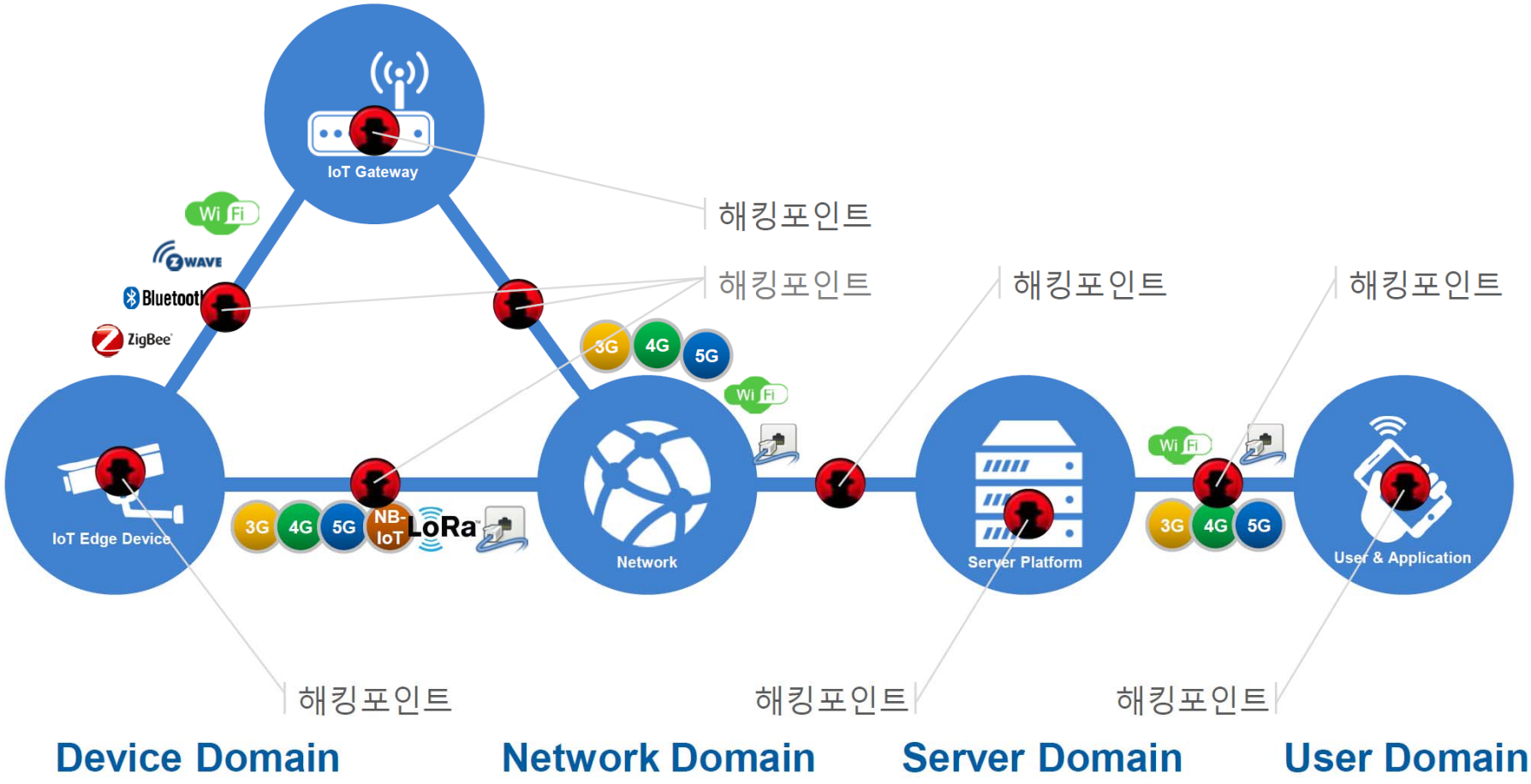
IoT 디바이스 보안

조 진 성
경희대학교 컴퓨터공학과
Mobile & Embedded System Lab.

IoT 보안 취약 지점



INITECH 이주화, KRnet 2017

IoT 보안의 취약성

▣ 보안에 대한 인식과 우려

- ⊙ IoT **보안과 관련한 조사 결과, 응답자의** 2/3 **이 보안에 대해 우려** *(SANS Institute)*
  - ■ **응답자의** 17.2% **는** IoT**가 보안에 취약하여 거의 재앙 수준이 될 것이라 우려**

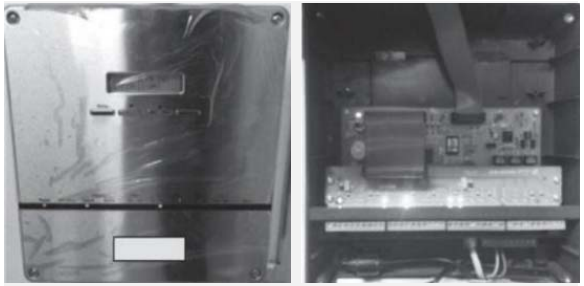
- ⊙ **가전제품 및 기타 디바이스가 인터넷으로 연결된 홈 네트워크 서비스에 대한 조사 결과, 약** 70%**의 응답자가 프라이버시 문제에 대해 우려하고 있다고 응답** *(Fortinet)*

▣ 보안을 배제하고는 IoT의 상용화 성공이 어려움

- ⊙ **지속적인 위협 인식과 연구가 필요**

2015년 07월

Firmware Replace Attack**을 통해** Chrysler **차량의 제어권 탈취** (2015.08, WSOCTV)



2014년 05월

냉난방 관리 셋톱박스와 보안업체 장비가 DDoS **공격에 악용되어,** A**게임사 유럽지사 게임에 공격 수행** (2014.05, ETNEWS)

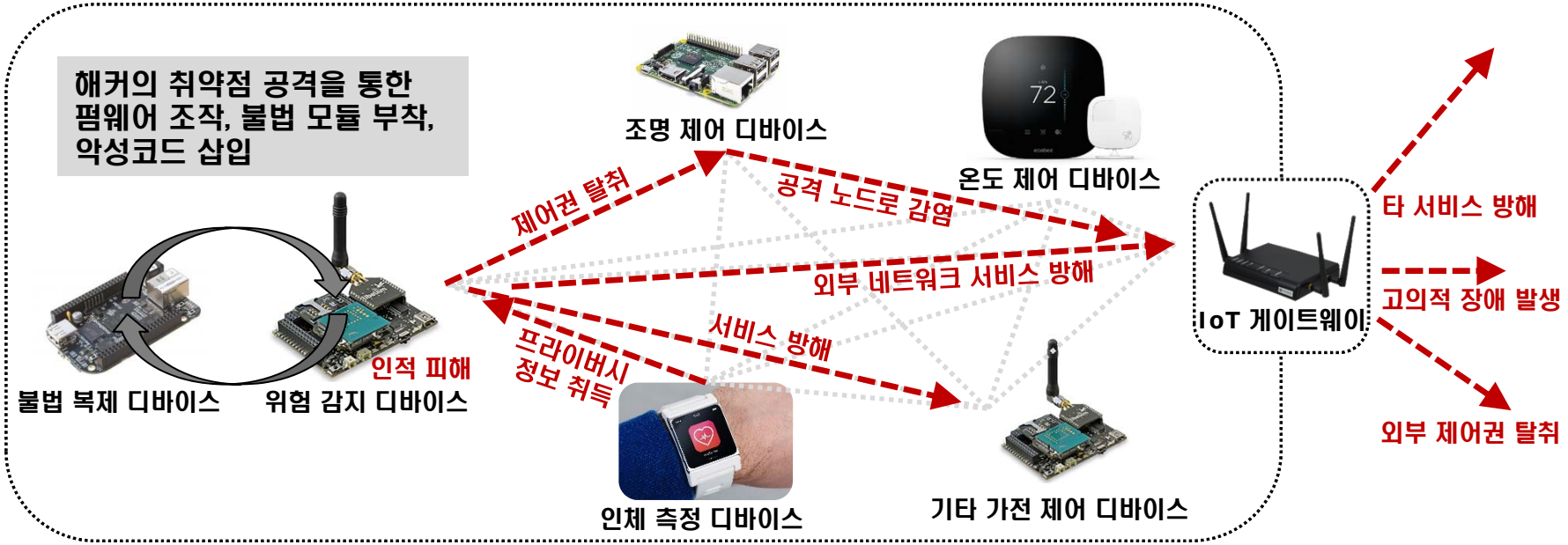
2014년 01월

약 10**만개의 가전제품 (냉장고,** PC**, 라우터, 스마트** TV**) 이 대량의 스팸 메일 살포에 악용** (2014.01, Proofpoint)

