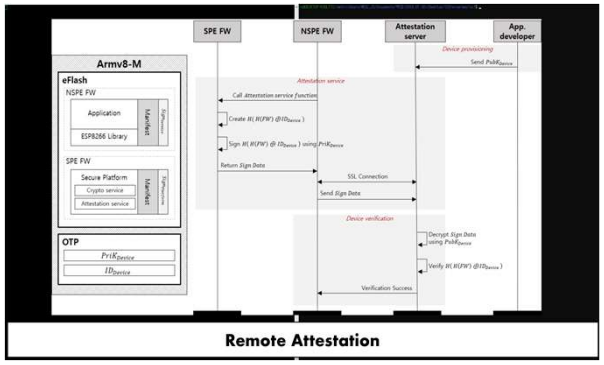
< Secure boot >



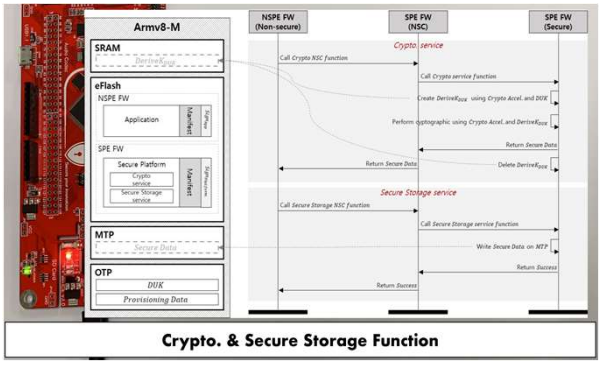
< Secure Firmware Update >



< Secure communication >



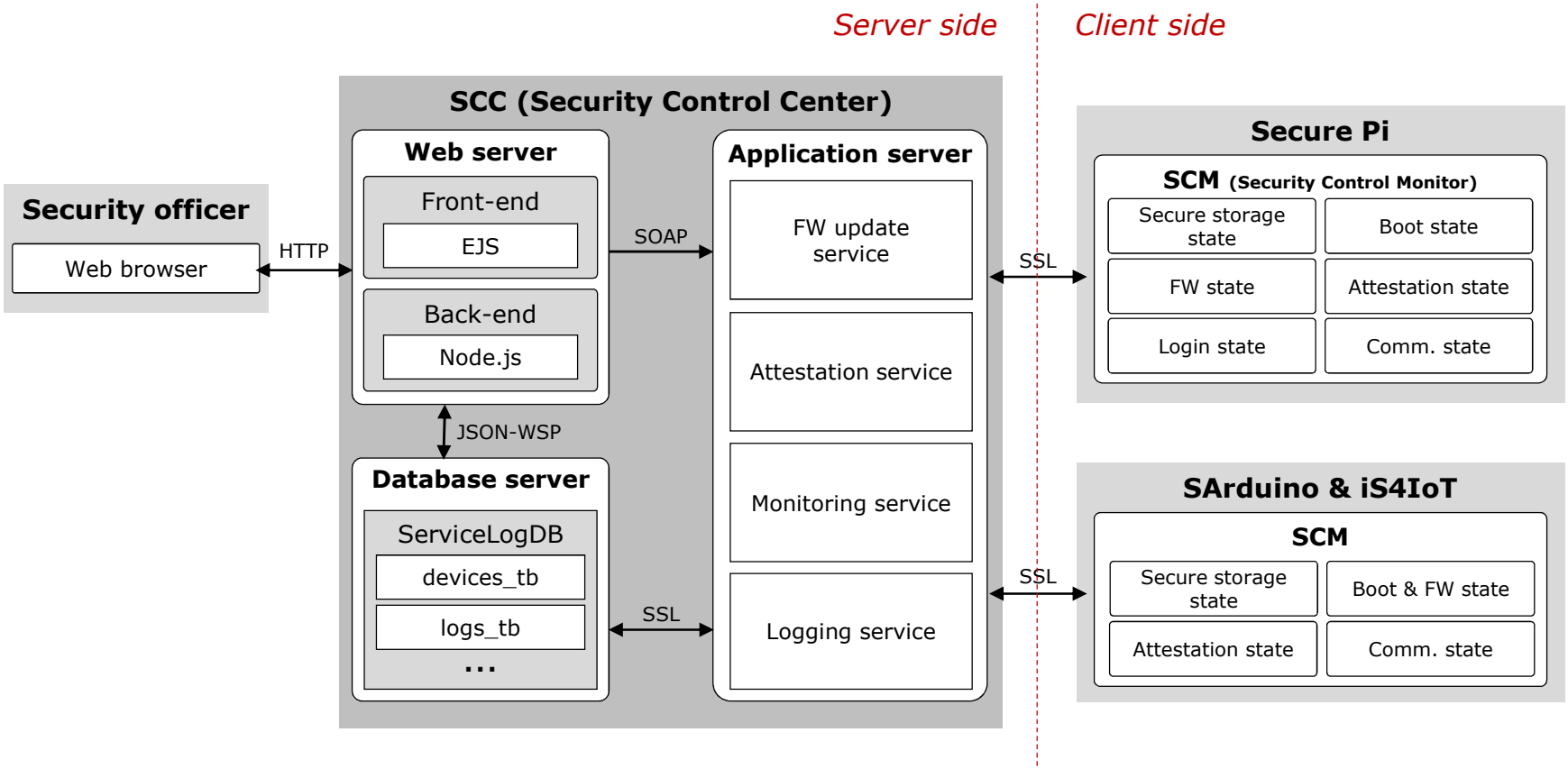
< Remote Attestation >



< Crypto. & Secure Storage Function >

SCC: Security Control Center

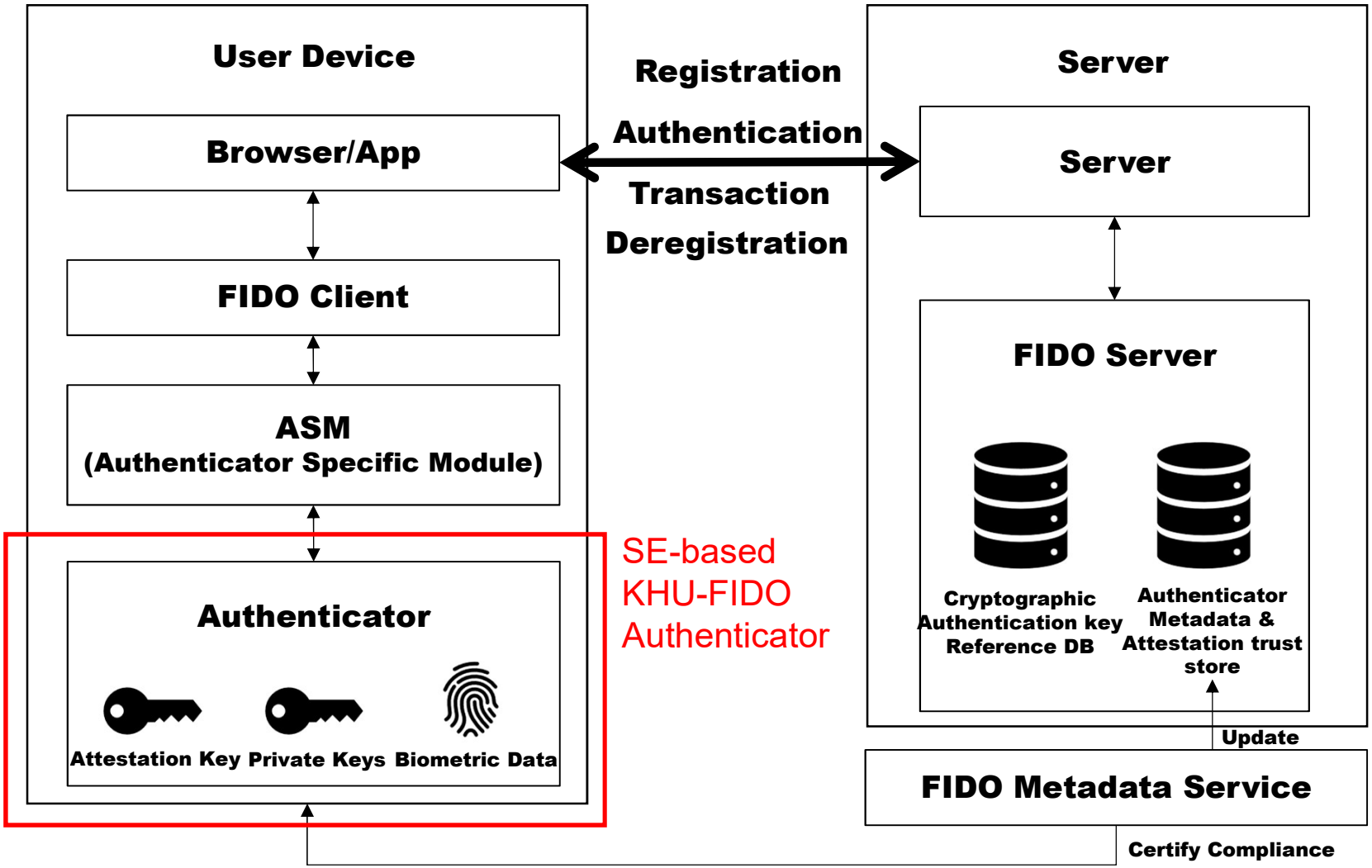
SCC System Architecture



IoT 디바이스 보안 플랫폼 응용

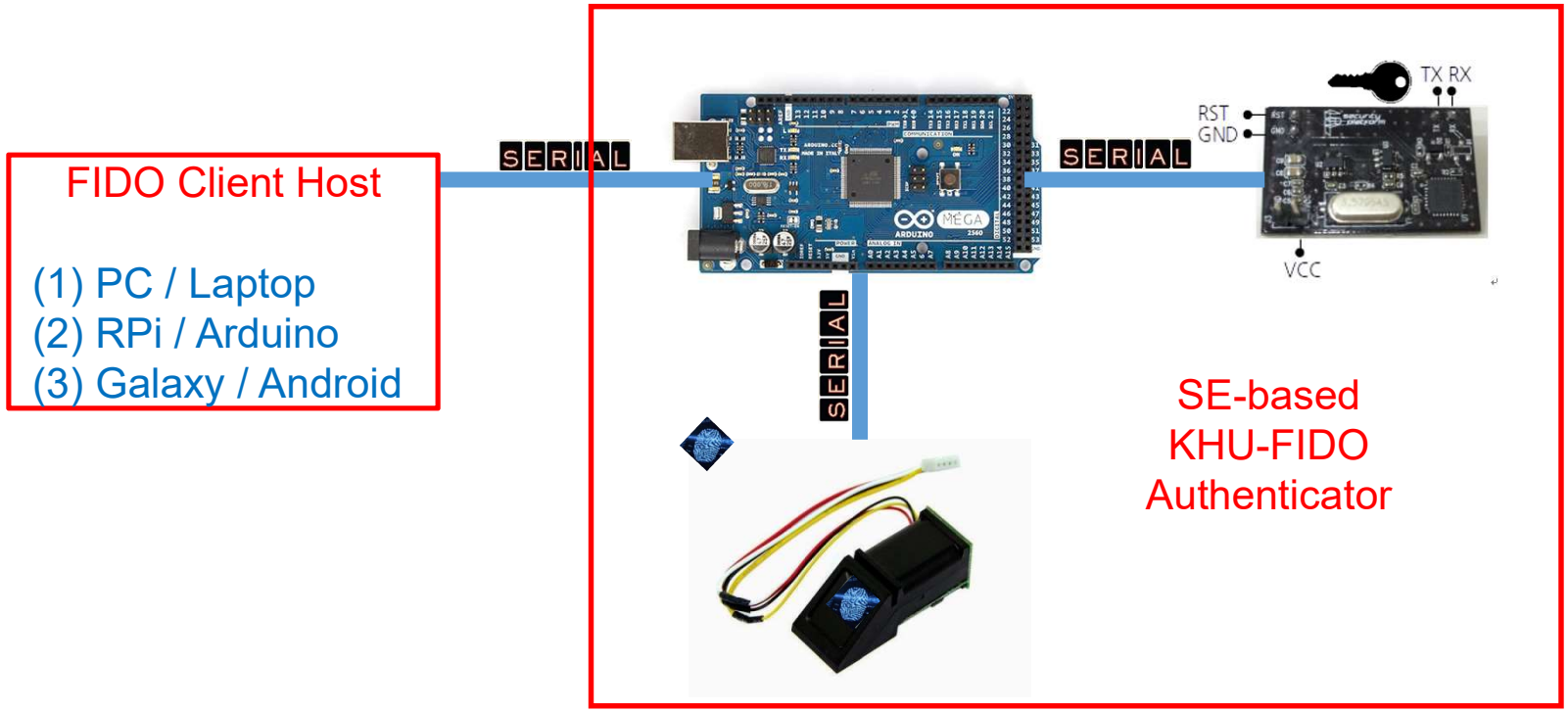
KHU-FIDO Authenticator

FIDO Architecture



KHU-FIDO Authenticator

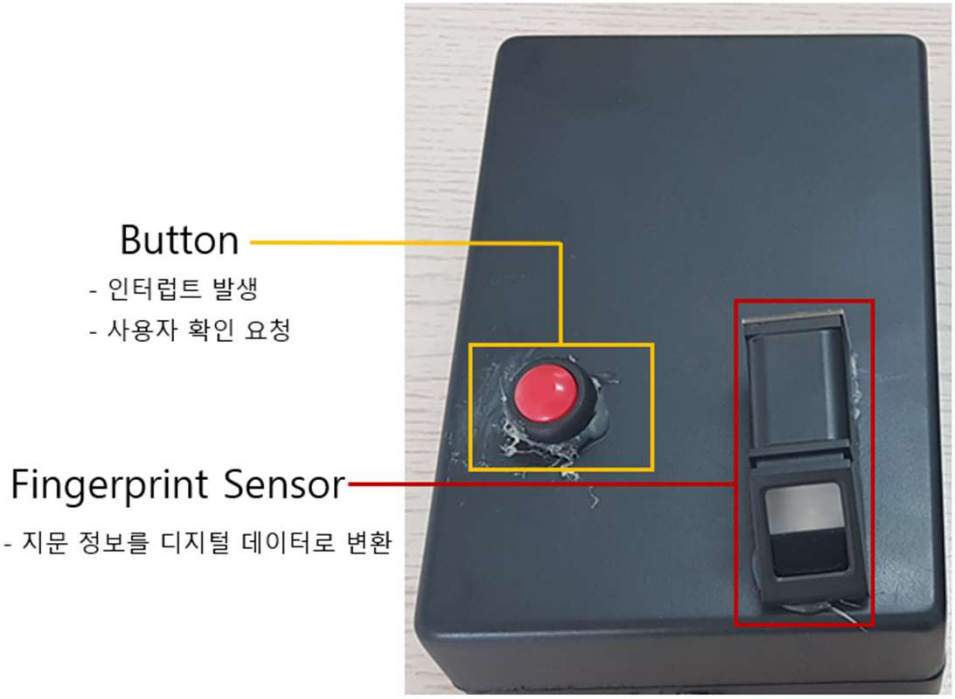
- **SE-based architecture**
  - Option 1) SE + Fingerprint sensor
  - Option 2) Arduino + SE + Fingerprint sensor



