IoT 시대의 보안 이슈 대응

2016. 06. 15

LG CNS

1. 스마트기기 보안 해킹 사례 (자동차 / 스마트 미터링)

스마트기기 서비스 해킹은 상호인증 취약점 공격 또는 펌웨어 내 악성코드 답재 등의 방식으도 이루어집니다.

C社 차량 해킹 사례

차량 서비스 보안 취약점 공격 (2015)

- 원격 F/W 업데이트도 차량 내 악성코드 답재
- 변경된 F/W를 동해 중앙동신허브(CAN)에 접근
- CAN을 동해 브레이크 원격 제어 (BlackHat '15)
- G社, T 社 차량도 해킹 사례 발표 (2015)

스마트 미터링 해킹 사례

스마트미터링 상호인증 취약점 공격 (2014.10)

- 스페인 스마트미터딩의 해킹 공격에 취약함을 받견
- 네트워크 정보를 변조하여 잘못된 전력 이용 정보를 전달
- 전기세를 줄이기 위해 정보 변조 공격 증가 예상

LG CNS

1. 스마트기기 보안 해킹 사례 (CCTV / IoT 가전)

CCTV 및 IoT 가전에 대한 해킹 사례는 다음과 같습니다.

T社 CCTV 해킹 사례

CCTV 촬영 영상 정보 접근 및 노출 (2013.09)

- 약 700대 CCTV의 실시간 영상 정보의 접근 시연
- 로그인 시 계정 정보가 온라인 상에서 암호화 없이 전송
- FTC(미국연방거래위원회)에서 시정조치 요구
- 해당사는 보안취약점 공지 및 2년마다 보안감사 받음

P 社 스마트 가전 해킹 사례

악성코드를 이용한 가전기기 원격 제어 (2013.08)

- 외부 공격자에 의한 원격제어를 통한 Black out 시연
- 끊임없이 원격 제어 명령어 전달로 정전 효과를 발생
- 악성코드를 사용자 시스템에 심어 명령어를 전송

LG CNS

2. IoT 서비스 유형 및 보안 특성

다양한 IoT 중에 대표적인 서비스로는 홈 IoT, 자동차 IoT, 스마트미터링 서비스가 있습니다.

구분	자동차 IoT 서비스	스마트미터링 보안 서비스	Home IoT 서비스
서비스 특성			
	• 차량 내 전자부품 간 통신을 하거나 차량-외부시설 간 통신 서비스	• 가정에서 사용한 전력량을 중앙 서버에서 측정 (원격 검침)	• 가전기기를 원격에서 제어하거나 상태 모니터링
보안 특성	• 현재까지는 자동차 전자기기에 탑재되는 보안모듈 중심 • 향후 차량-외부시설 간 통신을 위한 보안 서비스 확대 예상	• 국내에서는 2019년 보안 모듈 적용 의무화 예정 • 해외 스마트미터링 시장도 보안 의무화 시작 (독일, 2013)	• 가전기기의 안전한 원격제어를 위해 보안 필수 • 해커에 의한 기기 원격제어나 모니터링 차단 필요

LG CNS

3. 자동차의 IoT 보안

V2X(자동차 ↔ 외부 사물 통신) 및 차량 내부의 각종 전자기기 (엔진제어 모듈, 변속기 모듈, 브레이크) 제어 및 정보 조회를 위해 IoT 보안이 필요합니다.

V2X 통신에서의 IoT보안 용도

[IoT 보안 필요성]

앞 차가 장애물을 발견했을 때...

앞 차에서 보내는 신호를 믿고 브레이크를 밟을 것인가?

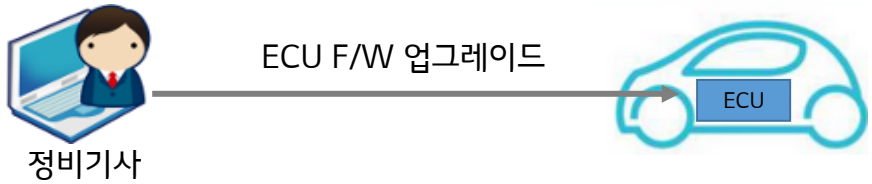
[IoT 보안 수행 업무]

- V2X 메시지에 대하여 PKI 기반의 전자서명 생성 및 검증을 통해 신뢰성을 보장

차량 내부에서의 IoT 보안 용도

[IoT 보안 필요성]

정비소에서 차량 내 주요 전자기기의 정보에 접근할 때...