IoT 보안의 취약성

IoT 보안 위협의 증가

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



Internet of Broken Things

- Open source HW 및 SW 활용 가능성 증대
- 플랫폼/서비스의 상호 운용 증대

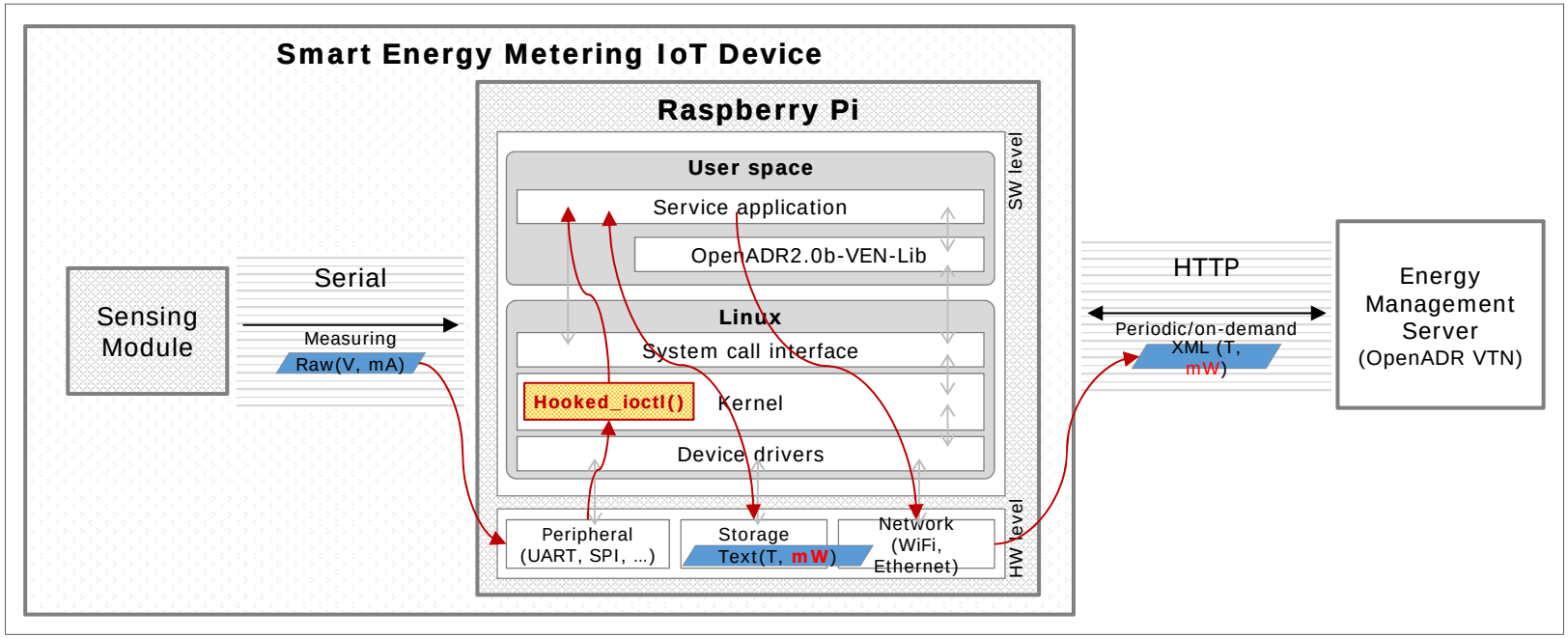
→ 많은 요소 기술들의 통합으로 보안 취약성이 높음

가상 IoT 디바이스 모의 해킹

▣ Smart Meter/Plug 디바이스 모의 해킹 (1)

⊙ Raspberry Pi 기반 Smart Meter IoT 디바이스 모의 해킹

■ 해킹된 smart metering 디바이스의 동작



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

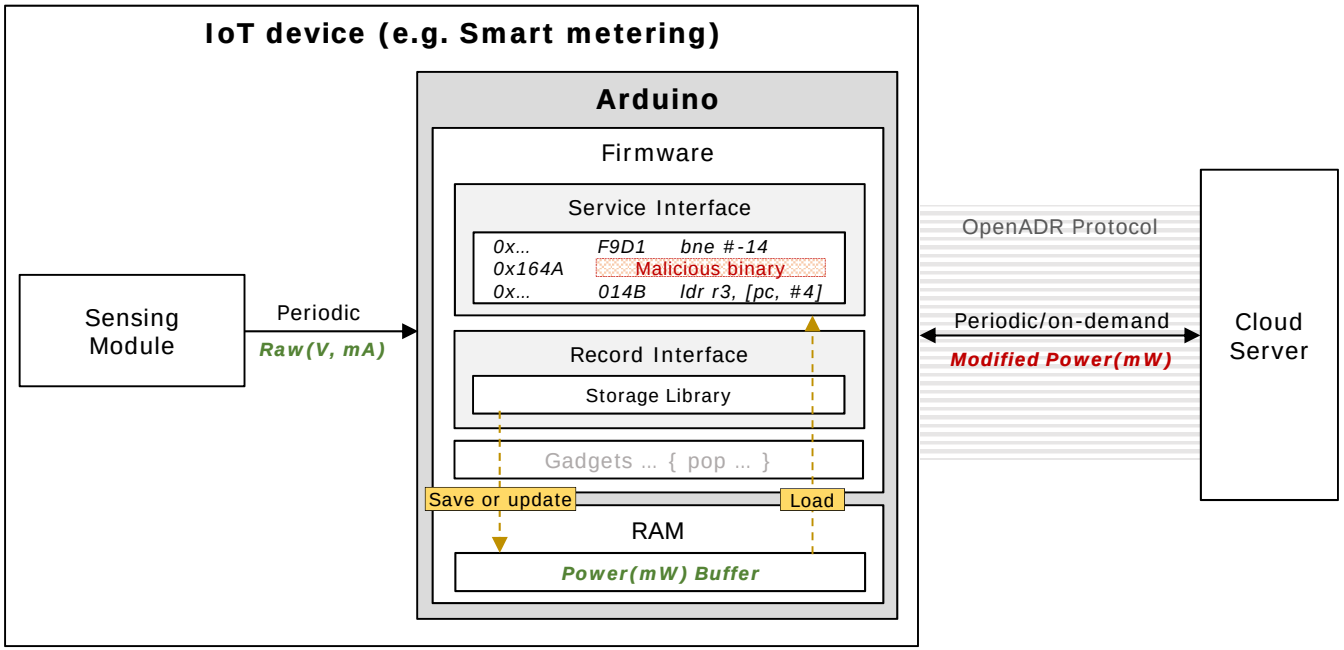
가상 IoT 디바이스 모의 해킹

▣ Smart Meter/Plug 디바이스 모의 해킹 (2)

⊙ Arduino 기반 Smart Meter IoT 디바이스 모의 해킹

■ 해킹된 smart metering 디바이스의 동작

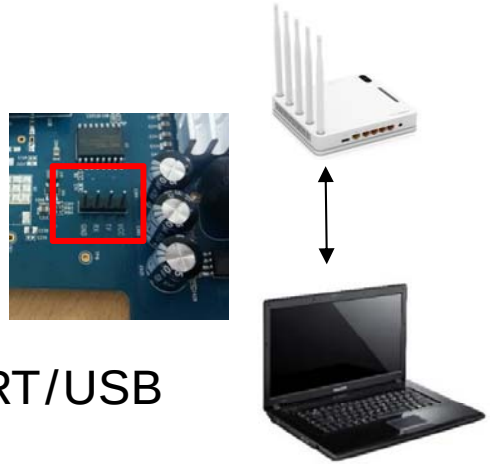
- 기존 대비 80% 감소된 평균 전력 소모량을 서버에 전송
- 디바이스 Reset에도 변조된 펌웨어 바이너리는 지속적으로 존재



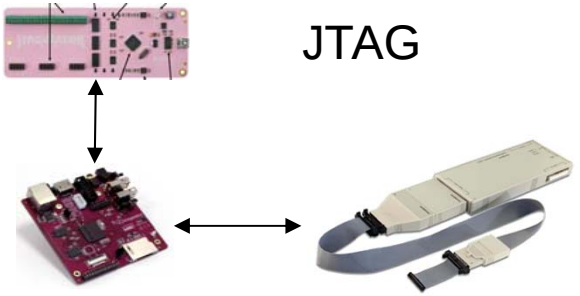
⊙ 동영상 데모 (https://youtu.be/egZ9bOUYUcc)