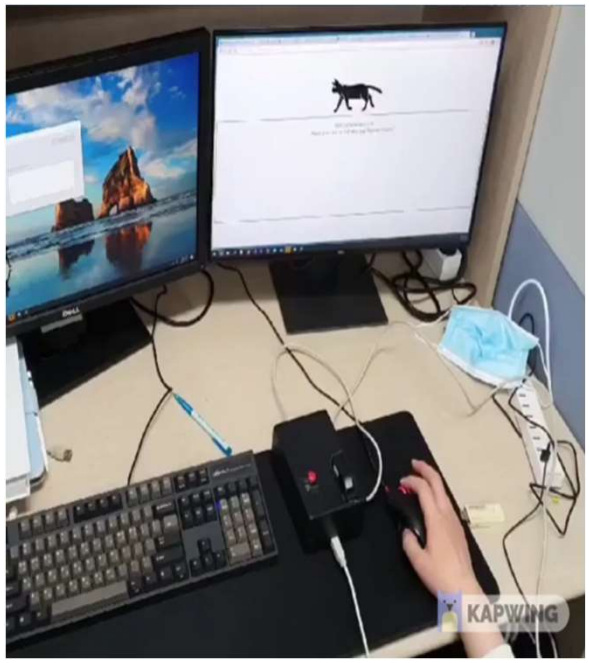
FIDO Application (1)

❖ PC (USB 연결) / 업무 웹 서비스 인증

- PoC →「FIDO-WEB」



「FIDO-WEB」모듈



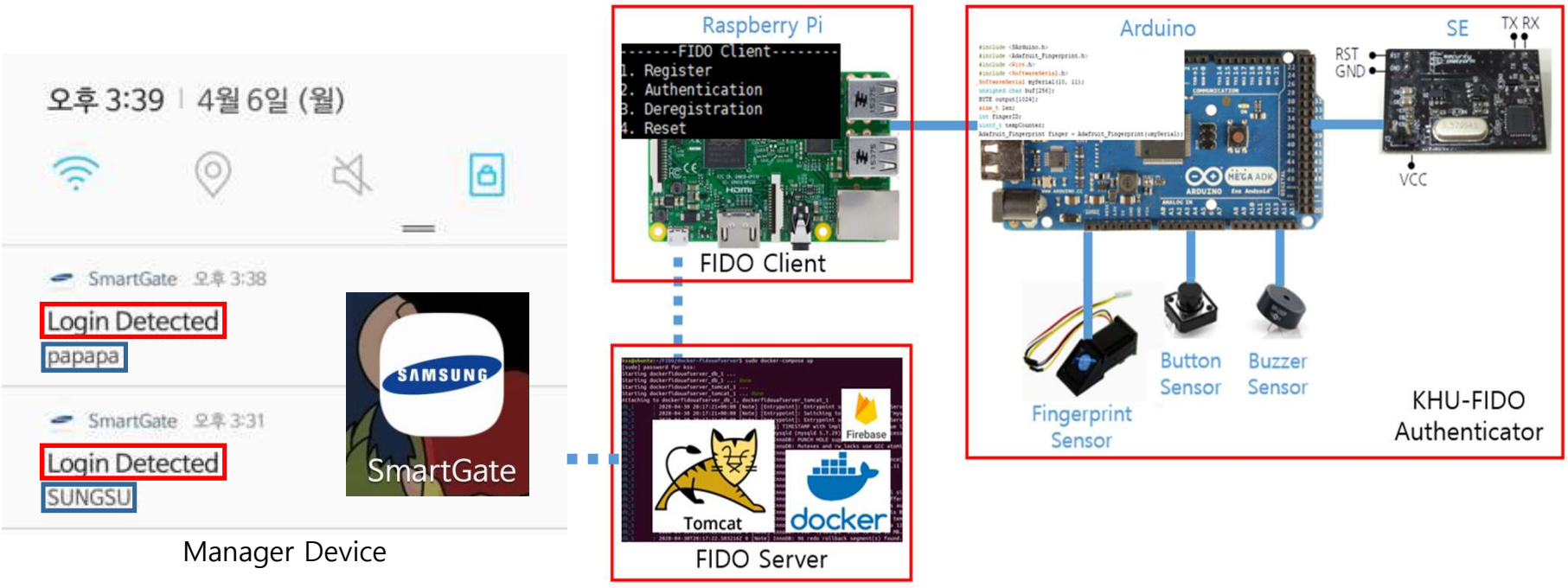
「FIDO-WEB」시연 영상

YouTube Link: https://youtu.be/diEjkB9lGNs

FIDO Application (2)

❖ Standalone / 개인 서비스 인증

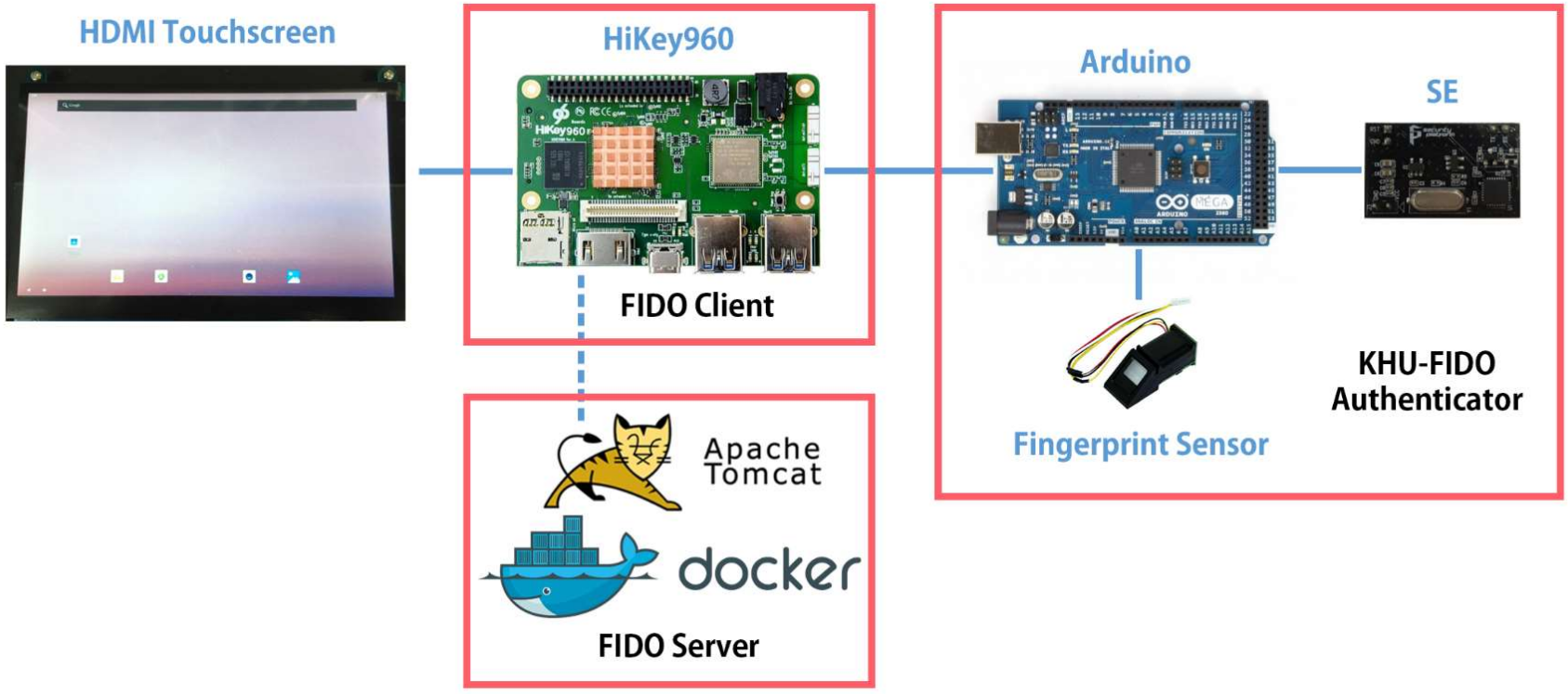
- PoC → 「SmartGate」
  - 사용자의 지문 정보를 이용해 FIDO 인증 수행
  - Manager Device는 사용자 이름이 포함된 푸시 메시지를 수신



「SmartGate」 인증 시스템 아키텍쳐

FIDO Application (3)

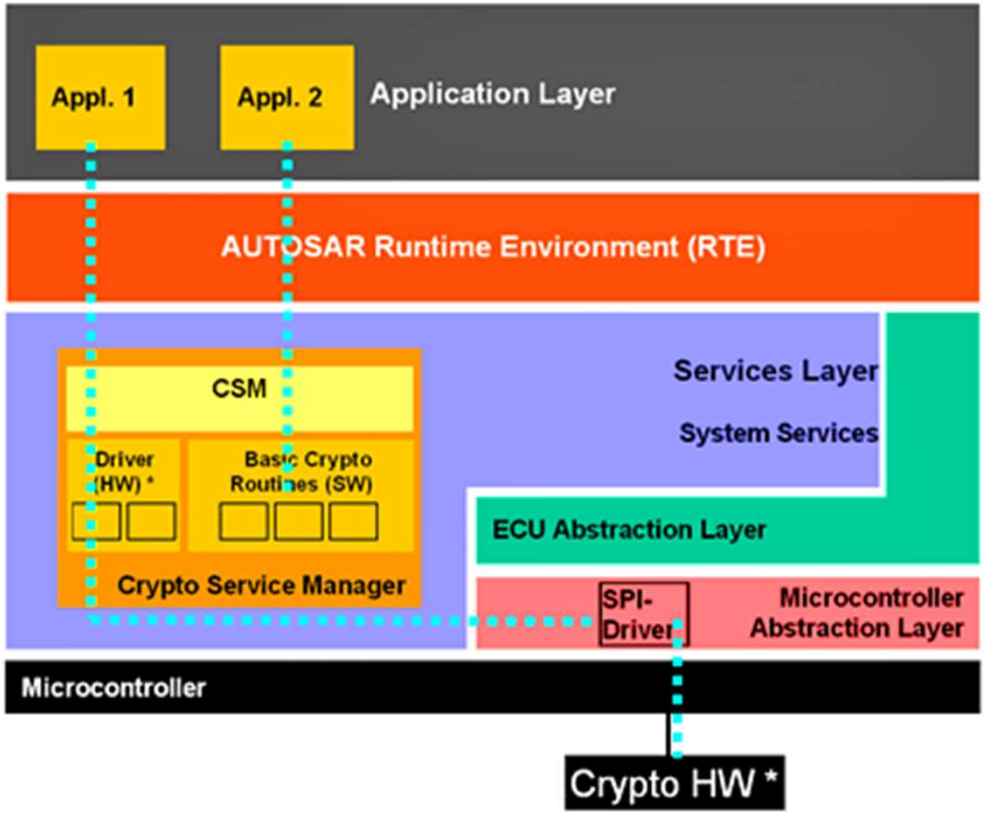
- **Android / 금융 서비스 인증**
  - PoC → 「FIDO-Mobilebank」
    - HiKey960 AOSP OP-TEE의 Trusted Application을 이용



