임베디드 보안

시스템 모듈에 내재된 보안 솔루션

개요

최근 많은 산업계에서 사물 인터넷(IoT)을 도입하는 주된 목적은 네트워크에 연결된 장치들로부터 방대한 양의 데이터를 수집하고 분석해 바람직한 비즈니스 가치를 창출하는 것에 있습니다. 하지만 인터넷에 연결된 장치가 늘어날수록 사이버 공격 대상과 위험 요소도 증가하게 됩니다. 또한 보호해야 하는 기기가 고성능의 IT 장치를 넘어 저전력, 초경량의 특성을 가지는 일상생활의 모든 사물로 확대되어 사이버 공격 시 개인 정보 유출이나 금전 피해 뿐만 아니라 전체 시스템이 마비되거나 이용자들의 생명에도 위협이 될 수 있습니다. 이러한 문제를 예방하기 위해서는 IoT 제품과 서비스의 설계부터 폐기까지 생애 주기 전반에 따른 다양한 보안 요구 사항들을 파악하고 단계별 맞춤형 보안을 내재해야 합니다.

보안 취약 사례

스마트시티는 도시 전역에서 정보를 수집하고 이를 분석하여 필요한 곳에 새로운 자원을 투입하거나 기존 자원을 효율적으로 활용해 도시 인프라 부족, 에너지 부족, 교통혼잡 등의 도시 문제들을 해결하고 있어 범정부 차원에서 주목을 받고 있습니다. 스마트시티 구성요소 중 가장 많은 IoT가 적용된 스마트 빌딩은 주요 설비에 IoT 센서를 설치해 모든 상황을 모니터링하고 스스로 상태를 판단해 최적의 운영을 지원합니다. 스마트 교통은 주차면 센서를 활용한 주차 유도 시스템, CCTV를 활용한 불법 주정차 단속, 교통신호 관제 등을 이용해 도시 스스로가 교통정보를 수집하고 교통 환경을 감지할 수 있도록 합니다.

지금까지 스마트시티는 도시 문제를 해결하는 것에 집중했다면 앞으로는 관리의 위협이 되는 보안 문제를 조금 더 다루어야 합니다. 플랫폼을 통해 모든 구성요소들을 통합적으로 관리하는 스마트시티에서 하나의 IoT 장치를 해킹해 동일 네트워크에 연결된 다른 장치들을 해킹하는 것은 전혀 어려운 일이 아닙니다.

최근 IP 카메라를 해킹해 다른 사람의 사생활을 훔쳐보는 범죄가 빈번히 발생하고 있습니다. 스마트시티를 구성하는 요소 중 하나인 CCTV 역시 동일한 방법으로 해킹되어 범죄 현장 영상을 삭제하거나 동일 네트워크에 연결된 교통 신호체계를 교란시킬 수 있습니다. 또는 전력, 가스, 수도를 통제하는 IoT 장치가 해킹되어 시민들의 삶에 필수적인 자원들을 이용하지 못하는 상황도 발생할 수 있습니다.

IoT 장치의 해킹 위험은 스마트시티에만 해당하는 것이 아닙니다. 지금까지는 IoT를 통해 얻을 수 있는 정보들이 제한적이라 그 피해 정도가 심각하지 않았습니다. 하지만 IoT가 우리의 일상은 물론 국가의 주요 기반 시설에 깊숙이 도입되고 있는 이 시점에서 임베디드 보안은 미룰 수 없는 중요한 과제입니다.

(주)시그마델타테크놀로지

최근 클라우드 컴퓨팅의 고도화로 많은 기업이 IaaS나 PaaS 형태의 비즈니스 모델을 구축하고 있습니다. 하지만 하나의 업체가 모든 인프라를 구축하기엔 인력, 시간, 비용, 경험부족 등의 문제가 발생할 수 있습니다.

시그마델타테크놀로지(SDT)는 AI 엔진, 임베디드 보안, 무선 IP 통신, 클라우드 라이브러리 등이 탑재된 동전 크기의 시스템 모듈을 통해 AIoT 인프라를 제공해 고객사의 기술적 부담을 덜어줍니다. SDT의 초소형 시스템 모듈로 기반 기술에 대한 고민 없이 고객사의 서비스 영역에만 집중해 AIoT 제품과 서비스를 개발해보세요.

주 소 서울 금천구 가산디지털1로 19, 706-1호
웹사이트 www.sigma-delta.tech
이 메 일 sales@sigma-delta.tech
전화번호 02-2629-4701

임베디드 보안

Platform Security Architecture(PSA)

1조 개의 장치가 네트워크에 연결되는 세상으로 나아가는 과정에서 임베디드 보안은 가장 중요하게 고려해야 하는 요소 중 하나입니다. 장치와 이를 통해 수집되는 데이터의 신뢰는 말할 것도 없고, 대규모의 장치가 시장에 배포된 이후에도 신뢰를 구현할 수 있어야 하기 때문입니다. 또한 개별 소비자에서 기업, 정부기관에 이르기까지 사용자의 신뢰를 얻는 것도 중요합니다.