상용 IoT 디바이스 모의 해킹

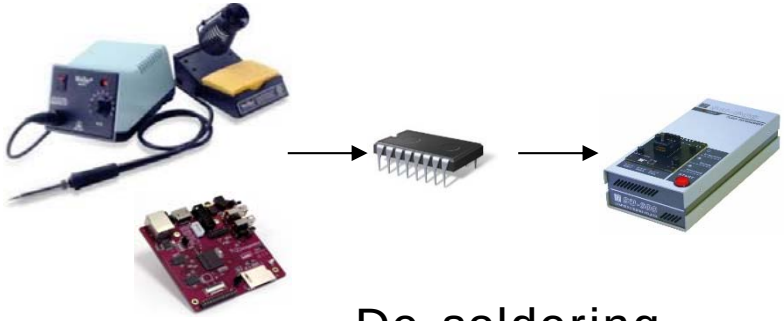
❖ IoT 디바이스 펌웨어 추출



UART/USB



JTAG

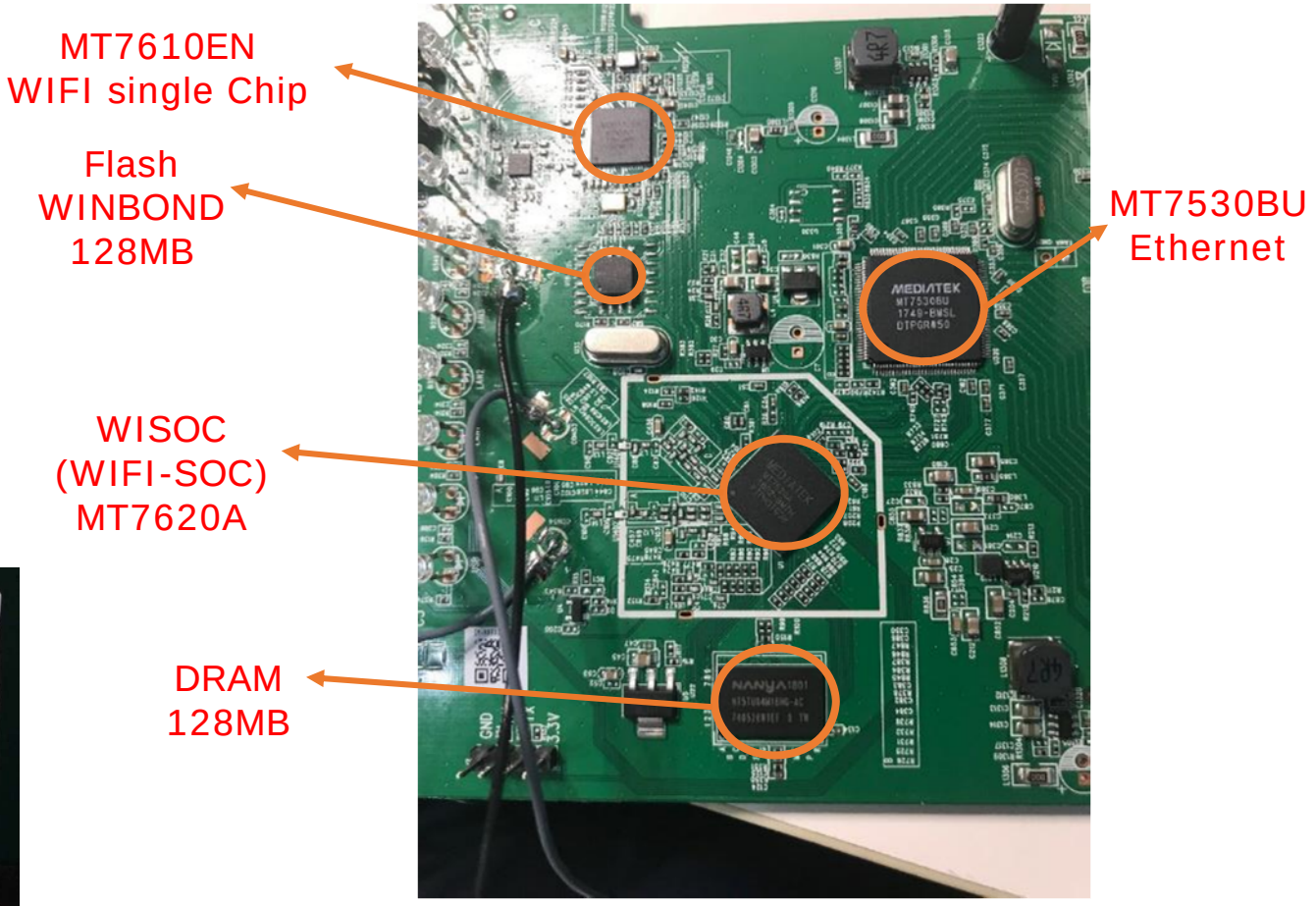


De-soldering

FW update file

상용 IoT 디바이스 모의 해킹

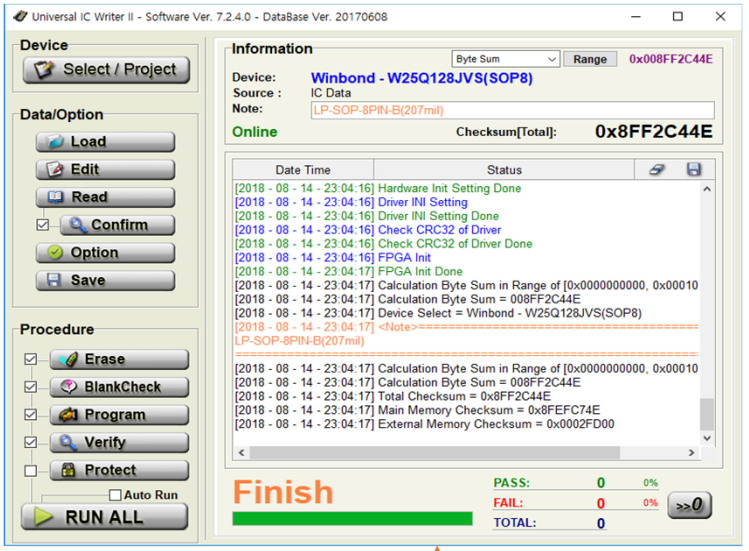
- **ipTIME A1004ns**
  - MIPS

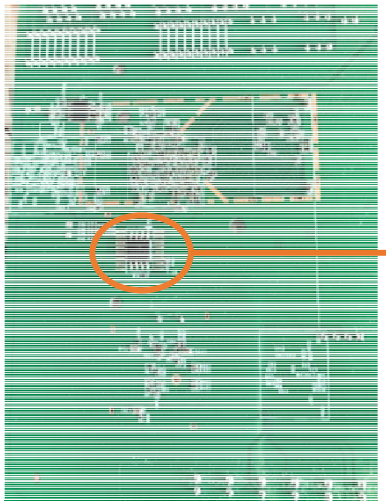


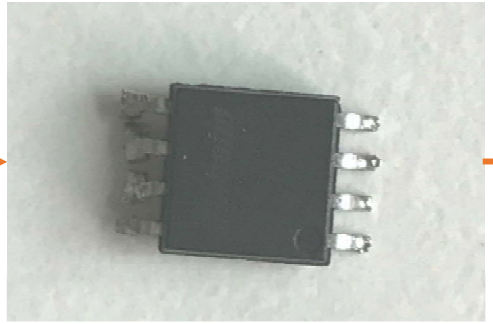
상용 IoT 디바이스 모의 해킹

▣ ipTIME A1004ns

⊙ 펌웨어 추출 (De-soldering)





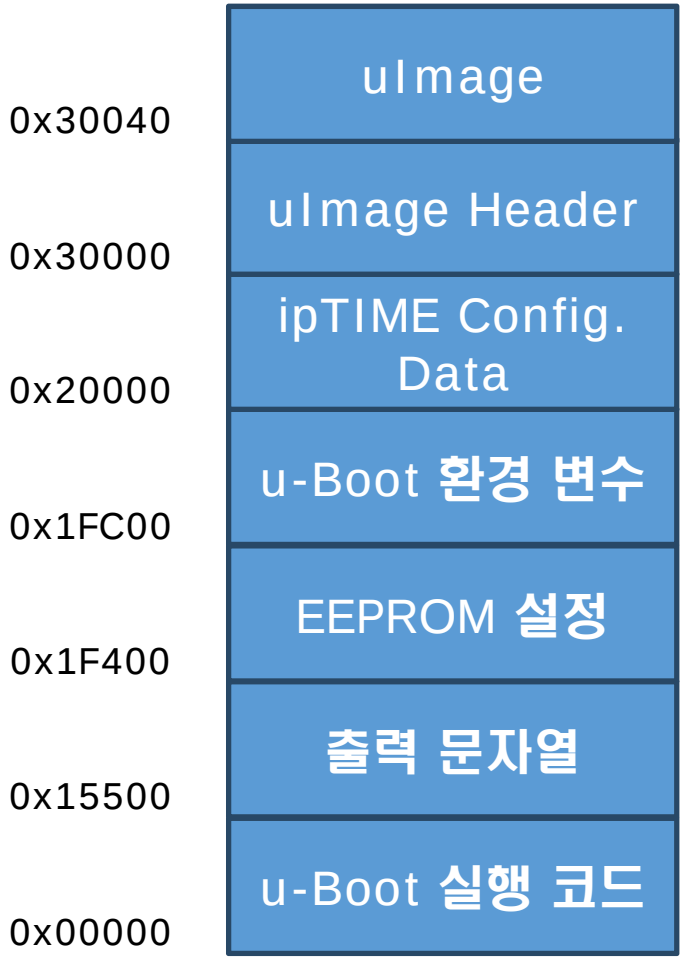


LEAPER-56
[FLASH 리더기]

상용 IoT 디바이스 모의 해킹

ipTIME A1004ns

- 펌웨어 구조 vs. 펌웨어 업데이트 파일(Linux kernel+RFS)




```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xC7AD8CC1, created:
2018-07-11 09:35:03, image size: 13708380 bytes, Data Address: 0x80000000, Entry Point: 0x8000C150, d
ata CRC: 0x4F752804, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image
 name: "a1004ns"
64            0x40            LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes
, uncompressed size: 6636764 bytes
2182300       0x214C9C        Squashfs filesystem, little endian, version 4.0, compression:xz, size:
11525506 bytes, 1632 inodes, blocksize: 131072 bytes, created: 2018-07-11 09:34:58
```

[펌웨어 업데이트 파일]