정당한 관리자가 기기를 제어 또는 정보를 조회하는가?

[IoT 보안 수행 업무]

- 자동차의 주요 부품 위조를 막기 위한 보안 모듈도 활용
- 상호인증, 보안부팅, 방화벽 역할 수행

LG CNS

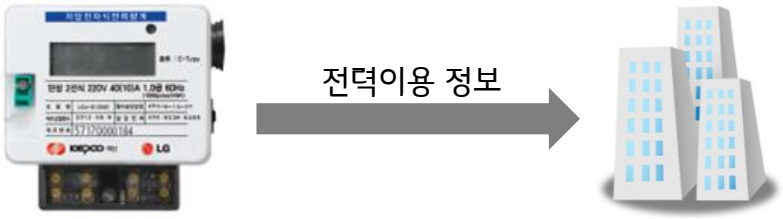
4. AMI 에서의 IoT 보안

AMI의 경우 전력 이용량과 같은 전송 정보의 위변조 시도가 발생하므로 강력한 보안 수준이 필요합니다.

AMI 보안 현황

[IoT 보안 필요성]

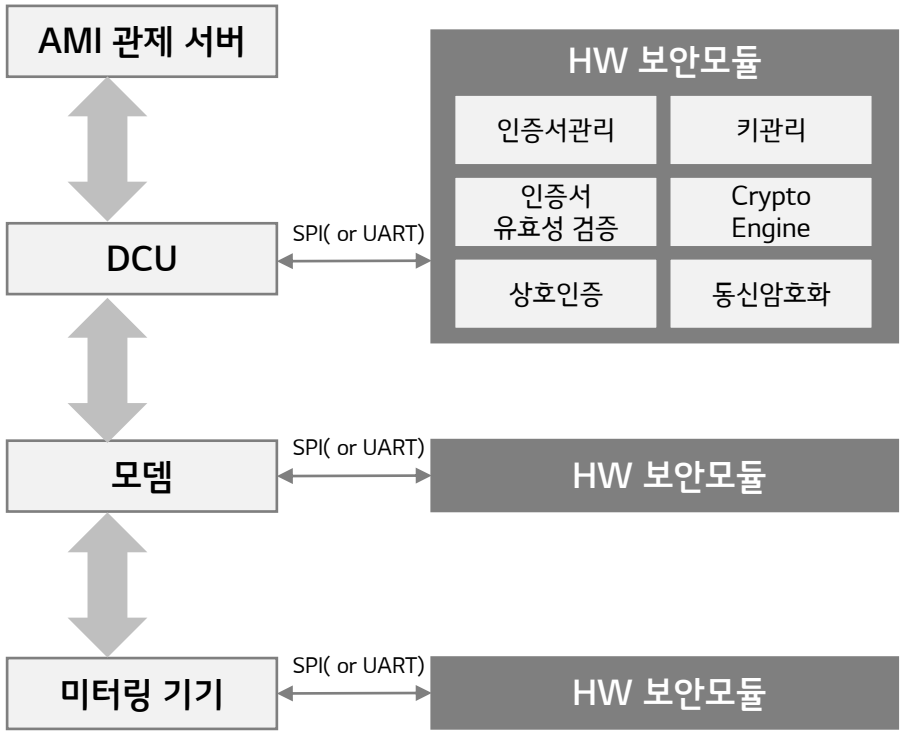
AMI가 전기 이용정보를 전력회사로 보낼 때...



AMI로부터 수신 받은 전력이용 정보를 신뢰할 수 있는가?

