IoT 해킹 취약점과 보안 구현 방안

THE TRUST BEYOND
THE SECURITY

보안, 그 이상의 믿음

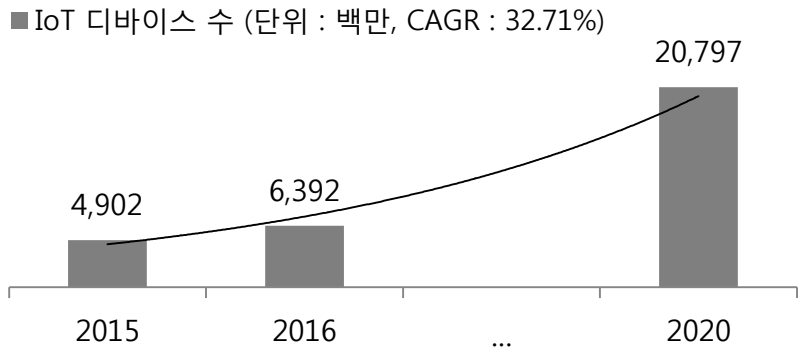
SK infosec

CONTENTS

SK infosec

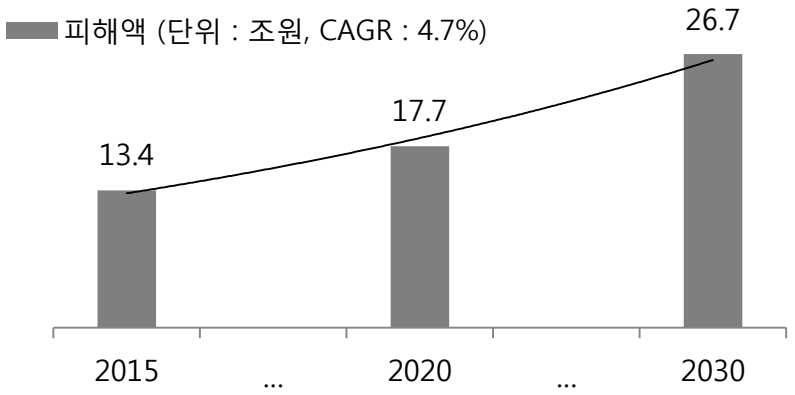
1. IoT 보안 위협의 증가

- **IoT 디바이스의 급격한 증가**
  - 2016년 64억 개, 2020년 200억 개 이상 (Gartner, 2015)



(Gartner, 2015)

- **IoT 보안 사고로 인한 피해 액수의 증가**
  - 국내 융합보안 피해 규모 2015년 13조 4천억, 2030년 26조 7천억원 (산업연구원)



(산업연구원, 2014)

2. IoT 보안 사고의 심각성

개인적인 보복을 위하여 타인 집의 Honeywell 온도조절기 조작

(Amazon.com, Customer Review, 2014. 03)

차량의 CAN bus 컨트롤러 해킹 시연

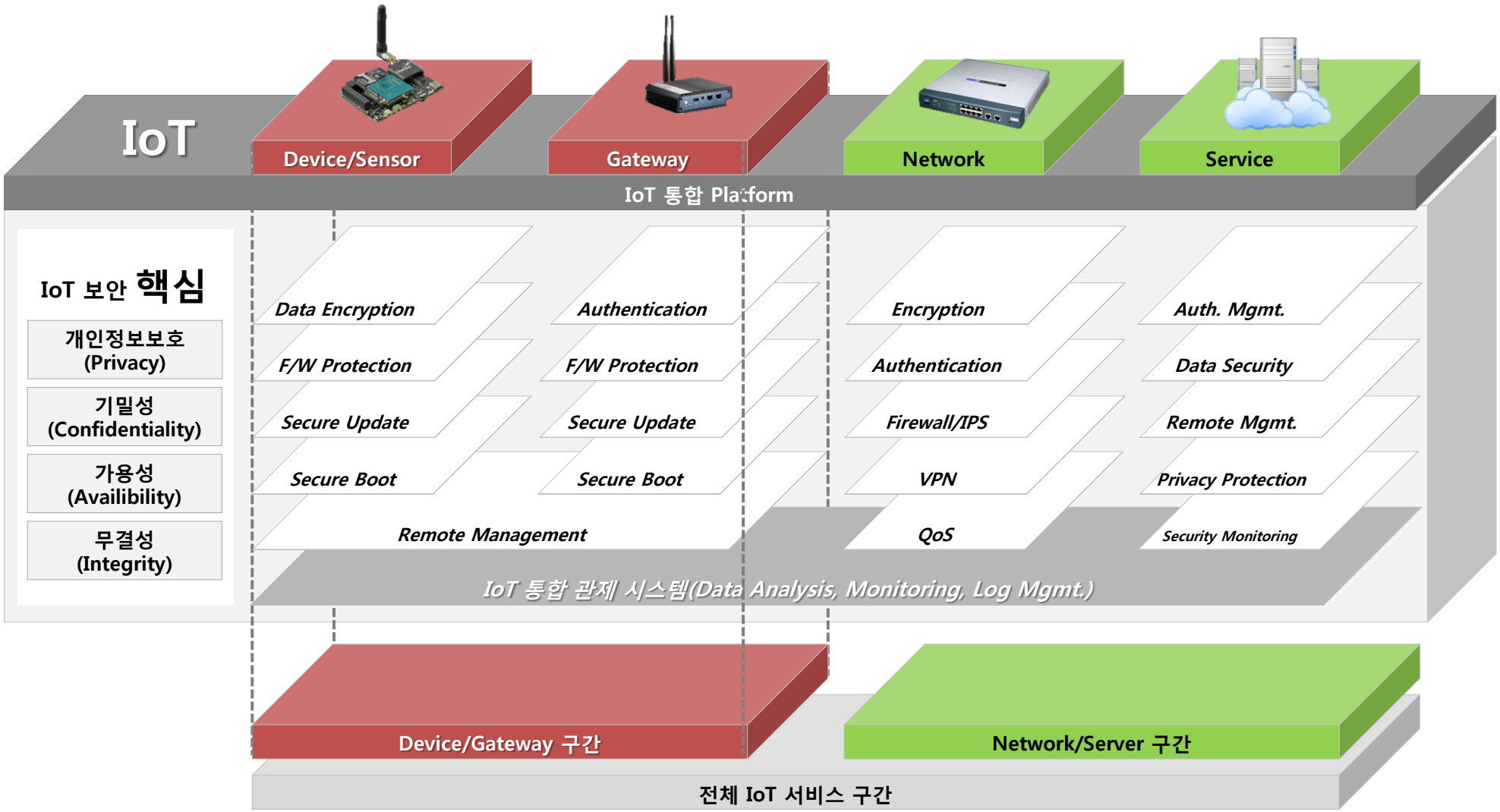
(BlackHat USA 2015 : Remote Exploitation of an Unaltered Passenger Vehicle)

3. IoT 보안 위협 사례

의료기기	- '15년 8월, 미국 FDA가 사이버 보안위협을 이유로 자동 약물주입펌프 사용 중지 권고
자동차	- '12년 블랙햇 보안 컨퍼런스에서 800미터 밖에서 인슐린 펌프 조작 가능 확인
스마트가전	- '15년 8월 테슬라 전기차 해킹공격 시연으로 시동 꺼짐, 감속, 계기판조작 등 시연
공유기	- 스페인 해커팀, 차량 N/W에 침투 가능한 회로보드(20달러) 공개, 경보해제 등 차량제어 시연
스마트시티	- '14년 9월 블랙펄 시큐리티 카메라 탑재 로봇청소기 원격조정 앱 해킹을 통한 사생활 감시 시연
드론	- '14년 3월 Team Cymru, 해커들이 D-Link 등이 제조한 약 30만개의 공유기 해킹사실 발표
	- IOActive Labs가 도로차량 감지기술의 보안결함을 이용, 신호 조작 등 주요 인프라 통제 가능 발표
	- '16년 Anonsec NASA 드론 해킹 시도
	- '16년 Nils Rodday, 경찰 수색용 드론 탈취 방법 공개