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
196608        0x30000         uImage header, header size: 64 bytes, header CRC: 0xC7AD8CC1, created: 2018-
07-11 09:35:03, image size: 13708380 bytes, Data Address: 0x80000000, Entry Point: 0x8000C150, data CRC: 0
x4F752804, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "a1004ns
"
196672        0x30040         LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, unc
ompressed size: 6636764 bytes
2378908       0x244C9C        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 11525
506 bytes, 1632 inodes, blocksize: 131072 bytes, created: 2018-07-11 09:34:58
```

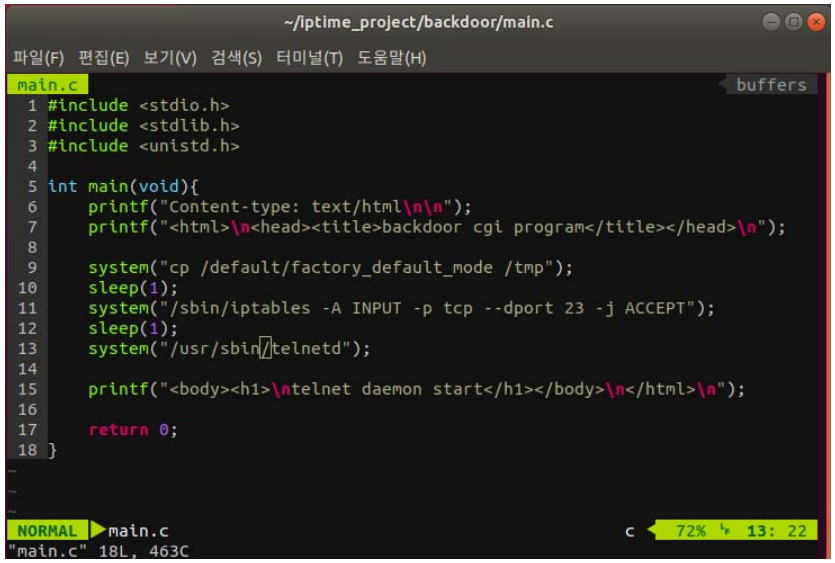
[추출된 펌웨어]

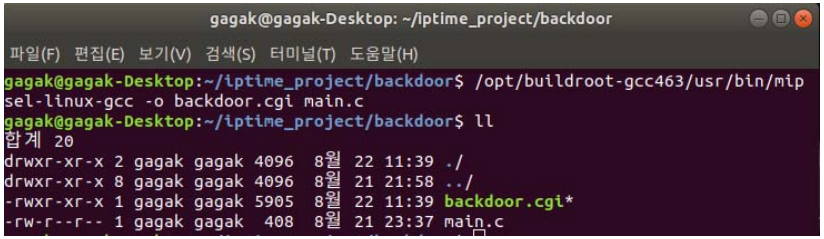
상용 IoT 디바이스 모의 해킹

▣ ipTIME A1004ns

⊙ 백도어 프로그램 작성