- AMI의 확산을 위해 보안 이슈가 선결되어야 함
- 이미 AMI 보안 표준이 수립되어 있음
  (DLMS-COSEM 표준에 2014년부터 보안 항목 강화)

AMI 보안 적용 방안



LG CNS

5. 각국의 IoT 보안 대응 현황

한국과학기술기획평가원의 "IoT 보안 위협 동향" 자료에 따르면 각국의 보안 대응 현황은 다음과 같습니다.

회사명	준비 현황
한국	- IoT 사이버보안 위협이 대두됨에 따라 관련 "사물인터넷 정보보호 로드맵" 발표(2014.10) - 에너지, 교통, 홈/가전/제조 등 5개 ICT 융합 제품 개발 시 설계부터 보안 기능 적용 추진 (정보보호산업 진흥계획)
미국	- 국립표준기술연구소의 주도 하에 사이버보안 프레임워크를 수립(2013.2) - FDA는 의료장비 보안 지침을 마련해, 이를 준수하지 않은 제품은 미국 내 판매 및 유통 금지(2013)
유럽	- 사물인터넷 보안 지침 마련과 함께 보안 인증, 표준화 작업에 초점 - 유럽데이터보호 감독기구 "Working Party 29"에서 사물인터넷 데이터 보호 권고안을 채택, 발표 (2014.9)
중국	- 공업정보화부에서 '사물인터넷 12차 5개년 계획'을 공개 ('11.12) - 사물인터넷 발전 10개 전문 행동계획을 수립하여 핵심 보안기술 개발 및 보안 평가 플랫폼 구축 추진

6. IoT 보안 관련 국내외 표준

국내외 IoT 보안취약점 자료 및 타사 IoT 솔루션 내용 분석으로 IoT 보안 요구사항을 도출하였습니다.

IoT 보안 현황 분석

- OWASP IoT 10대 취약점
- 사물인터넷(IoT) 정보보호 로드맵 (미래창조과학부)
- oneM2M 보안 요구사항
- 해외 IoT 기기 CC 인증 요구사항 (독일, 스마트미터링)

IoT 보안 요구사항

Device & Server	기기 및 서버 간 상호인증
	안전한 키 관리
	주요정보 보호 (암호화)
	연계정보 무결성 확보
	개인정보의 무분별한 수집 차단
	SW, FW의 무분별한 변경 차단
	악성코드 탐지 및 방어
Mobile	모바일 사용자 인증
Network	네트워크 해킹 공격 대응
	네트워크 동합 모니터링

LG CNS

7. IoT 기기 보안모듈 고려사항 (1/2)

IoT 보안 플랫폼은 다양한 기기에 적용 가능해야 하며, 다양한 OS 및 제한적인 HW 자원을 고려해야 함

다양한 기기 환경 고려

FW	JAVA도 개발	C / C++도 개발
OS	Linux	Android
	Windows CE	RTOS(OSEK)
	Embedded Windows	AUTOSAR Platform
Memory	File 형태도 관리	메모리에 직접 R/W
CPU	ARM cortexM	MPC55xx, 56xx, 57xx

...

| 다양한 유형의 IoT 기기 존재 |

- 다양한 OS 및 HW 환경에서 동작하는 보안 모듈 필요
- FW 개발 언어를 고려한 보안 모듈 필요
  : C , JAVA 등 다양한 개발 환경에서 동작 가능해야 함

제한적인 HW 자원

CPU	- 8/16bit ~ 32 Bit CPU 환경 - 16 bit 10MHz 이하의 저사양 CPU을 사용하는 기기 존재
Memory - EEPROM - Flash - SDRAM	- 기기 별도 메모리 사이즈 편차가 큼 (64KB ~ 2MB) - 10~30KB의 작은 여유공간을 가진 기기 존재

...

