IOT 보안 지침

개요서

IoT 보안 지침개요서
버전 2.0
2017 년 10 월 31 일

본 문서는 GSMA 의 구속력이 없는 영구 참조 문서입니다.

보안 분류: 비기밀

본 문서의 열람과 배포는 보안 등급에서 허가된 자에게 한정됩니다. 본 문서는 GSM 협회의 기밀이며 자작권 보호 대상입니다. 본 문서는 공급된 목적에 한하여 사용해야 하며, GSMA 의 사전 서면 승인 없이 보안 등급에 따라 허가받은 자 이외의 사람에게 이 문서 수록된 정보의 전부 또는 일부를 공개하거나 제공해서는 안 됩니다.

저작권 고지

면책 조항

GSM 협회("협회")는 본 문서에 수록된 정보의 정확성이나 완전성, 적시성에 대해 어떠한 진술이나 보증, 약속(명시적으로나 묵시적으로나)도 하지 않고 책임도 지지 아니하며 배상할 의무도 없습니다. 본 문서에 수록된 정보는 예고 없이 변경될 수 있습니다.

독점금지 고지

본 문서에 수록된 정보는 GSM 협회의 독점금지 준수 정책에 부합합니다.

목록

1 서론

1.1 요약

사물 인터넷(IoT)의 등장으로 혁신적인 커텍티드(connected) 상품과 서비스를 개발하려는 서비스 업체들이 속속 생겨나고 있습니다. 전문가들의 예측에 따르면 앞으로 10 년 사이에 수십만 가지 IoT 서비스가 수십 억 IoT 디바이스를 연결할 전망입니다. 이처럼 급격한 사물 인터넷의 성장은 서비스를 확대하고 고객층을 강화하려는 관련 기업에게 매우 좋은 기회입니다.

애널리스트 업계에서는 보안 문제가 신규 IoT 서비스의 보급에 큰 걸림돌이고 그와 동시에 유례 없이 점증하는 IoT 서비스에 대규모 접속이 일어남으로써 전 생태계가 더 큰 사기와 공격에 노출될 것이라고 지적하였습니다. 공격 집단이 이 분야에 점점 더 큰 관심을 갖고 있다는 증거는 이미 많이 나와 있습니다.

신규 서비스 업체들이 특정 시장을 대상으로 새롭고 혁신적인 서비스를 개발하면서 정작 그 서비스가 맞닥뜨릴 수도 있는 위협은 깨닫지 못할 수도 있습니다. 또한 업체 중에 통신망이나 인터넷에 연결되는 서비스를 개발한 전력이 없고 디바이스의 인터넷 연결로 인한 위험을 차단할 기술과 전문성이 없는 곳도 있을 수 있습니다. 반면, 공격을 노리는 측에서는 기술과 보안상의 약점을 파악해 허점이 노출되면 즉시 파고들 태세입니다. 디바이스를 무력화한 공격의 사례는 헤아릴 수 없이 많습니다. 무력화된 디바이스는 데이터를 유출하거나 다른 디바이스를 공격하기도 하고, 관련 여부를 떠나 각종 서비스를 마비시키기도 합니다.

자동차나 보건의료, 가전제품, 공공서비스업 등에 종사하는 서비스 업체 중에는 자사의 보안 요건이 해당 시장에 국한된 것으로 보는 곳이 많으나, 실상은 대개 그렇지 않습니다. IoT 서비스는 거의 다 엔드포인트 디바이스와 서비스 플랫폼 부속품을 구성요소로 하며 그 안에 들어가는 기술은 여타 통신, 컴퓨팅, IT 솔루션과 유사합니다. 그 뿐만 아니라, 설령 공격자의 동기와 보안이 뚫렸을 때 나타나는 영향이 다르더라도 이런 여러 가지 서비스가 직면하는 위협과 그것에 대응하는 솔루션은 대개 매우 유사합니다.

GSMA 가 대표하는 이동통신 업계는 오래 전부터 고객에게 안전한 제품과 서비스를 제공하고 있습니다. 안전한 제품과 서비스의 제공은 과정이자 곧 목표입니다. 솔루션이 위협을 차단할 수 있으려면 경계와 혁신, 대응능력, 그리고 꾸준한 개선이 필수입니다.

네트워크 운영사와 네트워크/서비스/디바이스 장비 업체는 새로 출시되는 IoT 서비스가 보안성을 갖추도록 IoT 서비스를 개발하려는 서비스 업체와 보안 전문성을 공유하고 싶어합니다.

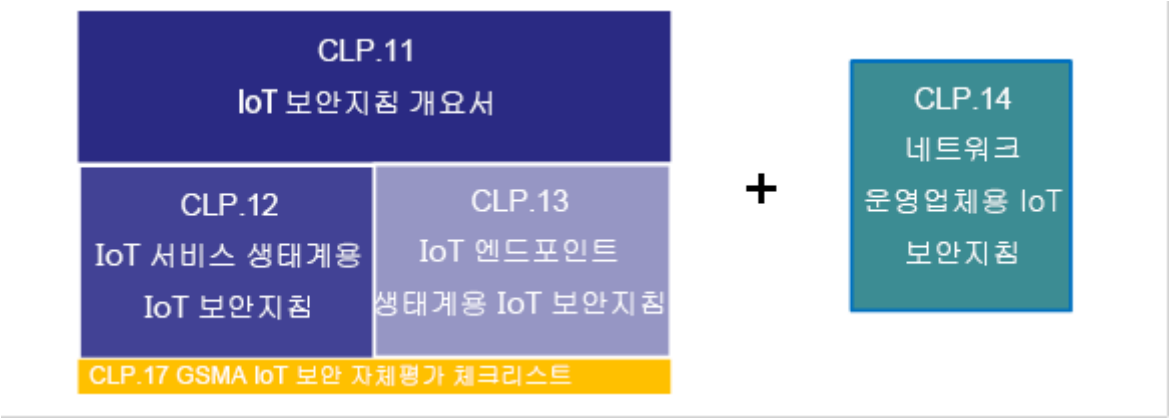
이에 GSMA 에서는 신규 IoT 서비스를 개발하고자 하는 서비스 업체를 위해 보안 지침을 수립했습니다.

1.2 GSMA IoT 보안 지침서 세트

본 문서는 태동기의 "사물 인터넷" 업계가 IoT 보안 문제를 함께 이해할 수도 있도록 마련한 GSMA 보안 지침서 중 그 첫 번째 부분입니다. 이 지침서는 안전한 IoT 서비스를 개발하는

방법을 보급해 서비스 분야 전체에서 보안 모범 사례가 정착되게 하는 데 목적이 있습니다. 지침서에서는 IoT 서비스에 만연한 보안 위협과 취약점에 대처하는 방안을 제시합니다.

GSMA 보안 지침서의 구성은 다음과 같습니다. 본 문서(예, 개요서)는 부속 문서를 읽기 전에 일종의 예비서로 읽는 것이 좋습니다.



도 1 - GSMA IoT 보안 지침서 구조

네트워크 운영사, IoT 서비스 업체와 IoT 생태계의 기타 협력사들은 시스템 보안과 데이터 보호를 위해 IoT 서비스 업체에게 서비스를 제공하고자 하는 네트워크 운영사를 대상으로 최상위 보안 지침을 제시하는 GSMA 문서 CLP.14 "네트워크 운영자용 IoT 보안 지침서(IoT Security Guidelines for Network Operators)"[13]를 읽어 보시기 바랍니다.

1.2.1 GSMA IoT 보안 평가 체크리스트

문서 CLP.17 [16]에 평가 체크리스트가 제시돼 있습니다. IoT 제품과 서비스, 구성품 공급업체는 본 문서를 통해 자사의 제품과 서비스, 구성품이 GSMA IoT 보안 지침에 부합하는지 스스로 평가할 수 있습니다.

GSMA IoT 보안 평가 체크리스트[16]를 작성하면 회사가 사이버 위험으로부터 제품과 서비스, 구성품을 보호하기 위해 강구한 보안 조치를 검증할 수 있습니다.

작성된 신고서를 GSMA 에 제출하면 평가 확인을 받을 수 있습니다. GSMA 웹사이트에서 아래 절차를 참고하십시오.

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.3 문서의 목적

IoT 보안 지침서의 목적은 IoT 기술 또는 서비스 구현 담당자에게 안전한 제품을 구축하는 설계 지침을 제공하는 데 있습니다. 이를 위해 본 문서에서는 기술 또는 서비스의 어떤 측면이 구현 담당자와 관련이 있는지 알려주는 중요한 모델을 제시합니다. 측면 또는 구성품이 확인되면 구현 담당자는 각 구성품과 관련된 위험을 평가해 보완 방법을 결정할 수 있습니다. 각 구성품은 *하위 구성품*으로 세분할 수 있으며, 여기에서 더 세밀한 위험을 기술할 것입니다.

각 위험에는 우선순위가 부여되며, 구현 담당자는 그것을 참고로 하여 위험의 비용과 시정 비용, 위험에 대처하지 않았을 때의 비용(있을 경우)을 산정합니다.

본 문서의 범위는 IoT 서비스의 설계와 구현에 관한 제언으로 한정됩니다.

본 문서에서는 IoT 사양이나 표준의 개발을 제안하지 아니하며 현재 시중에 나와 있는 솔루션과 표준, 모범 사례만을 언급합니다.

본 문서는 또 기존 IoT 서비스의 퇴출을 촉구하려는 목적도 없습니다.

지역에 따라 필요한 경우 국가의 법규가 본 문서에 명시된 지침에 우선할 수도 있습니다.

1.4 대상 독자

본 문서의 주된 독자는 다음과 같습니다.

- IoT 서비스 업체 - 새롭고 혁신적인 커넥티드 제품과 서비스를 개발하고자 하는 기업이나 조직. IoT 서비스 업체가 많이 활약하고 있는 업종으로는 스마트홈, 스마트 시티, 자동차, 운수, 건강, 전기, 가전 등이 있습니다.
- IoT 디바이스 제조업체 - IoT 서비스가 가능하도록 IoT 서비스 업체에게 IoT 디바이스를 공급하는 업체.
- IoT 개발업체 - IoT 서비스 업체를 대신해 IoT 서비스를 개발하는 업체.
- 스스로 IoT 서비스 업체이거나 IoT 서비스 업체를 대신해 IoT 서비스를 구현하는 네트워크 운영업체.

1.5 정의

용어	설명
액세스 포인트 이름	엔드포인트 디바이스가 연결되는 네트워크 연결 지점의 식별자. 여러 가지 서비스 타입과 연결돼 있으며 네트워크 운영업체별로 구성되는 경우가 많습니다.
공격자	정보를 탈취하거나 파괴하거나 제한하거나 위조할 목적을 지닌, IoT 서비스를 상대로 한 해커나 위협원, 위협 액터, 사기꾼, 그 외 악성 위협. 이 같은 위협은 단독 범인이나 조직 범죄, 테러, 적대적 정부 및 그 기관, 산업 스파이, 해킹 그룹, 정치 활동가, '하비스트' 해커, 연구자, 의도하지 않은 보안 또는 프라이버시 침해에서 올 수 있습니다.
클라우드	애플리케이션과 그 데이터를 호스팅하고 저장, 관리, 처리하는 인터넷상의 원격 서버 네트워크.
컴플렉스 엔드포인트	휴대전화나 위성 같은 장거리 통신, 또는 이더넷 같은 유선 연결을 통해 백엔드 서버로 상시 연결되는 엔드 포인트 모델. 자세한 내용은 CLP.13 [4]를 참고하십시오.
구성품	문서 CLP.12 [3]와 CLP.13 [4]에 수록된 구성품을 말합니다.
임베디드 SIM	디바이스에서 분리하거나 교체할 수 없는 SIM 으로서 GSMA SGP.01 [02]에 따라 프로필을 안전하게 바꿀 수 있습니다.

용어	설명
엔드포인트	경량 엔드포인트, 컴플렉스 엔드포인트, 게이트웨이, 기타 커넥티드 디바이스를 일컫는 일반적 용어. 자세한 내용은 CLP.13 [4]를 참고하십시오.
엔드포인트 생태계	현실 세계와 디지털 세계를 색다르게 연결하는 저 복잡도 디바이스와 리치 디바이스, 게이트웨이의 구성. 자세한 내용은 4.2 절을 참고하십시오.
사물 인터넷	복수의 기계와 디바이스, 어플라이언스가 조율된 형태로 복수의 네트워크를 통해 인터넷에 연결된 상태를 일컫는 말. 여기서 디바이스란 태블릿, 가전제품 외에도 통신 기능이 있어 데이터를 주고 받을 수 있는 자동차, 모니터, 센서 등 일상적인 기물을 통칭한다.
IoT 서비스	IoT 디바이스에서 나온 데이터를 이용해 서비스를 하는 컴퓨터 프로그램을 통칭합니다.
IoT 서비스 업체	새롭고 혁신적인 커넥티드 제품과 서비스를 개발하고자 하는 기업이나 조직.
네트워크 운영업체	IoT 엔드포인트 디바이스를 IoT 서비스 생태계와 연결하는 통신 네트워크의 운영자 또는 소유자.
조직의 신뢰 기반(RoT)	ID 와 애플리케이션, 통신의 암호화 보안 방법을 관장하는 암호화된 정책과 절차.
권고 사항	문서 CLP.12 [3]와 CLP.13 [4]에 수록된 제언을 말합니다.
위험	문서 CLP.12 [3]와 CLP.13 [4]에 수록된 위험을 말합니다.
보안 업무	문서 CLP.12 [3]와 CLP.13 [4]에 수록된 보안 업무를 말합니다.
서비스 액세스 포인트	통신 네트워크를 통해 IoT 서비스의 백엔드 인프라에 들어가는 지점.
IoT 서비스 생태계	기능을 제공하고 실무에 배치된 엔드포인트에서 데이터를 수집하는 데 필요한 일단의 서비스와 플랫폼, 프로토콜, 기타 기술. 자세한 내용은 3.1 절을 참고하십시오.
SIM(Subscriber Identity Module, 구독자 ID 모듈)	모바일 네트워크에서 디바이스의 모바일 네트워크 연결과 네트워크 서비스 접근을 허용하기 위해 사용되는 스마트 카드.
UICC	ETSI TS 102 221 에 명시된 보안 요소 플랫폼으로서 암호화를 통하여 분리된 보안 도메인에서 복수의 표준화 네트워크 또는 서비스 인증 애플리케이션을 지원할 수 있는 것을 말합니다. ETSI TS 102 671 에 명시된 임베디드 폼 팩터 안에 구현될 수도 있습니다.