자동차 ECU 보안

AUTOSAR CSM(Crypto Service Manager)

- AUTOSAR BSW(Basic SoftWare)계층에 속한 암호화 서비스 모듈
- 대부분의 상용차들의 ECU는 CSM을 탑재하지 않음

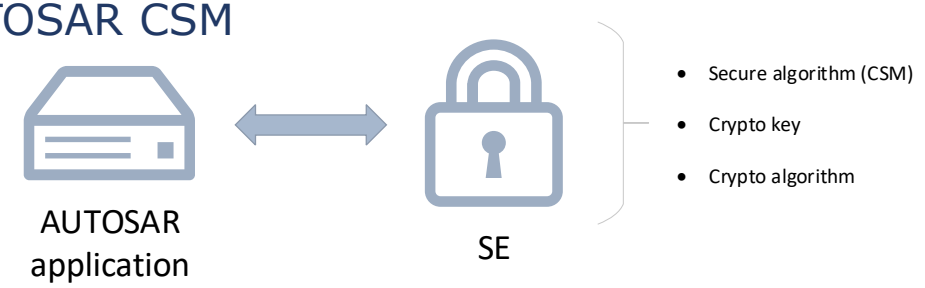


https://www.embedded.com/print/4213069

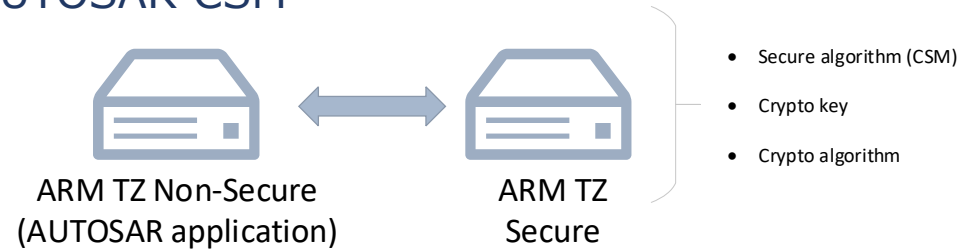
AUTOSAR CSM

PoC Implementation based on HSM (Hardware Security Module)