- 기존 ipTIME 펌웨어 내에 존재하는 telnetd 이용
- ipTIME에서 제공하는 toolchain을 이용하여 backdoor CGI build



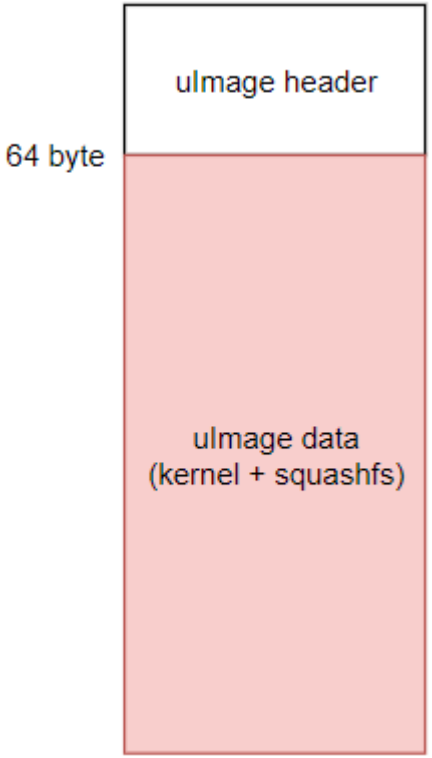


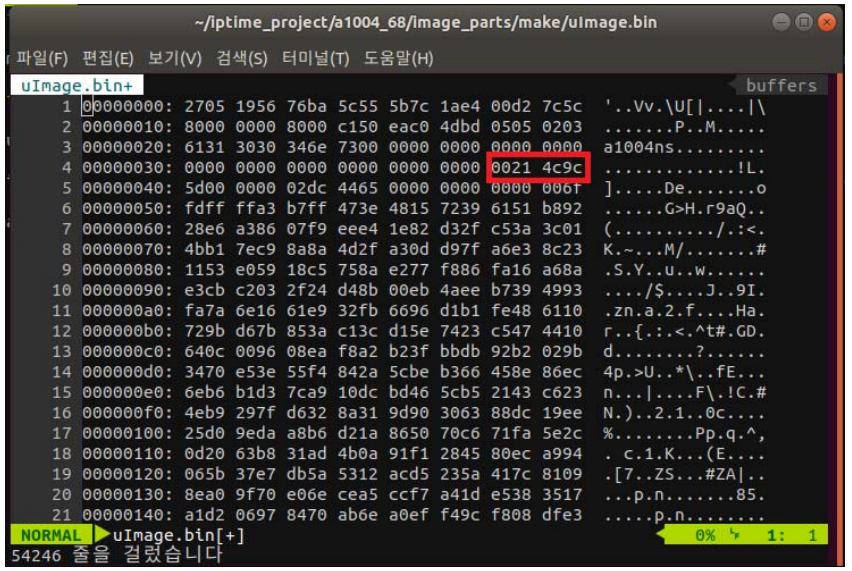
상용 IoT 디바이스 모의 해킹

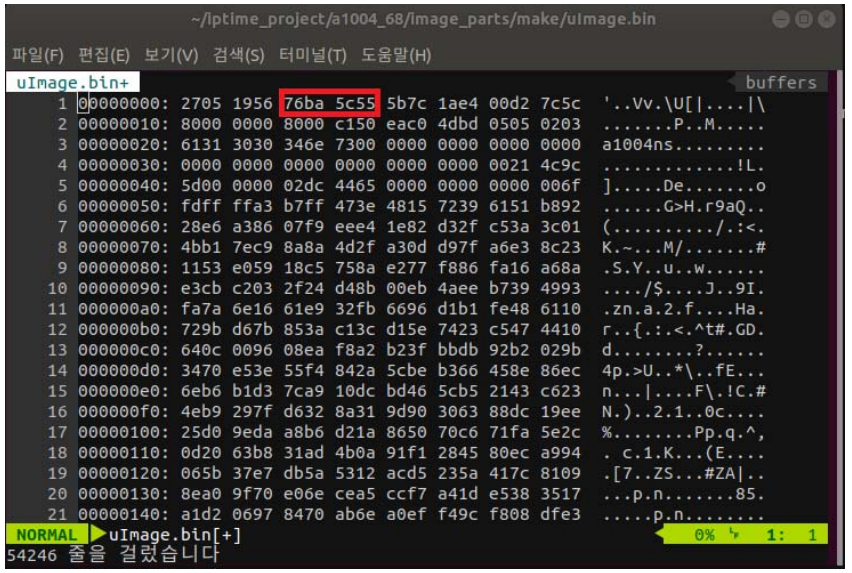
ipTIME A1004ns

펌웨어 업데이트 파일 생성

- uImage data 생성
- uImage header 수정



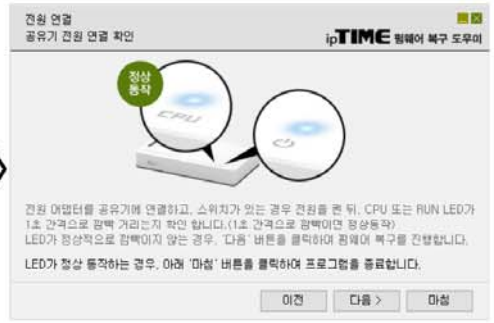


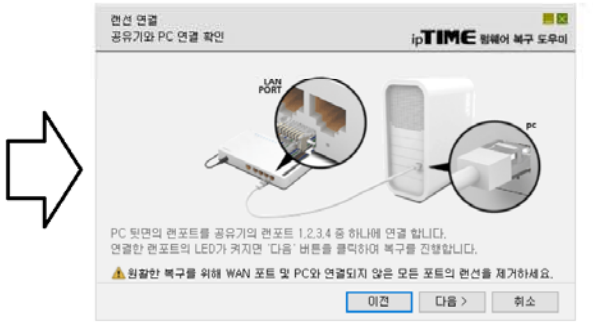


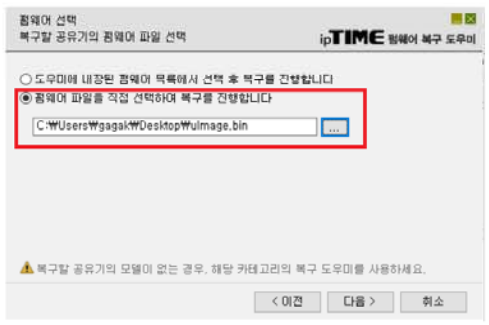
상용 IoT 디바이스 모의 해킹

▣ ipTIME A1004ns

⊙ 펌웨어 업데이트 파일을 통한 업데이트



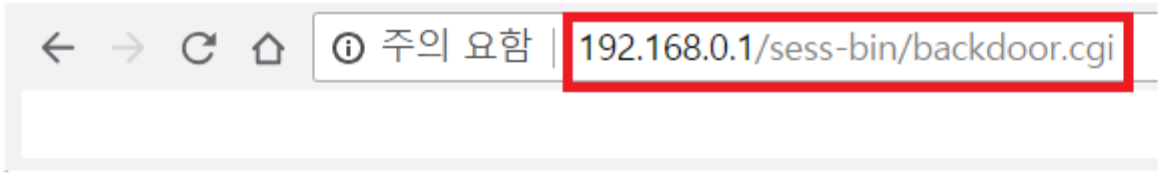




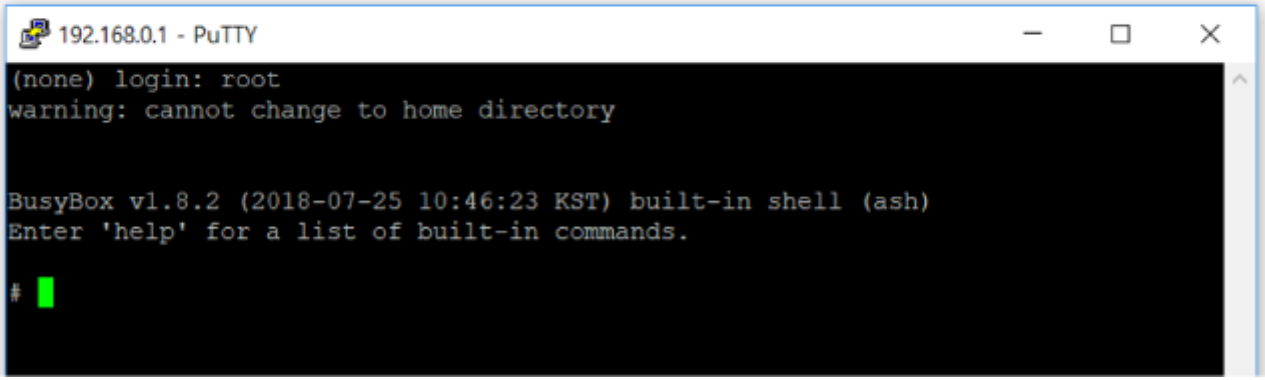
상용 IoT 디바이스 모의 해킹

ipTIME A1004ns

- 백도어를 통한 telnet 원격 접속
- backdoor.cgi 실행



telnet daemon start

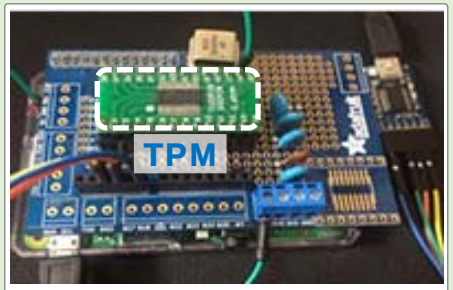


IoT 디바이스 보안 플랫폼의 필요성

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