1.6 약어

용어	설명
3GPP	3 세대 프로젝트 파트너십
API	응용 프로그램 인터페이스
APN	액세스 포인트 이름
CERT	컴퓨터 비상 대응팀

용어	설명
CLP	GSMA 커넥티드 리빙 프로그램
CPU	중앙처리장치
EAP	확장형 인증 프로토콜
EEPROM	전기적으로 지울 수 있고 프로그램 가능한 읽기 전용 메모리
GBA	범용 부트스트래핑 아키텍처
GPS	위성 위치 확인 시스템
GSMA	GSM 협회
GUI	그래픽 사용자 인터페이스
HIPAA	건강보험 이전 및 책임에 관한 법
IoT	사물 인터넷
LPWA	저전력 장거리 통신
LTE-M	기계 롱텀 에볼루션
NB-IoT	협대역 사물 인터넷
NIST	국립표준기술원
OBD	온보드 진단
OCTAVE	운영에 치명적인 위협, 자산, 취약성 평가
OMA	오픈 모바일 연대
PIA	프라이버시 침해 평가
PII	개인 식별 정보
RAM	랜덤 액세스 메모리
SIM	구독자 ID 모듈

1.7 참고 문서

참고	문서 번호	제목
[1]	해당 없음	“The Mobile Economy 2017” http://www.gsmamobileeconomy.com/
[2]	SGP.01	“Embedded SIM Remote Provisioning Architecture” https://www.gsma.com/iot/embedded-sim/
[3]	CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[4]	CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[5]	해당 없음	NIST Risk Management Framework http://csrc.nist.gov/groups/SMA/fisma/framework.html

참고	문서 번호	제목
[6]	CMU/SEI-2007-TR-012	Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process http://www.cert.org/resilience/products-services/octave/
[7]	사용하지 않음	사용하지 않음
[8]	TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org
[9]	RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) www.ietf.org
[10]	해당 없음	Conducting privacy impact assessments code of practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[11]	해당 없음	오픈 모바일 연대 http://openmobilealliance.org/
[12]	해당 없음	oneM2M Specifications http://www.onem2m.org/
[13]	CLP.14	IoT Security Guidelines for Network Operators https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[14]	GE.11-13201	Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	해당 없음	Right to Internet Access https://en.wikipedia.org/wiki/Right_to_Internet_access
[16]	CLP.17	GSMA IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/

2 사물 인터넷이 낳은 과제들

몇 년 전 국제연합에서는 인터넷이 인간의 기본권이며 전 세계 누구나 광대역 서비스를 이용할 수 있어야 한다고 선언했습니다[14]. 최근에는 프랑스, 그리스, 스페인 등[15]에서 인터넷 접속을 확대하고 개인의 정보 및 인터넷 접속을 부당하게 제한하지 못하게 하는 법이 제정되었습니다.

이 같은 조치는 인터넷의 발달에서 파생된 급격한 사회적, 기술적 변화의 결과입니다. 이로써 인터넷은 삶의 방식이자 온갖 정보의 주요 원천이 되었고 또 사랑하는 사람이나 친구와 연락을 주고 받을 때 가장 많이 이용하는 수단이 되었습니다 인터넷은 단순한 기술이 아니라 일상의 *한 부분*이 되었습니다.

상시 연결을 향한 욕구가 커지면서 최근 몇 년 사이 기술이 급격하게 발전하였습니다. 기술전문가 집단이 10 여 년 전부터 "사물 인터넷 시대가 오고 있다"고 외치긴 했으나 정보에 대한 유비쿼터스적 접근과 그에 필요한 비용 모델이 실용적인 비즈니스 모델의 탄생으로 이어진 것은 5 년 전부터입니다. 그 시기에 이르러 구성품 비용이 급격히 낮아졌고 무선 서비스의 범위와 속도가 크게 확대되고 또 높아졌습니다. 프로토콜과 배터리 수명, 나아가 비즈니스 모델까지도 정보와 연결에 대한 유례 없는 수요의 증가를 수용할 수 있도록 발전하였습니다.

그것이 바로 사물 인터넷의 핵심입니다. 중요한 것은 사물이 아닙니다. 사람입니다. 사람 인터넷입니다. 사람과 디지털 세상은 더 이상 서로 동떨어진 존재가 아니라 이 새로운 생활 양식을 매개로 그 어느 때보다 가까운 사이가 되었습니다.

사람의 실제 경험이 유례 없이 긴밀하게 디지털 세계과 연결돼 있으므로 디지털 세계는 보호를 받아야 합니다. 디지털의 보안이 현실 세계에 직접 영향을 미치기 때문입니다. 사물 인터넷은 세계가 함께 전진하여 유례 없이 거대한 지식과 경험, 혁신의 데이터베이스를 만들기에 좋은 기회입니다. 그러나 그 과정이 순탄하게 진행되려면 이 같은 연결의 원동력이 되는 기술을 확보해야 합니다. 그리하여 사생활과 신뢰성, 서비스의 질을 보장하고 이 대단한 효용과 이 긴요한 기본 욕구를 필요한 사람 누구나 충족할 수 있게 해야 합니다.

사물 인터넷이 효과적으로 발전하려면 성장에 수반하는 보안 문제를 해결해야 합니다. 주요 보안 문제는 다음과 같습니다.

- 가용성: 엔드포인트와 그 서비스 사이에 상시 연결상태를 유지하는 문제
- ID: 엔드포인트와 서비스, 엔드포인트를 운영하는 고객 또는 최종 사용자를 인증하는 문제
- 프라이버시: 개별 최종 사용자에 대한 피해 가능성을 낮추는 문제
- 보안: 시스템의 무결성을 확인하고 추적하고 감시하는 문제

2.1 가용성문제

사물 인터넷이 예상 속도로 발전하려면 엔드포인트 디바이스가 서로, 최종 사용자와 또 백엔드 서비스와 끊임 없이 통신할 수 있어야 합니다. 이를 위해 저출력 디바이스의 상시 연결을 책임지는 NB-IoT, LTE-M 과 같은 신기술이 도입되고 있습니다. 이는 현대 세계의

유비쿼터스 인터넷 접속이라는 문제와도 일맥상통합니다. 이것이 성공하려면 다음과 같은 물음에 대한 답이 필요합니다.

- 저전력 장거리 통신(Low Power Wide Area, LPWA) 네트워크(예: NB-IoT 와 LTE-M)를 어떻게 종래의 휴대전화 시스템과 비슷한 보안 수준으로 설치하고 운영할 것인가?
- IoT 엔드포인트가 네트워크 경계 전반으로 마이그레이션할 때 복수의 모바일 업체가 어떻게 같은 수준의 네트워크 보안을 지원할 것인가?
- 게이트웨이 엔드포인트를 이용해 통신하는 모세관 엔드포인트에 어떻게 네트워크 신뢰를 *전달*할 것인가?
- 보안 통신 환경에서 어떻게 경량 엔드포인트의 전력 제약 문제를 해결할 것인가?

2.2 ID 문제

엔드포인트가 IoT 제품이나 서비스 생태계 없이 작동하려면 피어(peer)와 서비스에게 자기의 ID 를 안전하게 밝힐 수 있어야 합니다. 이는 IoT 기술의 핵심이자 기본으로 서비스와 피어는 이를 통해 어떤 데이터가 누구에게 전달되고 있는지 보장할 수 있습니다. ID 와 직접 관련된 문제에는 정보와 서비스에 대한 접근만 있는 것은 아닙니다. 다음 물음에 대한 답도 구해야 합니다.

- 엔드포인트를 운영하는 사용자가 엔드포인트 신원과 긴밀하게 연계될 수 있을 것인가?
- 서비스와 피어가 어떻게 엔드포인트의 신원을 확인하여 최종 사용자의 신원을 확인할 수 있을 것인가?
- 엔드포인트 보안 기술이 피어와 서비스를 안전하게 인증할 수 있을 것인가?
- 불량 서비스와 피어가 인증받은 서비스와 피어로 가장할 수 있을 것인가?
- 디바이스의 신원을 어떻게 탬퍼링이나 조작으로부터 보호할 것인가?
- 엔드포인트와 네트워크에서 어떻게 IoT 서비스가 엔드포인트에 대한 접속 허가를 받을 수 있을 것인가?

2.3 프라이버시 문제

프라이버시를 더 이상 기본 제품과 서비스에 대한 추가항목으로 보면 안 됩니다. 실제 세계가 디지털 세계의 액션에 직접 영향을 받으므로, 프라이버시를 제품 설계 시점부터 고려하여 모든 액션이 승인을 받고 모든 신원이 검증을 받게 하며 동시에 그 액션과 관련 메타 데이터가 허가받지 않은 자에게 노출되지 않게 해야 합니다. 이것은 제품 또는 서비스의 아키텍처를 적절하게 정의할 때에만 가능하며, 소급하여 실행하기는 지극히 어렵고 비용이 많이 듭니다.

의료 기기, 자동차 솔루션, 산업 제어 시스템, 홈 오토메이션, 건물 및 보안 시스템 등은 사람의 실제 생활에 직접 영향을 미칩니다. 이들 제품과 서비스에 가능한 최고 수준의 보안을 확보해 물리적 피해와 프라이버시 관련 데이터의 노출 가능성을 낮추는 것은 엔지니어의 책임입니다.

그러므로 프라이버시가 최종 사용자뿐만 아니라 IoT 의 설계 방식에 어떻게 영향을 미치는지 자문해 봐야 합니다.

- 엔드포인트의 신원이 무허가 사용자에게 노출되는가?

- 고유한 엔드포인트 또는 IoT 서비스 식별정보를 통해 최종 사용자나 엔드포인트를 실제로 모니터링하거나 추적할 수 있을 것인가?
- 엔드포인트 또는 IoT 서비스에서 나오는 데이터가 위치나 액션, 상태(*수면* 또는 *활성*) 등 최종 사용자의 물리적 속성을 나타내거나 그것과 직접 관련이 있는가?
- 도출되는 사이퍼 텍스트의 패턴이 보이지 않도록 충분한 보안으로 기밀유지와 무결성이 확보되는가?
- 제품 또는 서비스가 사용자 고유의 개인식별정보(PII)를 어떻게 저장하거나 처리하는가?
- 최종 사용자가 IoT 서비스 또는 제품에서 PII 를 저장하거나 사용하는 것을 제어할 수 있는가?
- 데이터의 안전 확보를 위해 사용되는 보안 키와 보안 알고리즘을 갱신할 수 있는가?

2.4 보안 문제

최근 몇 십년 사이에 인터넷 보안은 크게 개선되었지만 현대 기술의 전반적 건강 상태에는 몇 가지 큰 격차가 있었습니다. 그 격차가 가장 두드러진 곳은 IoT 기술의 2 대 주축인 임베디드 시스템과 클라우드 서비스였습니다.

IoT 가 다수의 사용자 그룹과 물리적 시스템을 위험에 빠뜨리지 않으면서 성장하게 하려면 엔드포인트와 IoT 서비스 모두에 정보 보안 관행을 이식해야 합니다.

- 프로젝트 시작 시점에 제품이나 서비스에 보안 모범 사례가 이식되는가?
- 소프트웨어 또는 제품 개발 수명 주기에 보안 수명 주기가 이식되는가?
- 임베디드 시스템에서 작동하는 서비스와 애플리케이션 모두에 애플리케이션 보안이 적용되고 있는가?
- TCB(Trusted Computing Base)가 엔드포인트와 서비스 생태계에 모두 구현되는가?
- TBC 가 어떻게 애플리케이션 이미지와 서비스에 대해 자체 검증을 실시하는가?
- 엔드포인트 또는 IoT 서비스가 그 구성 또는 애플리케이션에 이상이 있는지 탐지할 수 있는가?
- 엔드포인트에 악성 거동의 징후가 있는지 어떻게 모니터링하는가?
- 제품 또는 서비스 보안 과정에 인증과 신원정보가 연계되는가?
- 무력화를 나타내는 이상징후에 대해 어떤 사고 대응 계획이 정의돼 있는가?
- 무력화를 빠르고 효과적으로 차단하기 위해 서비스와 리소스는 어떻게 분화해 두고 있는가?
- 무력화 후 서비스와 리소스는 어떻게 복원하는가?
- 공격을 탐지할 수 있는가?
- 무력화된 시스템 구성요소를 탐지할 수 있는가?
- 고객이 보안 문제를 어떻게 보고할 수 있는가?
- 엔드포인트를 업데이트하거나 패칭하여 취약점을 해소할 수 있는가?

3 모바일 솔루션

지금껏 IoT 에 연결 솔루션을 제공하는 기술은 많았지만 모바일 네트워크만큼 IoT 에게 큰 영향을 끼친 것은 없었습니다. 모바일 네트워크는 20 여년 전에 소비자와 업계에 무선 서비스를 제공하기 시작하였고 그 이후 안정적이고 안전하며 비용 대비 효과가 우수한 서비스를 제공하고 있습니다. 모바일 업계는 무선망을 장거리에 걸쳐서 관리해야 하는 특성상 네트워크 가용성에 폭넓은 경험을 갖고 있습니다. 네트워크 아이디는 수많은 표준과 디바이스 기술, 프로토콜, 분석 모델을 낳을 만큼 어려운 문제였습니다. 프라이버시와 보안은 모바일 업계의 오래 된 고민으로, 모바일 업계는 각종 모바일 기술에서 남용과 아이디 도용, 사기를 줄이고자 노력하고 있습니다.

모바일 업계에서는 NB-IoT 와 LTE-M 이라고 하는, 라이센스 기반의 LPWA(Low-Power Wire-Area) 무선 네트워크 기술를 제공하고 있습니다. 이 LPWA 네트워크 기술은 종래의 모바일 네트워크가 제공하던 광역 무선 연결을 훨씬 낮은 전력으로 제공하면서도 통신 효과에는 변함이 없습니다. 여러 네트워트 운영업체에서 LPWA 서비스를 채택하고 있어 NB-IoT 와 LTE-M 이 LPWA 네트워크 도입의 사실상 표준이 될 전망입니다.

각국의 NB-IoT 와 LTE-M 네트워크 도입에 관한 사항은 GSMA 홈페이지(https://www.gsma.com/iot/mobile-iot-initiative/)에서 더 자세히 확인할 수 있습니다.

3.1 가용성 문제의 해결

GSMA 의 "The Mobile Economy 2017" 보고서[1]에 다음과 같은 내용이 수록돼 있습니다.

- 2016 년 말 현재 전 세계 인구의 2/3, 즉 48 억 명이 모바일 구독자였습니다. 2020 년까지는 전 세계 인구의 3/4, 즉 57 억 명이 모바일 서비스를 이용할 전망입니다.
- 광대역 네트워크와 스마트폰의 성장세는 계속 이어질 전망입니다. 모바일 광대역 연결(3G 와 4G 기술)은 2016 년 전체 연결의 55%를 차지하였습니다. 2020 년께에는 3/4 에 가까워질 것입니다. 4G 연결의 비중도 2020 년 말까지 23%에서 41%까지 높아질 것으로 예측됩니다.
- 2016 년과 2020 년 사이에 모바일 연결이 23 억 회선 추가돼 비중이 73%까지 높아질 것으로 전망됩니다. 4G 의 비중 확대가 2016 년의 키워드로 자리잡은 가운데, 그 해 4G 회선은 55%까지 높아졌습니다. 그 결과 2020 년이 되면 2G 연결의 존재감은 크게 낮아질 것으로 보입니다.
- 전 세계 LPWA 디바이스 시장은 성장을 계속해 2020 년 경 14 억 회선 정도가 될 전망입니다. 2022 년 50 억 회선을 예상하는 업계 전문가도 있습니다.

3.2 ID 문제의 해결

ID 관리는 지난 수십 년 동안 큰 과제였으며 모바일 업계의 표준과 기술 구성을 크게 강화하는 역할을 했습니다. 모바일 산업은 대개 탈착식 SIM 카드와 연관돼 있지만, GSMA 에서는 "임베디드 SIM 원격 프로비저닝 아키텍처"[2]라고 하는 SIM 기반 솔루션을 만들었습니다. 이 솔루션은 IoT 에 적용하기에 좋아 엔드포인트 디바이스의 부품 단위 통합 심화와 생산비 절감,

OTA(Over-The-Air) 플랫폼을 통한 연결 관리를 실현할 수 있습니다. 그 결과 IoT 엔드포인트 디바이스의 연결 성능은 수명이 다할 때까지 유지됩니다.