| 극한 환경의 기기도 고려해야 함 |

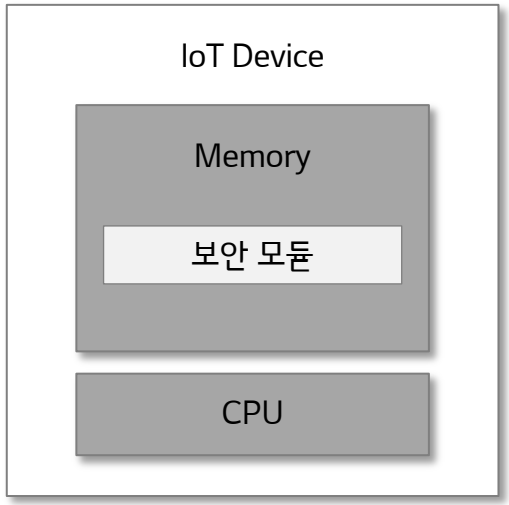
- 제한적인 메모리 환경에서 동작 가능한 보안 모듈
  : 보안 모듈 사이즈의 경량화 필요

LG CNS

7. IoT 기기 보안모듈 고려사항 (2/2)

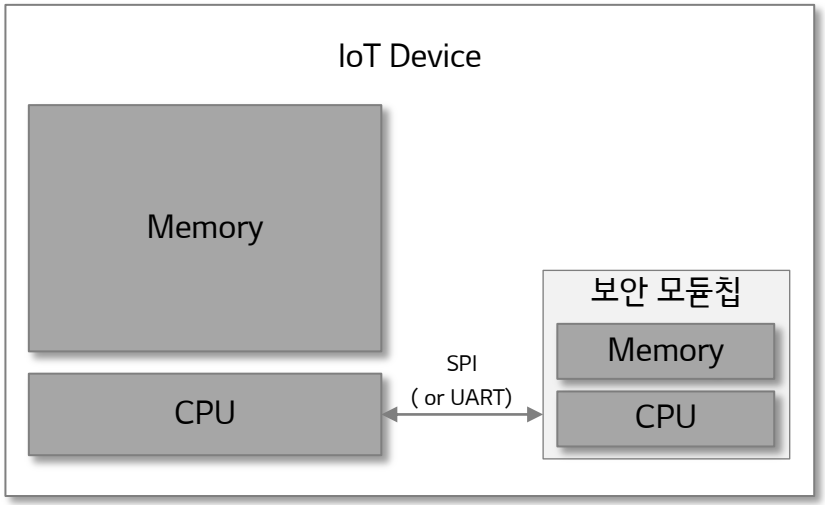
기기 보안모듈은 크게 SW 방식 및 HW 방식이 있으며, 각각의 서비스 환경을 고려한 적용이 필요합니다.

SW 방식의 기기 보안 모듈



- IoT 기기 내 펌웨어 형태의 기기 보안 모듈을 탑재
- HW 의 추가 변경이 필요 없어 적용이 상대적으로 용이
- 기 배포된 기기에도 추가 적용 가능
  (메모리 여유 공간이 있을 경우)
- HW 방식보다 보안성이 상대적으로 떨어짐