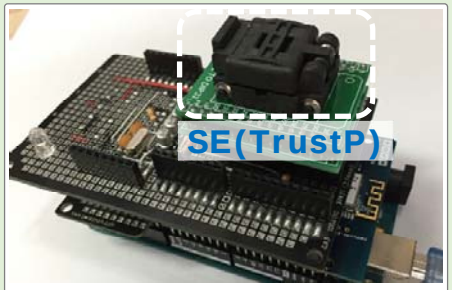
IoT 디바이스 보안 플랫폼 (MESL@KHU)

Secure Platforms for IoT Devices



Secure Pi
(Secure Raspberry Pi)

TPM



SArduino
(Secure Arduino)

SE

iS4IoT
(integrated Security for IoT device)

iSE

KHU-TEE
(ARM PSA TrustZone-m)

TEE

IoT 디바이스 보안 요소기술

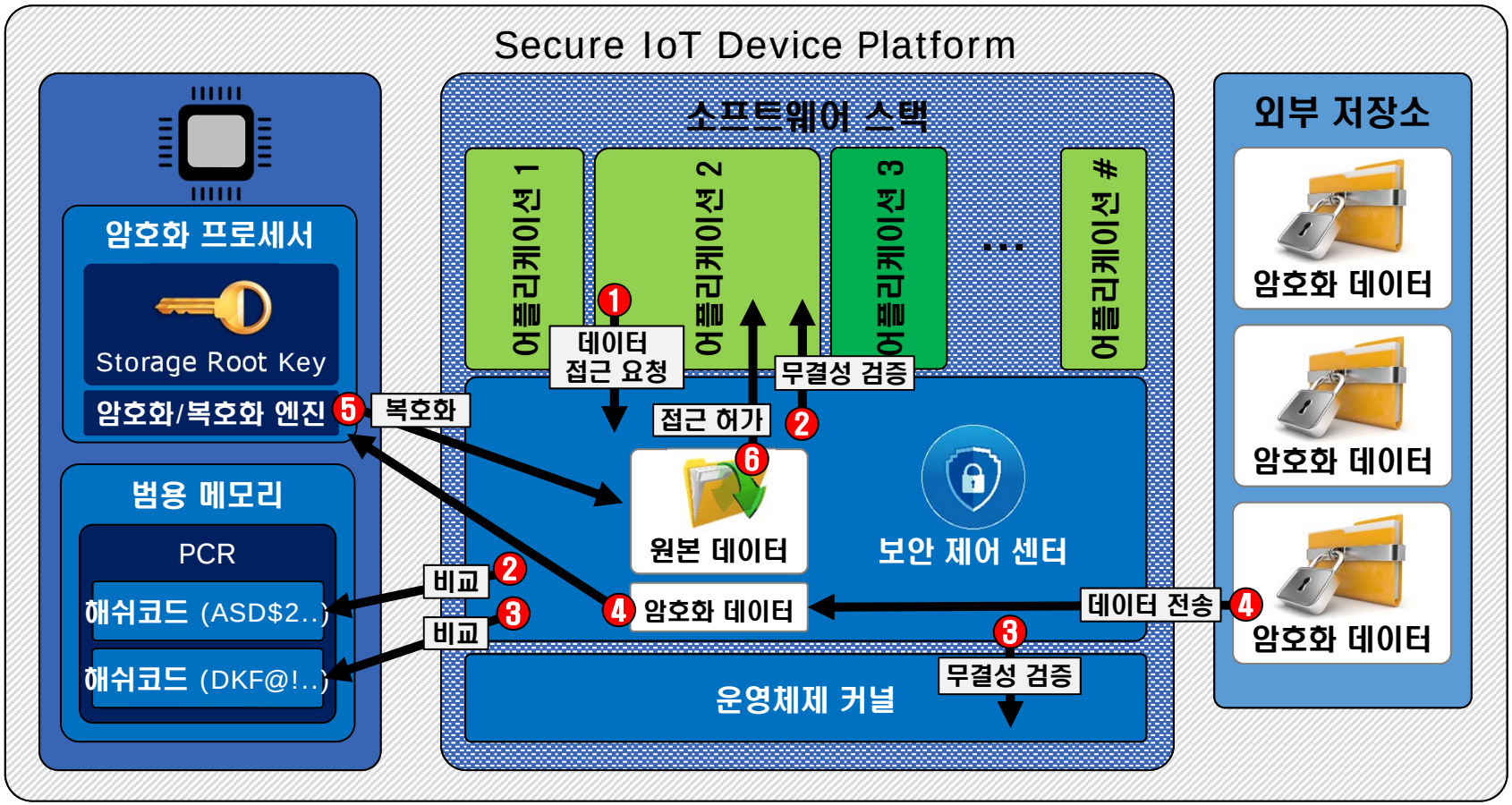
SECURE
플랫폼

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

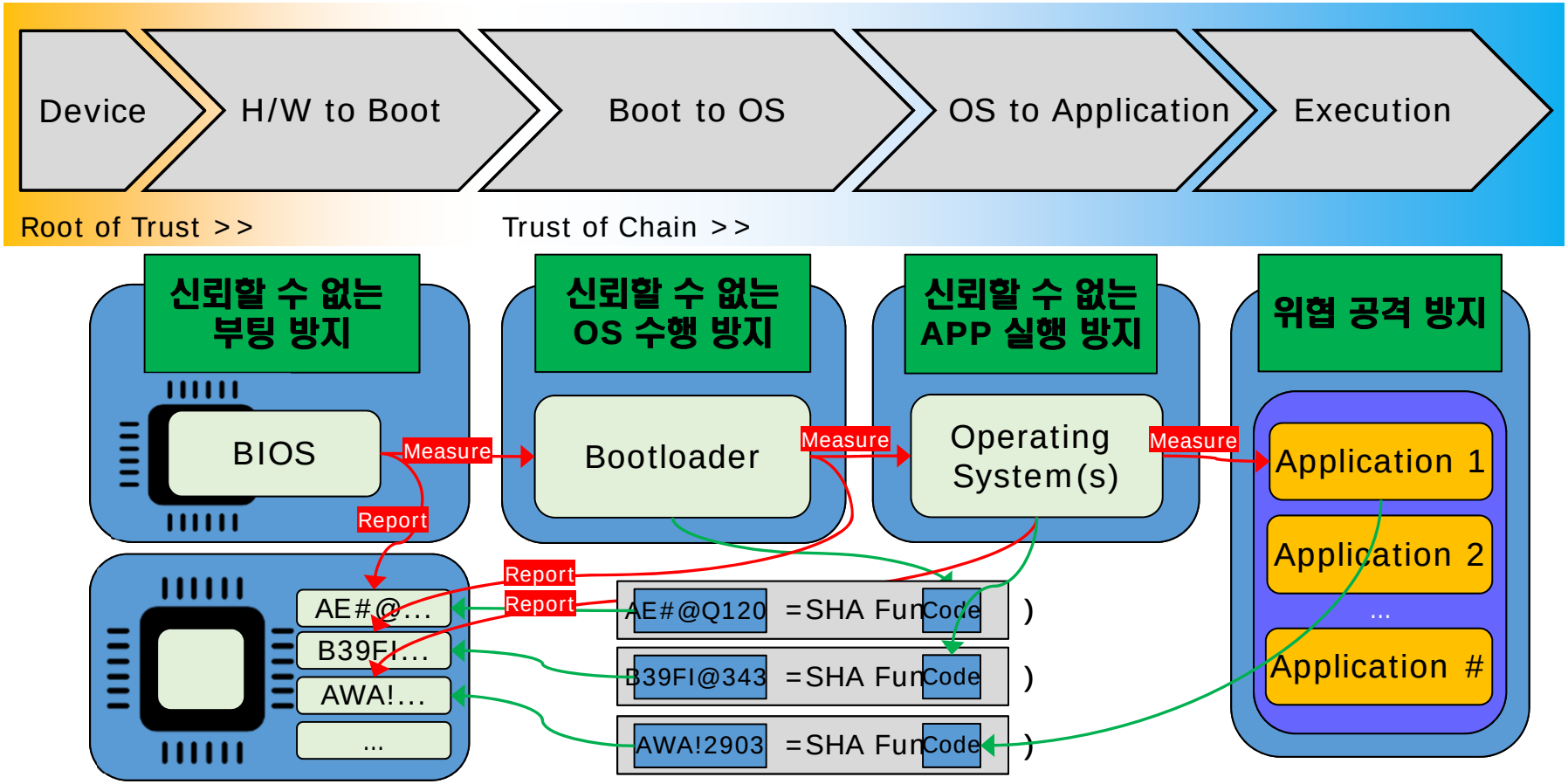
IoT 디바이스 보안 요소기술

▣ Secure Key Storage & Management

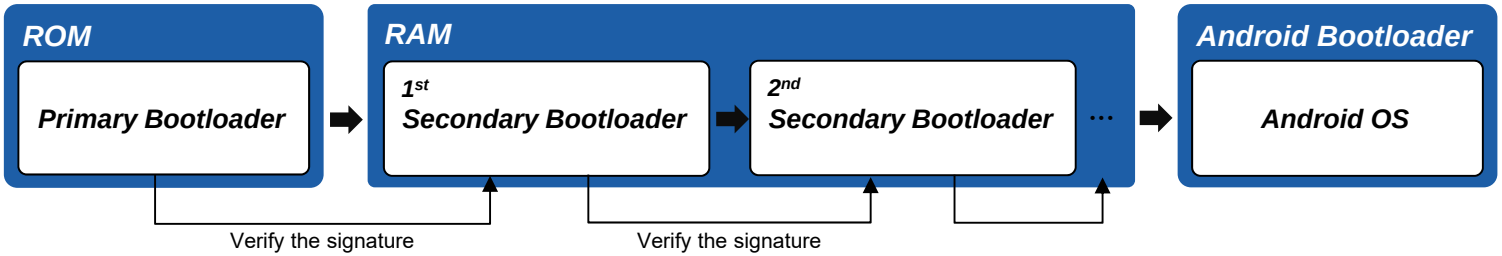


IoT 디바이스 보안 요소기술

Secure Boot



Secure Boot

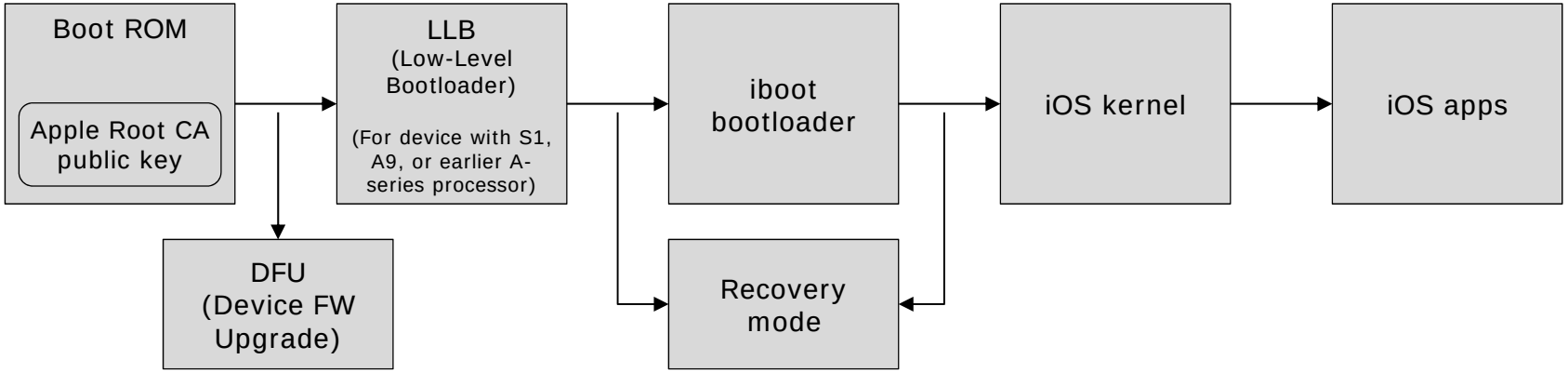


Hardware Roots of Trust

- Device-Unique Hardware Key (DUHK)
  - device-unique symmetric key
  - HW**모듈만 접근 가능**
- Samsung Secure Boot Key (SSBK)
  - **삼성** public key
