AWS를 통한 사물인터넷(IoT) 보안

안전한 클라우드 채택

2019년 4월

본 문서 사용에 대한 공지

본 문서는 정보 제공 차원에서 작성된 문서입니다. 이 문서의 발간 날짜를 기준으로 제공된 AWS의 제품 및 정책에 대한 정보가 수록되어 있으므로, 공지 없이 차후에 이 정보가 변경될 수 있음을 알려드립니다. 이 문서에 수록된 모든 정보는 고객 스스로 독립적으로 평가/ 판단하고, 고객은 AWS 상품 및 서비스를 사용함에 있어, 명시적이든 묵시적이든 상관없이, 어떤 형태의 보증도 없는 "현 상태(as is)"로 사용할 책임이 있습니다. AWS, 계열사, 공급 업체 또는 인가업체(자)의 그 어떠한 워런티, 진술, 계약 약정, 조건 또는 보증이 본 문서에 의해 부여되지 않습니다. 고객에 대한 AWS의 책무 및 법적 책임은 AWS 계약에 의해 관리되며, 이 문서는 AWS와 고객이 맺은 그 어떤 계약에도 속하지 않으며, 기존의 그러한 계약을 수정하지도 않습니다.

목차

목적

이 문서에서는 AWS 클라우드상에서 활용되는 사물인터넷(이하 IoT) 서비스의 보안에 대해 면밀하게 살펴보고자 합니다. 또한 각 조직의 IT 프로그램의 고위 책임자, 의사결정권자를 비롯하여, 안전한 IoT 솔루션 도입을 고려 중인 보안 전문가를 대상으로 작성되었습니다.

배경

IoT 기술을 활용하여 각 기업과 단체는 프로세스를 최적화하고, 제품 및 서비스를 향상하며, 다양한 방식으로 고객들에게 기술 혁신의 경험을 안겨주고 있습니다. 각 기업의 리더들은 이런 IoT 기술이 기업에 큰 혜택을 가져다 주는 것에 높은 기대를 갖고 있는 반면에, 보안, 리스크, 개인 정보 보호에 대한 우려 또한 여전히 갖고 있습니다. 이런 보안에 대한 우려는 상이하고 호환되지 않은 그리고 때때로 미흡한 보안 기능으로 인하여, 제대로 보안되지 않은 상태에서 배포되어, 고객/기업 소유의 데이터 노출에 대한 위험성이 증가된 것에 그 원인을 일부 찾아볼 수 있습니다.

각 조직은 스마트한 서비스를 제공함으로써 삶의 질을 대폭 향상하고, 기업의 운영 및 정보 역량을 높이며, (의료) 업체로부터 양질의 케어를 받고, 스마트한 도시 회복력을 구축하며 지속 가능한 환경을 조성할 수 있음에 상당한 기대를 갖고 있습니다. 또한, 아직 우리의 상상 속에 있는 수많은 잠재적 혁신을 구현해 줄 스마트 서비스를 제공하기 위하여 부단히 노력하고 있습니다. 최근에는 의료 산업 및 지방 자치 단체의 AWS IoT 채택이 증가한 것으로 나타나고, 다른 산업에서도 곧 이런 추세가 이어질 것으로 예상됩니다. 많은 지자체에서는 혁신적인 기술을 조기 도입하며, IoT와 같은 첨단 기술 융합에 앞장서고 있습니다. 그 일부 사례를 아래에 소개합니다:

- **미주리 주 캔자스시티:** 캔자스 시티(KC)는 KC 전차 철로와 호환, 운영되는 신규 시스템 관리를 위하여 통합된 스마트 시티 플랫폼을 구축했다. 비디오 센서, 도로면 센서, 접속망에 연결된 가로등, 공용 WiFi 네트워크, 주차 및 교통 관리 서비스를 통해, 에너지 비용 절감은 40%에 이르며, 신도시 개발에 17억 달러, 그리고 3,247개의 신규 주택 혜택을 제공할 수 있게 되었다.
- **일리노이 주 시카고:** 시카고는 교차로에 센서와 카메라를 설치하여, 꽃가루 농도 및 대기질을 관측함으로써, 도시 주민의 건강을 챙기고 있다.
- **이탈리아 카타니아:** 카타니아 시는 가까운 주차장 위치 정보를 알려주는 앱을 개발하여, 출퇴근 시민들에 공급 중이다.
- **브라질 헤시피:** 헤시피 시는 쓰레기 수거 트럭 및 청소 카트에 추적 디바이스를 설치하여 활용 중이다. 이 추적 기능을 통해, 헤시피 시는 청소 비용에 월 25만 달러를 절감하는 동시에, 해당 공공 서비스의 신뢰성과 운영 효율성을 대폭 개선하였다.
- **영국 웨일즈의 뉴포트:** 뉴포트 시에서는 스마트 시티 IoT 솔루션을 공급함으로써, 단 몇 개월 만에 대기질, 홍수 통제, 폐기물 관리 등을 개선하였다.
- **인도네시아 자카르타:** 인구 2800만 명에 달하는 자카르타 시는 자주 침수 피해를 겪는 도시이다. 이에 동도시는 운하 및 저지대의 수위 감지를 위한 IoT를 활용 중이며, 소셜미디어를 통해 시민들의 반응을 살피고 있다. 시 당국은 또한 조기 경보 및 대피 명령을 적시적소에 제공하여 정부 및 구급대원들이 가장 시급하게 도움이 필요한 곳을 파악하고, 대피 절차가 원활하게 진행될 수 있도록 지원하고 있다.