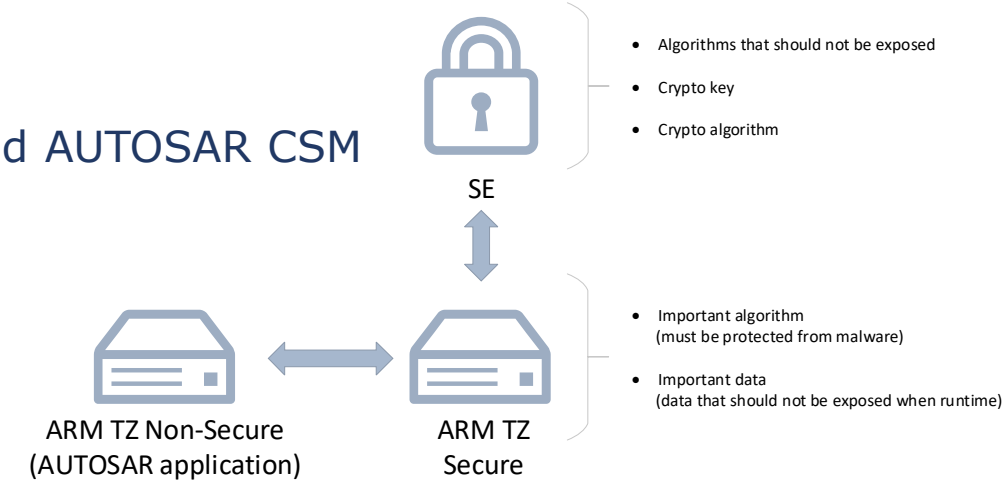
- SE(Secure Element)-based AUTOSAR CSM



- TEE(ARM TrustZone)-based AUTOSAR CSM

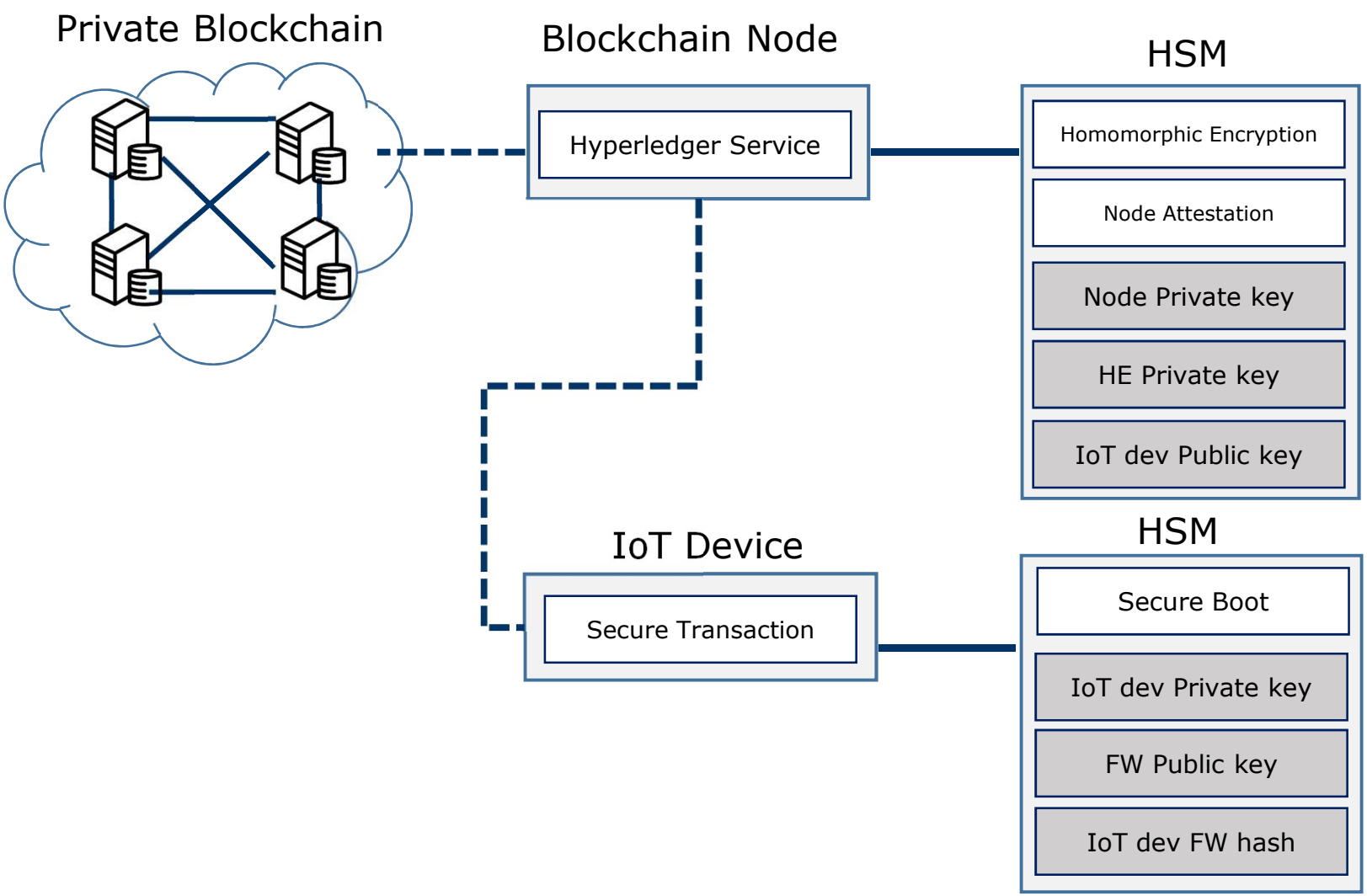


- SE & TEE(ARM TrustZone)-based AUTOSAR CSM



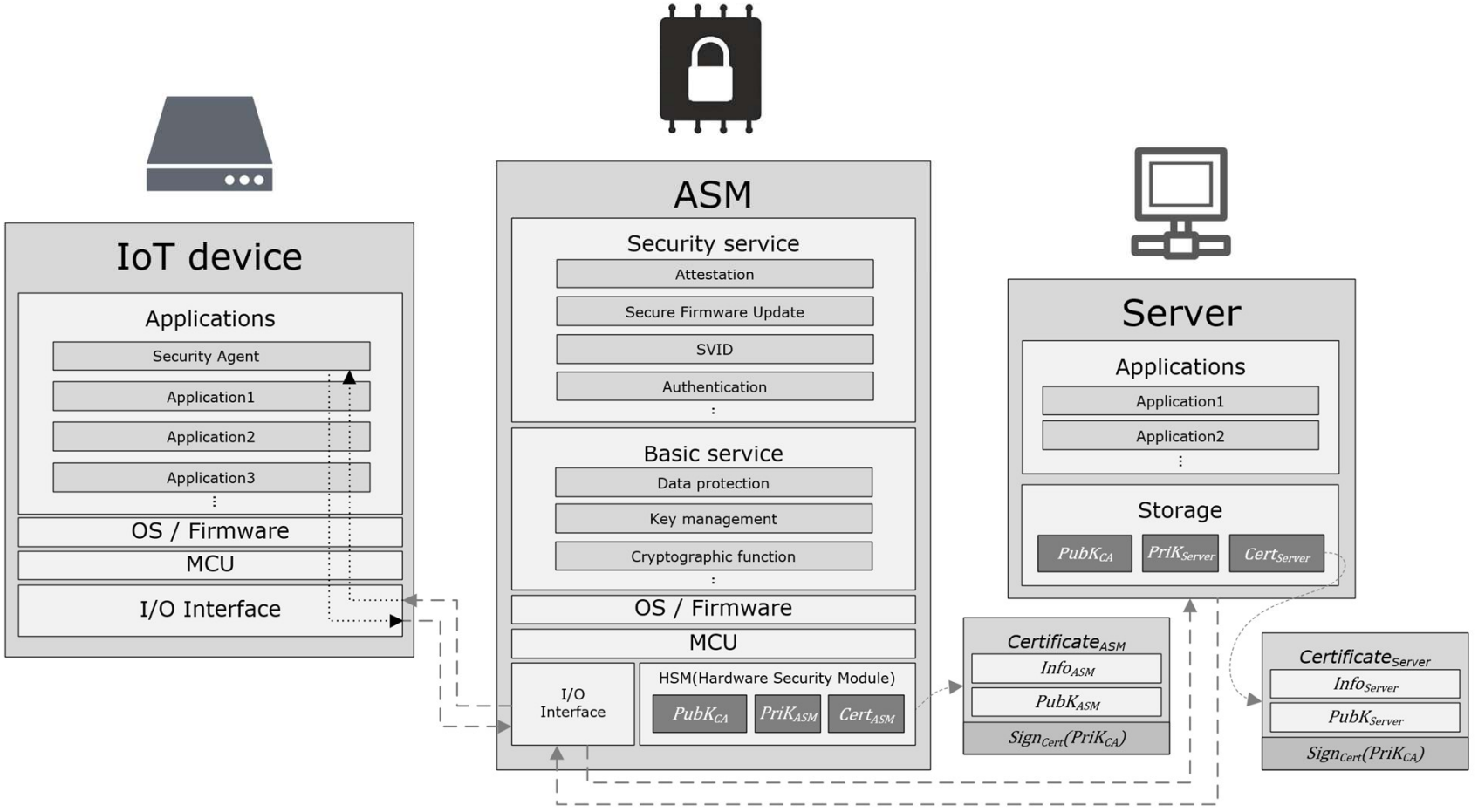
Blockchain IoT

Architecture



ASM: Augmented Security Module

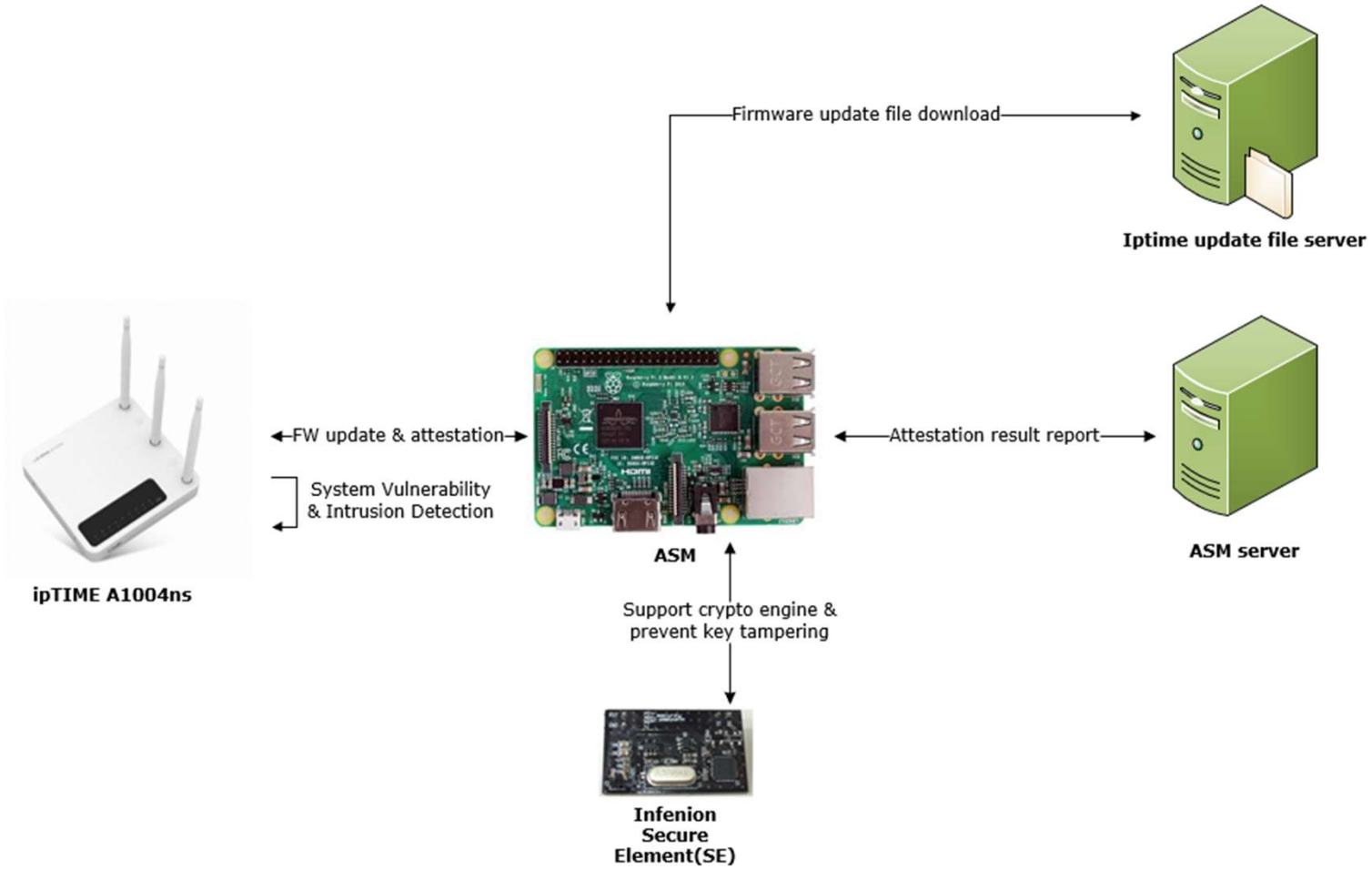
Architecture



ASM: Augmented Security Module

PoC on ipTIME

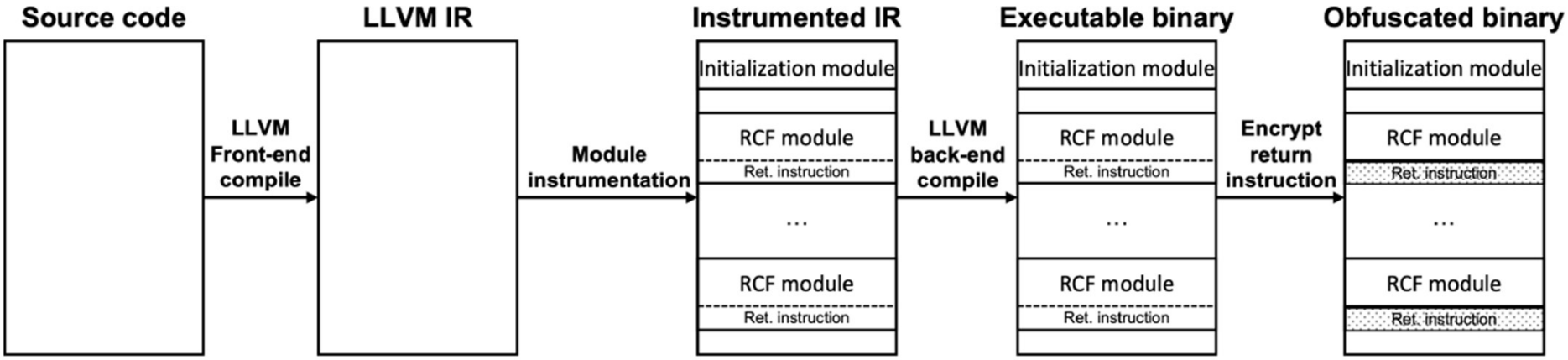
- Overall architecture



Firmware Security

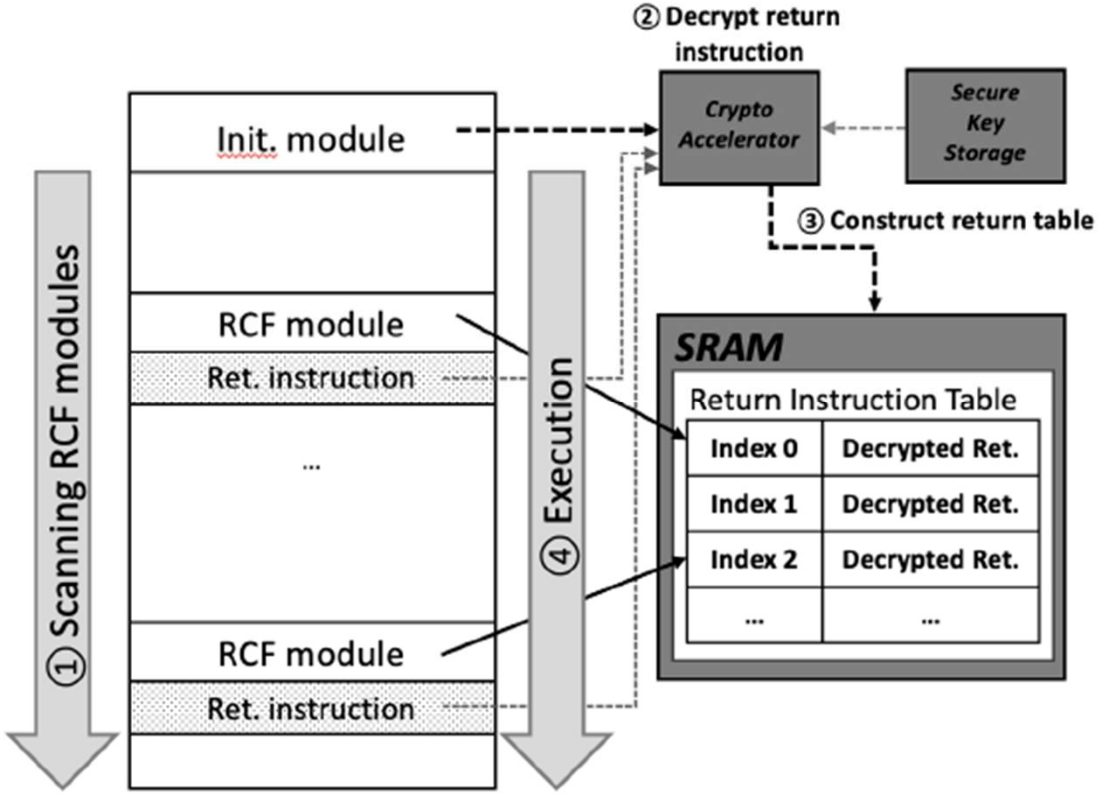
LLVM 기반 Baremetal Firmware 보안 강화 기법

- 펌웨어 난독화
  - Obfuscation

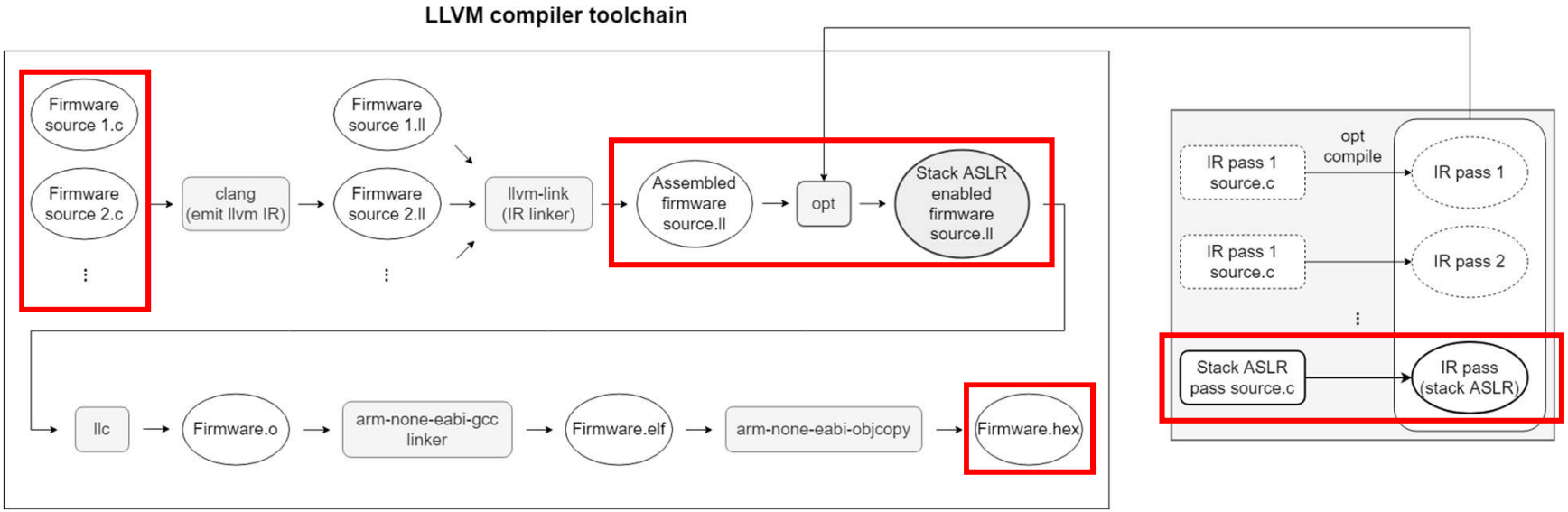


❖ 펌웨어 난독화