임베디드 SIM 과 같은 ID 기술은 보안을 기본으로 통합하는 트러스트 앵커(trust anchor)로 설계됩니다. 다음과 같은 공격에 견디도록 제조되는 것입니다.

- 글리치
- 부채널 분석
- 수동 데이터 인터셉트
- 물리적 탬퍼링
- ID 도용

이미 보안으로 가득한 이 기술에 또 한 가지 커다란 진전이 나타났으니 바로 차세대 트러스트 앵커에 IoT 의 새 기능이 추가된 것입니다. 이들 기술은 겸용이 됩니다. 즉, 트러스트 앵커가 종래의 컴퓨팅 트러스트 앵커와 유사하게 네트워크의 보안을 검증하는 일뿐만 아니라 애플리케이션 통신과 애플리케이션 그 자체의 보안을 지키는 일까지 하게 된다는 뜻입니다.

이 같은 겸용 기술은 3GPP GBA [8], OMA [11], oneM2M [12] 등이 제공하는 것과 같은 모바일 산업 보안 규격의 통합으로 더욱 강화될 전망입니다. 겸용 기술로 현장에서 디바이스를 안전하게 프로비저닝하고 안전하게 OTA 펌웨어 업데이트를 구현할 수 있으며 디바이스 기능과 ID 를 관리할 수 있습니다.

이들 기술을 함께 사용하면 복잡한 에지니어링 프로세스를 간소화해 간단한 구성품에 넣을 수 있습니다. 애플리케이션 엔지니어가 스스로 관리해야 하는 복잡한 기술을 만들지 않고 이미 네트워크 ID 를 관리하고 있는 네트워크 운영자가 애플리케이션 대신 그 업무를 수행할 수 있습니다. 이렇게 되면 엔지니어링의 복잡도가 낮아질 뿐만 아니라 사업의 일상적 관리 요건도 줄어듭니다.

3.3 프라이버시와 보안 문제의 해결

모바일 업계에서는 SIM 기능과 함께 복구형 프로토콜과 프로세스, 모니터링 시스템을 개발해 보안을 강화하고 사기와 기타 악성 활동의 여지를 낮춰 왔습니다. 예컨대, 3G 와 4G 기술은 상호 인증을 통해 엔드포인트와 네트워크의 ID 를 검증합니다. 이 프로세스로 도청자는 통신을 인터셉트할 수 없게 됩니다.

나아가, SIM 과 GBA [8] 또는 EAP-SIM [9]과 같은 기술의 적용으로 네트워크 기술을 확보할 수도 있습니다. 이 기술을 이용하면 잘 알려진 프로토콜로 애플리케이션 네트워크 피어와 통신할 때 쓸 수 있는 세션 보안 키로 SIM 을 프로비저닝할 수 있습니다. 이렇게 하면 도청자가 애플리케이션 프로토콜을 조작해 디바이스나 서비스를 무력화할 여지가 사라집니다. 따라서 이 모델로 네트워크와 애플리케이션의 보안을 모두 확보할 수 있습니다.

4 IoT 모델

아래 그림은 본 문서에서 사용되는 표준 IoT 모델이 서비스와 엔드포인트 생태계의 구성요소임을 보여주고 있습니다. 각 구성요소는 하위 구성요소들로 구성되는데, 이는 주요

구성요소만을 다루는 별도 문서에서 자세히 설명합니다. 예컨대, 엔드포인트 구성요소와 그 각각의 위험은 본 문서 세트에 포함된 엔드포인트 생태계 문서[3]에서 소개하고 서비스 구성요소는 서비스 생태계 문서[4]에서 소개합니다.

도 2 - IoT 모델의 예

이 다이어그램은 현대의 거의 모든 IoT 서비스와 제품 모델에서 상용화 가능 기술을 도입할 때 필요한 주요 구성요소를 정의합니다.

통신 네트워크 구성요소는 IoT 에 내재돼 있으며 본 모델에서는 두 생태계를 연결합니다. 이때 통신 링크의 각 '끝'(end)은 해당 엔드포인트 생태계 문서와 서비스 생태계 문서에서 설명합니다.

GSMA 의 "네트워크 운영자를 위한 IoT 보안 지침(IoT Security Guidelines for Network Operators)"[13]에서 네트워크 운영자를 위한 네트워크 보안 지침 권고 사항을 확인할 수 있습니다.

4.1 서비스 생태계

서비스 생태계란 기능을 제공하고 현업에 도입된 엔드포인트에서 데이터를 수집할 때 필요한 서비스와 플랫폼, 프로토콜, 그 외 기술의 집합을 말합니다. 이 생태계는 주로 엔드포인트에서 데이터를 모아 서버 환경 안에 저장합니다. 저장된 데이터는 그것의 시각적 묘사를 여러 사용자 인터페이스에 전달하여 사용자에게 렌더링할 수 있습니다. 이 데이터는 메트릭스나 파라미터, 명령어 형태를 띠기도 하는데 서비스 인프라에서 유래하는 API(예: oneM2M[12])를 통해 3 자에게 전달할 수도 있습니다. IoT 서비스 업체가 서비스를 수익화할 때 흔히 쓰는 방법입니다.

본 문서에서 소개하는 프로세스와 함께 사용될 서비스 생태계 보안 지침이 CLP.12 IoT 서비스 생태계를 위한 IoT 보안 지침(IoT Security Guidelines for IoT Service Ecosystem)[4]에 수록돼 있습니다.

4.2 엔드포인트 생태계

엔드포인트 생태계[4]는 저복잡도의 디바이스와 리치 디바이스, 그리고 실제 세계와 디지털 세계를 여러 가지 유무선 네트워크를 통해 연결하는 게이트웨이로 구성됩니다. 보편적인 엔드포인트의 예로는 모션 센서, 디지털 도어락, 자동차 텔레매틱스 시스템, 센서 주도형

산업제어시스템 등이 있습니다. 엔드포인트는 주변의 실제 환경에서 메트릭스를 수집해 그 데이터를 여러 가지 형식으로 미세 네트워크 또는 셀룰러 네트워크를 통해 서비스 생태계로 보냅니다. 종종 응답으로 명령어나 액션을 받기도 합니다. 여기에는 엔드포인트를 통해 또는 서비스 생태계에서 획득한 데이터를 렌더링하는 리치 사용자 인터페이스가 포함될 수도 있습니다.

본 문서에서 소개하는 프로세스와 함께 사용될 엔드포인트 생태계 보안 지침이 CLP.13 IoT 엔드포인트 생태계를 위한 IoT 보안 지침(IoT Security Guidelines for IoT Endpoint Ecosystem)[13]에 수록돼 있습니다.

5 위험 평가

위험 평가라는 개념은 수십 년 전부터 있었지만 기업에서는 정보 보안보다는 일반적인 사업 위험에 이 개념을 더 많이 적용합니다. 그러나 사업의 기술 측면을 안전하게 오래 운영하려면 정보 보안 위험 평가 절차 또한 중요합니다. 엔지니어링 팀이 사업의 성패를 가르는 IoT 기술에서는 당연히 위험 평가 절차가 조직 보안 실무 구축의 첫 단계가 되어야 합니다.

어느 조직이든 기술 위험을 미시적으로 파악해야 하지만 위험 평가는 다음과 같은 거시적 질문으로 시작해야 합니다.

- 어떤 자산(디지털 vs 실제)을 보호해야 하는가?
- 어떤 집단의 사람들(보이는 사람 또는 보이지 않는 사람)이 잠재적으로 위협적인 존재인가?
- 조직에 대한 위협이란 무엇인가?
- 취약성이란 무엇인가?
- 보호 대상 자산이 무력화되면 어떤 결과가 나타나겠는가?
- 자산이 무력화될 확률은 어느 정도인가?
- 여러 가지 공격자 *집단*과 마주했을 때 어떤 결과가 나타나겠는가?
- 해당 자산이 조직과 그 협력업체에게는 어떤 가치를 지니는가?
- 무력화되고 있는 자산이 안전에 미치는 영향은 어느 정도인가?
- 취약성을 시정하거나 완화하려면 어떻게 해야 하는가?
- 새로 생겨났거나 진화하고 있는 보안의 허점을 어떻게 모니터링할 수 있는가?
- 해결할 수 없는 위험은 무엇이며 그것이 조직에는 어떤 의미가 있는가?
- 사고 대응, 모니터링, 위험 해소에 어느 정도 예산을 배정해야 하는가?

위 질문을 출발점으로 삼는다면 엔지니어링팀과 정보기술팀이 조직과 더 효과적으로 일을 할 수 있을 것입니다. 관건은 기업의 기술 파트가 임원 파트와 위험 및 가치, 시정 계획에서 의견 일치를 보는 것입니다. 팀이 함께 일을 하게 되면 사업에 대한 위험뿐만 아니라 자산의 가치까지도 좀 더 현실적으로 볼 수 있습니다. 이는 남아 있는 보안 허점의 해결에 집행해야 하는 예산과도 직접적으로 관련이 있습니다.

아예 해결이 불가능한 위험도 존재합니다. 본 지침에서 그런 위험 가운데 몇 가지를 살펴볼 것입니다. 조직은 이 같은 위험을 살펴 수용 가능한 수준인지 판단해야 합니다. 그러면 조직은

자신의 한계와 기술의 한계 그리고 특정 유형의 위협에 대응하는 조직의 능력을 현실적으로 파악할 수 있습니다. 보안의 허점을 모두 비용 효율적인 방법으로 해결할 수 있다고 가정하는 것만큼 큰 자원의 낭비는 없습니다.

5.1 목표

위험 평가의 목표는 조직의 기술 파트에서 발견된 보안상 허점을 시정하고 모니터링하고 그것에 대응하는 일단의 정책과 절차, 통제장치를 만드는(또는 개선하는) 데 있습니다. 위험 평가의 결과물은 조직이 그 기술뿐만 아니라 기술을 관리하고, 설계하고 도입하는 방식까지도 조정하도록 유도해야 합니다. 위험 평가의 결과에 조직이 사용하는 정보와 자원의 가치가 제대로 반영되면 조직의 인력과 프로세스, 정책이 개선돼 사업 전반에 안전성이 확보됩니다.

위험 평가의 결과물 활용이 주는 주요 효과는 다음과 같습니다.

- 직원과 정보 고유
- 프로세스 개선
- 정책 정의(또는 갱신)
- 시정조치 실시
- 새로운 허점 모니터링
- 제품 또는 서비스 개선

이로써 조직은 인력과 프로세스 보안의 기본 플랫폼을 구축할 수 있습니다. 그리고 이 플랫폼으로 조직의 역할과 책임을 끊임 없이 평가하고 가다듬어야 합니다.

5.2 위험 모델 예시

본 문서에서는 위험 평가 및 위협 모델링 프로세스를 정의하지 않습니다. 아래에 위험 평가 프로세스의 예가 상세하게 제시돼 있으므로 참고하기 바랍니다.

- 미국 국립표준기술연구소(NIST)의 위험관리 체제(Risk Management Framework)[5]
- 컴퓨터 비상대응팀(CERT)의 OCTAVE 모델[6]

6 사생활 보호 문제

앞으로 많은 IoT 서비스와 제품이 데이터를 만들고 수집하고 공유하도록 설계될 것입니다. 이런 데이터 중에는 '개인정보'로 간주되지 않거나 소비자의 사생활을 침해하지 않아 데이터 보호법과 개인정보보호법의 적용을 받지 않는 것도 있을 것입니다. 기계의 실제 상태에 관한 정보, 내부 진단 데이터, 네트워크 상태에 관한 메트릭스 등이 그것입니다.

그러나 IoT 서비스 중 다수는 소비자 개인에 관한 정보나 개인과 관련된 정보를 다뤄 일반적인 데이터 보호법과 개인정보보호법의 적용을 받게 될 것입니다. 모바일 운영업체가 IoT 서비스를 제공한다면 이동통신과 관련된 사생활보호 및 보안 규칙까지도 적용받게 됩니다. '소비자' 중심의 IoT 서비스는 개인의 사생활과 직결된 상세 데이터를 생성하고 유통하고 사용할 가능성이 높습니다. 예컨대, 소비자의 쇼핑 습관과 거주지를 토대로 건강 상태를 추정하거나 프로필을 개발하는 것입니다. 소비자 IoT 서비스가 인기를 얻으면 소비자

데이터가 더 많이 생성되고 실시간 분석되며 국경을 넘어 여러 당사자가 이를 공유하게 됩니다.

데이터가 특정 개인과 연계되면 요즘처럼 복잡하고 서로 '연결된' 생태계에서는 다음과 같은 우려가 제기될 수도 있습니다.

- 누가 개인의 데이터를 수집하고 공유하고 이용하는가?
- 구체적으로 어떤 데이터를 수집하는가?
- 데이터를 수집하는 곳(어떤 기술 또는 인터페이스)은 어디인가?
- 데이터를 수집하는 때는 언제인가?
- 사용자에게서 데이터를 수집하는 이유는 무엇인가?
- 개인 정보의 프라이버시(단순한 보안 이상의 개념)는 어떻게 확보하는가?
- 개인이 본인 데이터의 공유 방식과 이용 방식을 통제할 수 있는가?

소비자 데이터를 기반으로 한 IoT 서비스의 제공업체와 그 데이터를 포착하거나 이용하는 협력업체는 개인의 사생활을 존중하고 ID 나 사생활 침해 정보를 안전하게 관리할 의무가 있습니다.

IoT 서비스 업체 앞에 놓인 난제 가운데 하나는 사생활과 데이터의 보호를 관장하는 법이 여럿이고 때로는 서로 일관성이 없다는 점이다. 관련된 데이터의 유형에 따라 국가마다 법이 다를 수도 있고 업체가 종사하는 업종과 서비스에 따라 달라지기도 합니다. 이것은 소비자 중심의 IoT 서비스 업체에게 여러 가지를 시사합니다.

우선, 커넥티드 자동차가 여러 나라를 돌아다닌다면 자동차의 데이터 전송에 여러 가지 법이 적용되는 상황이 벌어질 수도 있습니다. 또 자동차의 위치(정적 위치, 동적 위치)를 추적하는 내장 센서와 자주 가는 목적지로 운전자의 라이프스타일이나 취미, 종교 등 운전자가 개인 정보라고 여길 수도 있는 여러 가지 사실을 추정할 수 있습니다. 그런가 하면 보험사가 '내장 진단' 센서를 통해 운전 습관 정보를 수집해 보험료 인상의 근거로 삼을 수도 있습니다.

IoT 서비스와 디바이스(커넥티드 자동차 포함) 또한 여러 주권 국가를 오가며 여러 가지 법의 적용을 받을 수도 있습니다. 개인 정보 데이터가 데이터 소유자와 다른 국가로 전송되거나 다른 국가에 보관될 가능성도 있습니다. 다국적 IoT 서비스를 도입하기 전에는 이처럼 중요한 이슈에 대해 생각해 봐야 합니다.

또 다른 난제는 대부분의 데이터 보호법에서 일정 범주의 '개인 정보'(건강 관련 데이터)에 대해서는 수집 기업에게 당사자('데이터 주체'라고도 함)의 동의를 받은 후 처리하도록 요구하고 있다는 점입니다. 대부분의 법에서는 '개인 정보'를 살아 있는 자연인의 신원 또는 신원 확인이 가능한 정보로 규정하고 있습니다.

그러나 인터넷에 연결되는 디바이스가 많아지면 점점 더 많은 개인 정보가 분석되고 수집돼, 법에서 '개인적'이라고 보지 않는 사생활이 침해될 가능성이 생깁니다. 대규모 데이터와 클라우드 저장장치, 예측 분석이 만나면 사용자의 상세 프로필이 만들어질 수도 있습니다. 특히 데이터를 완전히 익명화하지 못해 다른 데이터에서 개인정보를 추정하는 상황이 벌어질 수도 있습니다.