Machina Research에 따르면 전 세계 IoT 시장 규모는 2024년까지 4조3000억 달러에 이를 것이라고 합니다.[1] 영국의 '비즈니스혁신기술부' 보고서에 따르면, 스마트 시티 솔루션과 이런 솔루션 배포에 따른 추가 서비스 분야의 글로벌 시장 규모는 2020년까지 4080억 달러로 늘어날 것으로 추산했습니다.[2] 또한, Forbes[3]는 "예지 정비, 자가 최적화 생산, 자동 재고 관리 등은 2020년까지 IoT 시장 성장을 선도할 주요 3대 사용 사례가 될"것이라고 예측했습니다. Forbes는 또한 IoT 솔루션을 구축, 배포할 경우 고객에게 미치는 영향이 막대하기 때문에, 각 기업들은 안정적인 인프라를 이미 갖춘 기존의 IT 벤더업체와의 거래를 선호할 것이라고 단언합니다.

IoT를 통해서 얻는 비즈니스 기회를 활용하고 싶지만, 사실 IoT를 도입할 경우, 보안 여부는 예전부터 장담하기 어려운 부분이 있었습니다. 솔루션에 필요한 기능 및 서비스가 항상 자동 보안 상태로 제공된 것은 아니었기 때문에, 해당 솔루션의 아키텍처 기반에는 잠재적인 보안상의 빈틈이 존재했습니다. 또한, 암호화된 통신 및 OTA(Over-The-Air) 업데이트 등과 같은 키 사례에서도 업데이트 및 유지 관리가 자동 실행되지는 않았습니다. 또한, 최종 배포 후에도 디바이스 및 게이트웨이를 원격으로 보안 패치하는 서비스를 지원하는 업체는 거의 없었기에, 디바이스는 보안 위험에 더욱 취약한 상태였습니다.

이에 대응하여, 보안을 중요하게 고려하는 AWS는 다양한 데이터 감도 및 기밀성과 보안 관련 요구사항을 충족하는 조치를 마련하여 다양한 산업 분야와 전 세계 방대한 지역에서 수백만 명의 고객을 지원하고 있습니다. AWS의 모든 서비스 계층에 보안이 확보되고, 이 보안이 IoT 디바이스까지 이어지도록 만들기 위해, AWS는 상당한 자원을 투자하고 있습니다. AWS는 고객 시스템과 데이터의 기밀성, 무결성, 가용성을 보호하는 동시에, IoT 솔루션에 요구되는 안전하고, 확장 가능하며, 보안된 플랫폼을 제공하는 것을 우선 과제로 삼고 있습니다.

보안 문제

보안 위험성과 그 취약점으로 인해, IoT 애플리케이션에서의 고객 데이터에 대한 보안 및 개인정보보호 기능이 잠재적으로 손상될 가능성이 있습니다. 디바이스의 수가 점차 증가하고, 데이터량도 방대하게 늘어나면서, 잠재적 피해 가능성 또한 증가하고 있습니다. 이에, IoT 디바이스로 인한 보안 위험성과 클라우드상에서 송/수신되는 디바이스간의 통신으로 인한 보안 문제를 어떻게 해결할 것인가에 대한 고민이 깊어지고 있습니다.

디바이스에 대한 패치, 디바이스 인증 그리고 디바이스 사용자 인증, 액세스 제어 등과 관련한 보안 문제와 함께, 클라우드상에서의 데이터 전송 중에, 또는 엣지 서비스와 디바이스간의 데이터 전송 중에 발생되는 데이터 보안 및 암호화에 대해서 고객들은 주로 우려하고 있습니다. 데이터의 무결성을 유지하고, 또한 디바이스의 신뢰성을 해치는 공격을 막으려면, IoT 디바이스의 보안성이 확보되어야 합니다. 디바이스가 인터넷을 통해 대량의 민감한 데이터를 전송할 수 있고, 최종 사용자가 디바이스를 직접 통제할 수 있으므로, "사물"의 보안은 솔루션의 모든 계층에서 철저하게 확보되어야 합니다.