- Execution



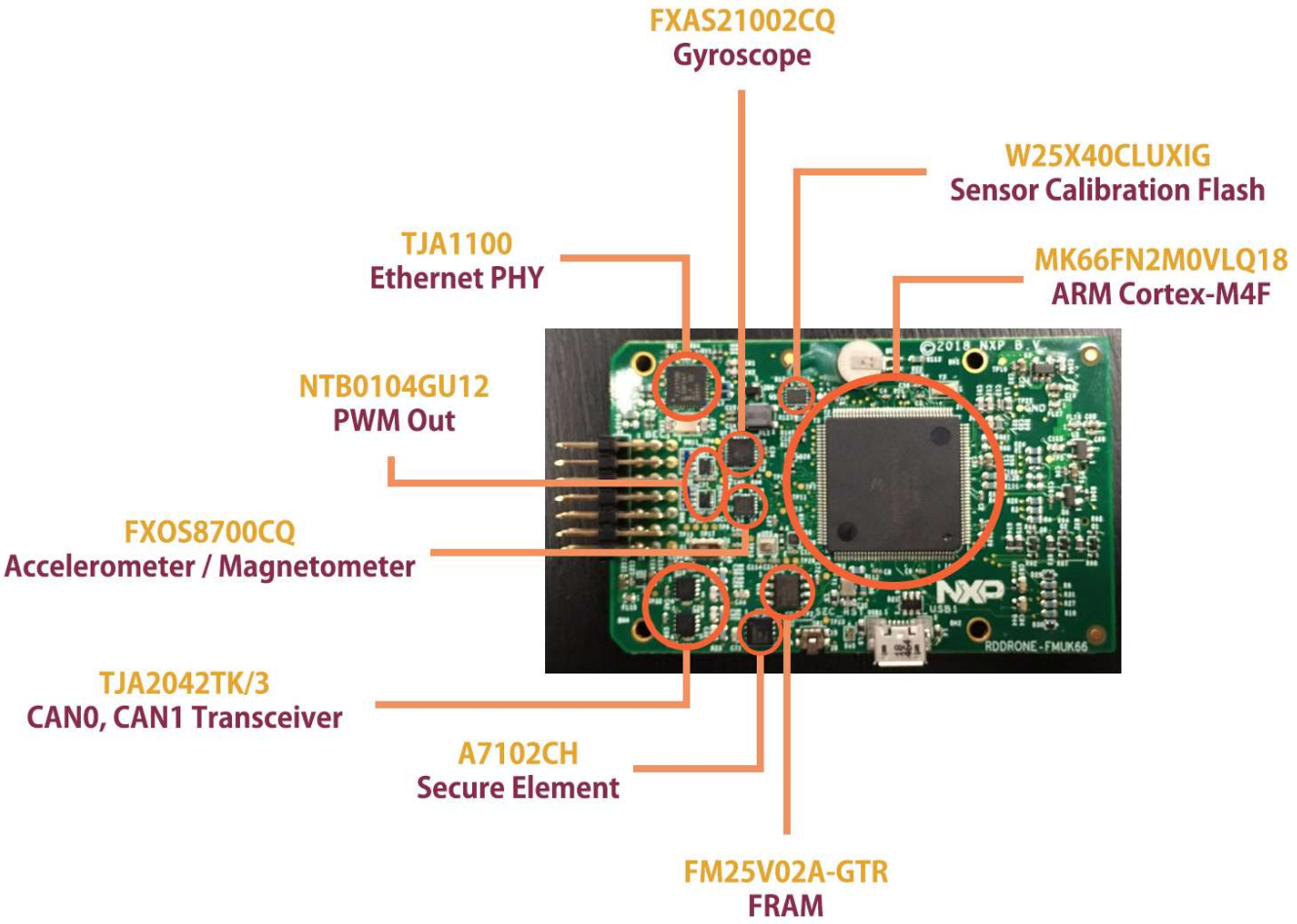
❖ LLVM-based Stack ASLR in Baremetal Firmware



Drone Security

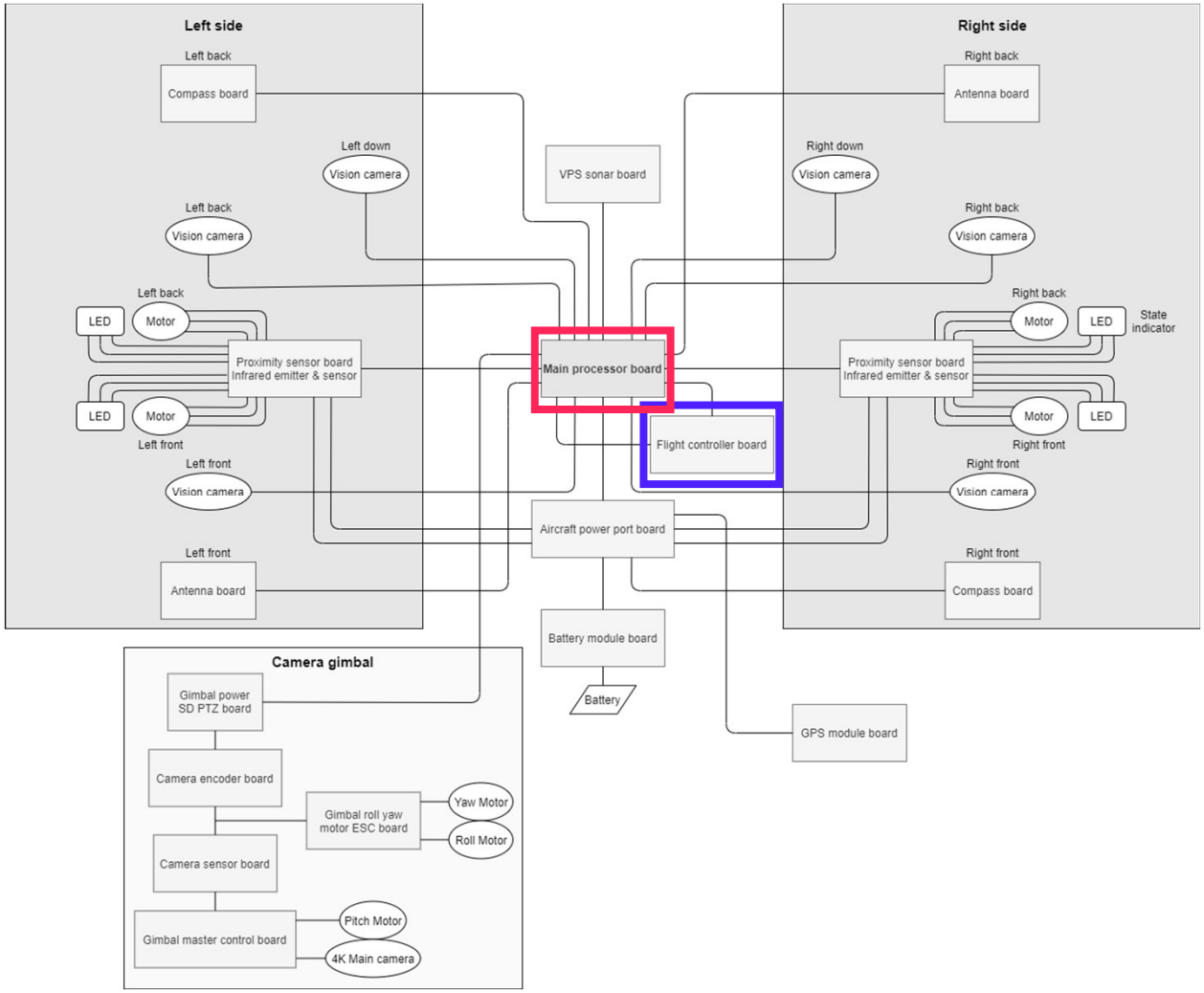
상용 드론 펌웨어 분석

❖ NXP Hovergames



상용 드론 펌웨어 분석

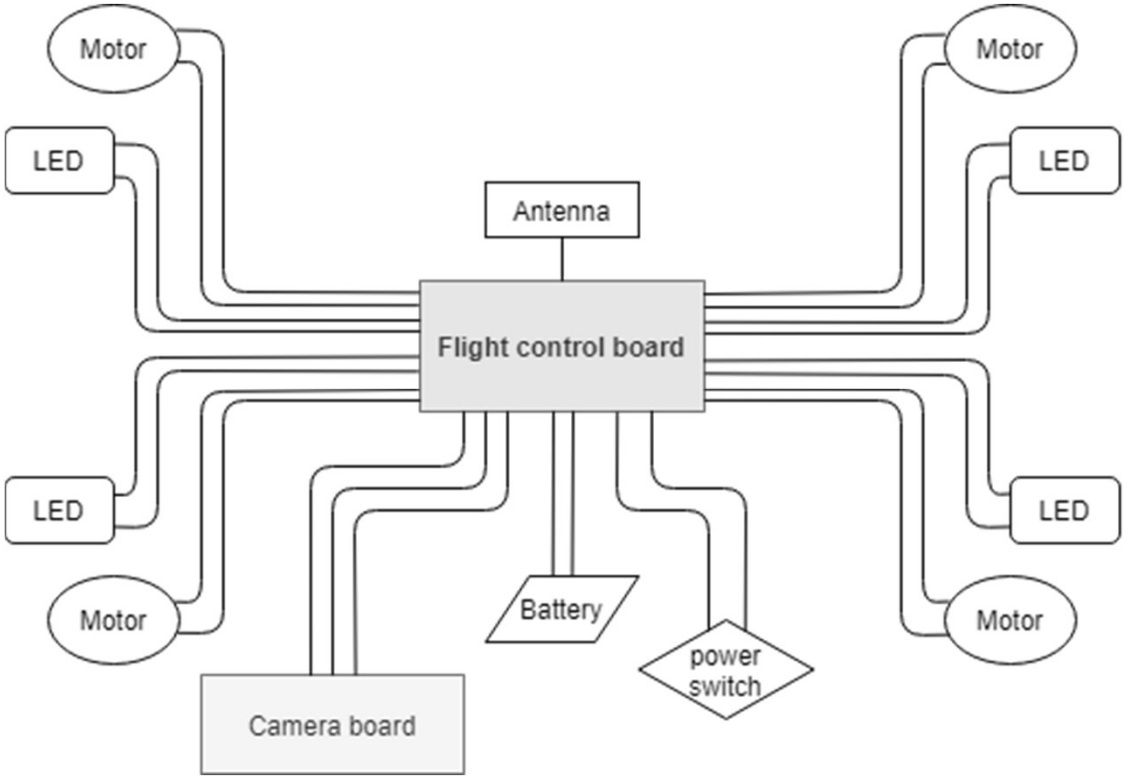
❖ DJI Phantom 4 pro V2.0



상용 드론 펌웨어 분석

Syma X5C

- Layout



상용 드론 취약점 사례 정리

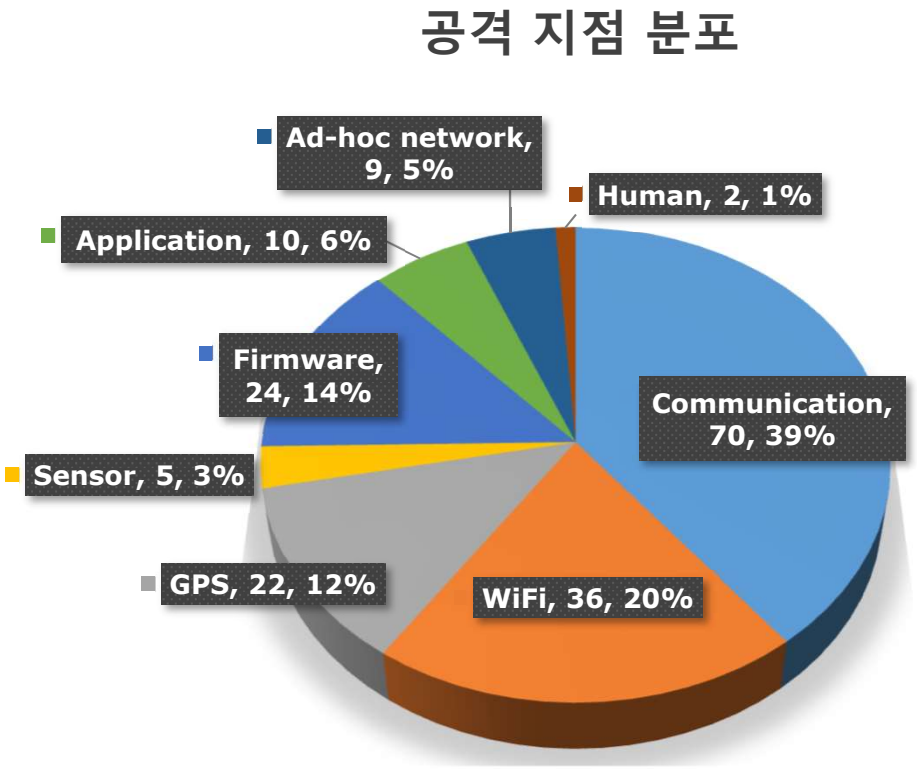
- **취약점 사례 정리 경과**
  - 많은 시행착오를 경험
    - 애매 모호한 설명, 복합적인 공격 사례, 방어 위주 사례, 중복 사례, 등등
  - 정리의 목적
    - HW 및 SW 구조별 취약점 분석
    - HW 및 SW 구조별 대응방안 도출

- **181건에 대해 다음의 형태로 정리**
  - 공개일
  - 대상 드론
  - Reference
  - 주요 내용
  - 분류
    - 공격 유형
    - 공격 대상
    - 공격 지점
    - 공격 형태
    - 공격 결과
    - Threat model