HW 방식의 기기 보안 모듈

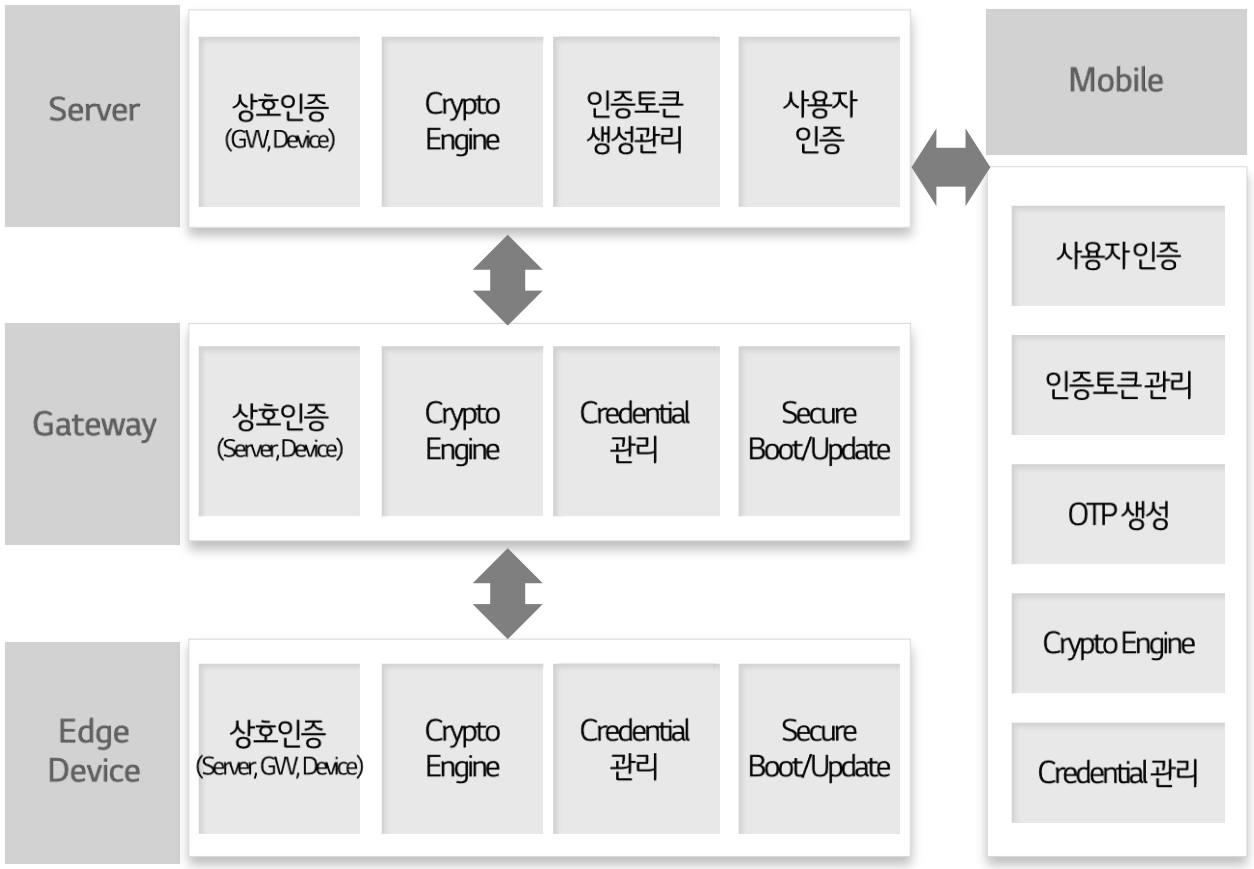


- IoT 기기 내 별도의 보안 전용칩을 부착
- HW 보안칩에서 제공되는 외부 공격 방어 기능으로 강력한 보안성을 보장
- 별도의 보안 전용칩 적용에 따른 기기 설계 변경 및 가격 부담 발생

8. IoT 보안플랫폼 구성요소

IoT 全 구성요소(Server, Gateway, Device, Mobile) 에 대한 보안 솔루션 구성은 다음과 같습니다.

보안플랫폼 구성도



주요 제공 기능

상호인증
- 기기, 게이트웨이, 서버 간 상호인증

주요 정보 암호화
- 개인정보 및 연계 정보 암호화

Credential 관리
- KEY, 인증도큰 정보의 안전한 관리

사용자 인증
- 스마트폰 + 사용자 복합 인증 서비스

Secure Boot
- 부딩 시 주요 프도그램 변경여부 점검

Secure Update
- 주요 프도그램 변경은 위한 권한 검증

LG CNS

9. 기능 소개 (상호인증)

서비스 다양성은 위한 여러 유형의 상호인증 서비스를 제공하며, 2Factor 인증으로 보안성은 강화하였습니다.