데이터 유출 관련 뉴스로 인해, 고객들이 IoT 보안에 대해 면밀하게 살펴보면서, IoT 보안에 대한 교훈과 더 나은 관리를 위한 모범 사례도 얻게 되었습니다. IoT 솔루션의 기초는 언제나 보안에서 시작하고, 보안에서 끝나야 합니다. 또한 IoT 구성[4]을 지속 감사하는 서비스를 사용하면, 보안 운영의 모범 수칙에서 벗어나는 일은 없는지 확인할 수 있습니다. 그래서 보안 수칙에서 벗어나는 징후가 감지되면 경보 알람이 발생되고, 이에 적절한 시정 조치가 실행되게 됩니다. 물론, 가장 이상적인 방법은 이런 시정 조치가 자동 실행되는 것입니다.

---

1 https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024.

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217- smart-city-market-opportunties-uk.pdf .

3 https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by- 2020/#74c8f8c7609b

4 구성(Configuration)은 디바이스들간의 상호 정보 교환 또는 디바이스 대 클라우드간의 정보 교환 시, 안전하게 정보를 유지할 수 있도록 고객이 환경을 설정하는 기술적 제어 장치.

다수의 디바이스가 시장에 진입하는 것에 대비하고, 동시에 온라인 상에 존재하는 보안 위협에 대응하려면, IoT 생태계의 모든 영역에 걸쳐서, (클라우드에 연결되었든 그렇지 않든 상관없이), 디바이스의 보안 및 보호, 감사 및 수정, IoT 디바이스의 플릿 배포 관리까지 모두 포함된 보안 서비스를 구현하는 것이 가장 이상적입니다.

정부 차원에서의 IoT 보안 대응 노력은?

민간 부분의 의료, 산업 건설 및 저전력 소비재 공급업계 등이 IoT를 적극 배포/활용하면서, 국가 및 지자체 차원에서도 이제는 IoT 도입과 보안 문제에 대응하기 시작했습니다(부록 2 참조). 이에 AWS는 IoT의 향후 정책 환경을 평가하는 것 외에도, AWS 고객들이 규정 준수의 의무를 다할 수 있도록, 다각도에서 규정 준수 프레임워크 관련 서비스를 지속적으로 추가하고 있습니다(부록 3 참조).

AWS IoT 서비스 및 보안 기능

AWS는 고객의 디바이스/연결성/데이터 보안을 지원하는 일련의 IoT 서비스를 제공합니다. 이런 서비스를 활용하면 디바이스 보호에서부터, 데이터 전송 중에 또는 휴지 상태에서의 데이터 보안까지, 엔드투엔드(End-to-End) 보안이 가능합니다. 또한, 보안 워터마크를 충족할 수 있는 보안 정책을 적용, 실행하는 기능도 제공됩니다.

AWS IoT는 폭넓고 심층적인 기능을 제공하기 때문에, 다양한 디바이스에서 그리고 거의 모든 사용 사례에서 IoT 솔루션을 구축할 수 있습니다. AWS IoT는 인공 지능(AI) 서비스와 통합되어 있으므로, (심지어 인터넷에 연결돼 있지 않아도), 디바이스를 더 스마트하게 만들어 활용할 수 있습니다. AWS 클라우드를 기반으로 한, 190개국의 수백만 명의 고객이 사용 중인 AWS IoT는 보유한 디바이스의 수가 점차 증가하고, 사업 환경/요구 사항이 진화한다고 해도 그 상황에 맞춰 쉽게 확장할 수 있습니다. AWS IoT는 포괄적인 보안 기능을 제공하므로, 예방적 보안 정책 수립을 비롯하여, 잠재적인 보안 문제에도 대응할 수 있습니다.

AWS IoT는 클라우드 서비스와 엣지 소프트웨어를 모두 제공하므로, AWS 고객은 인터넷이 끊긴 경우에도 안전하게 디바이스를 연결해 데이터를 수집하여 로컬 차원에서 스마트한 작업을 실행할 수 있습니다. 또한, 클라우드 서비스를 통해, 대규모의 다양한 디바이스를 빠르고 안전하게 연결하고, 전체 디바이스의 건전성과 보안을 유지하는 동시에, 전 IoT 센서 및 앱 상에서 발생되는 이벤트를 감지, 대응할 수 있습니다. IoT 앱 개발을 가속화하고자 하는 고객은 '드래그 앤 드롭 인터페이스'를 사용하여 디바이스와 웹 서비스를 쉽게 연결할 수 있습니다. 또한 AWS IoT를 사용하면, 데이터 분석 및 최첨단의 기계 학습(ML) 모델을 구축하는 것도 가능합니다. 이런 ML 모델을 클라우드 상에서 배포하거나 고객의 디바이스에 배포하여, 더욱 스마트하게 디바이스를 활용할 수 있습니다.