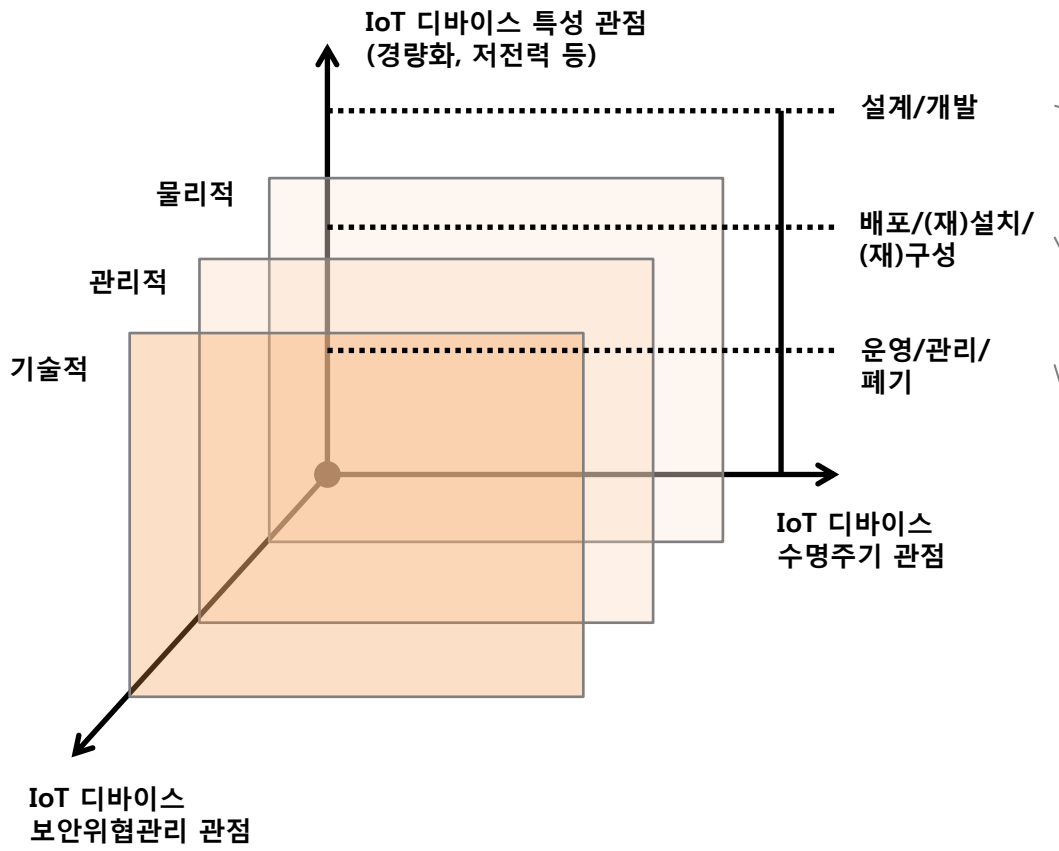
(출처: 정보통신기술진흥센터 블로그)

4. IoT 서비스 구간 분류



1. IoT 디바이스 수명 주기 별 보안 요구 사항

IoT 디바이스에 대한 관점 별 보안요소



(출처: IoT 디바이스 보안인증 기반연구, KISA)

보안 요구 사항

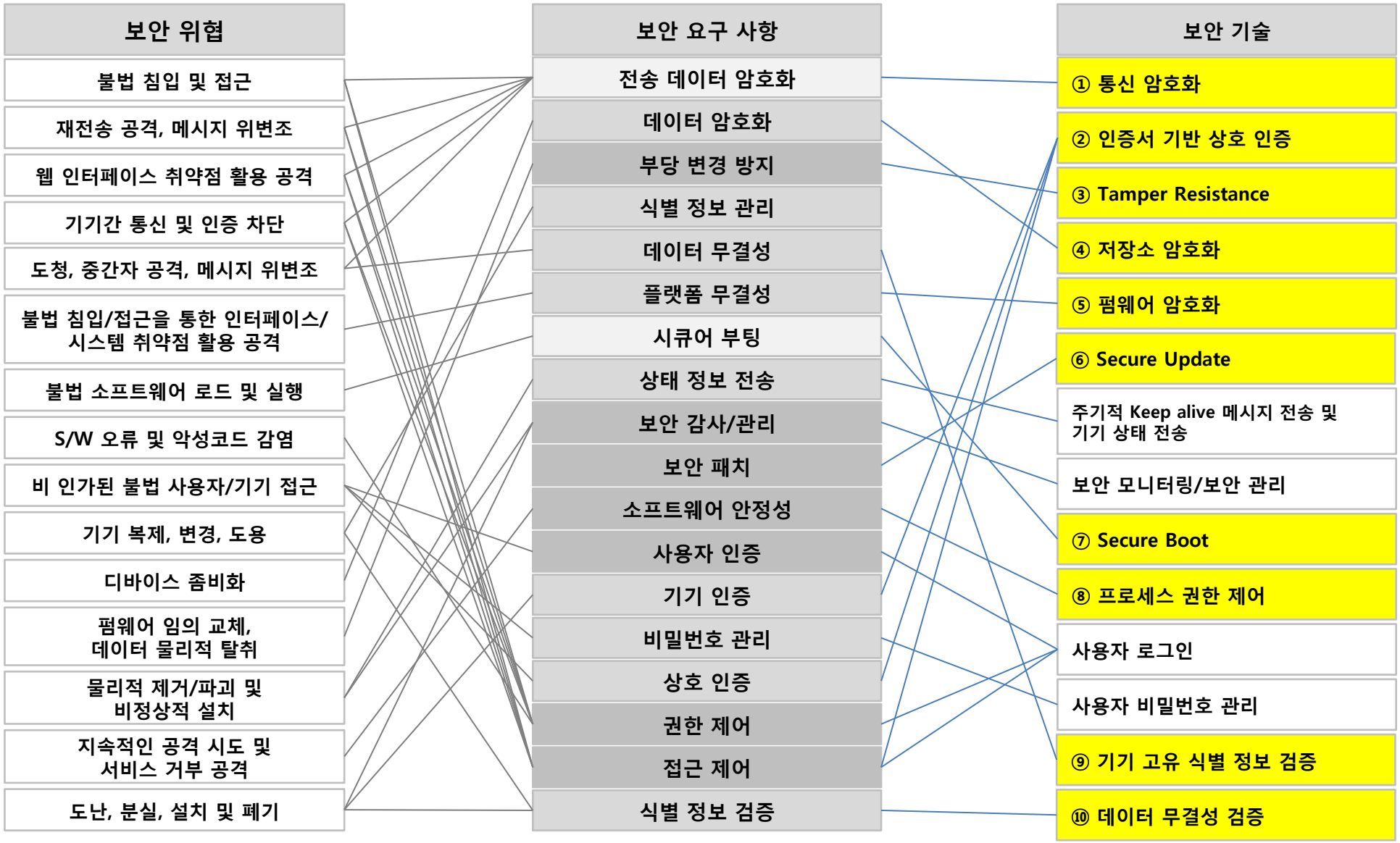
• 전송 데이터 암호화	• 사용자 인증
• 데이터 무결성	• 기기 인증
• 플랫폼 무결성	• 비밀번호 관리
• 시큐어 부팅	• 상호 인증
• 소프트웨어 안정성	• 권한 제어
• 접근제어	• 식별 정보 검증

• 데이터 암호화	• 사용자 인증
• 부당 변경 방지	• 기기 인증
• 식별 정보 관리	• 비밀번호 관리
• 데이터 무결성	• 상호 인증
• 플랫폼 무결성	• 권한 제어
• 상태 정보 전송	• 접근 제어
• 보안 감사/관리	• 식별 정보 검증
• 보안 패치	• 소프트웨어 안정성