  - Secure Boot**에서 사용**
- Device Root Key (DRK)
  - device-unique asymmetric key
  - TIMA Trusted Boot**에서 사용**

Apple iOS Security

Secure Boot



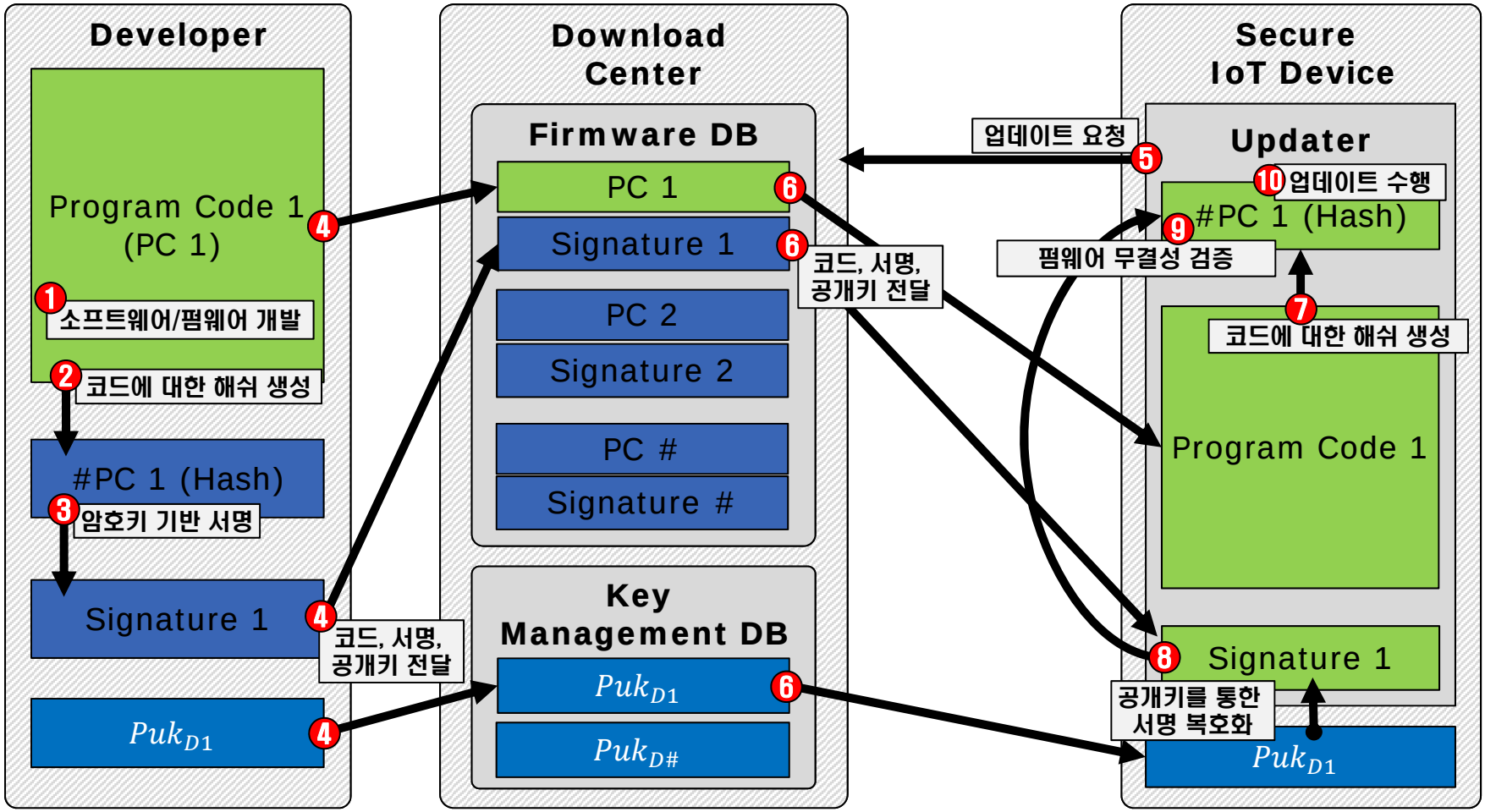
System Software Authorization

- TIMA Attestation과 유사

Hardware Roots of Trust

- Apple Root CA public key
  - Secure Boot에서 사용

Secure Firmware Update

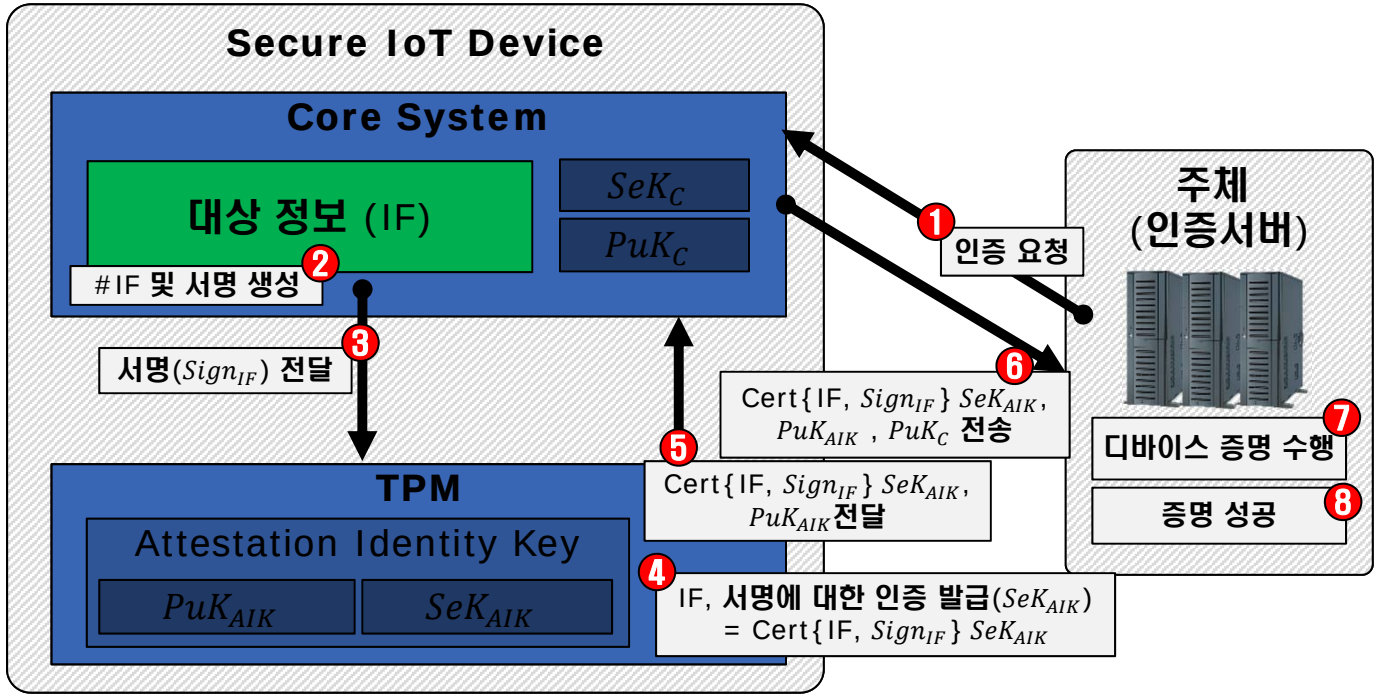


IoT 디바이스 보안 요소기술

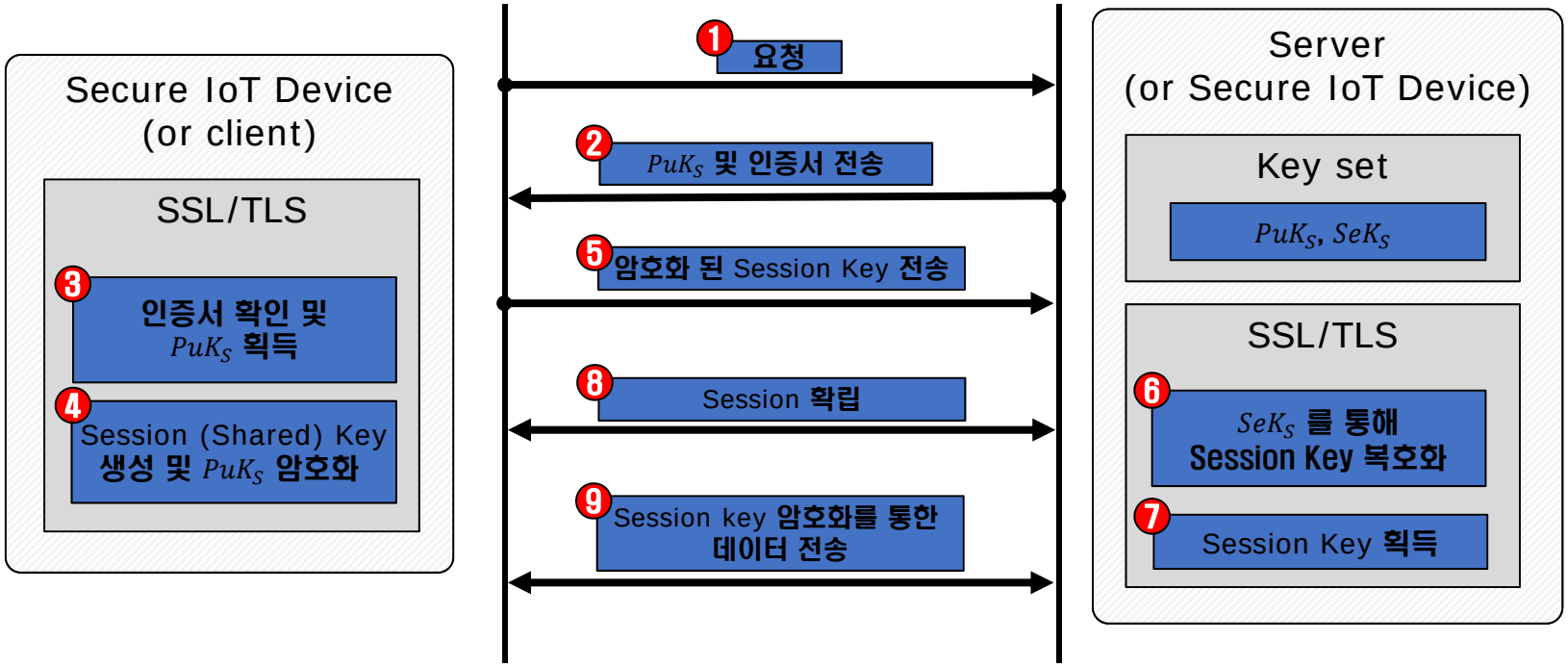
▣ Remote Attestation

⊙ 디바이스의 각종 정보/상태들의 무결성을 인증

- 실행 중인 S/W 정보
- 디바이스 상태 정보
- 기타 인증과 관련된 정보

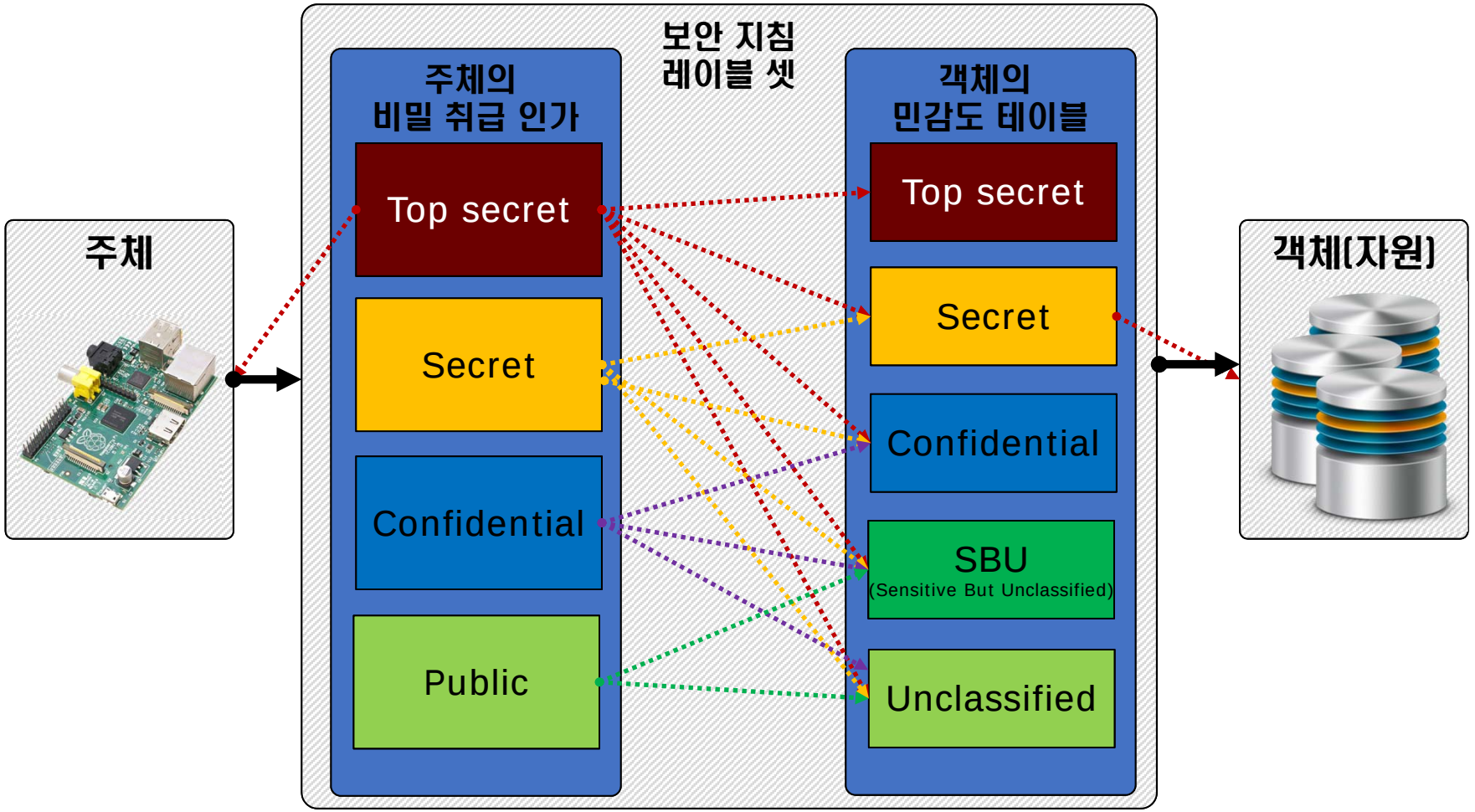


Secure Communication

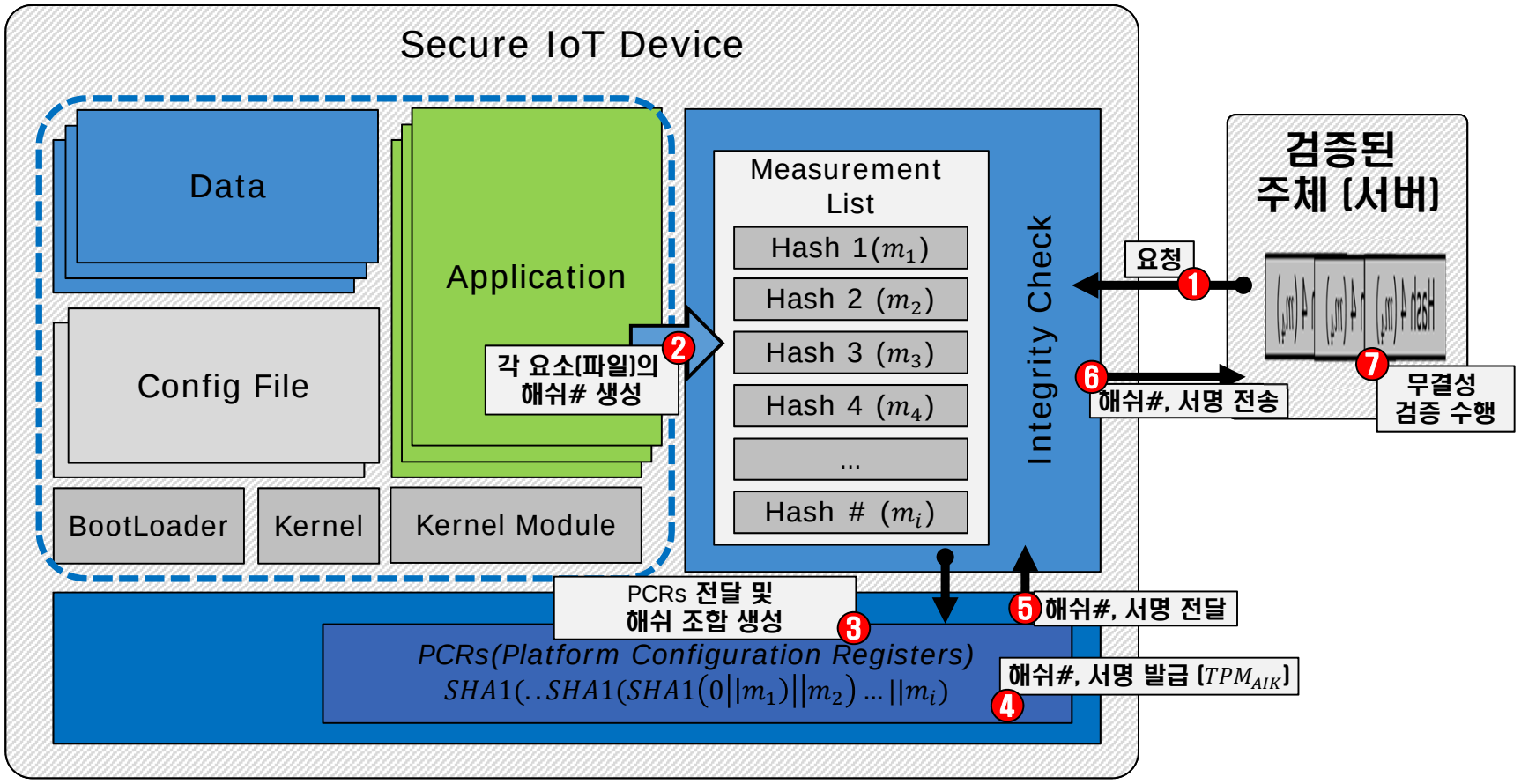


IoT 디바이스 보안 요소기술

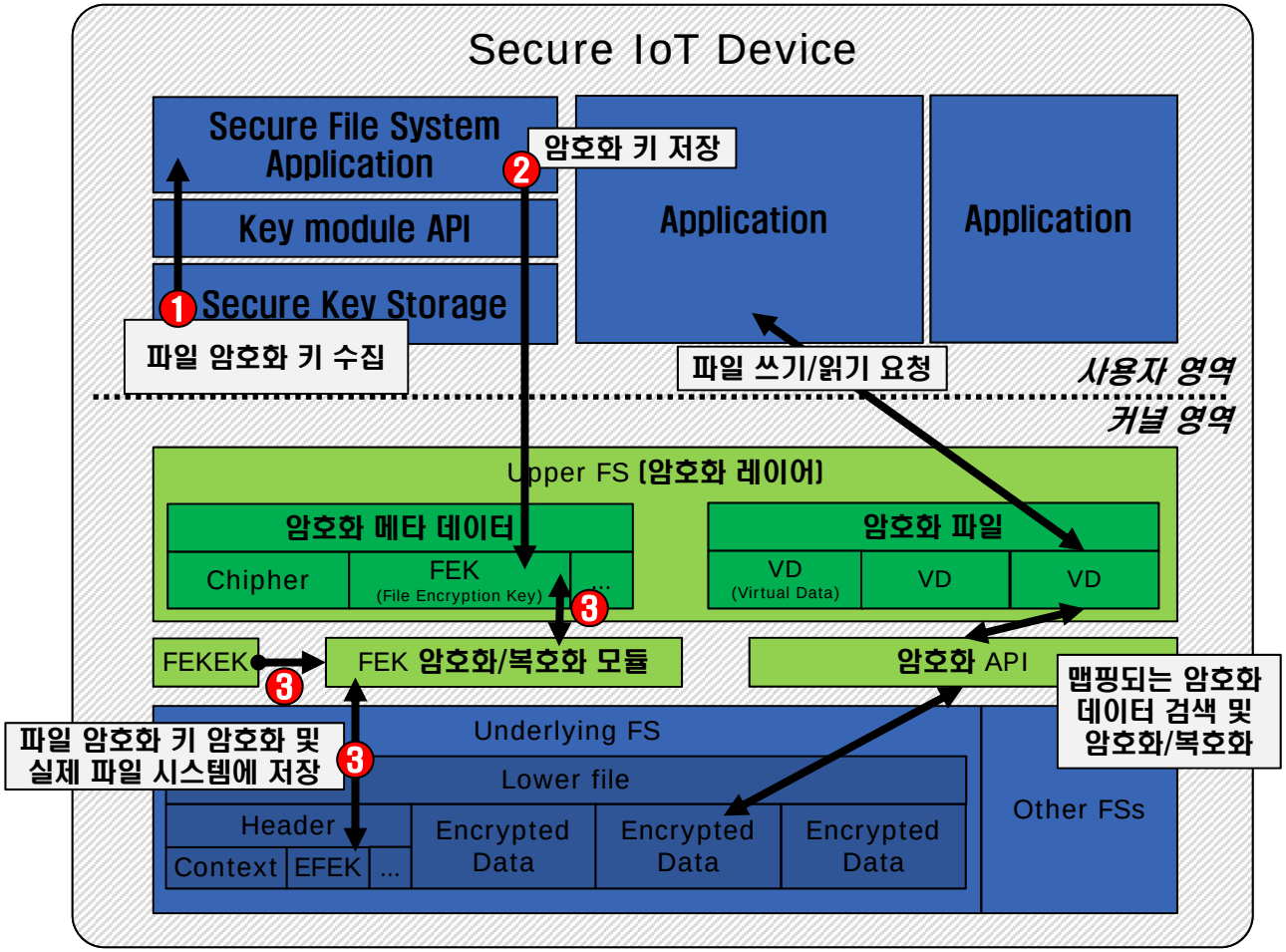
- Mandatory Access Control (MAC)



File(system) Integrity



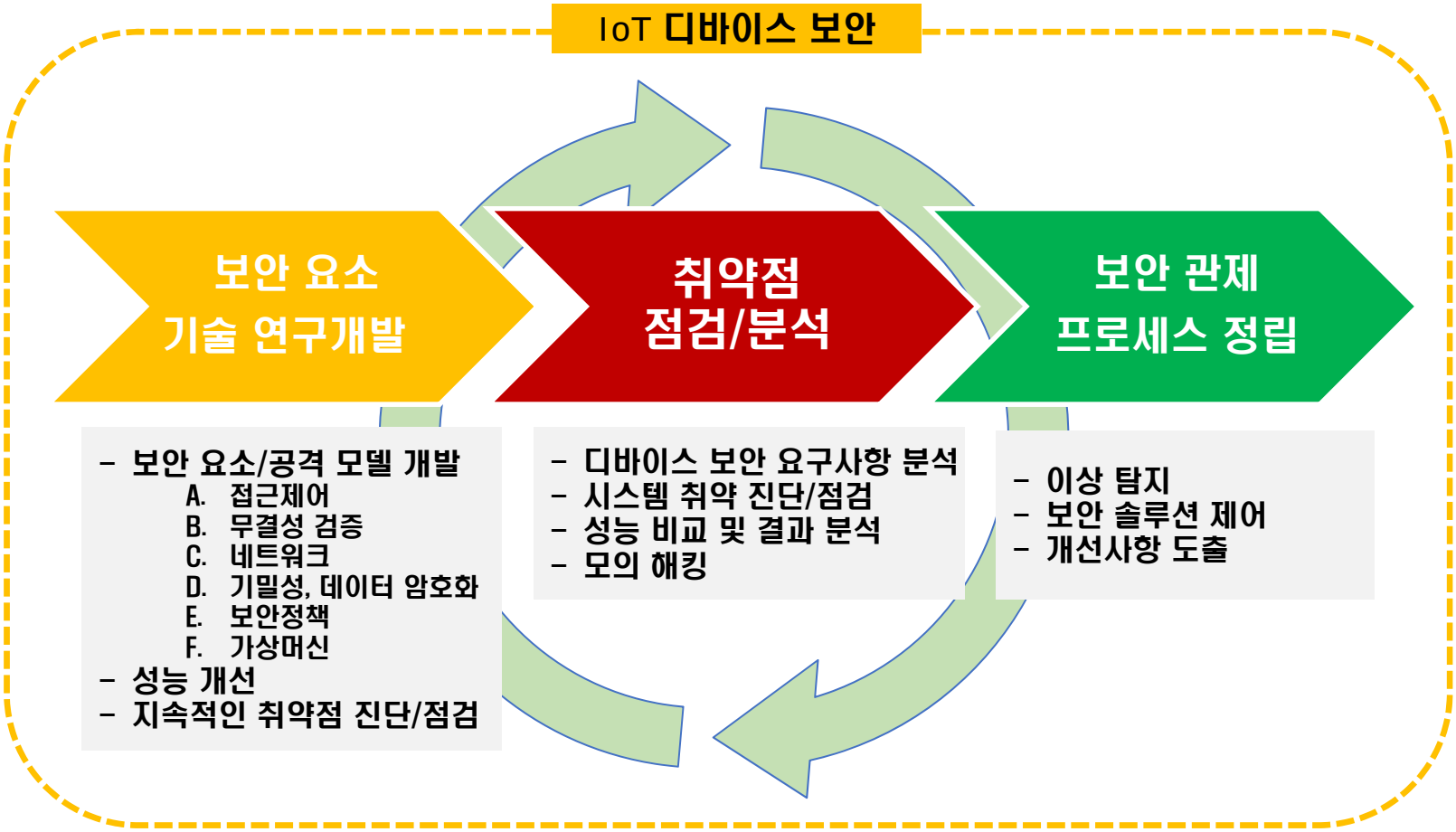