IoT 보안의 중요성이 대두되면서 보안 내재화에는 이견이 없지만 어떻게 설계해야 하는지는 의견이 분분합니다. IoT 장치는 단순하고 전력 소모가 적어야 해 지금까지의 고성능 IT 장치를 위한 보안과는 전혀 다른 보안이 필요합니다. 안전하게 개발했다고 해도 시장에 배포될 방대한 수의 장치들이 모두 안전하다고 보장할 수 없습니다. 또한 장치의 생애 주기 전반에 걸쳐 주기적인 펌웨어 업데이트가 필요한데, 무선 업데이트 과정 중 사이버 공격에 노출될 위험도 있습니다.

이러한 산업계의 어려움을 해결하기 위해 글로벌 반도체 IP 업체 Arm은 다양한 파트너사 및 정부기관과 협력해 국제보안 표준인 PSA를 제정했습니다. PSA는 모든 유형의 취약점으로부터 IoT 장치를 보호할 수 있도록 보안 설계 가이드라인을 제시합니다. 이를 기반으로 칩, 운영체제, 디바이스 업체들은 제품 설계의 아주 초기 단계부터 생애 주기 전 과정을 고려한 보안을 내재할 수 있습니다.

PSA 가이드라인을 준수해 설계된 장치에는 공식 인증서인 'PSA Certified'를 발급합니다. 해당 인증을 받기 위해서는 아래 8가지 조건을 충족해야 합니다.

1. Secure Processing Environment(SPE)
   Arm TrustZone, 방화벽 또는 듀얼코어 아키텍처와 같이 안전한 격리 환경을 구축해 민감한 자산을 분리해 보호해야 합니다.
2. Secure Boot
   보안 부팅은 인증된 암호 키로 서명된 부트 로더만 통과하고 실행시키며 잘못된 자격 증명을 가진 코드나 자격 증명이 없는 코드는 거부해야 합니다. 또한 작업 중 보안 이상이 감지될 경우 반드시 부팅 단계로 돌아가야 하며, 보안 부팅을 위한 코드는 누군가가 임의로 변경할 수 없도록 해야 합니다.
3. Secure Storage
   디바이스 키, 비밀번호, 고객 데이터 등 중요한 정보를 안전하게 저장할 수 있는 공간을 구축하고, 이 공간에는 권한을 가진 사람만이 접속할 수 있도록 해야 합니다.
4. Secure Firmware Update
   디바이스의 펌웨어를 안전하게 업데이트할 수 있도록 지원해야 합니다.
5. Cryptographic Service
   AES, TLS, SHA, ECDSA 등의 암호화/복호화 알고리즘을 지원해야 합니다.
6. Secure Communication
   서버와 안전한 통신을 보장해야 합니다.
7. 보안 상식
   #0000, #1234와 같은 단순한 암호를 지정할 수 없도록 하거나 디바이스를 리셋할 때 이전 사용자 정보를 무조건 삭제하는 등 보안과 관련된 기본적인 상식을 요구합니다.
8. Hardening & Lifecycle Management
   디바이스가 시장에 배포된 이후에도 안전하게 관리될 수 있도록 지속적으로 지원해야 합니다.

SPE와 None-SPE(NSPE)

- Arm TrustZone, 방화벽 구조

인증받지 않은 관리자는 SPE 내부로 접근할 수 없도록 방화벽 설치
ex. SDT32L4M, SDT32F4M 등

- 듀얼코어 아키텍처

보안이 필요한 작업은 철저히 코어 2에서만 수행되며, 작업 완료 후 코어 1으로 전달
ex. SDT62M, SDT63M 등

Secure Workflow

SDT는 제품 개발부터 시장에 배포된 이후까지 고객의 IoT 제품과 서비스가 안전할 수 있도록 Secure Workflow라는 보안 솔루션을 제공합니다. Secure Workflow는 완벽하게 안전한 IoT 보안을 구축하기 위해 총 6단계로 구성되어 있으며, 전 단계에 걸쳐 복제, 위조, 도용, 복사 및 도청을 차단합니다.