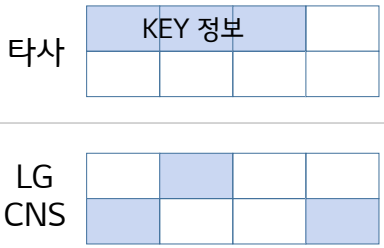
상호인증 서비스 특징

| 서비스 특성에 따른 다양한 상호인증 서비스 제공 |

- 4개 유형의 상호인증 서비스 제공으로 다양한 유형의 IoT 서비스 지원
- 서버와 연결이 끊어진 상태에서도 GW-Device, Device-Device 간 상호인증 서비스 제공

상호인증 안정성

| 분산 저장 방식으로 안전한 KEY 관리 |



- 정해진 위치에 키를 저장
- 시작위치만 알면 KEY 노출

- 랜덤 위치에 키를 분산 저장
- KEY 정보 파악이 어려움

| 2 Factor 상호인증으로 보안 강화 |

Master Key + 상호인증 도큰

- Master Key와 상호인증 도큰의 조합으로 상호인증 수행
- Master Key가 노출되더라도 보안성 유지

LG CNS

9. 기능 소개 (기기등록)

다양한 유형의 기기 등록 서비스를 제공하여, 서비스 특성에 따라 기기 등록 방식을 선택할 수 있음

기기등록 정의

- 상호인증을 위해 필요한 M.K. (Master Key) 정보를 신규 기기에 등록하는 업무
- M.K. 정보를 안전하게 기기에 등록하는 것이 중요 (Initial Key도 M.K.를 암호화하여 전달)

기기등록 서비스 특징

| 다양한 시점에서 기기등록 서비스 이용 가능 |

제조 공장

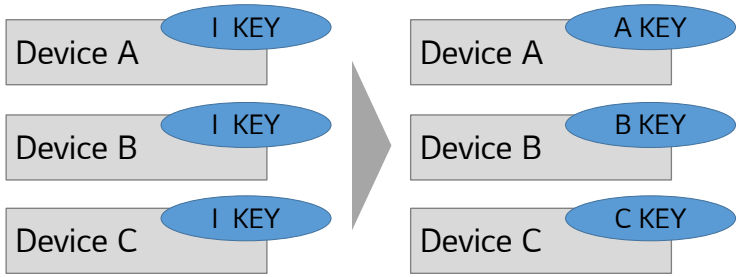
매장 (대리점)

최종 사용자

- 다양한 상황에서의 기기등록 서비스 제공
- 최종 사용자에 의한 기기등록이 일반적임
- 보안성은 제조 > 매장 > 사용자 순으로 높음

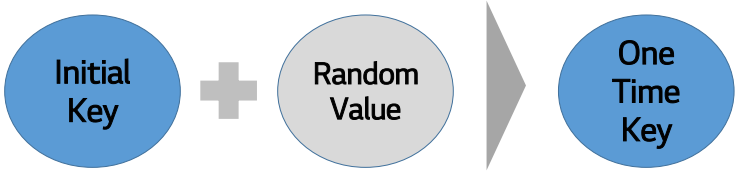
기기등록 안정성

| 기기 별 Initial Key 갱신 서비스 |



제조 단계에서 기기마다 다른 Initial Key도 갱신

| 1회용 KEY도 주요정보(M.K.) 전달 |



Initial Key를 한번 더 변조한 1회용 Key를 사용

LG CNS

9. 기능 소개 (Secure Boot)

FW의 무분별한 변경을 막기 위해 기기 부팅 시점에 OS 및 주요 FW의 변경이 발생했는지 점검합니다.

Secure Boot

- 부팅 시점에 OS 및 주요 FW가 변경되었는지 점검하는 기능
- 인가 받지 않은 OS (또는 FW) 변경이 발생할 경우 부팅되지 않거나 서비스가 동작을 막음

Secure Boot 절차

1. 기기 제조 단계	점검 대상 FW 정의	Secure Boot 시 점검할 주요 FW를 선택
	FW 이미지 추출 및 등록	FW의 이미지 정보를 추출, 결과값은 랜덤 분산 저장
2. 실제 이용 단계 (Booting 時)	현재 FW의 이미지 추출	Booting 시점의 FW 이미지 정보 추출
	미리 등록된 이미지 정보와 비교	추출한 이미지 정보와 미리 저장한 값이 동일한지 비교
	비교 성공 時, 기기 상태정보 갱신	비교 성공 時, 기기 상태정보 변경

9. 기능 소개 (Secure Update)

인가 받은 서버 또는 기기가 요청한 업데이트만 가능하도록 하여, 무분별한 FW의 변경을 막습니다.