• 부당 변경 방지	• 사용자 인증
• 보안 감사/관리	• 권한 제어
• 보안 패치	• 접근 제어
• 소프트웨어 안정성	

1. 디바이스 보안 위협, 보안 요구 사항 및 기술

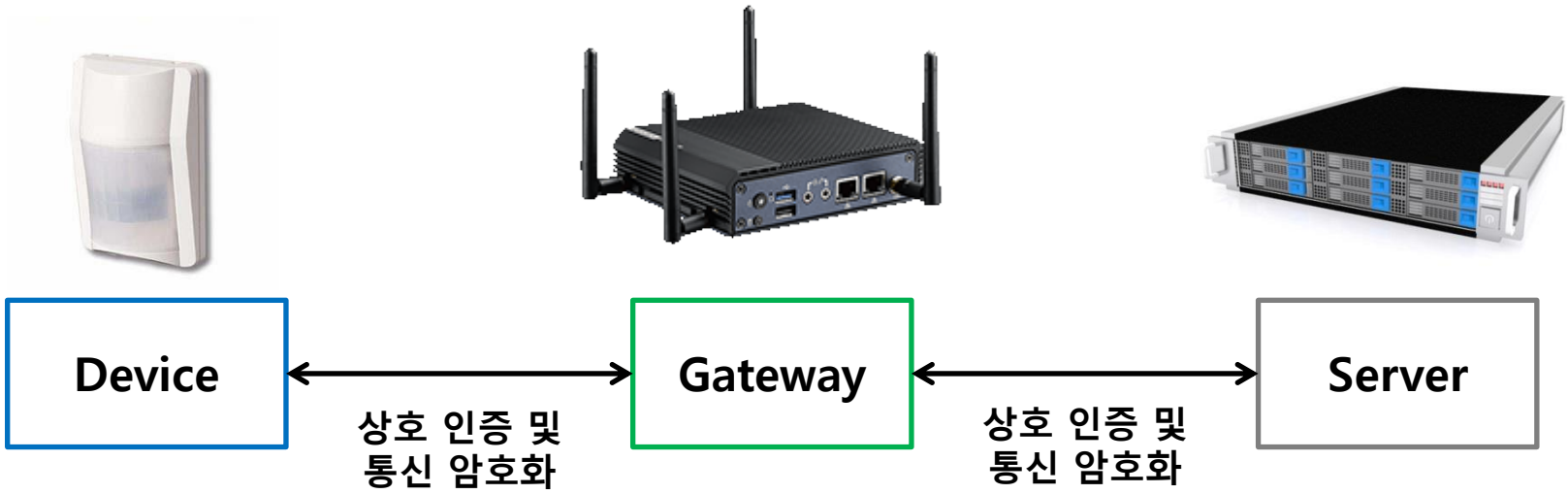
2. IoT 보안 기술



SK infosec

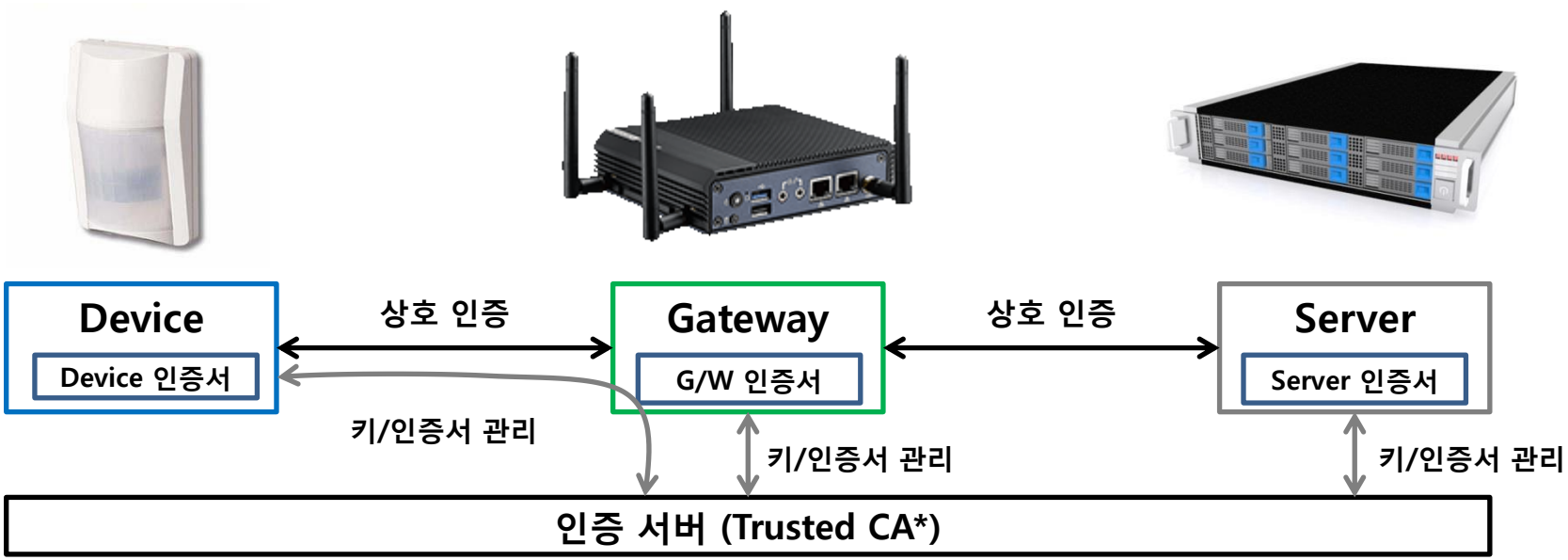
① 통신 암호화

- 위협 : 공격자가 디바이스와 게이트웨이 및 서버 간 통신 내용을 도/감청 또는 위/변조
- 통신 주체간 상호 인증 및 통신 암호화 수행



② 인증서 기반 상호 인증

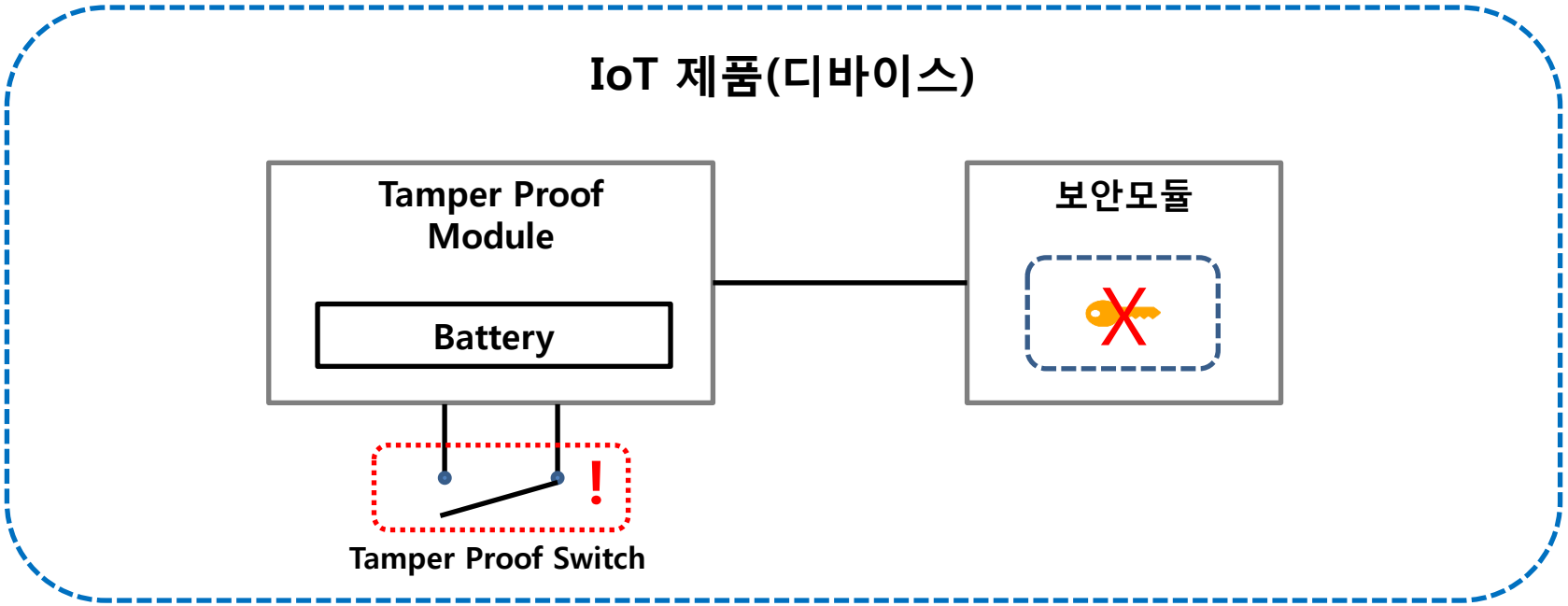
- **디바이스/게이트웨이/서버 상호 인증**
  - 위협 : 공격자가 디바이스와 게이트웨이 및 서버 간 통신 내용을 가로챌 수 있음
  - 신뢰할 수 있는 주체가 발급한 인증서를 이용하여 상호간에 인증을 수행
- **키/인증서 관리**
  - 각 구성 요소간 신원 인증에 사용하는 키/인증서를 인증 서버에서 원격으로 관리