File(system) Encryption



IoT 보안 관제 및 취약점 분석

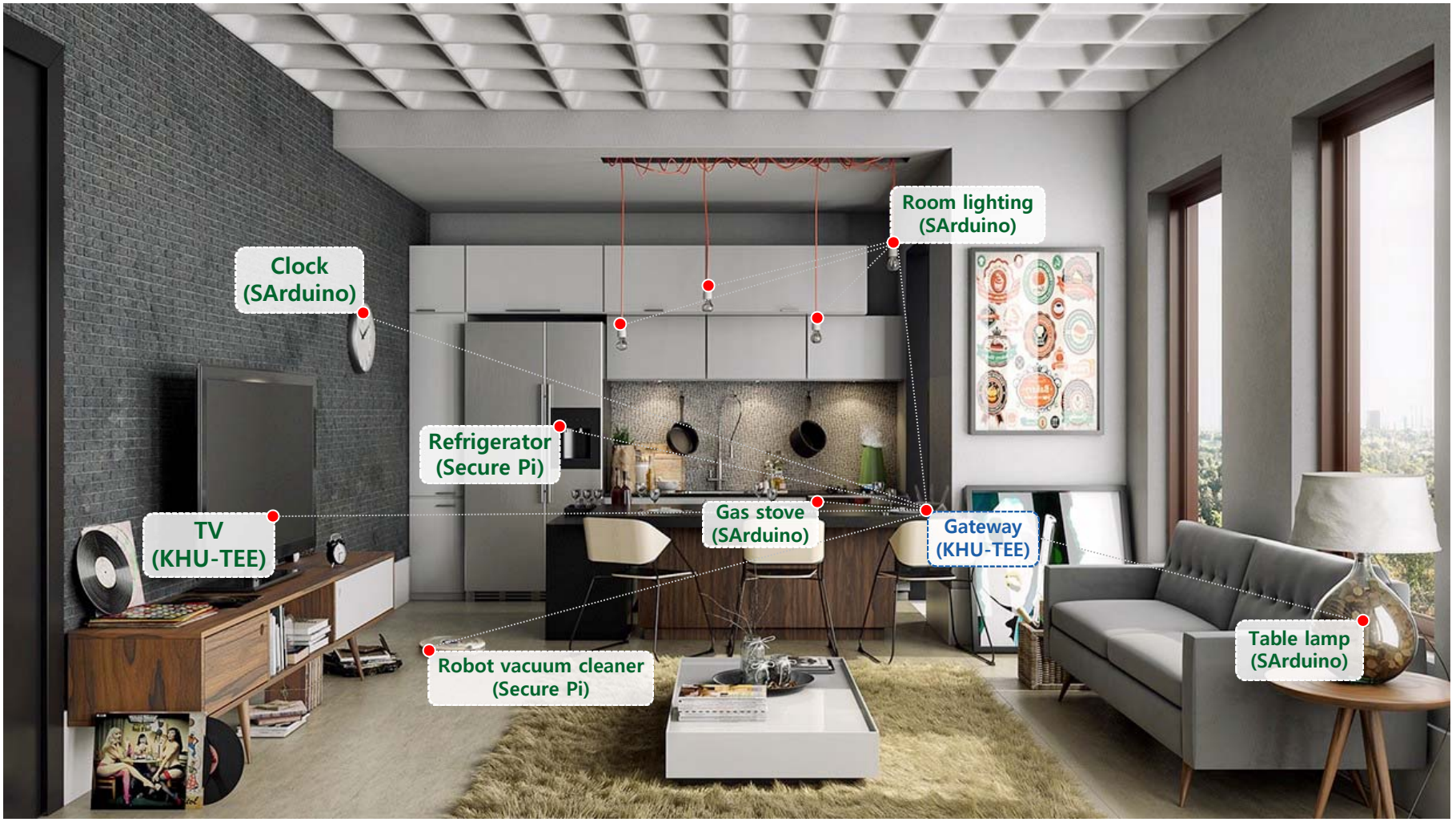
▣ IoT 디바이스 및 서비스 보안 문제의 대응

⊙ 취약점, 다양한 공격 유형 분석을 통한 보안 관제 프로세스의 정립



IoT 디바이스 보안을 위한 신뢰 플랫폼 활용

▣ Secure Pi / SArduino / iS4IoT / KHU-TEE



IoT 디바이스 보안을 위한 신뢰 플랫폼 활용

iS4IoT / KHU-TEE / KHU-TEE+SE

Secure SSD

- 디바이스 고유 키를 통한 데이터의 안전한 백업 및 불법 복제 방지
- 사용자 권한 별 암호화 키 기반 따른 파티션/파일 접근 제어
- 자체 인증서(Certificate)을 통한 각 파티션 유효성 보장
- 파티션 무결성 보호 기술을 통해 파일 시스템 변조 방지

Secure SSD

자동차 전장부품 (예: ADAS, Advanced Driving Assistance System)

- 전자 제어 장치 고유의 인증 키를 통해 외부의 불법 접근을 제한
- Secure Boot를 통해 네트워킹이 가능한 차량 내 제어 시스템의 무결성 보장

Connected Car

IoT 블록체인

- 평문으로 보관되는 디바이스의 정보를 안전하게 보관
- 무결성 검증 시 연결된 디바이스를 순서대로 확인하는 시간을 디바이스 인증을 통해 단축
- 디바이스를 통한 자동 물품 구매 시 안전한 결제 제공

IoT Blockchain

Q & A

http://mesl.khu.ac.kr