개인의 의무(health) 기록을 비밀로 관리해야 하는 이유는 그 기록이 상업적으로 남용될지도 모르는 가능성 때문입니다. 미국에서는 1996 년 제정된 건강보험 이전 및 책임에 관한 법(Health Insurance Portability and Accountability Act, HIPAA)에서 의무 기록의 무단 공개 위험을 차단하기 위한 사생활 및 보안 요건을 정하고 있습니다.

HIPAA 는 유럽연합의 유사 규정과 마찬가지로 의무 기록에 *개인의 신원정보*가 포함돼 있을 때에만 적용됩니다. 혈액 감시 장치(사용자의 신원을 구별하지 않음)에 저장된 데이터는 이 요건의 적용을 받지 않는 반면 같은 데이터가 스마트폰 앱이나 클라우드 서버에 들어 있으면 적용 대상이 될 가능성이 높습니다. 데이터를 특정 개인과 연결지을 수 있기 때문입니다. 예컨대 스마트폰에는 사용자를 나타내는 여타의 정보가 들어 있게 마련이고 클라우드 서버에서는 신원을 알 수 있는 개인 계정과 데이터가 연계될 것이기 때문입니다. 각국 정부는 사람에 관한 정보와 인사이트가 설사 '개인의 신원 확인이 가능한' 것이 아니더라도 사생활에 영향을 미칠 수 있음을 알게 되었습니다. 이에 규제에 대해 더욱 더 위험 위주로 접근하는 한편 법적 정의에 집중하기보다는 데이터 이용이 사생활에 미치는 영향을 더 포괄적으로 검토하고 있습니다.

IoT 생태계에서 신뢰가 쌓이려면 데이터 보호와 사생활 입법이 기술에 좌우되지 않고 규칙이 인터넷 생태계의 모든 주체에게 일관되게 적용되도록 정부가 나서야 합니다. 또한 IoT 서비스 업체가 정부기관의 개입을 최소화하려면 IoT 서비스나 제품을 개발할 때 처음부터 부록 A 에 명시된 단계를 따르는 것이 좋습니다.

7 본 지침서의 효과적 활용법

보안은 엔지니어링 프로젝트의 시작 시점에서 최고로 구현되지만, IoT 제품이나 서비스를 이미 설계, 제작했거나 도입한 조직에서도 본 지침은 효과를 발휘할 수 있습니다. 제품이나 서비스가 어느 단계에 있든 본 문서의 효과를 극대화하기 위해서라면 따라야 할 유용한 프로세스가 있습니다.

- 기술적 모델의 평가
- 현 제품 또는 서비스의 보안 모델 검토
- 권고 사항 검토와 평가
- 구현과 검토
- 지속적인 라이프사이클

7.1 기술적 모델의 평가

이 프로세스의 첫 단계이지 가장 중요한 단계는 조직의 IoT 제품/서비스를 파악하는 것입니다. 담당 팀은 보안 검토와 위험 평가를 실시하기에 앞서 조직의 솔루션에 어떤 요소가 사용되었는지, 그것이 서로 어떻게 작용하는지, 그것이 환경과는 어떻게 상호작용하는지 파악해야 합니다. 제품/서비스의 구현 현황을 제대로 이해하지 못하면 완벽한 검토를 할 수 없습니다.

먼저 시스템의 구성요소 각각을 설명하는 문서를 만듭니다. 각 구성요소가 어디에서 공급돼 어떻게 사용되고 있고 어떤 권리가 필요하며 전체 솔루션과는 어떻게 통합되었는지 파악합니다. 각 구성요소를 각 엔드포인트 생태계[3]와 서비스 생태계[4] 지침서의 모델

파트에 기술된 기술과 매핑합니다. 문서가 특정 구성요소와 매칭되지 않아도 됩니다. 일반적인 분류만 매핑하는 것이기 때문입니다. 마이크로컨트롤러, 커뮤니케이션 모듈, 트러스트 앵커처럼 구성요소의 분류만 이용하면 됩니다. 다음 사항을 고려하십시오.

- 해당 제품/서비스를 구축하는 데 어떤 구성요소가 사용되는가?
- 특정 구성요소에 어떤 인풋과 아웃풋이 적용되는가?
- 그 인풋과 아웃풋에 어떤 보안 통제장치가 이미 적용되고 있는가?
- 구성요소에 어떤 권한 수준이 적용되었는가?
- 구성요소 구현을 책임지고 있는 사람은 누구인가?
- 구성요소의 모니터링과 관리를 책임지고 있는 사람은 누구인가?
- 구성요소에서 관찰된 위험을 해소하는 프로세스는 무엇인가?

위 물음에 답을 찾게 되면 기술 요소가 서로 어떻게 작용하는지, 전체 제품/서비스가 각 요소에 어떻게 영향을 받는지 알 수 있습니다.

이 프로세스는 CERT OCTAVE 위험 관리 모델의 첫 단계와 두 번째 단계, 또는 NIST 위험 관리 체계[5]의 Frame 단계에 해당합니다. 이는 핵심 비즈니스 자산의 프로필 개발과 보안 목표 설정에 유용하며 회사가 위험을 평가하고 모니터링하고 대응하는 방식의 토대가 됩니다.

7.2 현 보안 모델의 검토

다음으로, 검토 대상 엔드포인트 또는 서비스의 보안 모델 부분을 읽습니다. 여기서는 공격자가 특정 기술을 무력화하기 위해 사용하는 모델을 소개합니다. 이 모델은 다년간 보안 평가와 역설계, 임베디드 시스템 설계를 실시하며 얻은 경험에 기초하고 있습니다.

보안 모델 검토가 끝나면 개발 중인 제품/서비스에서 어떤 기술이 가장 취약한지, 즉 공격자에게 가장 좋은지 더 명확하게 드러납니다. 이 정보는 조직과 공유해 엔지니어와 경영진 모두가 현 모델에 대한 위험과 위협을 알게 해야 합니다.

그러나, 기억해야 할 점은 이 시점에서 조직이 개입해 보안 모델을 조정해서는 *안 된다*는 점입니다. 아키텍처를 바꾸기에는 아직 이릅니다.

이 프로세스 역시 CERT OCTAVE 위험 관리 모델의 첫 단계와 두 번째 단계, 또는 NIST 위험 관리 체계[5]의 Frame 단계에 해당합니다. 보안 모델을 검토하면 보안의 허점이 드러나고 우선해야 하는 보안 목표가 눈에 보이게 되므로 기술 모델을 개선하기에 좋습니다.

7.3 권고 사항 검토와 평가

이 시점에서는 권고 사항 단원을 검토해 보안 업무의 해결 *방안*을 평가해야 합니다. 이 단원에서는 권고 사항의 구현 방법은 제시하지 않는 대신 특정 권고 사항의 구현을 가로막는 요소가 무엇인지 실마리를 제시합니다.

권고 사항마다 *방법(Method)* 단원이 제공됩니다. 이 단원에서는 상응하는 위험 요소의 시정이나 완화에 도움이 되는 방법을 개략하여 소개합니다. 이 방법에서는 전체적인 위험을 낮춰 적정 수준의 현실적인 노력으로 최대 이익을 얻는 개념을 상위 레벨로부터 설명합니다.

비용(Expense) 단원에서는 조직이 특정 권고 사항을 실행에 옮길 때 준비해야 하는 추가 비용이 있다면 설명합니다. 엔지니어링 시간이나 원재료처럼 대부분의 비용은 명확하지만 이윤 마진과 예산 한도를 경영진에서 이미 정해 놓은 제품과 서비스의 경우, 덜 명확한 비용이 여기에 적용되는 파이낸싱을 바꿔놓을 수도 있습니다. 구체적인 수치는 제시하지 않지만, 추가 비용을 유발할 수도 있는 기술과 서비스는 제시합니다.

위험 단원도 있어 특정 권고 사항을 구현하지 *않을* 때 나타날 가능성이 높은 보안의 허점을 독자에게 보여줍니다. 회사에서 일부 위험에 대해 영업 가이드라인 안에 속하는 것이라고 인정하더라도 독자는 각 단원을 검토해 특정 권고 사항을 아예 구현하지 않았을 때 또는 제대로 구현하지 않았을 때 나타나는 부작용을 회사가 충분히 이해하도록 해야 합니다. 이는 "데이터 암호화" 같은 권고 사항에게는 단순해 보일 수도 있지만, 예컨대 '암호적으로 고유하지 않은 메시지에 대해 공격을 반복하라'와 같은 일부 위협의 미묘함은 훗날 독자에게 놀라움이 될 수도 있습니다.

경우에 따라 추가 검토 목적으로 *참고 문서* 제시되기도 합니다. 본 문서에서는 기술이나 위험, 해소 계획에 관해 일일이 자세하게 설명하지는 않으나 여타 표준과 검증된 전략에서는 그렇게 합니다. 본 문서에서는 각 권고 사항의 자료에 대해 참고 문서를 제시합니다.

권고 사항 단원의 검토에서 나오는 아웃풋은 보안 업무 단원과 바로 연계해야 합니다. 이제 보안 업무는 그것을 제대로 구현하기에 적합한 권고 사항으로 채워집니다. 그리고 그 보안 업무는 다시 조직의 구성원에게 할당된 구성요소와 연계됩니다.

권고 사항 평가는 NIST 위험 관리 체계[5]의 Assess 단계, CERT OCTAVE 방법론[6]의 6-8 단계에 해당합니다.

7.4 구현과 검토

이 단계에 이르면 보안 업무도 명확하게 윤곽이 잡히게 되며, 회사는 보안의 취약점과 가치, 위험을 더 상세히 파악하게 됩니다. 회사는 이제 조정 대상이 되는 구성요소 별로 명확한 아키텍처 모델을 만들고 조직에서 선택한 위험 평가 프로세스를 이용해 각 구성요소의 위협 모델을 개발한 후 각 구성요소와 보안업무에 적합한 권고 사항과 위험을 반영합니다. 아키텍처 모델이 완성되면 권고안을 구현해 보안 업무를 실행하면 됩니다.

구현이 완료되면 권고안 단원과 구성요소 단원에서 모두 위험을 검토해야 합니다. 조직은 구현 과정에서 이들 단원에 명시된 요건이 충족되도록 해야 합니다. 이어서 구성요소가 조직의 제품과 서비스 안에서 설계된 맥락에 비춰 구현의 결과로 보안 문제가 해결되는지 확인해야 합니다. 본 문서에서 현장에서 설계되고 있는 제품이나 서비스를 일일이 다루지는 못하기 때문입니다. 가능하다면 외부 컨설팅 회사에게 구현 상태의 평가를 의뢰해 진정으로 보안 모범 사례에 부합하는지 확인합니다.

구현과 검토는 NIST 위험 관리 체계[5]의 Respond 단계, CERT OCTAVE 방법론[6]의 8 단계에 해당합니다.

7.5 지속적인 라이프사이클

보안 라이프사이클은 여기서 끝나지 않습니다. 보안은 처음부터 프로세스 엔지니어링에 내재합니다. 엔드포인트와 IoT 서비스는 마치 살아 있는 생명처럼 수명이 있으며 그 수명이 끝날 때까지 계속해서 서비스를 해야 합니다.

요건은 시간이 지나면서 변합니다. 암호 알고리즘도 낡거나 가치가 떨어집니다. 새 프로토콜과 무선 기술은 제품, 서비스와 호환성이 있어야 합니다. 임베디드 제품이 활약하는 이 생태계는 계속 변하므로 수시로 검토해 기밀성과 무결성, 가용성, 인증성능을 유지해야 합니다.

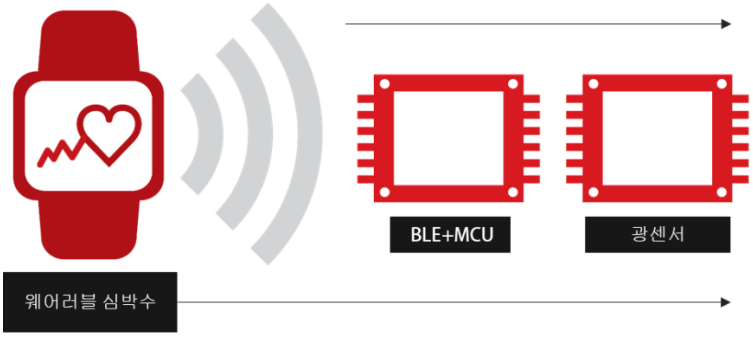
지속적인 보안 라이프사이클의 관리는 NIST 위험 관리 체계[5]의 Monitor and Frame 단계, CERT OCTAVE 방법론[6]의 1, 4, 5 단계에 해당합니다.

8 보기 - 웨어러블 심박수 모니터

이 사례에서는 본 지침을 이용해 간단한 심박수 모니터(HRM)의 설계를 평가합니다. 엔드포인트는 엔드포인트 생태계 문서로 평가하고 설계의 서비스는 서비스 생태계 문서로 평가합니다.

8.1 엔드포인트 개요

먼저, 엔드포인트의 하드웨어 설계를 평가해봅니다.



도 3 - 간단한 HRM 과 주요 구성요소

HRM 은 간단한 무선 웨어러블 디바이스용 기본 구성품, 즉 상온 광센서와 블루투스 저에너지(BLE) 송신기 기반의 마이크로컨트롤러로 구성됩니다. 센서는 심박 데이터를 포착하고 마이크로컨트롤러는 센서에서 나오는 데이터를 분석해 내장된 BLE 송신기로 보낼 데이터를 선별합니다. 이 보기에서 사용되는 BLE 스택은 버전 4.2 입니다.

동전 모양의 셀 배터리가 동력이 되어 데이터를 HRM 에서 다른 디바이스, 예컨대 스마트폰이나 태블릿으로 보냅니다. 이 디바이스가 작동하는 데 다른 구성품은 필요 없습니다.

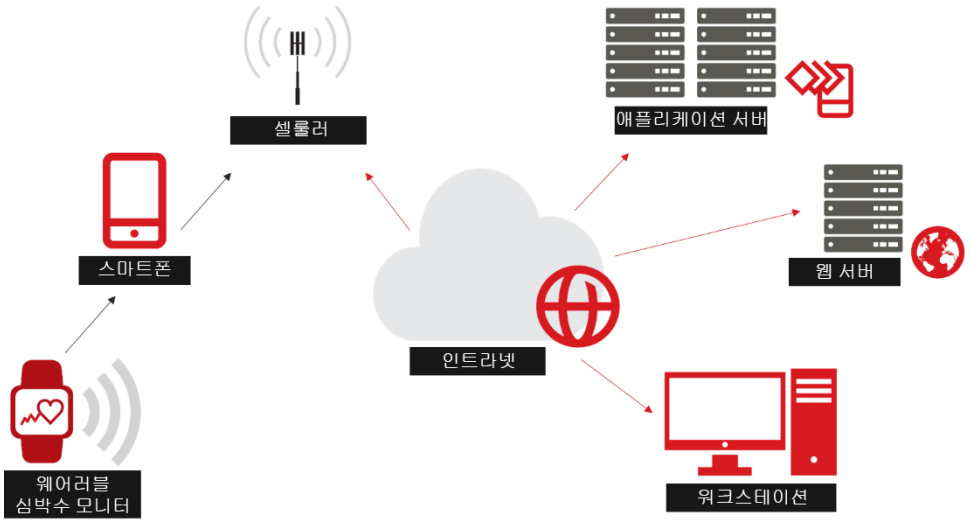
엔드포인트 생태계 문서에 따르면, 이 디바이스는 경량 엔드포인트 급에 속할 것입니다.