**Trusted CA : Trusted Certified Authority. 신뢰할 수 있는 인증서 발급 주체*

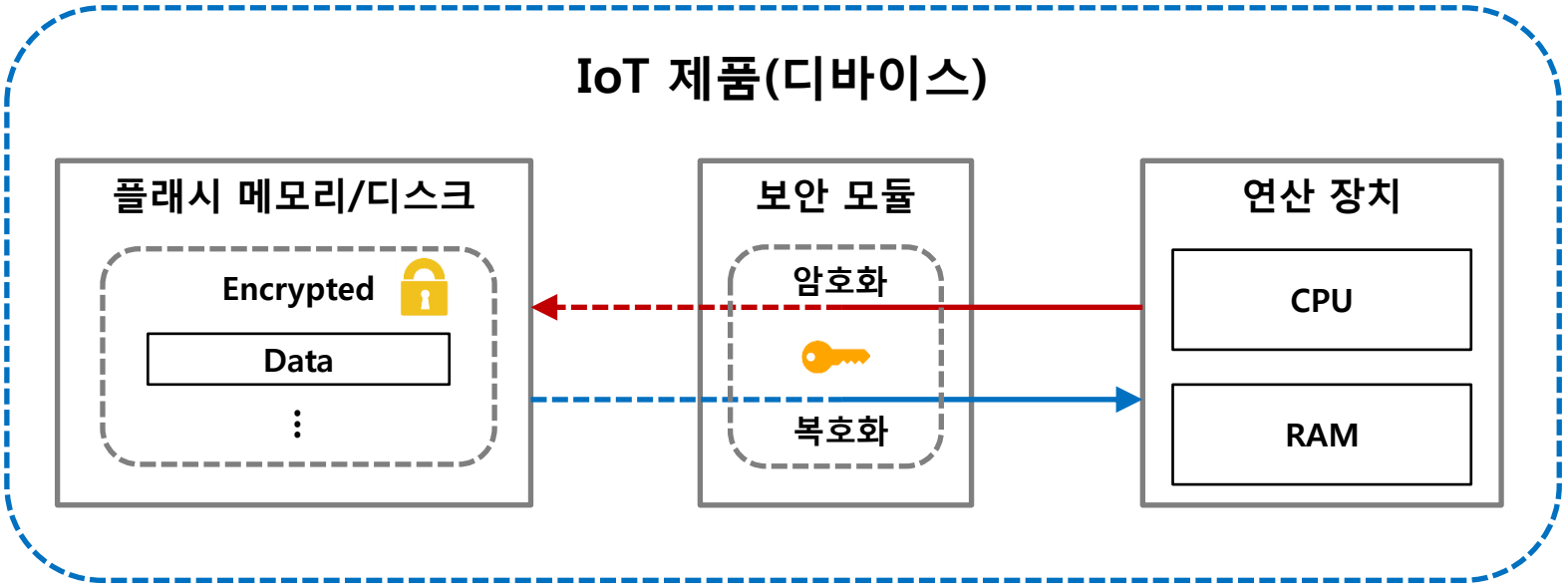
③ Tamper Resistance

- 위협 : 공격자가 플래시 메모리를 직접 분리하여 데이터 탈취 및 펌웨어 교체
- 제품을 분해 시 Tamper Proof 모듈에서 감지, 보안 모듈에 저장된 키를 파기하거나 제품을 동작 불가로 상태로 전환



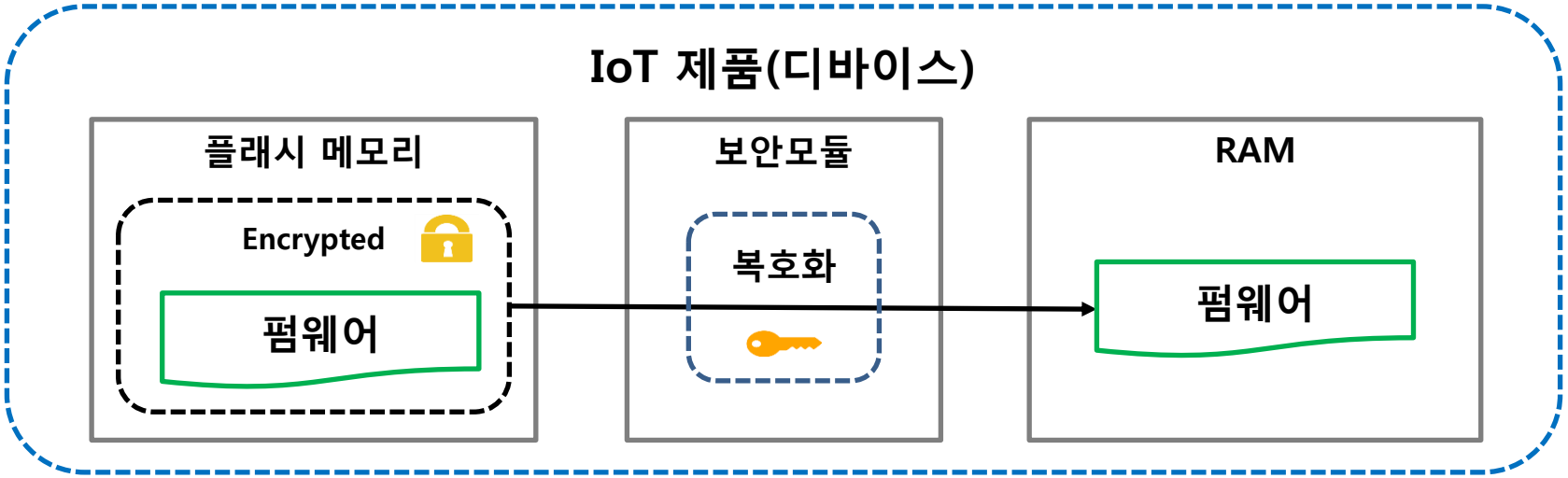
④ 저장소 암호화

- 위협 : 공격자가 디바이스를 분해, 플래시 메모리나 디스크에 저장된 데이터를 추출
- 보안 모듈을 이용하여 디바이스의 저장 장치의 모든 데이터를 자동으로 암/복호화



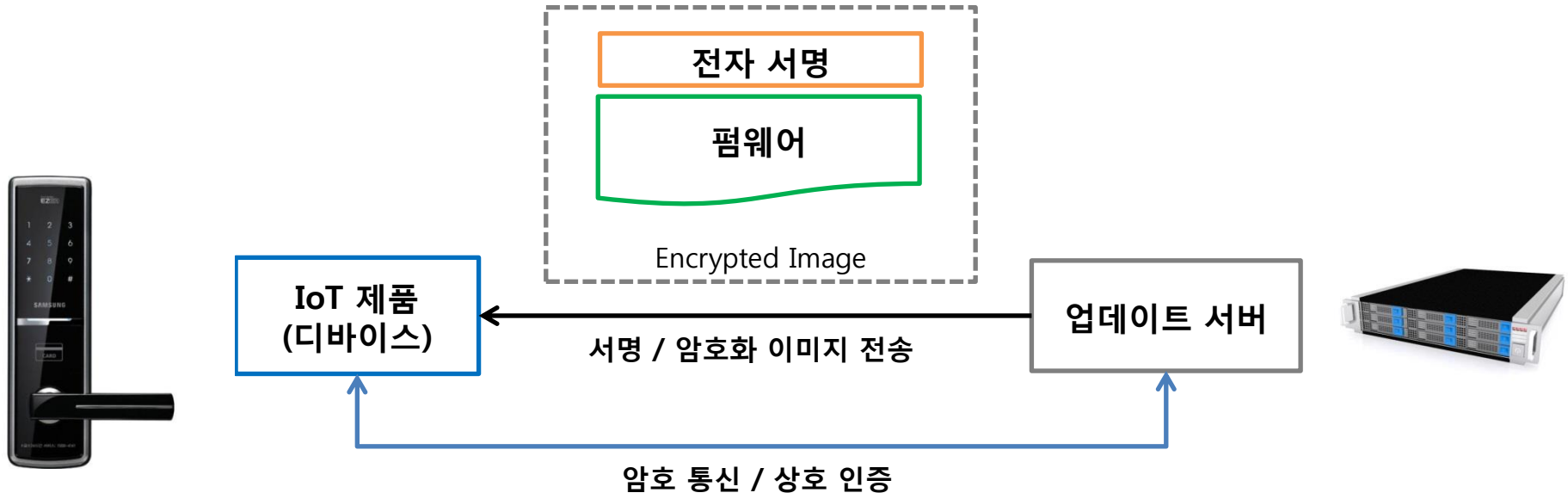
⑤ 펌웨어 암호화

- 위협 : 공격자가 디바이스의 펌웨어를 추출, 내재된 취약점을 찾아내 동종 기기 공격
- 디바이스의 펌웨어를 암호화하여 공격자의 펌웨어 추출/분석 무력화