상용 드론 취약점 사례 분석

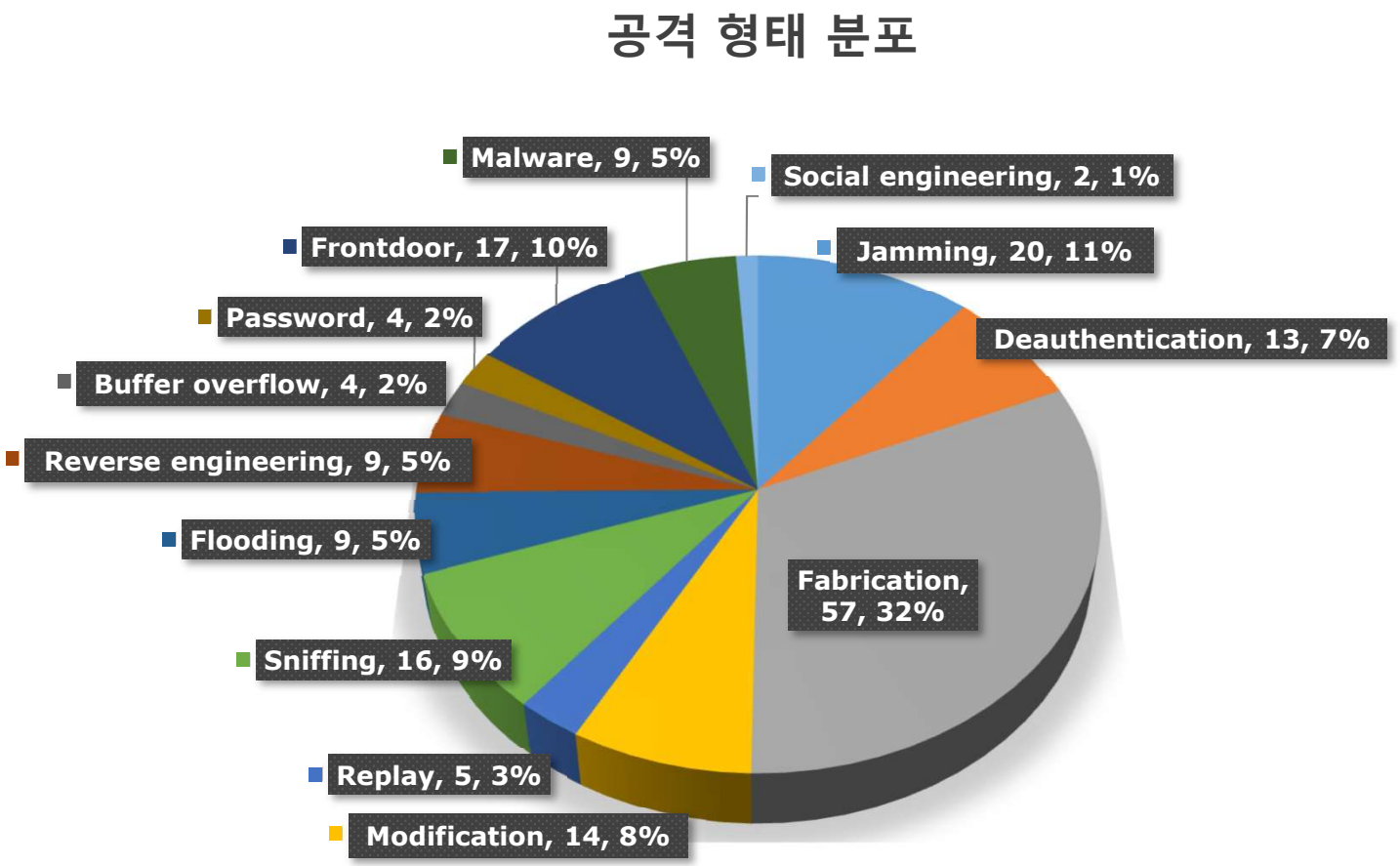
❖ 공격 지점 분석 (총 178건)

- Communication(WiFi 포함) 공격이 59%로 제일 큰 비중임
- 쉽게 공격할 수 있는 GPS도 12%를 차지함
- Drone/RC/Smartphone/Laptop/Server 등의 Firmware/Application도 20%를 차지하며 제어권이 탈취되는 큰 영향을 미칠 수 있음



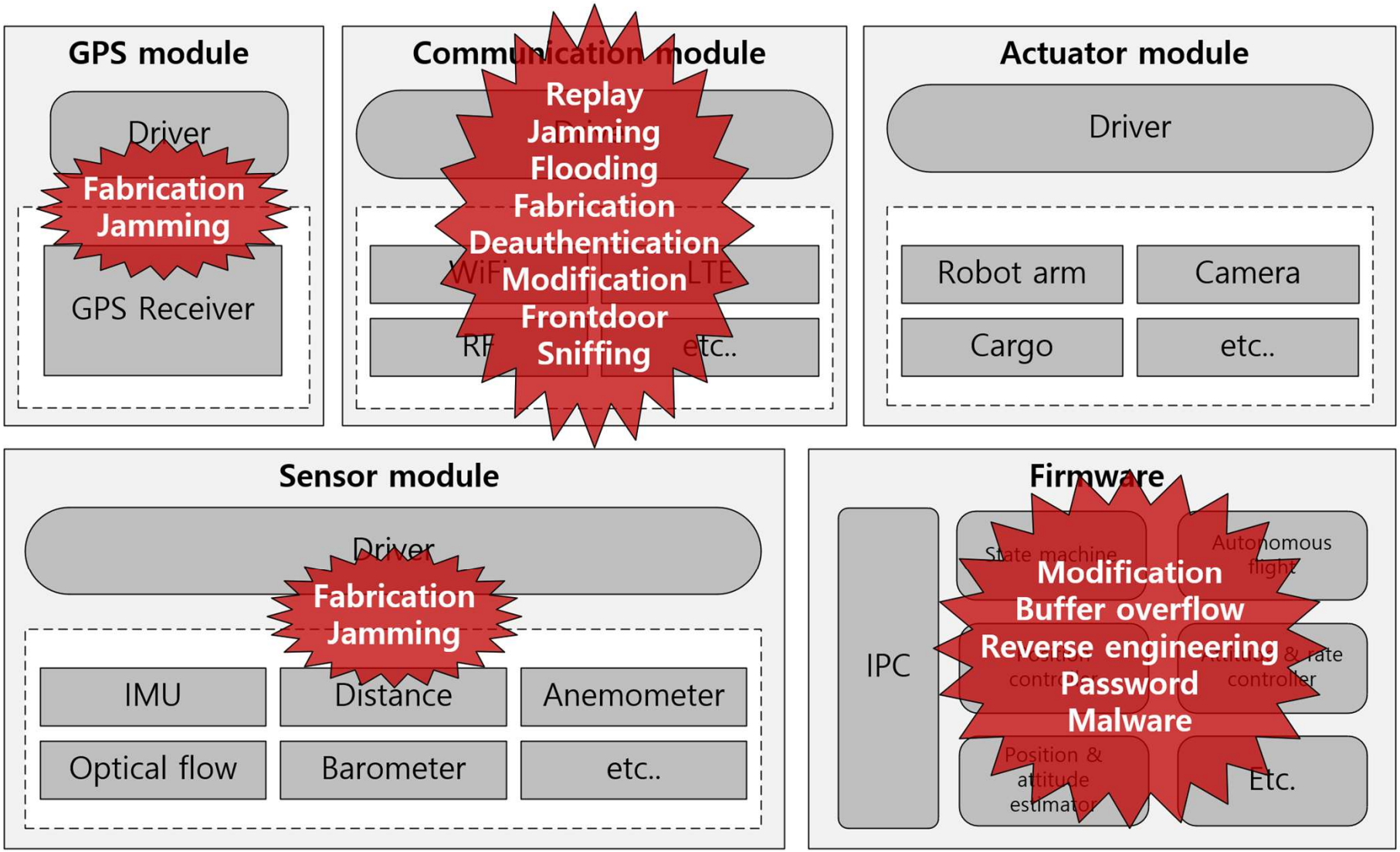
상용 드론 취약점 사례 분석

- **공격 형태 분석 (총 178건, 다중 공격 형태 1건 추가 179건)**
  - Communication/GPS 등의 Fabrication 공격이 31%로 제일 큰 비중임
  - 공격 지점별 공격 형태를 별도로 분석할 필요 있음