1. Secure Device
   하드웨어 보안은 현장에 배포되어 있는 고객의 IoT 제품과 서비스를 보호하기 위해 필수적인 요소입니다. SDT는 하드웨어 보안을 위해 Secure Boot Manager(SBM), Arm TrustZone, Secure Element, Secure Authenticator 등의 기능들을 시스템 모듈 내에 설치하고 탑재합니다.
2. Secure Manufacturing
   SDT는 정보 유출 및 해킹으로부터 안전한 시설에서 하드웨어를 제조합니다. 이 단계에서는 제한된 공간 내에서 zero-trust 보안을 구축하기 위해 3단계와 4단계를 함께 실시하기도 합니다.
3. Secure Mastering
   지적 재산권의 도난, 불법 복제 및 위조를 방지하기 위해 하드웨어와 하드웨어에 로드되는 모든 소프트웨어와 펌웨어 이미지에 서명하고 암호화하는 과정을 수행합니다.
4. Secure Programming
   Mastering 단계에서 암호화된 이미지를 제품에 안전하게 주입하는 단계입니다. Secure Mastering과 Secure Programming 단계를 통해 보안 환경에서 승인받은 개발자만이 접근할 수 있도록 해 하드웨어를 안전하게 보호할 수 있습니다.
5. Secure Provisioning
   보안 인증서를 이용해 디바이스와 클라우드 간 통신 과정 중에 발생할 수 있는 도청의 위험으로부터 고객의 데이터를 안전하게 보호합니다.
6. Secure Deployment
   항상 새롭게 변화하는 IoT 생태계에 대응하기 위해 클라우드를 통한 펌웨어 업데이트와 디바이스 생애 주기 관리는 필수입니다. Secure Deployment를 통해 고객사는 수백만 대 이상의 기기를 안전하게 관리할 수 있습니다.

보안 인증서(Certificate)

SDT는 IoT를 위한 보안 인증서를 발급하는 기관(Certificate Authority; CA)으로, 고객의 지적 자산과 물리적 자산을 보호하기 위해 최선을 다하고 있습니다.

SDT의 보안 인증서는 공개키기반구조(Public Key Infrastructure; PKI)를 이용해 발급됩니다. PKI란 암호화 키와 복호화 키가 서로 다른 공개키(비대칭키) 알고리즘을 이용해 송수신 데이터를 암호화하고 사용자를 인증하는 시스템입니다. 공개키 방식은 데이터를 암호화하고 이를 풀 수 있는 열쇠가 다르기 때문에 완벽한 보안이 가능합니다.

이러한 보안 인증서는 SDT의 시스템 모듈이 탑재된 디바이스에만 발급될 뿐만 아니라 서버, 게이트웨이, 펌웨어, 클라우드 등 모듈과 연결된 모든 통신 객체에도 발급되어 데이터 전송이 발생하는 전 단계를 완벽하게 보호할 수 있습니다.

IoT 시스템 모듈

기존 시스템 모듈		SDT의 부가가치
통신 솔루션	CPU	**임베디드 보안**
전력 관리	ROM	**클라우드**
운영체제	RAM	**AI 엔진**

SDT의 IoT 시스템 모듈에는 CPU, ROM, RAM과 같은 하드웨어 기능과 함께 통신, 보안, 클라우드 등 낯설고 어려운 기술 솔루션들이 모두 구현되어 있습니다. 이더넷, 와이파이, 블루투스, Wi-SUN FAN, LTE Cat.M1 또는 LTE와 같이 다양한 유무선 통신을 바로 이용할 수 있습니다. 또한 Amazon AWS, Microsoft Azure, Arm Pelion, Samsung SmartThings와 같은 클라우드 플랫폼과 연결될 수 있도록 인프라 서비스와 인증서도 탑재되어 있습니다.

국제보안 표준 PSA에 준수하여 설계된 SDT 시스템 모듈은 보안 부팅, 보안 프로그래밍, 보안 스토리지 등 고객에게 필수적인 보안 요소들을 모두 제공하여 스마트시티, 스마트홈, 의료기기 등 다양한 산업에 안전하게 적용할 수 있습니다.

제품 라인업

	SDT32L0M	**SDT32L4M**	**SDT32F4M**
코어	– Cortex-M0+	– Cortex-M4F	– Cortex-M4
MCU	– STM32L0	– STM32L4	– STM32F4
메모리	– 20KB RAM – 192KB Flash	– 320KB RAM – 1024KB Flash	– 260KB RAM – 2048KB Flash
보안	– PSA Certified(예정) – TRNG	– PSA Certified – Mbed TLS – TRNG	– PSA Certified – Mbed TLS
I/O	– USART, SPI, I^2C, ADC, DAC	– USART, SPI, I^2C, ADC, DAC – CAN, USB	– USART, SPI, I^2C, PWM, GPIO, ADC – Ethernet, CAN
	SDT32F7M	**SDT62M**	**SDT63M**
코어	– Cortex-M7	– Cortex-M4F – Cortex-M0 (for security)	– Cortex-M4 – Cortex-M0 (for security)
MCU	– STM32F7	– Cypress PSoC62	– Cypress PSoC63
메모리	– 512KB RAM – 1MB Flash	– 288KB RAM – 1024KB Flash	– 288KB RAM – 1024KB Flash
보안	– PSA Certified – Mbed TLS – TRNG	– PSA Certified(예정)	– PSA Certified(예정)
I/O	– USART, SPI, I^2C, I^2S, ADC, DAC – Ethernet, CAN, USB	– UART, SPI, I^2C, I^2S – USB	– UART, SPI, I^2C, I^2S – USB