8.2 서비스 개요

서비스 측면에서 보면, 스마트폰이나 태블릿에 설치돼 있는 애플리케이션은 메트릭스를 엔드포인트에서 가용한 네트워크 연결을 통해 백엔드 서비스까지 보냅니다. 이 애플리케이션의 백엔드 서비스는 단순히 포착되고 있는 메트릭스와 디바이스 소유자를 연계하고 애플리케이션 서버의 로컬 데이터베이스에 그것을 저장하는 역할에 그칩니다.

모바일 애플리케이션이나 서비스의 웹사이트를 통해 그 데이터를 시각화할 수 있습니다. 웨어러블 기술의 사용자는 서비스 업체의 사이트에 접속해 엔드포인트에서 포착된 메트릭스로 더 많은 액션을 취할 수 있습니다.

이것이 커스터마이징이나 불필요한 복잡함이 없는 단순하고 흔한 서비스 모델입니다.



도 4 - 간단한 백엔드 서비스로 향하는 데이터의 흐름

8.3 용례

이 기술을 개발하는 기업은 최종 사용자가 하루 종일 심박 데이터를 추적해 애플리케이션과 백엔드 데이터베이스에 모두 저장하는 것을 목표로 합니다. 사용자가 시간 경과에 따른 심박수를 보고 전체적인 건강 상태를 추적하게 하는 것입니다. 사용자는 건강한 생활습관을 유지하느냐 그렇지 않느냐에 따라 건강이 좋아지거나 나빠지는 모습을 보게 됩니다. 사용자가 HRM 데이터의 좋은 추세와 나쁜 추세 모두를 평가해 자극제로 삼을 수 있는 것입니다.

기업에서는 이 데이터를 기초로 의료기기 제조업자와 건강관리 서비스업자, 그 외 데이터 활용 가능 조직과 짝을 이뤄 어떤 소비자에게 심장마비나 발작 같은 건강 문제가 발생할 가능성이 어느 정도인지 판단하고자 합니다.

8.4 보안 모델

이 사업의 엔지니어링팀은 엔드포인트와 서비스 문서의 FAQ 를 이용해 해당 제품과 서비스에 어떤 이슈가 연관돼 있는지 파악했습니다.

엔드포인트 측면에서는 다음과 같은 우려가 제기되었습니다.

- 클로닝
- 엔드포인트 가장
- 서비스 가장
- 사생활 보호

서비스 측면에서는 다음과 같은 우려가 제기되었습니다.

- 클로닝
- 서비스 해킹
- 엔드포인트 이상 거동 규명
- 무력화 제한
- 데이터 손실 저감
- 착취 저감
- 사용자 프라이버시 관리
- 가용성 향상

담당 팀은 각 FAQ 단원에서 제안한 바와 같이 위 이슈 각각의 권고 사항을 검토하였다. 이어 보안 강화의 정도가 가장 크고 경제성까지 갖춘 권고 사항을 구현하기로 했습니다.

이 보기에서는 엔드포인트를 크게 바꿀 필요가 없습니다. 엔드포인트에는 이렇다 할 기능이 없으므로 애플리케이션 보안과 통신 모두 엔드포인트에 최소한의 보안만 적용하면 됩니다. 엔드포인트 애플리케이션은 한 디바이스에서만 잠깐 보이므로 디바이스 펌웨어가 *잠겨* 있는 한 이 용례에서 엔드포인트에 대해 공격이 일어날 가능성은 거의 없습니다.

그러나 사생활 보호가 이슈이므로 조직에서는 적어도 TCB(Trusted Computing Base)의 개인화 PSK 버전을 도입해야 합니다. 그러면 암호화 토큰이 엔드포인트마다 고유하게 돼 엔드포인트 하나가 무력화되더라도 엔드포인트 전체가 무력화되지는 않습니다.
개인화된(고유한) 키가 잠긴 마이크로컨트롤러에 인코딩된다면 이 용례는 클로닝과 가장, 사생활보호라는 위협으로부터 안전하다고 믿어도 좋습니다. IoT 서비스[3]와 엔드포인트[4] 문서에 각 생태계의 맥락에서 TCB 란 무엇인지 자세히 설명돼 있습니다.

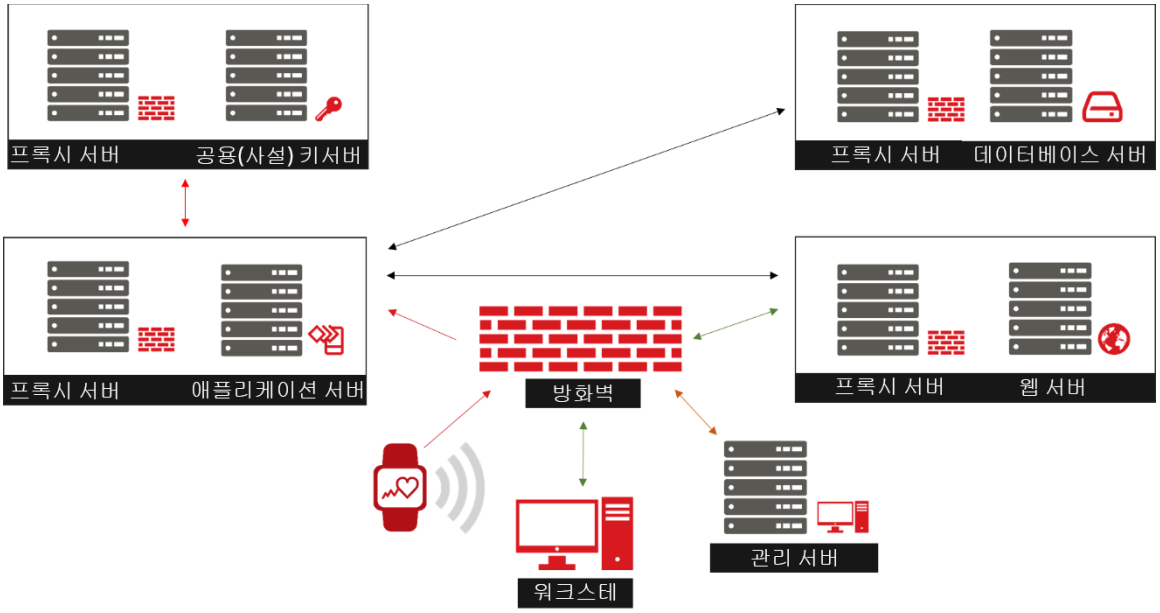
반면 서버 인프라는 큰 폭의 변화가 필요합니다. 엔지니어링팀은 권고 사항에서 얘기하듯 서버 인프라가 심각한 남용의 위험에 놓여 있음을 깨닫습니다. 그리고 다음과 같은 이슈가 있음을 인정합니다.

- 서비스 거부 공격의 효과를 처음부터 끝까지 모두 완화하기는 불가능합니다.

- 서비스로 들어오거나 서비스에서 나가는 트래픽을 제한하는 진입 또는 이탈 제어장치는 없습니다.
- 서비스 계층(tier) 간에 임무의 구별은 없습니다.
- 개인화 PSK 토큰이 들어 있는 별도의 보안 데이터베이스는 없습니다.
- 서비스 운영 시스템에서는 적절한 보안 조치가 구현되지 않습니다.
- 엔드포인트 이상 거동을 평가하지 않기 위해 채취하는 메트릭스는 없습니다.

8.5 결과

권고 사항 구현 후 조직은 지침을 통해 확인된 위험을 적절히 해소하는, 훨씬 더 잘 정의된 백엔드 서비스 아키텍처를 갖게 되었습니다.



도 5 - 도출된 서비스 생태계

위 그림에서 서비스 생태계의 변화는 쉽게 눈에 띕니다. 서비스의 각 등급을 단계로 구분해 수요 급등 시 기술을 쉽게 확보하고 *또한* 확대할 수 있게 하였습니다. 데이터베이스 단계와 인증 단계, 두 가지를 추가하여 핵심이 되는 시스템을 외부 세계와 직접 만나는 서비스로부터 격리하였습니다. 보안 프론트-엔드를 적용해 내부 네트워크를 DoS, DDoS 공격 등 시스템의 전체적인 가용도를 떨어뜨리는 여러 가지 공격으로부터 지키고자 하였습니다. 마지막으로 관리 모델을 만들어 경영진이 생산 환경에 안전하게 접속할 수 있게 하였습니다. 한 가지, 엔드포인트 거동에서 무력화 또는 펌웨어나 하드웨어 설계의 결함을 나타낼 때를 포착하는 분석 모델이 위 다이어그램에 빠져 있습니다.

8.6 요약

전체적으로, 이 간단한 기술이 "있는 그대로"로 도입되었다면 쉽게 무력화될 수도 있었습니다. 그러나 엔드포인트를 간단히 경제적으로 몇 가지 바꾸자 기술은 아키텍처의 변경 없이도 현장에서 오랫동안 쓸 수 있게 되었습니다.

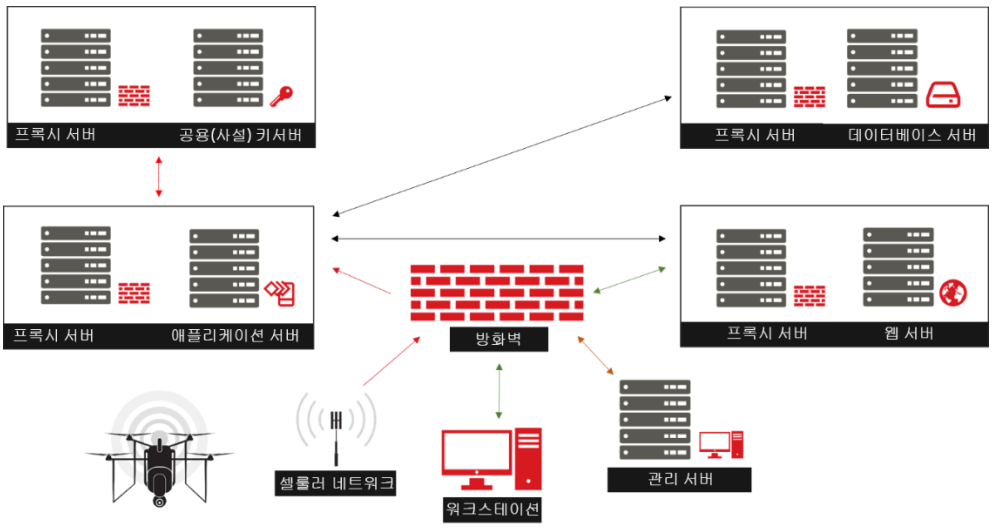
서비스 생태계를 확대하자 사용자와 회사에 대한 위협이 *모두* 크게 줄어들었습니다. 클로닝과 가장의 위협은 사라졌습니다. 엔드포인트마다 고유한 암호화 토큰을 부여한 결과 프라이버시가 확보되었습니다. 핵심 정보가 들어 있는 시스템은 대중과 접촉하고 남용이 심한 시스템과 격리하여 보안을 확보하였습니다. 이 모델은 조금 더 복잡하기는 하지만 생산 환경의 전체적 위험을 떨어뜨립니다.

9 보기 - 개인용 드론

이 보기에서는 본 지침을 이용해 작은 개인용 드론 장치를 평가합니다. 엔드포인트는 엔드포인트 생태계 문서로 평가하고 설계의 서비스는 서비스 생태계 문서로 평가합니다.

9.1 엔드포인트 개요

먼저, 엔드포인트의 하드웨어 설계를 평가해봅니다.



도 6 - 드론과 주요 구성품

이 개인용 드론은 여러 가지 구성품이 치밀하게 짜여 있습니다. 드론의 처리 기능은 고성능입니다. 복수의 모터와 센서, 그 외 장치가 모두 동시에 효율적으로 작동해야 하기 때문입니다. 이 모델은 주 운영체제(Linux)가 별도 칩의 NVRAM 에 저장돼 있는 ARM Cortex-A8 CPU 를 이용합니다. 움직임과 빛, 속도 등을 탐지하려면 여러 가지 센서가 필요합니다. SD/MMC 카드가 영상과 센서 메트릭스, 메타데이터를 저장합니다. 카메라가 달려 있어 조종자가 드론의 눈으로 볼 수 있습니다. 셀룰러/GPS 조합 모듈이 탑재돼 드론이 고유

프로토콜의 범위를 벗어나도 드론과 조종자의 연결을 확보합니다. GPS 는 유도와 최소 자동화에도 사용됩니다.

리튬 폴리머(LiPo) 배터리가 드론에 동력을 제공합니다. 비행 시간은 모든 기능을 켜 놓은 상태에서 약 2 시간입니다.

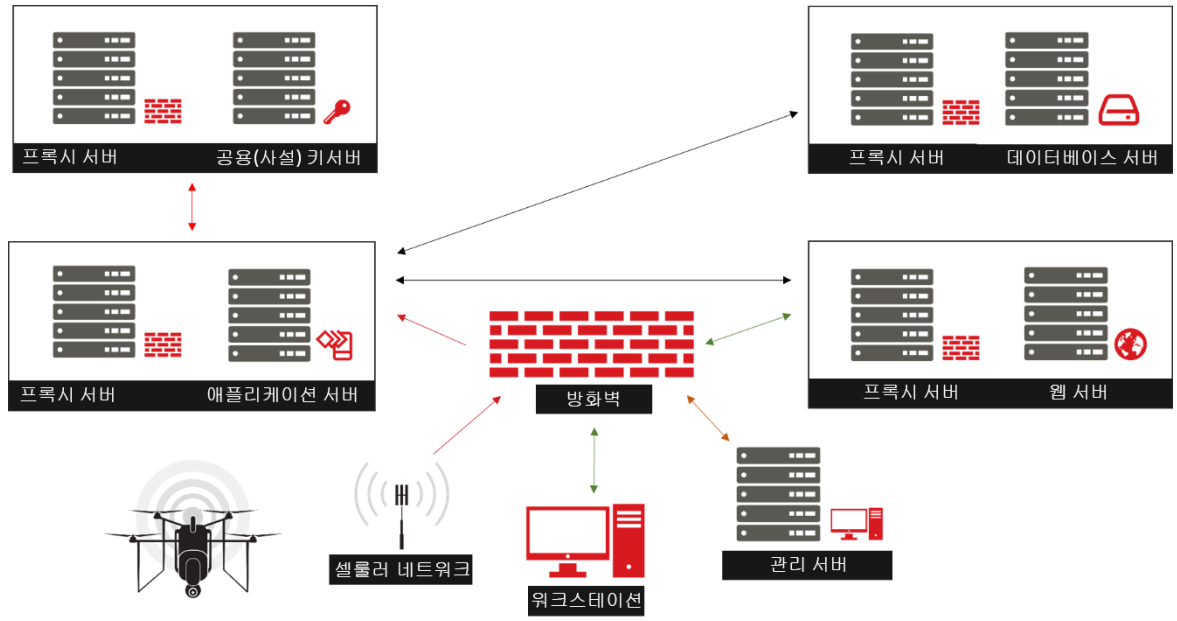
엔드포인트 생태계 문서에 따르면, 이 디바이스는 복잡한 엔드포인트 급에 속할 것입니다. 셀룰러 모듈이 들어 있기는 하나 엔드포인트 간에 메시지를 라우팅하지 않으므로 게이트웨이로 보지 않습니다.