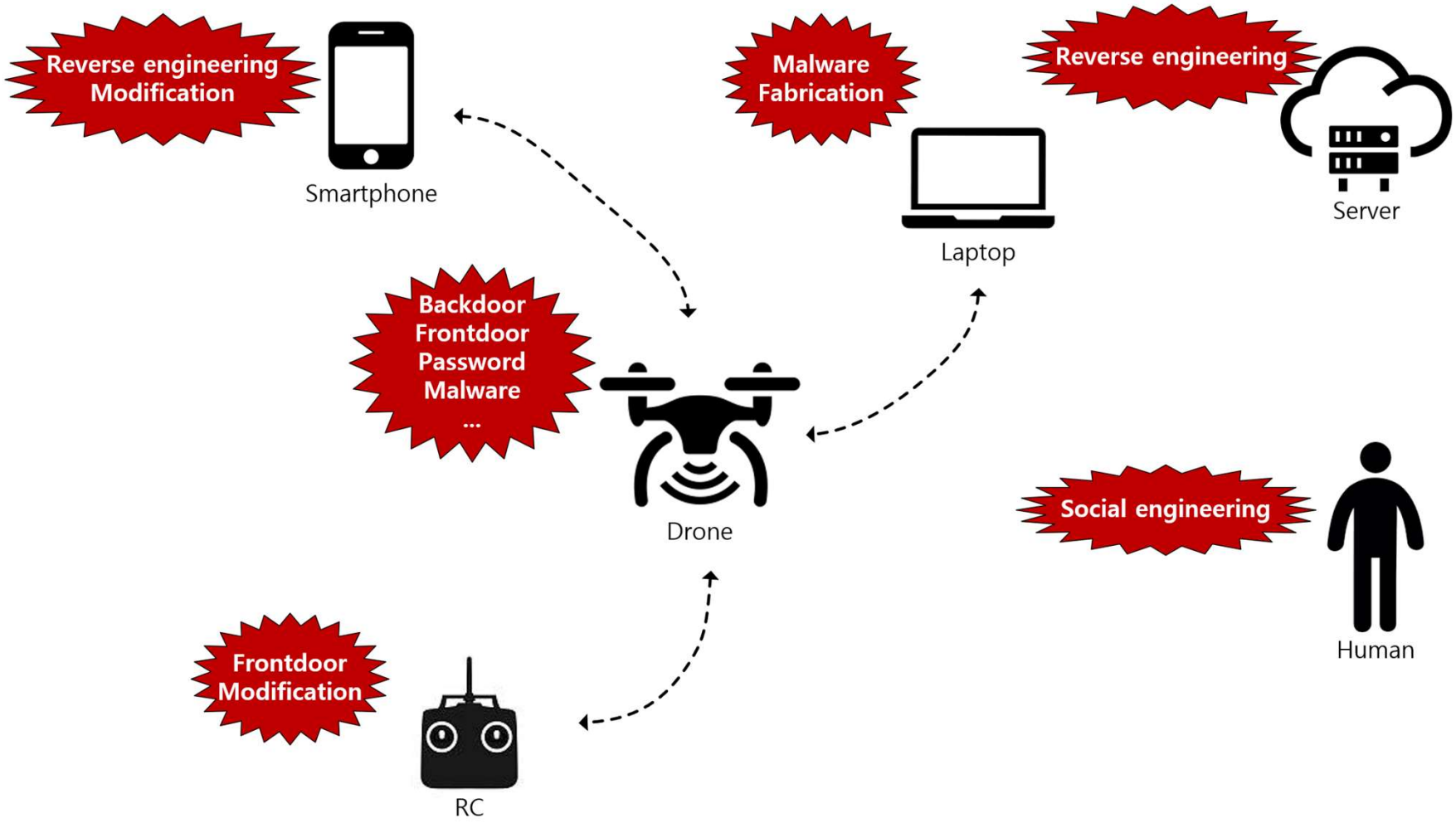
드론 SW 구조별 취약점 분석

❖ Drone



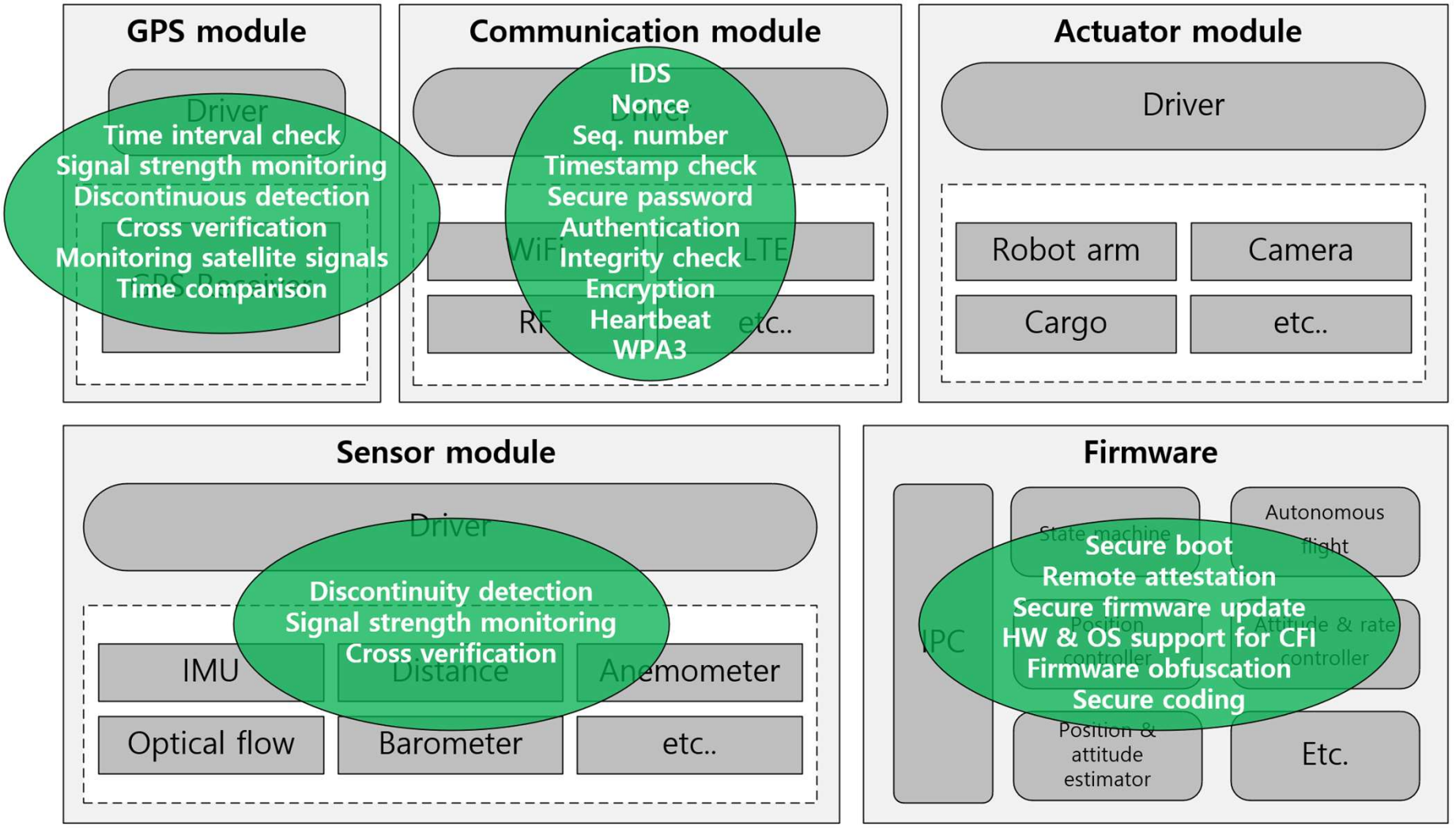
드론 SW 구조별 취약점 분석

- **Drone – RC – Smartphone – Laptop – Server – Human**



드론 SW 구조별 취약점 대응기술

❖ SW 구조별 취약점 대응기술: SoK



Automotive Security

자동차 보안 위협 및 보안 기술

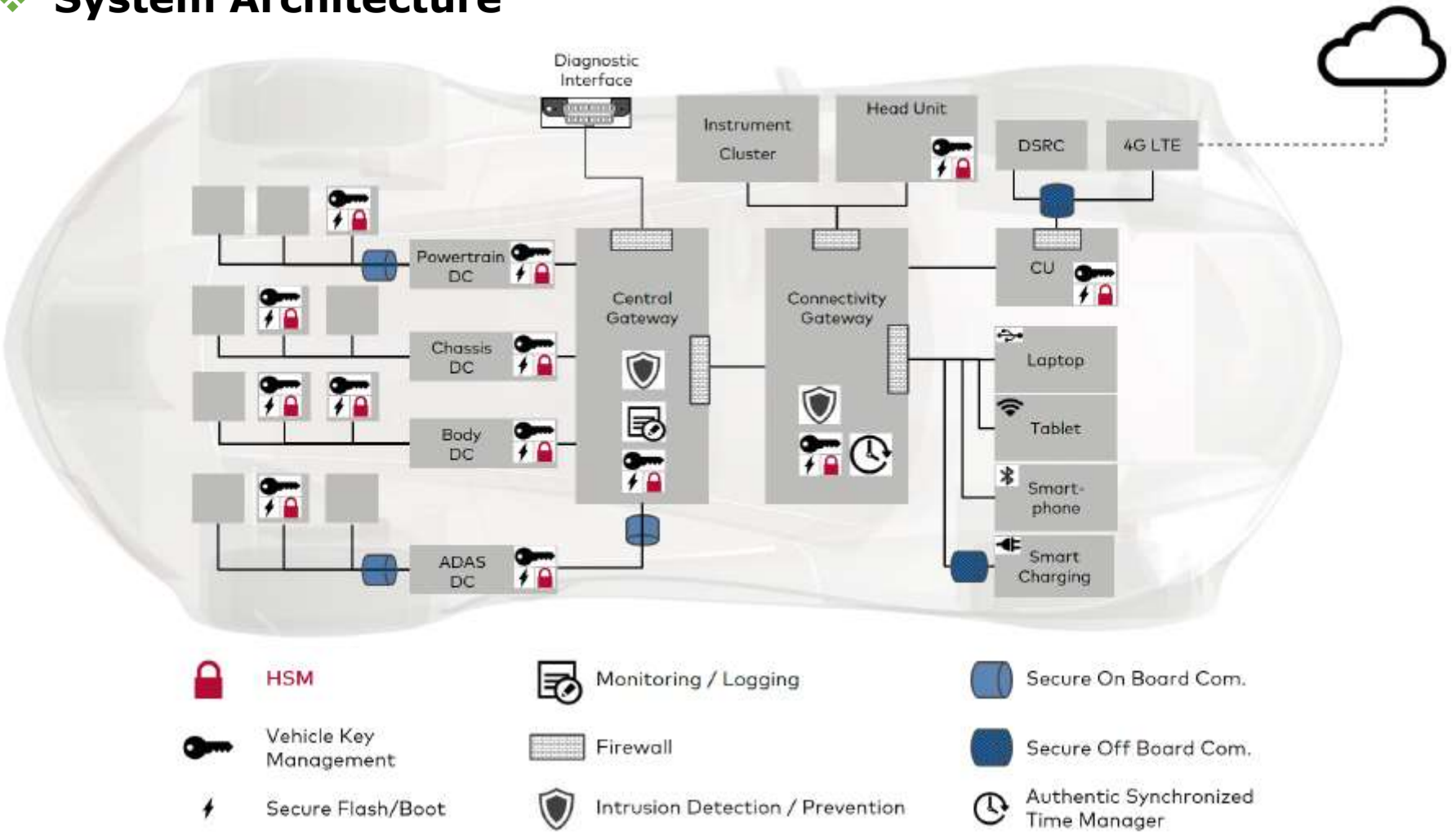
분류	보안 위협
전장 플랫폼	– ECU 소프트웨어 결함, ECU 리버스 엔지니어링 – ECU 펌웨어 해킹 및 위/변조 – 위장 ECU 장착 – IVI(In-Vehicle Infotainment) 해킹, 악성 감염 스마트 센서 물리 공격(블라인딩, 스푸핑, 재밍)
내부 네트워크	– 차량 내부네트워크에 악의적인 제어 메시지 주입 – 정상적인 내부네트워크 방해(패킷 삽입, 삭제, 임의조작, 지연 등), 도청 – DoS, 리플레이, 스푸핑, 패킷 폐기 공격
외부 네트워크	– 무선 통신망 해킹, DoS 공격 – 위장 OBU(Onboard Unit), RSU(Road Side Unit) – 악의적인 차량(Misbehavior Vehicle) – 거짓 정보(Fake message) 제공 – 차량 접속 기기 해킹
관리, 진단	– 프라이버시 침해, OBD-II 해킹 – 원격 업데이트 및 진단 프로토콜 해킹 – 해킹에 의한 사고원인 분석/증거 보존의 어려움

분류	보안 기술
전장 플랫폼 보안	– 시큐어 부트, 시큐어 플래싱, 접근제어 – 애플리케이션 샌드박스, 플랫폼 가상화 – HSM(Hardware Security Module) – 부채널 방지 – Autosar CSM(Cryptographic Security Manager), SecOC(Secure Onboard Communication)
내부 네트워크 보안	– 침입 탐지 시스템(IDS), 차량용 방화벽(F/W) 침입 방지 시스템(IPS) – ECU 인증, 키관리, 암호화 – 위협탐지(Rule-Based, Machine Learning-Based)
외부 네트워크 보안	– V2X 메시지 인증, 암호화 – 차량 PKI, V2X 메시지 서명(고속) 검증 – IEEE 1609.2, CAMP VSC3
보안 관리, 진단	– 보안 모니터링, 보안 취약성 분석 – 차량 이상징후, 비정상 행위 분석 – 원격 SW/FW 보안 업데이트 – J2735 기반 보안성 평가 – 포렌식 및 사고 원인 분석 기술

자율주행 자동차 보안기술 동향, 전자통신동향분석, 2018.2

System Security

System Architecture



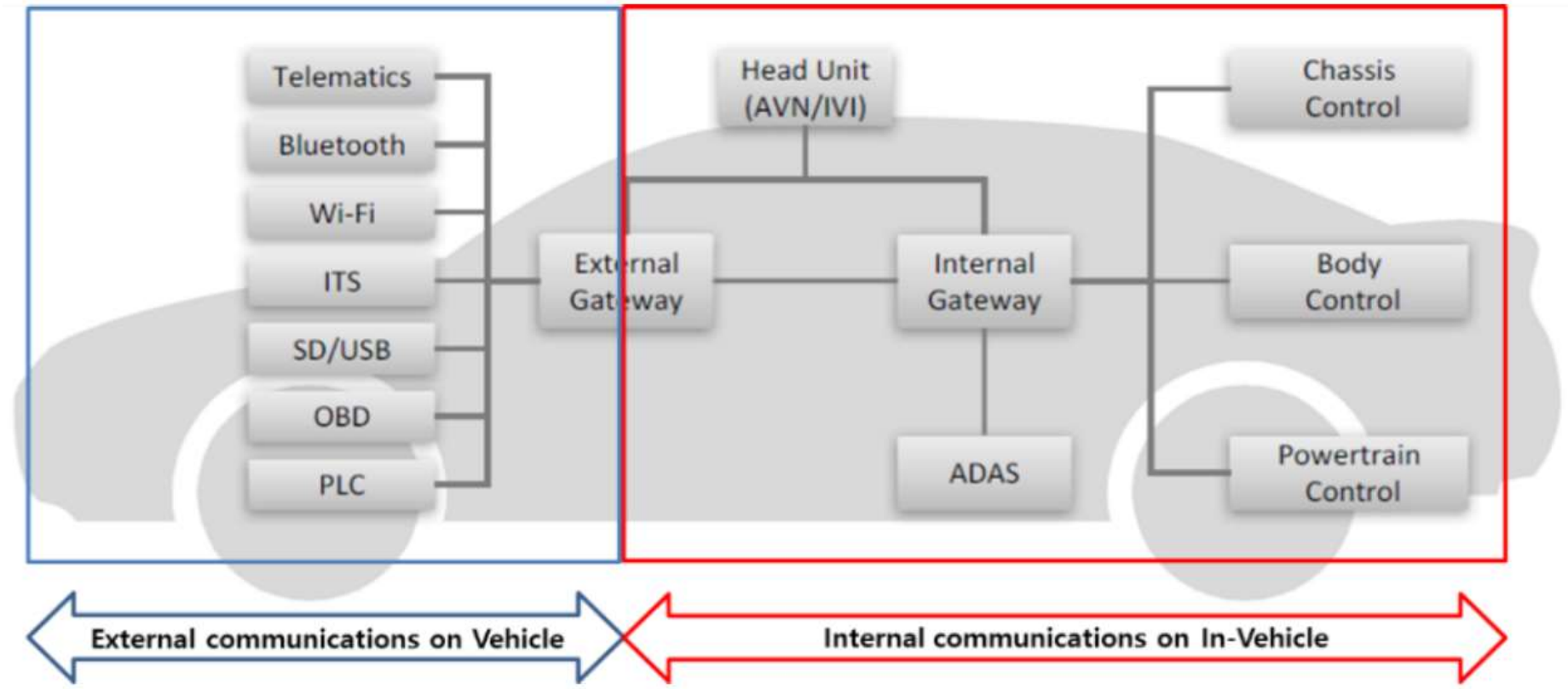
https://www.infineon.com/ispn

System Security

- **Secure Boot**
  - 펌웨어 무결성 검증
- **Secure Firmware Update**
  - 정상 펌웨어 검증
- **Secure Communication**
  - 암호화 데이터 전송
- **Secure Storage**
  - 키를 포함한 데이터 암호화 저장
- **Secure Attestation**
  - 펌웨어 상태 검증
- **HSM-based**
  - TPM (Trusted Platform Module)
    - http://trustedcomputinggroup.org
  - SE (Secure Element)
    - http://globalplatform.org
  - ARM TrustZone
    - ARM TrustZone-A
    - ARM PSA (TrustZone-M)
  - Security SoC