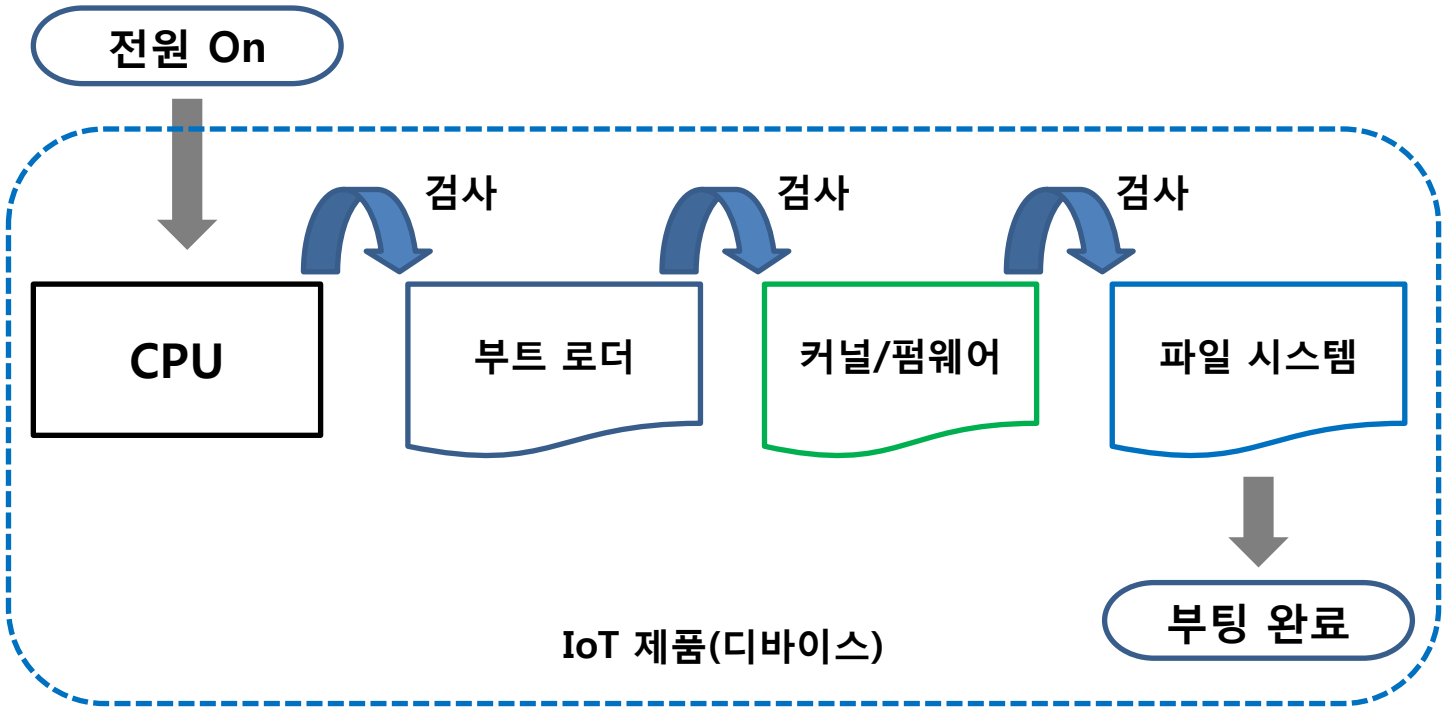
⑥ Secure Update

- 위협 : 펌웨어를 업데이트 시, 공격자가 업데이트 서버와 디바이스의 중간에서 위/변조된 이미지로 무단 교체
- 업데이트 서버와 디바이스간 상호 인증, 펌웨어 서명 및 암호화를 통하여 무결성 확보



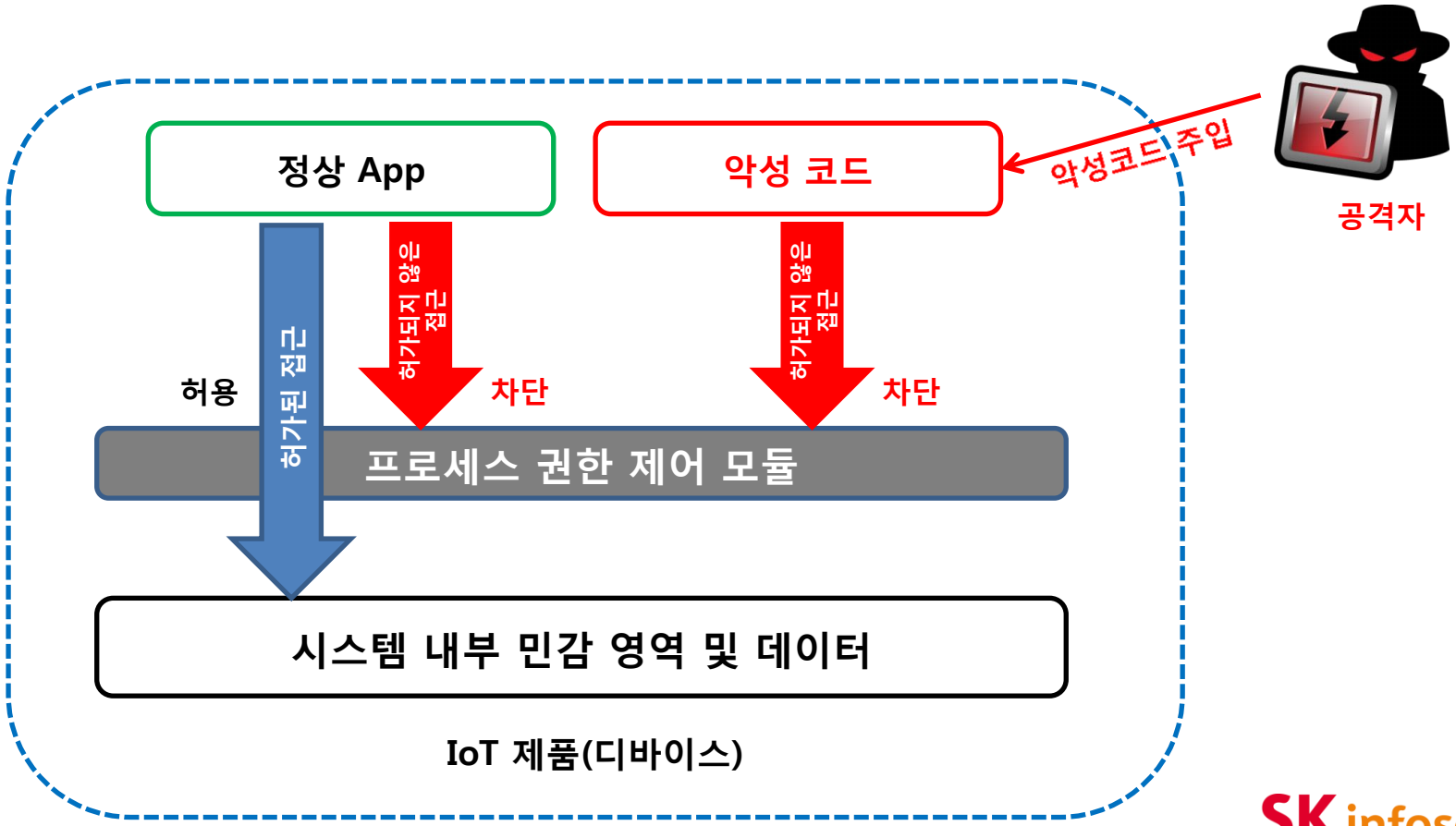
⑦ Secure Boot

- 위협 : 공격자가 부팅 파일(커널 등)을 무단으로 교체하여 원하는 동작 실행
- 각 부팅 단계에서 다음 단계의 바이너리를 검사하도록 하여 부팅에 관여하는 파일을 교체할 수 없도록 방지



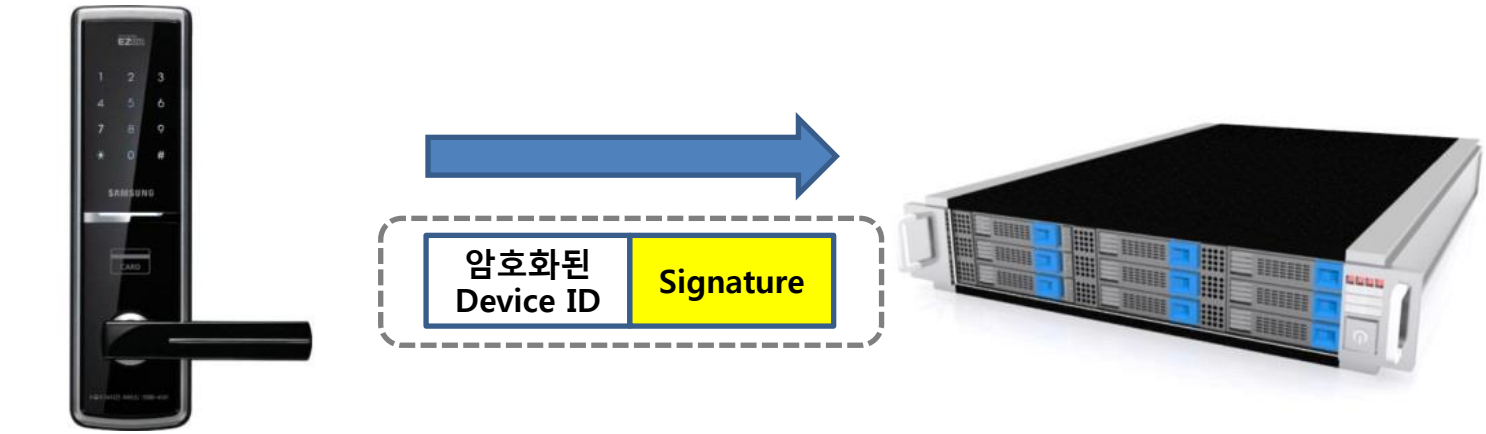
⑧ 프로세스 권한 제어

- 위협 : 공격자가 주입한 악성 코드 또는 잘못 작성된 프로그램이 민감한 영역에 접근
- 디바이스에서 동작하는 프로세스 별 데이터 접근 권한/방법을 제한