9.2 서비스 개요

서비스 측면에서 보면, 비행 중에 배타적인 무선 인터페이스의 손실이 탐지되면 백엔드만이 조종자 연결에 사용됩니다. 드론이 비행 중이고 셀룰러 연결이 가능하다면 드론은 조종자가 LTE 네트워크를 통해 연결할 때까지 기다릴 것입니다. 만일 LTE 를 통한 조종이 불가하다면 앞서 이륙한 곳으로 자동 착륙을 시도할 것입니다.

그러나 드론에 가벼운 자동화 기능이 있다면 좌표와 회항 경로를 입력해 돌아오는 동안 사진이나 짧은 비디오를 찍게 할 수 있습니다. 이 같은 미디어 파일은 LTE 를 통해 실시간으로 백엔드 서버에 업로드해 조종자에게 자동화 실행 중 경로와 시점을 보여줄 수도 있습니다.

그러므로 시스템에 연결되는 드론이 저마다 높은 수준의 서비스 가용도를 지니려면 견고한 백엔드 서비스가 필요합니다. 셀룰러 링크를 통해 영상과 고해상도 이미지를 전송하려면 네트워크 트래픽의 급증을 수용할 수 있는 가용도 역시 필요합니다. 또한 조종자가 웹 브라우저에서 미디어의 업로드 현황을 볼 수 있는 웹 인터페이스도 꼭 있어야 합니다.



도 7 - 백엔드 서비스로 향하는 데이터의 흐름

9.3 용례

이 기술을 개발하는 회사에서는 최종 사용자가 드론으로 야외 영상을 찍을 수 있게 하려고 합니다. 그러나 일부 고객은 그 동안 이 드론으로 영화 촬영을 하였습니다. 가격 대비 카메라와 안정성이 매우 좋기 때문입니다. 따라서, 이 드론은 저작권과 프라이버시가 중요한 고액의 영화 촬영에도 사용될 것입니다.

9.4 보안 모델

이 사업의 엔지니어링팀은 엔드포인트와 서비스 문서의 FAQ 를 이용해 해당 제품과 서비스에 어떤 이슈가 연관돼 있는지 파악했습니다.

엔드포인트 측면에서는 다음과 같은 우려가 제기되었습니다.

- 엔드포인트 ID
- 엔드포인트 가장

- 트러스트 앵커 공격
- 소프트웨어와 펌웨어 탬퍼링
- 보안 원격 관리
- 무력화된 엔드포인트 탐지
- 서비스 가장
- 사생활 보호

서비스 측면에서는 다음과 같은 우려가 제기되었습니다.

- 사용자 프라이버시 관리
- 가용성 향상

담당 팀은 각 FAQ 단원에서 제안한 바와 같이 위 이슈 각각의 권고 사항을 검토하였다.
이어 보안 강화의 정도가 가장 크고 경제성까지 갖춘 권고 사항을 구현하기로 했습니다.

이 보기에서는 서비스 인프라를 크게 바꿀 필요가 없습니다. 엔드포인트 제품의 서비스에 필요한 트래픽의 급증을 수용할 수도 있도록 서비스 인프라를 이미 넓게 구축해야 했기 때문입니다. 아키텍처는 그 전부터 일부 서비스에 일시적인 장애가 나타났을 때에도 효과적으로 확장하고 자원의 가용성을 유지할 수 있도록 잘 구축되고 안전한 아키텍처가 필요했습니다. 그러나 조직은 사용자 프라이버시를 더 조사하기로 하였습니다. 예상치 못한 회사의 틈새시장에서 이것이 주된 논쟁점이 되었기 때문입니다.

그러나 서버 인프라는 큰 폭의 변화가 필요합니다. 엔지니어링팀은 권고 사항에서 얘기하듯 서버 인프라가 심각한 남용의 위험에 놓여 있음을 깨닫습니다. 그리고 다음과 같은 이슈가 있음을 인정합니다.

- 부트로더는 운영체제 커널을 실행하기 전에 애플리케이션을 제대로 검증하지 않아 탬퍼링의 위험을 유발합니다.
- 애플리케이션 또는 통신의 보안을 관리하는 TCB 가 없습니다.
- 적절히 구현되는 TCB 나 트러스트 앵커가 없기 때문에 엔드포인트 가장이 문제가 되며, 이는 데이터 유출로 이어질 수도 있습니다.
- 잘 구현된 TCB 없이는 엔드포인트가 서비스를 제대로 인증할 수 없습니다.
- 잘 구현된 TCB 없이는 엔드포인트가 배타적인 무선 인터페이스를 통해 조종자를 제대로 인증할 수 없습니다.
- 엔지니어링 팀에서는 LTE 의 보안에 의존해 통신 채널이 무력화되지 않게 하였습니다. 그러나 엔드포인트 가장이나 펨토셀 용도 변경의 위협을 고려하지 않았습니다. 두 가지 모두 LTE 의 보안을 우회해 약한 서비스 보안을 무력화합니다.

9.5 결과

위 문제에 대해 권고 사항을 구현한 후 조직은 지침서을 통해 확인된 위험을 적절히 해소하는, 훨씬 더 잘 정의된 백엔드 서비스 아키텍처를 갖게 되었습니다.

이미 생산 중인 기존 드론 시스템에 대해서는 엔지니어링 팀이 개인화된 공개키 보안 모델을 구현하는 펌웨어 업데이트를 배포하고 있습니다. 이 펌웨어 업데이트는 부트로더를 개선할 뿐만 아니라 핵심 아키텍처로 보안을 베이크(bake)합니다. 개인화된 공개키 모델을 적용했으므로 엔드포인트의 초기 보안 허점을 이용해 타인의 엔드포인트를 가장하려는 시도는 성공할 수 없습니다. 엔지니어링 팀에서 기존의 사용자-엔드포인트 매핑 데이터베이스를 이용해 사용자 별로 개인화 키를 만들었기 때문입니다. 이로써 올바른 웹 자격증명이 없는 사용자는 타인의 개인화된 공개키 업데이트를 내려 받아 설치할 수 없습니다. 이 프로세스는 복잡하고 구현에 시간도 많이 걸리지만 그만큼 값진 기능을 합니다.

앞으로 나오는 드론 기술은 내부 CPU 트러스트 앵커를 이용할 것입니다. 이 트러스트 앵커는 개인화된 공개키 TCB 에 연결되므로 각 엔드포인트는 처음부터 매우 높은 보안 수준을 갖추게 됩니다.

이런 식으로 강력한 암호화를 갖추는 것은 매우 중요합니다. 회사에서 우려할 만한 사항으로 상정한 다른 유형의 공격 가능성까지 차단하기 때문입니다. 엔지니어링 팀은 검증과 인증에 강력한 암호화와 TCB 를 적용하여 드론에 불량 서비스가 제공되는지 쉽게 찾아낼 수 있습니다. 드론은 불량 서비스가 탐지되면 처음 이륙한 곳에 착륙하기만 하면 됩니다.

다른 서비스도 보안이 불량한 드론을 탐지하면 내부적으로 경보를 울릴 수 있습니다. 그러면 당시 관리팀에서 무력화됐을지도 모르는 드론을 어떻게 처리할지 결정하면 됩니다. 이렇게 하면 보안 사건에 대하여 일정 수준의 민첩성을 확보할 수 있고 조직은 해당 엔드포인트의 이상 거동이 소프트웨어 문제인지, 하드웨어 문제인지 평가할 수 있습니다.

9.6 요약

엔지니어링 팀이 상당한 시간을 들여 기계적 엔지니어링과 백엔드 서비스 측면에서 복원력 좋은 아키텍처를 만들었지만, 안전한 엔드포인트 기술의 확보에 큰 노력이 필요했습니다. 이 시나리오는 회사 전체에 큰 위협을 가하지는 않았지만 다행히도 고객의 니즈에 *충분히* 부합하는 솔루션이 있었습니다. 이것이 더 큰 안전을 요하는 기술이었다면 여기 도입한 솔루션으로도 충분하지 않았을 것입니다.

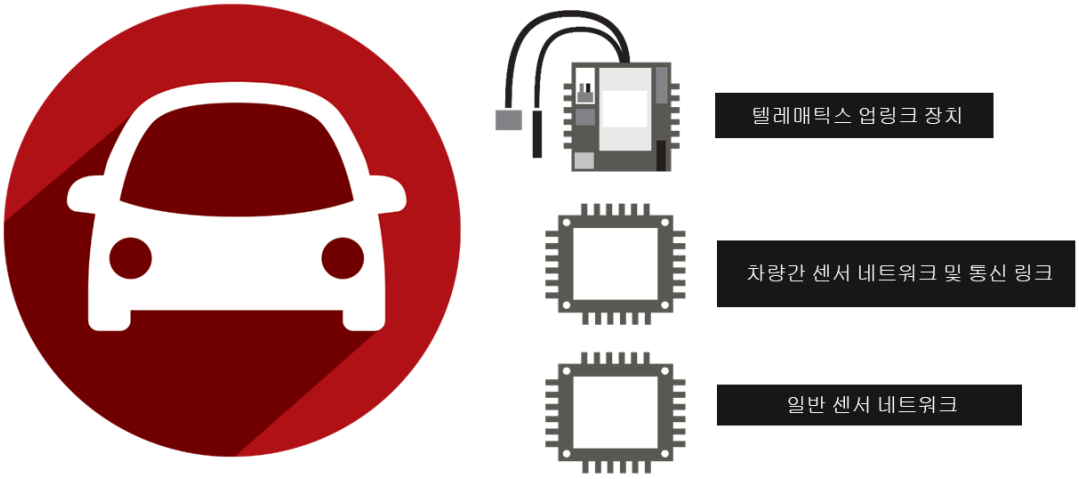
개인화된 공개키 TCB 나 개인화 PSK TCB 같은 TCB 의 변종에 관해서는 IoT 서비스[3]와 엔드포인트[4] 생태계 문서에서 더 자세히 알 수 있습니다.

10 보기 - 자동차 센서 네트워크

이 보기에서는 새 자동차 급에 도입되고 있는 자동차 센서 네트워크를 본 지침으로 평가합니다. 엔드포인트는 엔드포인트 생태계 문서로 평가하고 설계의 서비스는 서비스 생태계 문서로 평가합니다.

10.1 엔드포인트 개요

먼저, 엔드포인트의 하드웨어 설계를 평가해봅니다.



도 8 - 자동차 센서 네트워크와 통신 시스템

위 모델은 간단한 다이어그램을 가지고 제대로 설명하기에는 너무 복잡하지만 3 대 구성요소는 다음과 같습니다.

- 센서 네트워크를 관리하고 운전자를 대신해 복잡한 결정을 내리고 백엔드 시스템과의 연결을 유지하는 텔레매틱스 업링크 장치
- V2V 이벤트를 탐지해 반응하는 차량 간(V2V) 시스템
- 텔레매틱스 업링크 장치에 메트릭스를 제공하는 일반 센서 네트워크

현대의 자동차 시스템에서는 텔레매틱스 장치가 차의 컴퓨터 네트워크에 소속돼 센서 데이터와 백엔드 통신을 기반으로 의사결정을 합니다. 이 장치는 자동차를 운전하는 사람과 함께 또는 그 사람을 대신해 결정을 내립니다. 이 장치는 자동차가 제대로 작동하게 하고 비상시 현명한 결정을 하고자 하며 백엔드 네트워크에서 명령을 받습니다.

V2V 센서 네트워크는 인접한 자동차를 식별하고 센서에서 나오는 메트릭스를 토대로 의사결정을 합니다. 텔레매틱스 장치가 주로 구성품(브레이크, 타이어 공기압 감시장치 등)의 상태를 토대로 의사결정을 하는 반면 V2V 시스템은 다른 차량의 존재를 가지고 의사결정을 하거나 긴급 상황 시 인접한 차량에 경고를 보냅니다.

일반 센서 네트워크는 텔레매틱스 장치, 때로 V2V 장치에 데이터를 보내는 일련의 구성품입니다. 이 장치들은 일반 센서 네트워크에서 수집된 정보를 근거로 중요한 이벤트에서 정확하게 의사결정을 합니다.

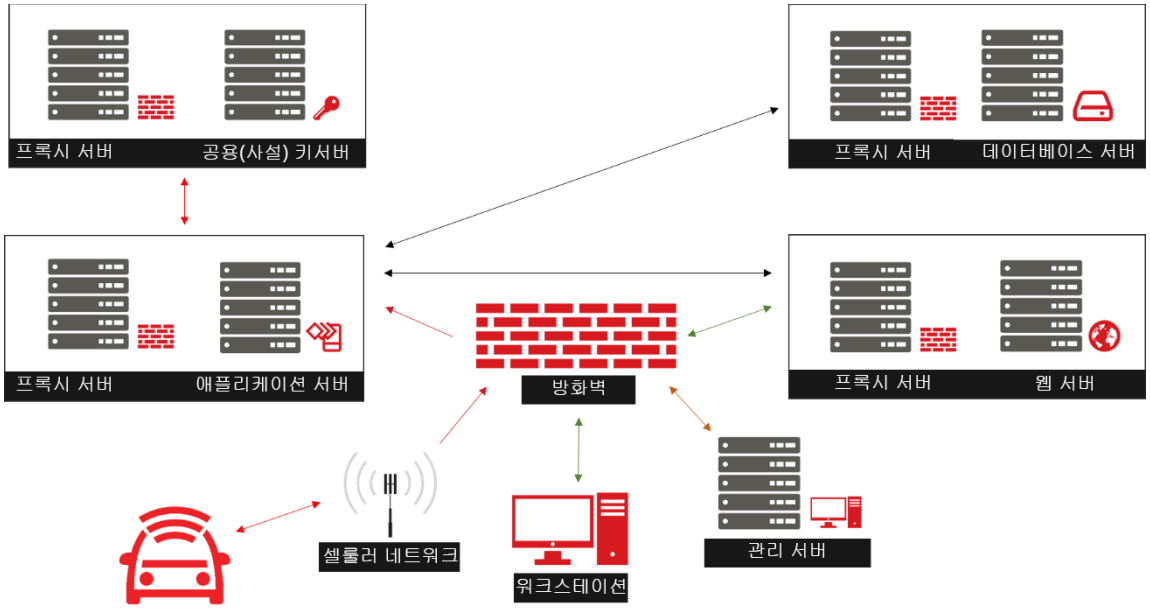
엔드포인트 에코시스템 문서에 따르면 이 시스템에는 어떤 IoT 엔드포인트 등급에도 잘 맞는 구성품이 있습니다. 텔레매틱스 업링크 장치는 게이트웨이처럼 작동합니다. V2V 장치는 복잡한 엔드포인트처럼 작동합니다. 일반 센서 디바이스는 사실상 모든 경량 엔드포인트입니다.

10.2 서비스 개요

서비스 측면에서, 자동차 센서 네트워크는 백엔드 환경에 메트릭스를 보냅니다. 이 데이터는 소비자에게 제공될 수도 있고 제공되지 않을 수도 있습니다. 아니면, 제조사가 저장했다가 구성품의 문제 가능성을 관찰하거나 찾아낼 수도 있습니다. 그러면 서비스 경고가 발령되고 이어서 소비자에게 전달됩니다.

시스템은 또 보강돼 "원격으로 문 닫기" "시동걸기" 등 여러 가지 유용한 서비스를 소비자에게 제공할 수도 있습니다. 가까운 미래에 이들 시스템이 자동차에 탑재돼 자동화 유도 시스템을 통한 원격 운전이 가능하게 될지도 모릅니다.