Network Security

- In-vehicle / External / V2x communication
- Sensor & Actuator Network for autonomous vehicles



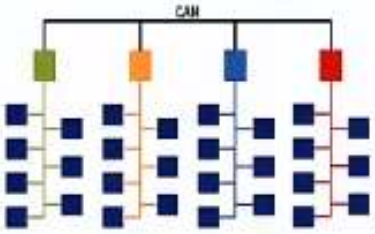
자동차 보안 기술, 김휘강, KRnet2019

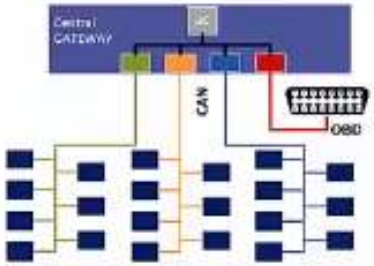
How to Secure Automotive Ethernet

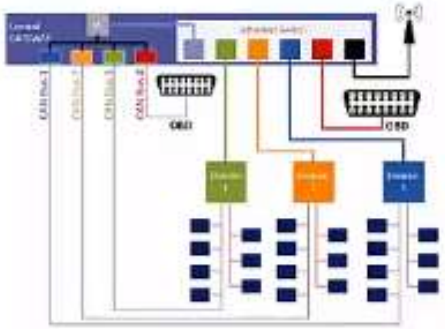
Introduction and motivation

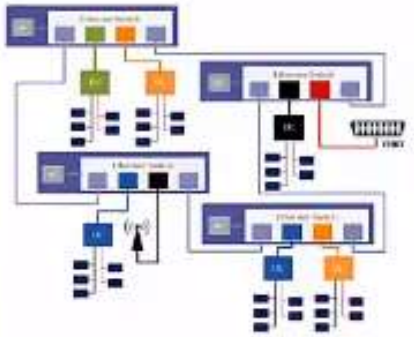
Trends in E/E architecture

escrypt
SECURITY. TRUST. SUCCESS.









Yesterday	Today	Tomorrow	Future
▪ Many small ECU's performing a specific function ▪ Signal based communication	▪ Use of a central Gateway for cross-domain communication ▪ Security introduction with CAN firewall and SecOC etc.	▪ E/E Architecture with support of security features ▪ Application of service oriented communication and high performance ECUs ▪ Still cyclic messages being used	▪ Using ring based network to achieve redundancy ▪ Introduction of vehicle computers (using security enhanced high performance microprocessors)

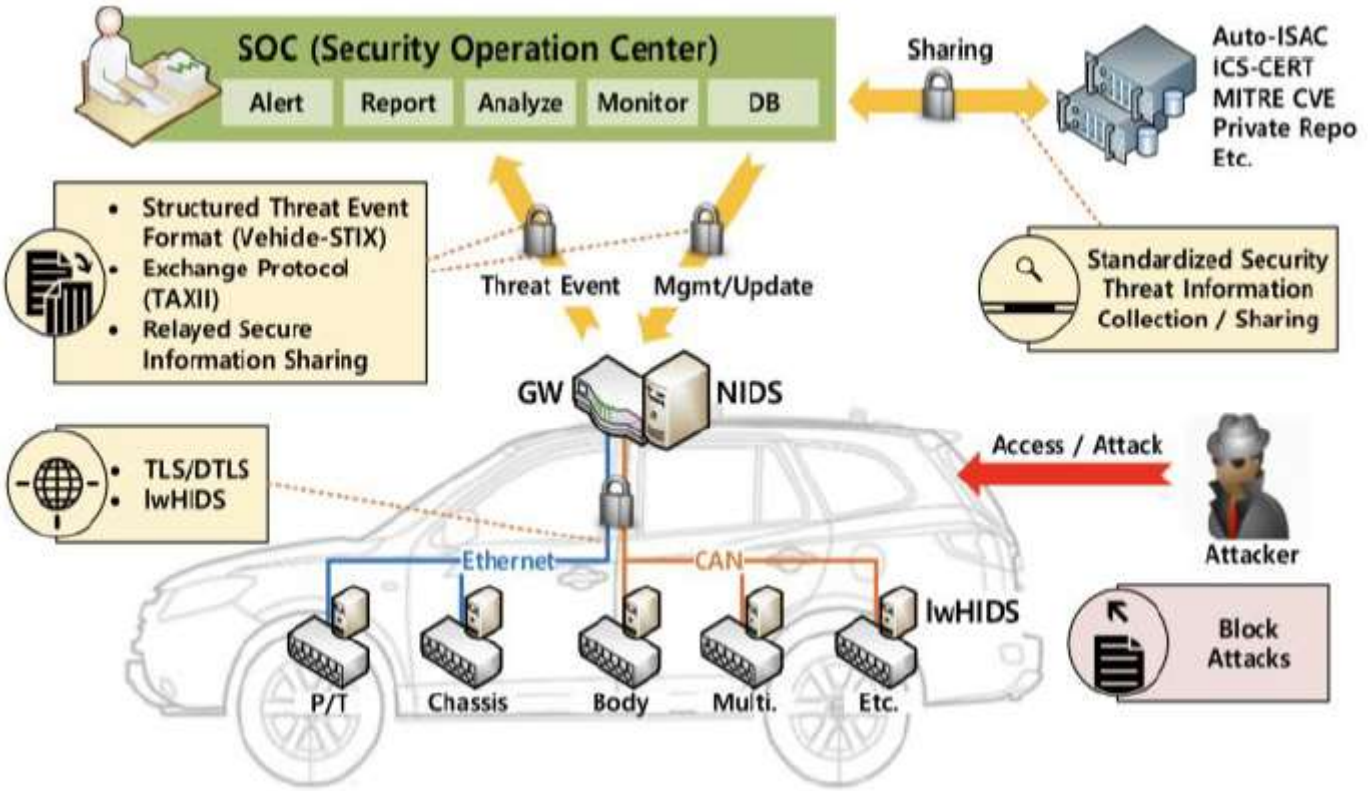
IDS & Surveillance

IDS

- N-IDS (Network IDS)
- H-IDS (Host IDS)

Surveillance (보안 관제)

- STIX/TAXII
- 관제 시스템간의 연동

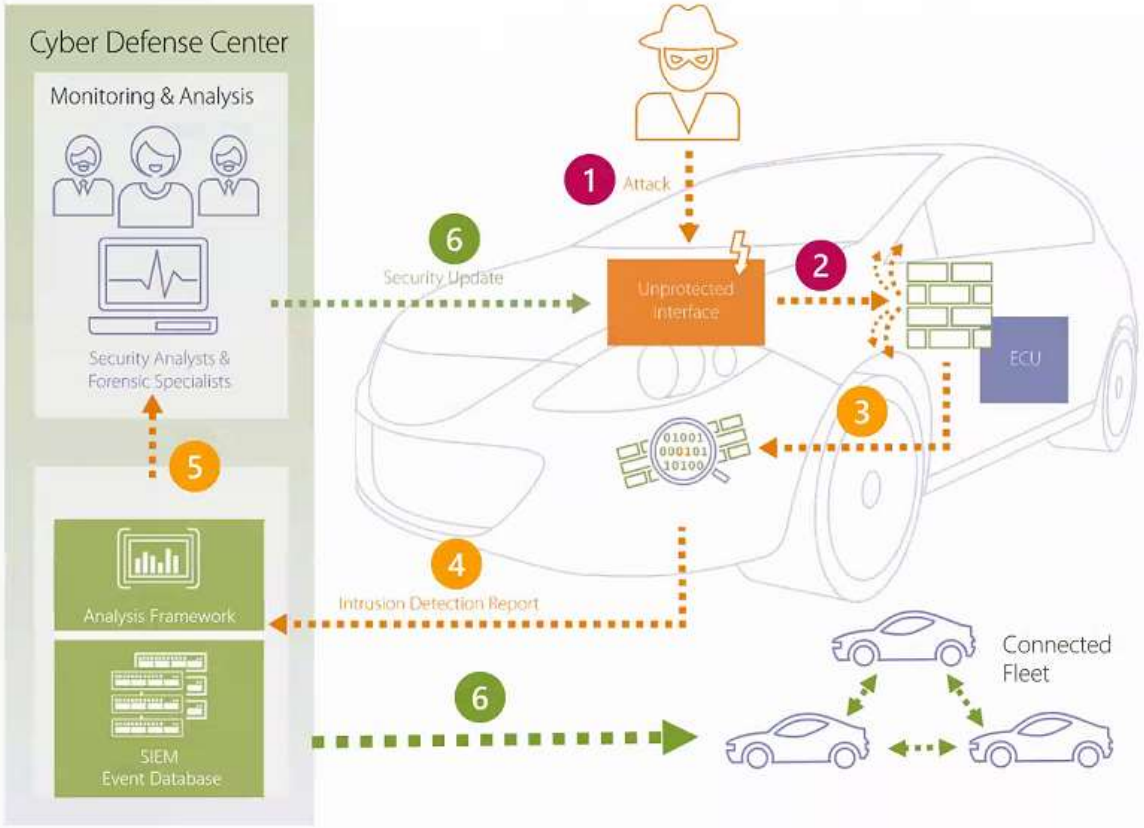


커넥티드 카 환경에서의 차량 보안 위협 정보 공유 시스템, KCC 2019.

How to Secure Automotive Ethernet

Intrusion Detection System
Full system overview

escrypt
SECURITY. TRUST. SUCCESS.



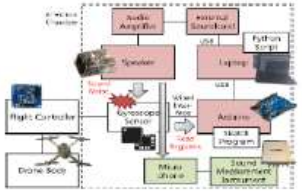
1. **Attack:** Misuse of 0-day exploit in web browser
2. **Security is not absolute:** The OEM's secure flashing implementation was vulnerable and the attacker was able to flash and run arbitrary code, e.g., in order to send malicious signals.
3. **Firewall:** The filtering mechanisms blocks illegitimate signals, e.g, from an invalid source, and informs the IDS. The attacker is not able to control other ECUs.
4. **Intrusion Detection:** The in-vehicle IDPS solution detects the anomaly (i.e., potential attack) on the in-vehicle network, it creates and sends an Intrusion Detection Report
5. **Monitoring & Analysis:** The IDPS backend collects all anomaly reports from the vehicle fleet and enables security analysts and forensic specialist to analyze the attack and identify the vulnerability
6. **Intrusion Prevention:** A security update to remedy the vulnerability will be deployed to the entire vehicle fleet

Attack & Malware

In-Vehicle Network Attack
(DEFCON, SBS), 2015

텔레매틱스 기기의 취약점을
이용한 원거리 공격

Sensor Jamming
(USENIX Security), 2015



드론 내 자이로 센서 공격

Sensor Fault Accident
(ABC News), 2016

TESLA 차량의 카메라센서
오작동으로 인한 사망사고

Sensor Spoofing
(DEFCON), 2017

TELSA 차량의
레이다 센서
스푸핑 공격

SW Fault Accident
(CNN), 2018

우버 자율주행 차량의
보행자 사망사고

Sensor Fault Accident
(ABC News), 2018

구글 Waymo
자율주행
차량 교통사고

Sensor Fault Accident,
2019

TESLA 차량의 카메라센서
오작동으로 인한 사망사고

자동차 보안 기술, 김휘강, KRnet2019

Q & A

http://mesl.khu.ac.kr