Secure Update

- 상호인증을 통해 Update 요청 서버(또는 기기)를 확인
- Update에 필요한 FW 파일이 인가 받은 서버(또는 기기)로부터 전달된 것이 맞는지 검증
- Update를 완료하면, 안전한 방식으로 FW의 이미지 정보를 갱신

Secure Update 절차

1. 요청자 검증 단계	요청자 검증을 위한 상호인증	요청자를 신뢰할 수 있는 상호인증을 통해 검증
2. 업데이트 단계	FW 서명 정보 생성 (요청자)	상호인증을 통한 세션키로 FW 서명값 생성
	FW 서명 정보 검증 (기기)	업데이트 전에 수신 받은 FW 파일의 성명 검증
	FW 업데이트	FW 를 업데이트하고, 완료 후 기기 상태정보 갱신
3. FW 이미지 갱신 단계	FW 업데이트 상태 정보 점검	FW 이미지 정보 갱신 전에 기기 상태 정보 확인
	신규 FW의 이미지 정보 등록	FW 이미지 정보를 랜덤 분산 저장

LG CNS

9. 기능 소개 (주요 정보 보호)

연계정보 및 Credential 정보에 대하여 암복호 및 서명 검증을 통해 안전한 정보 보호를 보장합니다.

연계정보 보호	• 연계 정보 보호를 위한 Crypto 서비스 : Encryption & Decryption, Signature & Verification • MITM(Man In The Middle Attack) 공격 방지를 위한 대응 서비스 : 연계 정보 내 서명생성 및 검증 기능 을 이용하여 중간자에 의한 데이터 변조 차단 : 연계 보안은 상호인증을 통한 Session Key로만 수행하기 때문에 중간자가 내용 확인할 수 없음
Credential 보호	• IoT 보안 플랫폼의 Credential 유형 : Master Key, 상호인증 토큰, Secure Boot를 위한 FW (또는 OS) 이미지 정보 • Credential 보호 방안 (SW 방식 보안 모듈) Credential 정보를 “Trusted Memory”(랜덤 분산 저장 영역)에 보관 (HW 방식 보안 모듈) Smart Card 칩을 이용하여 Credential 정보를 외부에서 읽지 못하도록 함

LG CNS

10. 각 사별 보안 준비 현황

많은 Global Company에서 HW 보안모듈을 포함한 전체적인 보안플랫폼을 준비하거나 출시하고 있습니다.

회사명	준비 현황
LG CNS	- 기기보안 모듈 및 보안관리서버를 포함한 통합 보안 플랫폼 확보 - 기기보안 모듈의 경우 SW 방식 및 HW 방식 모두 제공 - Chip 기반의 AMI 보안 모듈 제작 (2016.08 출시 예정)
삼성전자	- IoT 기기에 공통으로 적용되는 Chip 기반 모듈(ARTIK) 발표 - ARTIK 에는 HW기반의 보안모듈이 포함되어 있으며, 키관리, 상호인증을 위한 보안 연산을 담당
Microsoft	- 2015.09.29에 IoT 서비스 플랫폼 (Azure IoT Suite) 발표 - 플랫폼 내 사용자 인증, Access Control, 데이터 암복호, NW보안, Threat 관리 등 보안기능 탑재 - 기기에 탑재되는 보안모듈은 별도 제공하지 않으며, MS 플랫폼 표준에 따라 개발하도록 가이드
Cisco	- 북미 셋톱박스 보안 모듈 공급사(NDS) 인수 - Home IoT, 자동차, 에너지, 제조 분야에 대한 IoT 보안 서버 플랫폼 및 IoT 기기 보안 모듈 공급
Gemalto, Infineon, NXP	- 스마트카드 및 IoT 기기에 탑재되는 보안 칩 전문 제조사 또는 칩 COS 제조사 - 자동차 보안 모듈 (HSM) 및 스마트폰 보안 모듈(eSE) 제작
ARM	- ARM 기반 CPU를 위한 보안 플랫폼 발표 (mbed)

LG CNS

감사합니다.

LG CNS