가장 중요한 결정은 자동차의 처리장치에서 내려지겠지만, 일부 결정은 클라우드에서 내려질 가능성도 충분합니다. 클라우드에서는 기계 학습(ML)과 인공지능(AI)이 행동 모델이나 통계 모델을 더 많이 이용해 더욱 더 복잡한 결정을 내릴 수 있습니다.



도 9- 백엔드 서비스로 향하는 데이터의 흐름

10.3 용례

이 기술의 존재 이유는 자명합니다. 즉 안전이 중요한 상황에서 복잡한 의사결정을 내릴 수 있는 더 스마트한 자동차를 만드는 것입니다. 관건은 최대한 많은 센서에서 정보를 받아 아주 짧은 시간에 중요한 결정을 내리는 것입니다. 자동 제동, 타이어 펑크 알림, 운전자 이상 경고 등 중요한 상황을 센서와 잘 설계된 컴퓨터 시스템을 통해 기민하게 처리할 수 있습니다.

이 기술에서 한 가지 재미있는 점은 사용자가 기술을 속속들이 들여다볼 수도 있다는 것입니다. 컴퓨터가 일정한 방식으로 작동하도록 사용자가 구성할 필요가 없습니다. 대신 컴퓨터는 센서 메트릭스를 통해 현재의 지형을 통과할 수 있어야 합니다. 그러면 컴퓨터가 환경에 구애 받지 않고 바르게 작동합니다.

10.4 보안 모델

이 사업의 엔지니어링팀은 엔드포인트와 서비스 문서의 FAQ 를 이용해 해당 제품과 서비스에 어떤 이슈가 연관돼 있는지 파악했습니다.

엔드포인트 측면에서는 다음과 같은 우려가 제기되었습니다.

- 엔드포인트 가장
- 서비스 또는 피어 가장
- 부채널 공격
- 무력화된 엔드포인트 탐지
- 보안 위험 시 안전 확보

서비스 측면에서는 다음과 같은 우려가 제기되었습니다:

- 엔드포인트 이상 거동 규명
- 사용자 프라이버시 관리

앞선 보기에서 설명하지 못했지만 이 환경에서 가장 큰 위험은 피어와 관련된 가장의 위험입니다. 이런 유형의 환경에서 엔지니어들이 갖는 한 가지 우려는 컴퓨터가 제대로 인증되지 않은 데이터에 근거해 중요한 결정을 내리는 것입니다.

중요한 순간에 센서 데이터는 매우 빠르게 처리되어야 하므로 비대칭 암호화 또는 PKI 기반 통신을 실행하기가 늘 쉽지만은 않을 수도 있다는 이론이 가능합니다. 그러나, 그것은 정확한 주장이 아닐 수도 있습니다. 정확한 보안 모델이라면 시간을 다투는 상황을 미리 파악해 가까운 엔드포인트의 세션 키를 캐싱해야 합니다. 예를 들어, 두 개체가 일정한 속도로 마주보고 접근한다면 둘이 충돌할 수도 있는 거리에 도달하기 전에 서비스 생태계의 보안 애플리케이션이 그 두 엔드포인트 고유의 세션 키를 준비할 수 있습니다. 그러면 엔드포인트 사이에 안전한 통신이 가능하며, 위험한 상황(예: 자동차 충돌)의 가능성이 탐지됐을 때 순간적으로 안전한 세션을 다시 협상할 겨를이 없더라도 센서를 계속 사용할 수 있습니다.

따라서, TCB 구현의 증강이 필요합니다. 한 가지 흥미로운 해결책은 GBA 입니다. 여기서는 텔레매틱스 업링크 장치에 사용된 UICC 가 시스템을 통해 키값을 엔드포인트로 안전하게 배포할 수 있습니다. 이 프로토콜을 적용하면 가장 기본적인 엔드포인트에도 복수의 중요한 상황에서 이용 가능한 안전한 세션 키를 시드할 수 있습니다. 그러면 경량 엔드포인트가 퍼블릭 키 세션 초기화에 필요한 핵심 연산을 수행하지 못하더라도 환경은 신뢰기반(RoT)으로부터 항상 시드됩니다.

이 환경에서 또 한 가지 중요한 이슈는 무력화된 엔드포인트를 탐지하는 것입니다. 예컨대, 환경이 어떻게 타이어 공기압 감시장치(TPM)처럼 간단한 센서가 무력화되었는지 알 수 있을까요? 컴퓨터가 타이어 펑크 신호를 보내는 TPM 을 믿고 중요한 의사결정을 내린다면 안전 문제가 발생할 수도 있습니다. 따라서, 디바이스의 거동과 그 신뢰도를 부트업 단계마다 재평가해야 합니다. 디바이스는 모두 탬퍼에 대한 내성을 지녀야 하며 무력화가 발생한다면 네트워크에 이를 알릴 수 있어야 합니다. 역으로, 센서 네트워크에 있는 다른 디바이스들이 네트워크 내 피어의 신뢰도를 판단할 수도 있어야 합니다.

10.5 결과

권고 사항이 구현되면 자동차 센서 네트워크는 자동차 통신망에 대한 공격에 대해 견고한 방어태세를 갖추게 됩니다. GBA 가 시스템 내 엔드포인트에 키값을 배포하는데, 부트업을 할 때마다 배포해 이전 키값의 재사용을 막습니다. 여기에 탬퍼 내성과 전(全) 엔드포인트의 강력한 TCB, 조직적 신뢰 기반이 더해져 환경은 훨씬 더 낮은 위험으로 작동할 수 있습니다.

그러나 이 같은 변화와 별개로 안전은 여전히 중요한 요소입니다. 엔지니어링팀과 회사 수뇌부, 회사 법무팀, 보험 중개인은 안전과 직결되는 기술을 평가해 사용자의 안전을

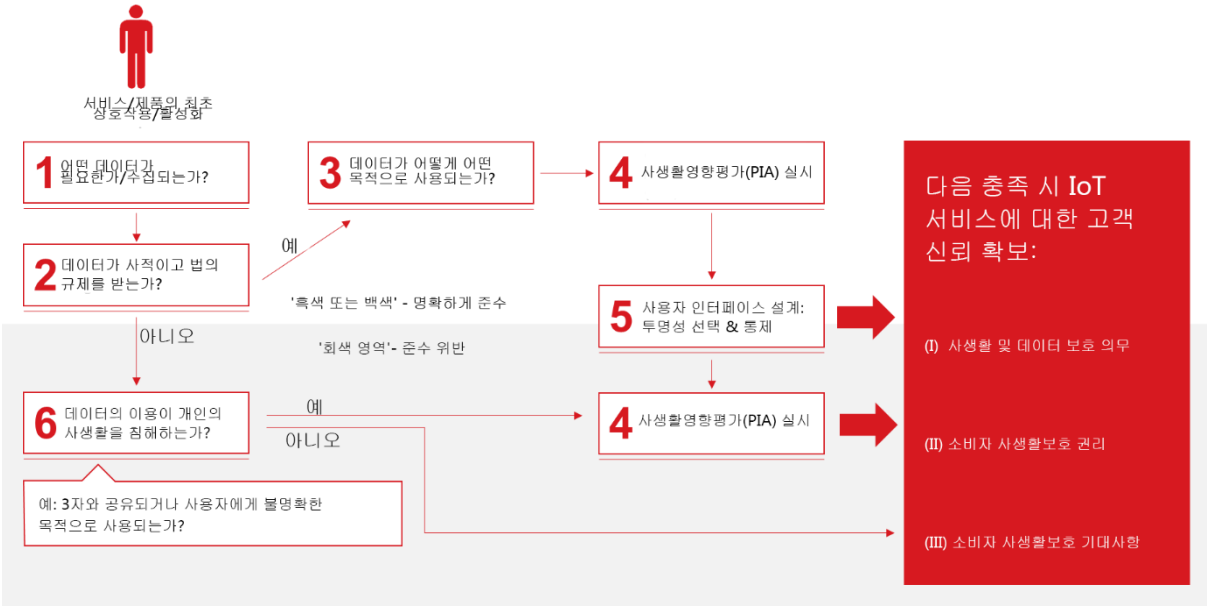
위협하지 않고도 보안을 구현할 수 있는지 판단해야 합니다. 안전이 중요한 상황에서도 아키텍처를 일부 조정해 보안을 구현할 수는 있지만 안전을 무엇보다 최우선해야 하는 때가 있습니다.

10.6 요약

이와 같은 시스템은 엔지니어링이 워낙 잘 돼 있어서 생태계를 공격하려면 큰 수고가 필요합니다. 그러나 통신 아키텍처의 작은 결함이 환경의 무력화로 이어질 수 있습니다. CANbus 네트워크처럼 사면이 닫힌 곳에서는 엔드포인트 하나의 결함이 시스템 전체를 취약하게 만들 수도 있습니다. 안전이 중요한 환경에선 용납할 수 없는 일입니다.

부록 A IoT 서비스 업자를 위한 프라이버시 고려사항

GSMA 는 IoT 생태계의 신뢰도를 높이고 공적인 제도의 개입을 최소화하고자 다음과 같이 단계별 사생활 침해 위험 최소화 지침을 마련하했습니다. IoT 서비스 업체에서는 아래 단계를 따라 IoT 서비스 또는 제품 개발 초기 단계에 각 질문에 대한 답을 구하기 바랍니다.



도 10 - 설계 의사결정 트리를 통한 GSMA IoT 프라이버시

단계	고려사항
1 단계	**IoT 서비스 또는 제품이 제대로 작동하려면 사용자에게서 또는 사용자에 관하여 어떤 데이터를 수집해야 하는가?** 데이터를 이용하는 비즈니스 모델이라면 맨 먼저 서비스나 제품이 제대로 기능하기 위해 소비자에게서 또는 소비자에 관해서 어떤 정보가 필요한지 파악해야 합니다. 서비스에게 필요한 데이터의 종류는 정적인 데이터(소비자의 이름, 집주소 등)와 동적인 데이터(실시간 위치 등)로 나눌 수 있습니다. 만일 제품이 사용자의 보(步)수와 칼로리 소모량을 추적하는 피트니스 손목밴드라면, 그것을 착용하고 있는 사람의 체중과 연령, 성별, 이동거리, 심박수를 알아야 하겠지만, 그 사람의 실제 위치는 아마도 알 필요가 없을 것입니다. 필요한 데이터의 종류를 평가할 때에는 그 데이터를 사용하고자 할 때 당사자의 동의가 필요한지, 동의를 어떻게 받을지, 당사자에게 프라이버시 환경설정 권한을 부여할지 여부를 결정하는 것도 중요합니다. 제품에 화면이 없다면 스마트폰(예: 모바일 앱, 온라인 대시보드)으로 사용자에게 프라이버시 선택권을 제공하는 방법도 생각해 볼 수 있습니다.

2 단계	**데이터가 '개인적'이고 법으로 규제를 받는 것인가?** 다음 단계는 법에서 정한 데이터 보호 및 프라이버시 요건을 찾아내는 것입니다. 생각해 봐야 할 사항은 다음과 같습니다. • 해당 국가/시장에서 '개인적' 데이터의 정보는 무엇인가? • 수집되는 데이터가 '개인적'이고 법으로 규제를 받는 것인가? 그렇다면 그 데이터를 처리할 수 있는 법적 근거를 확인했는가? • 프라이버시와 관련된 면허 조건(예: 이동통신 사업자)의 적용을 받는가? • 일반적인 데이터 보호법 외에 회사의 데이터 수집 모델과 관련하여 적용되는 연방/주/지방/업종 차원의 법이 있는가? ○ 금융/결제 서비스, 건강관리 규정 ○ 국외 데이터 전송에 관한 제한 가능성
3 단계	**데이터는 어떻게, 어떤 목적으로 사용되는가?** 준법 요건이 무엇인지 확인했다면, 다음은 서비스와 관련해 원하는 결과를 얻기 위해 수집한 데이터를 어떻게 사용할지 그리고 누구와 공유할지 계획을 세워야 합니다. 다음 질문을 통해 데이터 취급과 관련된 보안 문제와 프라이버시 문제에 모두 대처할 수 있습니다. • 데이터를 저장하고 전송할 때 모두 기밀을 유지해야 하는가? • 데이터 흐름을 명확하게 정의하였는가? 즉 데이터가 가치사슬 전반에서 어떻게 어떤 목적으로 사용되고 공유되는지 확인합니다. • 제공하려는 서비스와 관련해 수집된 데이터가 종류 별로 필요한 이유를 댈 수 있는가? • 협력업체와 처음부터 프라이버시 책임 소재를 정의하고 합의했는가? (제품 설계에 책임 소재가 반영돼 있는가?) • 소비자 데이터를 공유하는 회사와 적절한 계약을 체결했는가? (예: 분석 업체가 데이터를 자사의 영리를 목적으로 사용하는 행위를 제한) 위와 같은 계약이나 제약은 양자 간에 적용해도 좋지만, 윤리강령이나 지침을 정해 놓고 협력업체에게 준수를 요청하는 방법도 좋습니다. 후자의 경우 위반 시 결과와 책임을 명시해야 합니다.

4 단계	**프라이버시 침해 평가 실시** 프라이버시 침해 평가(PIA)의 내용은 다음과 같습니다. • 자사 제품이나 서비스가 개인에게 어떤 프라이버시 위험을 유발하는지 확인합니다. • 개인 정보의 오용에서 발생할 수도 있는 개인의 피해 위험을 낮춥니다. • 개인에 관한 데이터를 처리하는, 더 효율적이고 효과적인 프로세스를 설계합니다. PIA 요건은 데이터 보호와 프라이버시 관련 법에서 갈수록 보편적 요소가 되고 있습니다. 영국 정보감독원(Information Commissioner’s Office)에서 제정한 지침[10], 국제개인정보보호전문가협회(International Association of Privacy Professionals)에서 제정한 지침을 비롯해 PIA 시행 요령에 관한 지침이 다수 제정돼 있습니다. PIA 시행 시 일반적으로 생각해 봐야 할 사항은 다음과 같습니다. • 프로젝트로 인해 자사 또는 협력업체가 개인에게 중대한 영향을 미칠 수도 있는 결정이나 행위를 하게 될까? • 개인에 관한 정보가 프라이버시에 관한 우려나 예상을 일으킬 만한 성질의 것인가? 예컨대, 의무 기록, 전과 등 사람들이 개인정보라고 여기는 정보인가? • 프로젝트 때문에 사람들이 침해라고 느낄 수도 있는 방법으로 누군가를 접촉해야 하는가?

5 단계	**사용자 인터페이스 내 프라이버시의 구현**
	소비자에 대한 프라이버시 위험을 평가한 후에는 소비자를 대상으로 그런 위험에 대한 경각심을 어떻게 높일지, 위험을 어떻게 완화할지 고민하고, 더불어 프라이버시 환경설정을 하는 방법을 제시해야 합니다. 궁극적으로, 이 단계의 목적은 회사의 법적 의무에 부합하고 소비자의 니즈와 기대에 부응하는 서비스가 사용자가 원하는 방식으로 제공되게 하는 데 있습니다. 이는 본인의 프라이버시를 본인이 관리할 수 있다고 소비자를 안심시켜 신뢰를 쌓기 위함입니다.
	• 소비자에게 프라이버시 위험에 대한 경각심을 어떻게 높이고 어떻게 현명한 선택을 하게 할 것인가?
	• 법에서 요구할 경우, 소비자의 동의를 받았는가? 동의의 주요 요소: 공개, 이해, 자발성, 행위능력, 합의)
	• 전송, 보관 시 데이터가 안전한가?
	• 소비자 데이터를 보관해야 하는 기간이 있는가? 그 이유는 무엇인가?
	• 소비자의 여정이 신뢰를 얻는 데 도움이 되는가? 예를 들어,
	  ○ 소비자가 서비스 이용의 대가로 어떤 데이터를 제공하는지 알고 있는가?
	  ○ 소비자가 프라이버시 환경을 간단한 방법(예: 웹 방식의 '허가 대시보드' '적시' 프롬프트, 콜센터, 모바일 앱, 음성 지원 명령 등)으로 설정할 수 있는가?