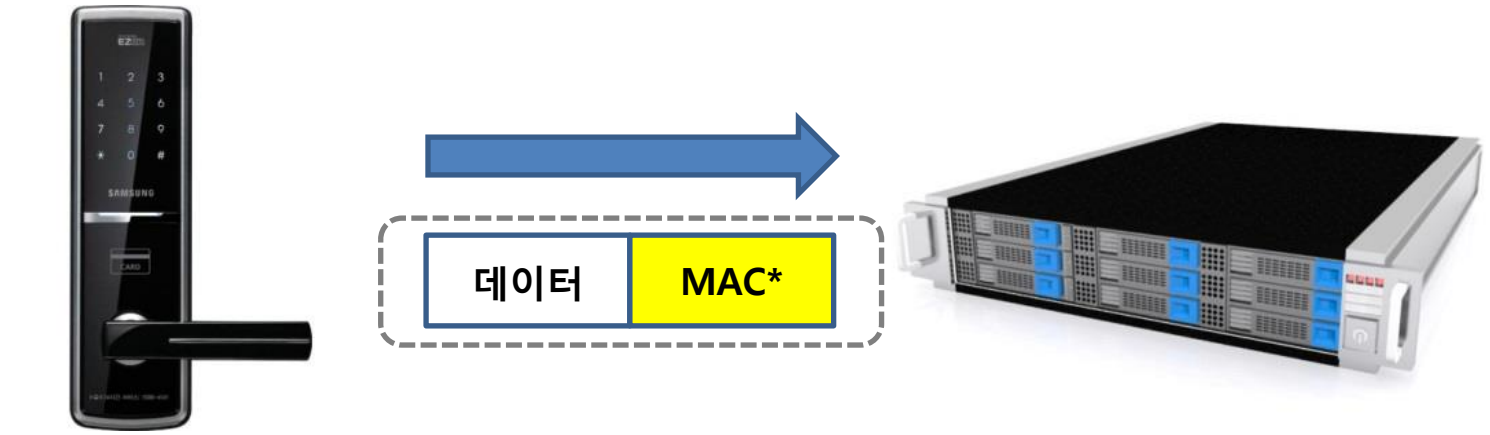
⑨ 기기 고유 식별 정보 검증

- 위협 : 디바이스 복제, 위조 또는 허용되지 않은 디바이스로 서비스 접속
- 기기 생산 단계에서 고유 식별 정보를 암호화하여 기기 내부에 저장, 기기 인증 시 고유식별 정보를 전송하여 검증



⑩ 데이터 무결성 검증

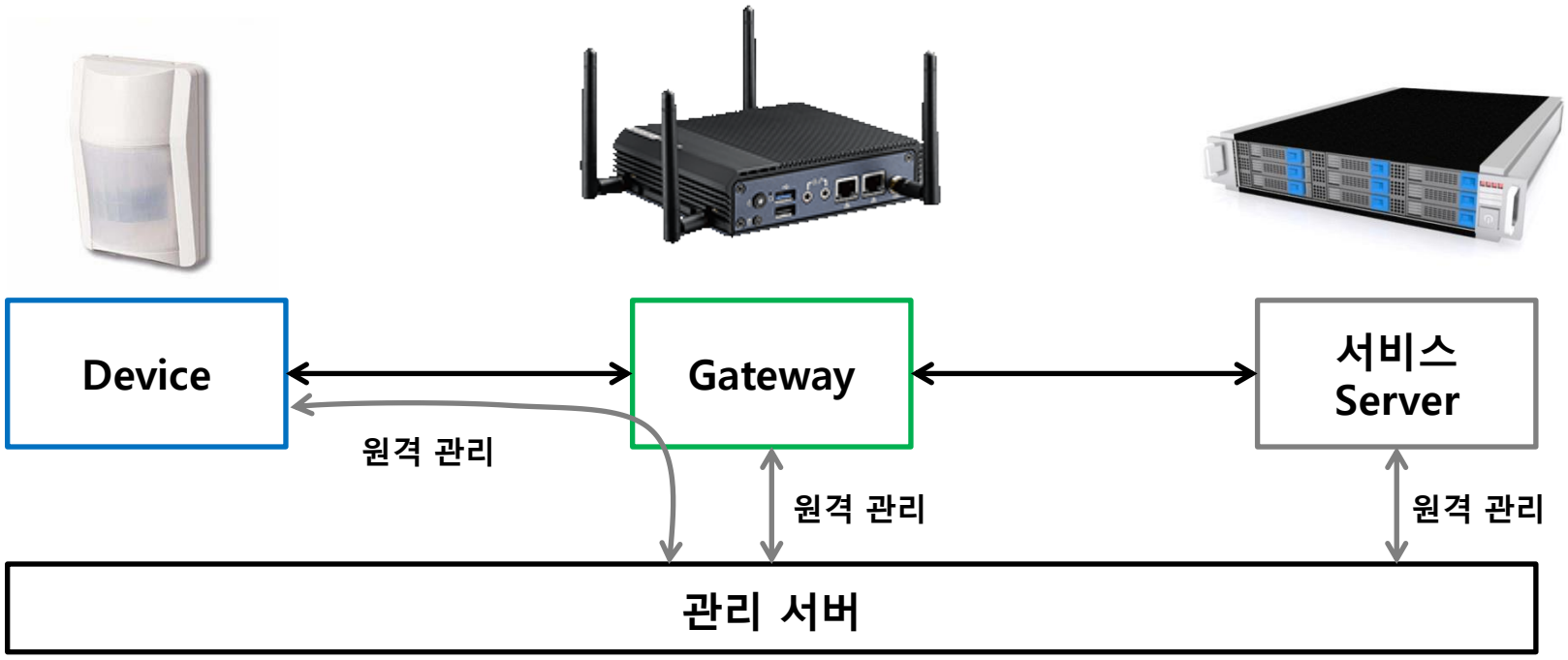
- 위협 : 제품에서 보낸 데이터를 공격자가 변조전달, 허가되지 않은 제품으로 데이터 전송
- 데이터에 대해서 메시지 인증 코드를 생성하여 첨부하고, 서버에서 이를 검증



** MAC : Message Authentication Code. 메시지 인증 코드*

⑪ 원격 관리

- IoT 서비스를 구성하는 각 구성 요소들을 원격으로 관리(On/Off 등)



① 정보보호와 프라이버시 강화를 고려한 IoT 제품 및 서비스 설계

② 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증

③ 안전한 초기 보안 설정 방안 제공

④ 보안 프로토콜 준수 및 안전한 파라미터 설정

⑤ IoT 제품 및 서비스의 취약점 보안패치 및 업데이트 지속 이행

⑥ 안전한 운영 및 관리를 위한 정보보호 및 프라이버시 관리체계 마련

⑦ IoT 침해사고 대응 체계 및 책임추적성 확보 방안 마련

2. 디바이스의 능력에 따른 보안 고려

3. IoT 보안 설계 고려사항

등급 0 :
연산 및 통신 능력의 제약으로 단독으로 안전한 통신이 불가능한 장치

- 주기적 Keep alive 메시지 전송 및 기기 상태 전송
- 데이터 무결성 검증

등급 1 :
IoT 전용 프로토콜을 사용할 수 있는 장치

- 통신 암호화
- 인증서 기반 상호 인증
- 저장소 암호화
- Secure Update
- 프로세스 권한 제어
- 사용자 로그인
- 사용자 비밀번호 관리

등급 2 :
통신 및 연산에 제약을 크게 받지 않는 장치 (GW 등)

- Tamper Resistance
- 펌웨어 암호화
- 보안 모니터링/보안 관리
- Secure Boot
- 기기 고유 식별 정보 검증

등급 3 :
등급 2보다 강력한 성능을 가진 장치 (PC 등)

- Anti-Virus
- 폐쇄형 방화벽
- 보안 정책 설정/관리
- 사용자/시스템/보안 이벤트 로그 생성

** 출처 : IoT 디바이스 보안 인증 연구(KISA, 2015)*

SK infosec

3. Secure Element 선정/적용

- Secure Element에서 암호 키/인증서의 관리를 수행하며, 칩 내부의 암호 키를 읽어낼 수 없음
- 장치의 Capability에 따라 적합한 종류의 SE를 사용

장치의 Capability에 따른 Secure Element

경량 IoT 디바이스	Gateway	Server
• 디바이스 인증 같은 한정적인 기능을 제공하는 SE를 사용	• 데이터 암호화, 디바이스 인증, 키 관리 등의 다양한 기능과 인터페이스를 제공하는 SE를 사용 (TPM, 스마트 카드 등)	• 다양한 기능뿐만 아니라 처리 성능이 높은 고성능 SE를 사용 (HSM 등)
		

** SE : Secure Element*

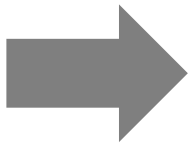
** HSM : Hardware Security Module*

4. 통신/네트워크 보안을 위한 고려 사항

통신 내용의 도/감청 및 위/변조 방지

통신 주체간 신원 확인 및 상호 인증

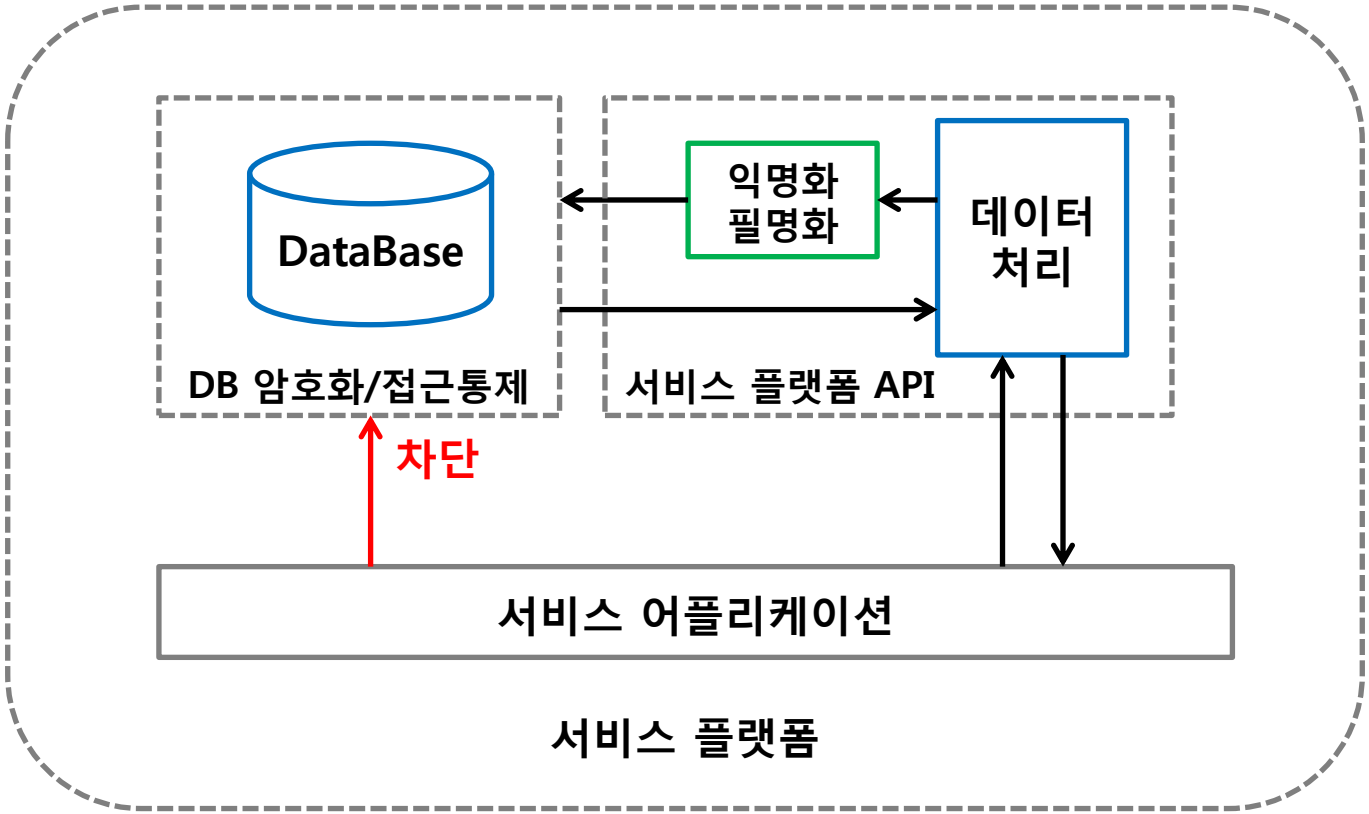
유해 트래픽 또는 네트워크를 통한 공격으로부터 보호



네트워크 보안 및 통신 암호화/상호 인증을 사용하는 구성

5. 서비스 플랫폼 구성

- 저장 데이터는 **익명화/필명화 처리** 후 **암호화** 하여 저장
- 데이터에 접근하기 위한 API의 **권한 관리**



6. 모바일 환경의 보안 요소

스마트폰	인증	단말 인증	앱 다운로드 인증	사용 인증
	기기 보안	루팅 체크	카메라/녹음/캡처	분실 정책
	앱 보안	앱 무결성 체크	앱 난독화	앱 레핑
	악성코드 보안	Virus 백신	시큐어 브라우저	
	모바일 가상화			
N/W	In-bound	피싱/멀웨어 방지	테더링 차단	White List AP 관리
	Out-bound	SSL	VPN	트레픽 제어
보안운영	통합모니터링	모바일 모니터링	단말 통합관제	FDS
앱 개발 운영	개발/테스트	시큐어코딩	OS(Android/iOS) 종류 별 취약점 패치	단말 별 보안점검
	배포/운영	단말 별 배포	신규 OS 출시대응	신규 단말 출시대응

보안 적용 절차

제품 설계 분석,
보안 요구 사항 도출

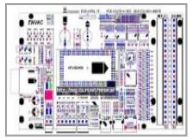
제품 보안 진단
적용 보안 기술 도출

보안 기능 적용 계획 및
적용 방안 수립

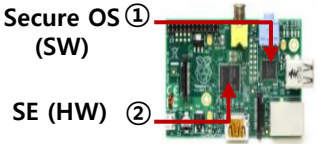
보안 기능 적용 및 테스트

보안 적용 방법

기 설계된 IoT 디바이스 적용 방안



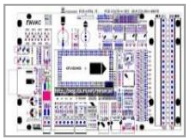
제품설계(추가설계)



보안기능 추가 및 제품개발

신규 IoT 디바이스 적용 방안

보안기능이 추가된
OSHW를 이용한 제품개발



제품설계

IoT 보안 디바이스

SK infosec

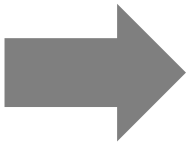
2. 제품 출시 이후 관리 방안

제품에 대한 정기적 보안 진단

원격 관리를 통한 이상징후 모니터링

보안 취약점 및 버그에 대응하기 위한 신속한 업데이트

보안 사고 발생 시 신속한 원인 분석 및 재발방지 방안 수립/적용



제품의 보안 이슈에 대한 선제적 대응과 신속한 조치 이행

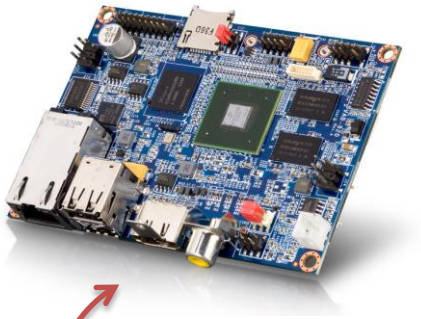
디바이스 보안 적용 절차

임베디드리눅스 디바이스의 경우 MPU, TPM, 부트로더, OS커널 및 시스템 파일에 보안 적용

*RTOS 및 펌웨어를 사용하는 디바이스의 경우는 MCU, 인증칩, 부트로더에 보안 적용

1. 기존 HW 보드에 보안칩 추가

- x86, ARM, PowerPC, MIPS, etc.



TPM 공간 확보 후
PCB Artwork

보안칩: 하드웨어 보안 모듈
(Secure Element)

2. 보안 OS Porting

- 하드웨어 별 보안OS 제공

[보안 OS (Linux/RTOS) Porting]

- BSP Test

  * BSP(board support package)
- SE 활용 모듈
- Security Library
  - 시큐어부트
  - 접근제어
  - 파일시스템 암호화
  - 통신암호화
  - 인증 등
- Application 개발 API

3. 보안적용 생산 및 사후관리

- 기존 개발된 Application 적용

[어플리케이션 포팅]

- 홈G/W, 가전 등 용도별 App.