6 단계	**데이터의 이용이 개인의 프라이버시에 영향을 미칠 수 있는가?** 제품이나 서비스와 관련해, 법에서 정한 '개인적' 데이터에 속하지는 않지만 소비자에게 프라이버시라는 느낌을 줄 수 있어 처음부터 이를 감안해야 하는 데이터가 수집될 수도 있습니다. 관련 데이터가 소비자의 프라이버시에 영향을 주는지 그렇지 않은지 확인하려면 다음을 생각해 봐야 합니다. • 서비스/제품에서 나온 (개인적이지 않은) 데이터를 여러 출처에서 나온 다른 데이터와 결합해 특정 소비자의 사생활을 추론할 수 있을 것인가? 예를 들면, 생활양식이나 습관, 종교에 관한 추론으로 다음에 해당하는 것을 말합니다 ○ 건강 보험의 가입 자격에 영향을 미치는 것 ○ 3 자(소매업자, 보험사)가 이용해 특정 소비자에 대한 가격 차별을 할 수 있는 것 • 자사의 제품이나 서비스가 미래의 어떤 시점에 변경될 가능성이 높다면 그 변경이 소비자의 프라이버시에 어떤 영향을 주겠는가? ○ 그 변경으로 소비자에 관해 새로운 데이터(예컨대 위치 데이터)를 수집해야 하는가? ○ 기존 데이터 또는 신규 데이터를 최초 수집 목적과 다른 목적으로 이용할 3 자(예: 광고업자)에게 제공하거나 판매하는가? • 그런 변경이 일어난다면 다음과 같이 해야 합니다. ○ 변경에 따라 새 법의 적용을 받는다면 잠재적으로 회사에 미칠 영향을 확인합니다. ○ 소비자에게 알리고 필요 시 동의를 받는 절차를 마련합니다. ○ 소비자에게 본인의 프라이버시 환경설정을 바꿀 수 있는 수단을 제공합니다. • IoT 서비스 업체가 고려해야 할 사항을 몇 가지 추가한다면 다음과 같습니다. ○ 가치사슬 내 각 협력업체와 계약을 통해 책임 소재를 명확하게 정합니다. ○ 명확한 시정 절차를 마련해 문제가 발생하거나 프라이버시 침해를 당할 경우 소비자가 연락할 곳을 정해 둡니다.

아래 다이어그램은 위에서 설명한 단계를 도식화하는 한 가지 방법을 보여주고 있습니다.

부록 B 자동차 추적 시스템을 이용한 보기

이번 보기에서는 IoT 보안 지침의 관점에서 자동차 추적 시스템을 평가합니다. 프로세스는 본 개요서의 단원 6 "본 지침서의 효과적 활용법"에서 추출한 것입니다.

B.1 기술적 모델의 평가

첫 단계 "기술적 모델의 평가"에서는 엔지니어링 팀이 제품 아키텍처를 토대로 디바이스가 어떻게 작동하는지 평가합니다. 솔루션에 사용된 기술을 항목별로 정리하여 인력을 정비하고 보안 업무를 배정하고 진척도를 관리합니다.

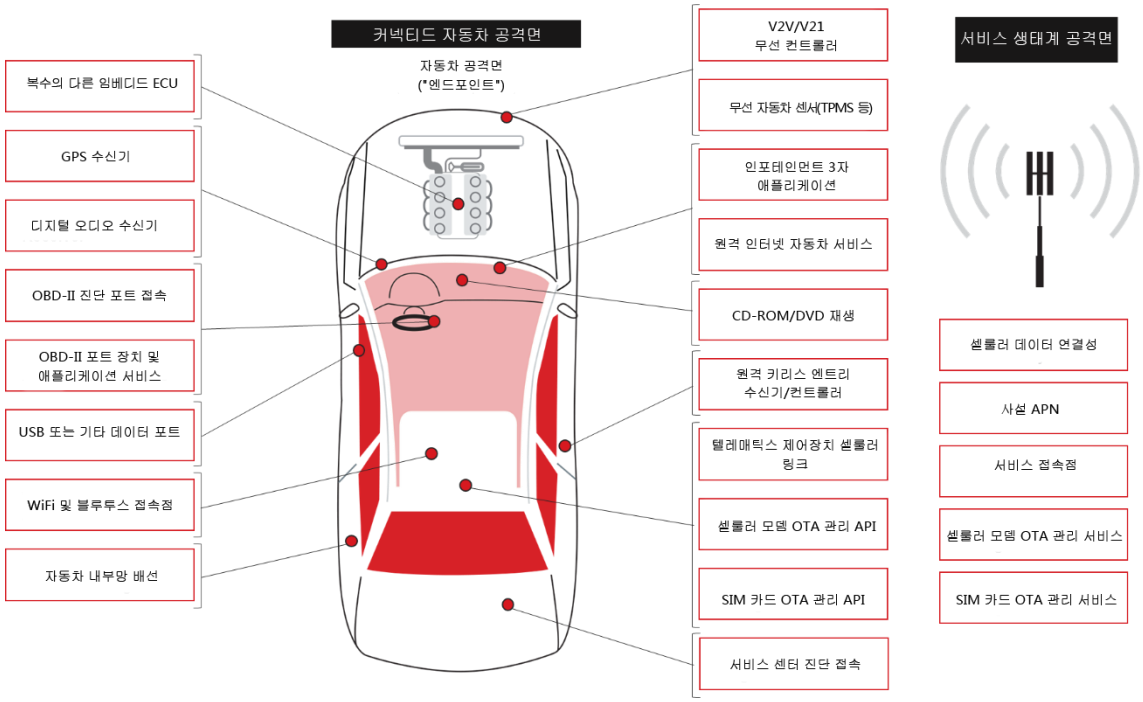
단순하게, 보기의 자동차 추적 시스템은 다음과 같은 기능을 갖는 것으로 가정합니다.

- **엔드포인트 생태계**
  - 다음과 같은 기능을 갖춘 가능한 간단한 그래픽 사용자 인터페이스(GUI)
    - ID 와 비밀번호로 로그인
    - 추적 기능 끄기
    - 추적 기능 켜기
    - 현재 위치 파악 및 시각화
  - 백엔드 서비스와 연결하는 셀룰러 모듈
  - 셀룰러 모듈용 SIM 카드
  - 백엔드 전원용 리튬 폴리머 배터리
  - 중앙처리장치(CPU)
  - 비휘발성 RAM 속 임베디드 애플리케이션
  - RAM
  - EEPROM
- **서비스 생태계**
  - 셀룰러 데이터 연결성
  - 보안 사설 APN
  - 서비스 액세스 포인트
  - 셀룰러 모뎀 OTA 관리 서비스
  - SIM 카드 OTA 관리 서비스

팀은 각 기술과 관련된 정보를 표시한 후 각 지침서의 모델 단원을 확인해 적합한 기술 모델을 찾습니다. 이 엔드포인트는 복잡한 엔드포인트입니다. 서비스 및 네트워크 모델은 표준 모바일 기반의 IoT 서비스입니다.

B.2 보안 모델의 검토

기술 모델의 윤곽이 드러났다면 보안 모델의 검토를 준비해야 합니다. 보안 모델에서는 도청자가 솔루션을 어떻게 공격할 수 있을지 평가합니다.



도 11 - 커넥티드 자동차 공격의 통로

여기 보기에서는 공격과 관련된 위협이 다음 두 가지뿐입니다.

- 셀룰러 네트워크
- 자동차에 대한 로컬 공격

로컬 네트워크 연결은 없고 모바일 네트워크 연결만 있으므로 공격자는 셀룰러 네트워크 연결을 무력화하거나 사설 APN 을 통해 통신 채널로 들어오거나 서비스 접속 지점 또는 셀룰러 모뎀 또는 OTA 관리 서버 또는 SIM 카드 OTA 관리 서버를 통해 들어와야 합니다.

그 외 디바이스를 무력화하는 방법은 물리적 공격뿐이며, 위 다이어그램과 같이 몇 군데 진입 지점이 있습니다. 그러므로 본 IoT 서비스의 경우, 엔드포인트에 크게 집중해야 합니다.

B.3 보안 업무 검토와 할당

보안 모델의 평가가 끝나면 보안 업무의 할당은 간단합니다. 각 팀에서 평가가 필요한 솔루션 구성요소마다 한 사람씩 배정합니다. 평가는 상위 레벨(엔드 포인트, 네트워크, 서비스)이 아니라 구성요소 이하 레벨에서 실시해야 합니다. 이는 CPU 와 운영체제, 네트워크 서비스 등에 CPU 를 배정해야 한다는 뜻입니다.

각 구성요소에 담당자가 배정되면 프로세스를 시작해도 됩니다. 이는 이 단계에서 팀이 다음 사항을 알고 있다는 뜻입니다.

- 기술이 어떻게 구성돼 있는가?
- 기술이 보안에 어떤 영향을 미치는가?

- 어떤 엔지니어링 관계자가 해당 기술을 담당하는가?

B.4 권고 사항 검토

권고 사항 검토 단계에서는 팀원 각자가 권고 사항을 *최대한 많이* 읽어 의미를 파악해야 합니다. 의식적으로 그렇게 해야 합니다. 엔지니어는 특정 구성요소에 관한 권고 사항에만 매몰되지 말고 시간을 들여, 상위 레벨에 한해서라도 권고 사항을 최대한 많이 이해해야 합니다. 그래야 그 구성요소가 제품/서비스의 전체적인 보안에 어떻게 영향을 미치는지 제대로 파악할 수 있기 때문입니다. 이렇게 하면 엔지니어 그룹이 토론을 통해 비용 대비 효과와 수명, 관리 측면에서 어떤 시정 전략 또는 완화 전략이 최대의 균형을 이룩할 수 있는지 가늠할 수 있습니다.

권고 사항 검토가 끝나면 *구성요소 담당자*가 특정 권고 사항이 이미 적용되었는지 판단할 수 있습니다. 적용되지 않았다면 *준비 중*이라고 표시합니다. 이를 통해 엔지니어 그룹은 도입 전에 권고 사항의 적용 가능성을 논의할 수 있습니다. 이 방식은 전략적으로도 더 유리합니다. 일부 권고 사항에서 다른 권고 사항의 실행이나 기존의 관리수단에 영향을 미치는 부작용이 나타날 수도 있기 때문입니다.

이번 보기에서 팀은 다음 사항을 판단했을 것입니다.

- 애플리케이션 트러스트 베이스를 사용해야 함
- 조직의 신뢰 기반(RoT)를 규정해야 함
- 디바이스 개인화를 구현해야 함
- 탬퍼링에 강한 케이싱을 구현해야 함
- 엔드포인트 비밀번호 관리를 강화해야 함
- 엔드포인트 통신 보안을 강화해야 함
- 암호 사인이 들어간 이미지를 구현해야 함
- 프라이버시 관리를 실행해야 함
- 디바이스 전원 경고를 통합해야 함

B.5 구성요소 위험 검토

다음으로, 구성요소 단원을 평가해 특정 요소를 제품이나 서비스에 구현하거나 통합할 때 수반하는 각종 위험을 찾아내야 합니다. 이 단원은 업무 경감을 위해 구성요소 담당자만 검토해도 됩니다. 그렇지만 가급적 많이 읽는 것이 좋습니다.

권고 사항과 구성요소 위험 단원을 검토한 결과 다음과 같은 보안의 허점이 발견되었습니다.

- 비밀정보가 비보호 EEPROM 에 저장되어 있음
- 비밀정보가 내부 RAM 에서 처리되지 않았음
- 사용자 인터페이스는 비밀번호를 보호해야 함
- 사용자 프라이버시를 사용자에게 알려야 함

B.6 구현과 검토

이제 담당 팀은 서로 합의한 보안 요건에 맞도록 솔루션을 조정할 수 있습니다. 필요하다면 구성요소를 다시 구현하고 보안 관리장치를 추가합니다.

본 보기에서는 팀이 SIM 카드(애플리케이션 기반의 트러스트 앵커 기술이 들어 있는 것)를 프로비저닝할 수 있는 GSMA 회원과 협력하고 있음을 알게 되었습니다. 따라서 기존 SIM 카드를 이용해 트러스트 앵커 문제를 해결할 것입니다. 또 표준 GSMA 기술로 SIM 을 현장에서 개인화할 수 있으므로 개인화 문제도 해결됩니다.

SIM 기술은 또 공중을 통해 통신 보안키를 프로비저닝 할 수 있어 통신 인증과 프라이버시 문제도 해결할 수 있습니다.

회사 고유의 SIM 구역은 회사가 인증서 체인을 이용해 피어를 인증할 수 있는 RoT 베이스로 프로그램할 수 있습니다. 이로써 조직의 신뢰 기반과 피어 인증 요건이 해결됩니다.

제품 케이싱은 탬퍼에 강한 포장으로 업데이트 됩니다.

EEPROM 은 SIM 트러스트 앵커에 저장된 보안키로 암호화된 데이터로 인코딩됩니다.

부트로더는 경보 접수 후 트러스트 앵커를 이용해 애플리케이션 이미지를 인증합니다.

엔드포인트는 재프로그램돼 비밀번호 입력 시 이를 차단하여 사용자의 안전한 암호 입력을 지원합니다.

프라이버시 관리 GUI 가 추가돼 사용자는 회사에서 어떤 정보를 수집하는지 보고 통제할 수 있습니다.

비밀정보는 같은 칩의 내장 메모리에서만 처리됩니다.

이 같은 구현이 정의되고 나면, 팀에서는 보안 권고 사항과 위험을 모두 재평가하고 보안 모델을 검토해 변경사항이 문제를 해소하였는지 파악합니다.

B.7 지속적인 라이프사이클

팀에서 승인 받은 구성을 구비하였으므로 기술 도입 준비는 끝났습니다. 그러나 보안은 여기서 그치지 않습니다. 팀은 엔드포인트의 보안 이상을 모니터링하는 방법과 기술에 새로 발견된 보안 허점이 없는지 확인하는 방법을 찾습니다.

이어 사고 또는 허점을 어떻게 찾아내 시정하고 회복할지 계획을 세웁니다. 그러면 시간이 지나도 조직이 진화하는 기술과 보안의 양상에 당황하지 않게 됩니다.

부록 C 문서 관리

C.1 문서 이력

버전	날짜	변경 내용	승인권자	편집자 / 회사
1.0	2016-02-08	New PRD CLP.11	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security
1.1	2016-11-07	GSMA IoT 보안 평가 제도에 대한 언급 추가됨. 사소한 편집 교정	PSMC	Ian Smith GSMA
2.0	2017-09-29	문서에 LPWA 네트워크 정보 추가. 사소한 업데이트.	IoT Security Group	Rob Childs

C.2 기타 정보

유형	설명
문서 담당자	GSMA IoT Programme
연락처	Rob Childs - GSMA

당 기관은 문서 품질을 중시합니다. 오류 또는 누락 발견 시 의견과 함께 연락 바랍니다. prd@gsma.com 으로도 연락할 수 있습니다.

의견, 제언, 질문은 언제든지 환영합니다.