[통합 테스트]

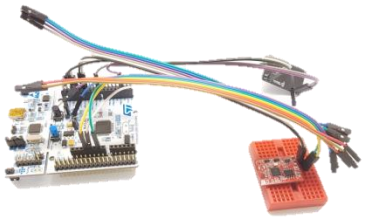
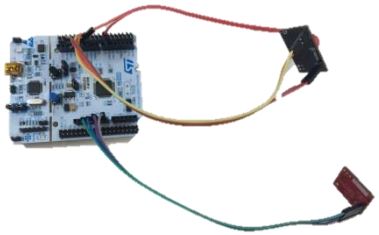
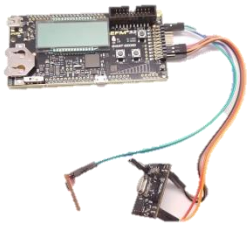
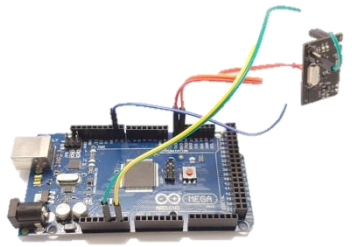
- H/W, S/W 통합 테스트
- Working Sample 제작

[사후 관리]

- 커널 업그레이드, 보안 패치
- 보안 침해 내역 관제

SK Infosec IoT 디바이스 보안 솔루션

2종의 RTOS를 탑재한 4종의 H/W 프로토타입/SDK 제공

	mbedOS	FreeRTOS	mbedOS w/o Update	FreeRTOS w/o Update
H/W				

	▪ CPU : STMicroelectronics STM32F4 (ARM Cortex-M4 아키텍처 기반 MCU)
	▪ RAM : 96KB SRAM
	▪ 저장공간 : 512KB Flash
	▪ H/W 보안 모듈 : Infineon Optiga Trust P
	▪ 무선 통신 모듈 : NDevice NDsocket (Wi-Fi)
	  ▪ IEEE 802.11b/g/n
	  ▪ WPA/WPA2 PSK 암호화 지원
		▪ CPU : STMicroelectronics STM32F4 (ARM Cortex-M4 아키텍처 기반 MCU)
		▪ RAM : 96KB SRAM
		▪ 저장공간 : 512KB Flash
		▪ H/W 보안 모듈 : Infineon Optiga Trust P
		▪ 무선 통신 모듈 : NDevice NDsocket (Wi-Fi)
		  ▪ IEEE 802.11b/g/n
		  ▪ WPA/WPA2 PSK 암호화 지원
			▪ CPU : Silicon Labs EFM32 Gecko (ARM Cortex-M3 아키텍처 기반 MCU)
			▪ RAM : 16KB SRAM
			▪ 저장공간 : 128KB Flash
			▪ H/W 보안 모듈 : Infineon Optiga Trust P
			▪ 무선 통신 모듈 : NDevice NDsocket (Wi-Fi)
			  ▪ IEEE 802.11b/g/n
			  ▪ WPA/WPA2 PSK 암호화 지원
				▪ CPU : Atmel ATMEGA2560 16MHz (AVR 기반 8bits MCU)
				▪ RAM : 8KB SRAM
				▪ 저장공간 : 256KB Flash
				▪ H/W 보안 모듈 : Infineon Optiga Trust P
				▪ 무선 통신 모듈 : NDevice NDsocket (Wi-Fi)
				  ▪ IEEE 802.11b/g/n
				  ▪ WPA/WPA2 PSK 암호화 지원

S/W	▪ OS : ARM mbedOS
	▪ 게이트웨이를 통한 원격 관리
	▪ 보안 기능
	  ▪ Secure Boot
	  ▪ 펌웨어 암호화
	  ▪ 디바이스 – 게이트웨이간 상호 인증 및 통신 암호화
	  ▪ Secure Update
		▪ OS : FreeRTOS
		▪ 게이트웨이를 통한 원격 관리
		▪ 보안 기능
		  ▪ Secure Boot
		  ▪ 펌웨어 암호화
		  ▪ 디바이스 – 게이트웨이간 상호 인증 및 통신 암호화
		  ▪ Secure Update
			▪ OS : ARM mbedOS
			▪ 게이트웨이를 통한 원격 관리
			▪ 보안 기능
			  ▪ 디바이스 – 게이트웨이간 상호 인증 및 통신 암호화
				▪ OS : FreeRTOS
				▪ 게이트웨이를 통한 원격 관리
				▪ 보안 기능
				  ▪ 디바이스 – 게이트웨이간 상호 인증 및 통신 암호화

용도	▪ ARM mbed 플랫폼 기반 디바이스 ▪ Cortex-M4 계열 CPU를 사용하며, F/W 업데이트가 요구되는 디바이스 - 스마트홈 가전 제품 등	▪ FreeRTOS를 OS로 사용하는 디바이스 ▪ Cortex-M4 계열 CPU를 사용하며, F/W 업데이트가 요구되는 디바이스 - 스마트홈 가전 제품 등	▪ ARM mbed 플랫폼 기반 디바이스 ▪ 통신 데이터 보호 및 상호 인증 기능만을 요구하는 디바이스 - F/W 업데이트가 불필요한 디바이스	• Arduino플랫폼 기반 디바이스 • 통신 데이터 보호 및 상호 인증 기능만을 요구하는 디바이스 - F/W 업데이트가 불필요한 디바이스

2. Secure Gateway

Access Point, SOHO Router, IoT Gateway로 이용 가능한 H/W Appliance 공급

* Secure Element 및 Secure OS를 탑재한 H/W에 고객사 Application 추가 탑재 가능

Secure Element 내장 Hardware

Secure OS

- **Linux 기반의 Secure OS**
- **Gateway 기능 제공**
  - 유/무선 네트워크 지원
  - 라우팅 등
- **보안 기능 제공**
  - 시큐어부트
  - 접근제어
  - 파일시스템 암호화
  - 통신암호화
  - 인증 등
- **Application 개발 API**

SK Infosec 소개

SK인포섹은 정보보호 서비스, 보안솔루션, 융·복합보안 및 고객 IT서비스를 제공하는 종합보안 전문기업입니다.

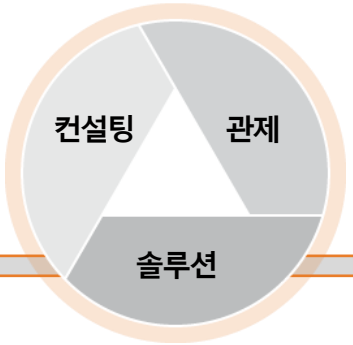
보안컨설팅

- 컴플라이언스
- 정보보호관리체계
- 개인정보보호
- 종합정보보안
- 모의해킹
- ICT/Biz. 컨설팅

보안관제

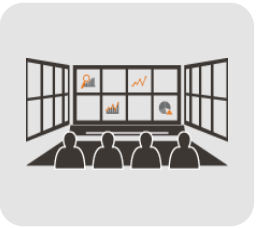
- 원격 관제(Big Data플랫폼)
- 파견 관제(SIEM/ESM)
- 클라우드 관제
- Intelligence 관제
- Top-CERT
- Forensics

체계설계 → 구현 → 이행지원 → Project관리 → 현황분석 → 위험진단 → 체계설계



탐지/분석 → 침해대응 → 결과보고 → 개선 → 현황/예방 → 정보수집 → 탐지/분석

융합보안



- 물리융합보안컨설팅
- 물리보안시스템 구축
- 통합상황실 구축
- 메인컨트롤러/SW 보유

IT통합상담&PC/OA공급 서비스

- IT Service Desk & IT/보안 Call Center
- 차세대 One Stop Total OA 서비스
- 시스템기반 자산관리
- PC/OA 공급서비스

Enterprise 보안솔루션

Network/Cloud									Server/Application				Endpoint			
F/W	WAF	IPS (IDS)	Anti-DDoS	APT 대응	DPI	DPI	SDN/NFV* 보안	Cloud 보안	E-mail APT 대응	웹쉘 탐지	악성코드 탐지	개인정보보호 (서버)	개인정보보호 (단말)	모바일 보안	IoT 보안	PC 가상화

(*) SDN/NFV: Software Defined Network, Network Function Virtualization, 특정 장비, 업체, 프로토콜, 표준에 얽매이지 않는 새로운 네트워크 기술

SK infosec

마치며...

"IoT는 기술의 진보처럼 보이지만 궁극적으로 인간의 삶을 풍요롭게 하고 살찌우는 도구가 되어야 한다"

– Kevin Ashton –

Q&A

IoT 보안 컨설팅 / 솔루션 기술 문의: 여현국 과장 (arbalest@sk.com)

IoT 비즈니스 협력문의: 장우진 부장 (wjjang@sk.com)

SK infosec

SK infosec

보안, 그 이상의 믿음

에스케이인포섹㈜ 13486 경기도 성남시 분당구 판교로255번길 46 4층 E-mail: skinfosecmkt@sk.com TEL : 02)6361-9114 FAX : 02) 6361-9998

201606