현재 AWS IoT 서비스[5]는 혁신적이고 포괄적인 IoT 솔루션을 제공합니다. 하지만, 이 백서에서는 IoT 보안의 기초가 되는 아래의 5가지 서비스를 중심으로 설명하고자 합니다. 이 서비스에 대한 기본 설명 및 보안 기능이 아래에 수록되어 있습니다.

- **Amazon FreeRTOS:** 마이크로컨트롤러 기반의 엣지 디비이스를 쉽게 프로그램밍, 배포, 보호, 연결, 관리할 수 있게 해주는 오픈 소스 운영 체제.
- **AWS IoT Greengrass:** 로컬 컴퓨팅, 메시징, 데이터 캐싱, 동기화 및 연결된 디바이스에서 ML 추론 기능을 제공하는 소프트웨어.
- **AWS IoT Core:** 연결된 디바이스가 쉽고 안전하게 클라우드 애플리케이션 및 다른 디바이스들과 상호 작용하게 해주는 관리형 클라우드 서비스.
- **AWS IoT Device Management:** 클라우드 기반의 디바이스 관리 서비스. 이 서비스를 사용할 경우, IoT 디바이스를 대규모로 안전하게 온보딩, 구성, 모니터링 및 원격 관리할 수 있음.
- **AWS IoT Device Defender:** 고객의 IoT 구성을 지속적으로 모니터링하고 감사하여, 모범 보안 수칙에서 벗어나지 않는지 확인해 주는 IoT 보안 서비스.

Amazon FreeRTOS – 디바이스 소프트웨어

서비스 개요: Amazon FreeRTOS(a:FreeRTOS)는 저전력 소형 엣지 디바이스를 쉽게 프로그래밍, 배포, 보안, 연결, 관리하는 것을 지원하는 마이크로컨트롤러[6]용 오픈 소스 운영 체제입니다. Amazon FreeRTOS는 마이크로컨트롤러용으로 널리 사용되는 오픈소스 운영 체제인 FreeRTOS 커널을 기반으로 하며, AWS IoT Core와 같은 AWS 클라우드 서비스에, 또는 AWS IoT Greengrass를 실행하는 강한 엣지 디바이스에 고객의 저전력 소형 디바이스를 직접 안전하고 쉽게 연결하는 소프트웨어 라이브러리를 통해 확장할 수 있습니다.

보안 기능: Amazon FreeRTOS에는 데이터 암호화 및 키관리 지원을 포함하여, 디바이스의 데이터 및 연결성 보안을 지원하는 라이브러리가 제공됩니다. Amazon FreeRTOS에는 디바이스를 클라우드에 안전하게 연결하는 것을 돕는 TLS v1.2(Transport Layer Security)가 포함돼 있습니다. Amazon FreeRTOS는 배포 중, 고객 디바이스의 코드 손상을 예방하는 코드 서명 기능을 비롯하여, 원격으로 디바이스를 업데이트하는 OTA 업데이트를 통한 기능 강화 및 보안 패치도 제공합니다.

---

[5] AWS IoT 서비스에는 Amazon FreeRTOS, AWS IoT Greengrass, AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT Things Graph, AWS IoT Analytics, AWS IoT SiteWise 및 AWS IoT Events가 포함돼 있다. 자세한 내용은 https://aws. amazon.com/iot 참조.

[6] 마이크로컨트롤러는 가전제품, 피트니스 트래커, 산업 자동화 센서 및 자동차를 포함한 많은 디바이스에서 찾아볼 수 있는 간단한 프로세서가 포함된 단일 칩이다. 이런 소형 디바이스 중 상당수는 클라우드에 연결되거나 다른 디바이스에 로컬로 연결되어 유용한 서비스를 제공한다. 예로, 스마트 전기계량기는 클라우드에 연결돼 전력 사용량을 알려주고, 건물 보안 시스템은 로컬로 연결된 통신을 사용해 건물 관계자 출입 시, 문이 열리게 해 준다.

AWS IoT Greengrass – 엣지 컴퓨팅용 소프트웨어

서비스 개요: AWS IoT Greengrass는 연결된 디바이스에서 로컬 컴퓨팅, 메시징, 데이터 캐싱, 동기화, ML 추론 기능 등을 사용할 수 있게 해주는 소프트웨어로,[7] 인터넷 연결이 간헐적인 상태라고 해도, 연결된 디바이스에서 이런 기능을 사용할 수 있습니다. 따라서, 디바이스가 다시 연결된 후 AWS IoT Greengrass는 해당 디바이스의 데이터를 AWS IoT Core와 동기화 해주므로 인터넷 연결과 상관없이, 이 기능들이 계속 제공됩니다. AWS IoT Greengrass는 AWS 클라우드를 로컬 디바이스까지 원활하게 확장해 주므로, 디바이스에서 생성된 데이터를 로컬로 작업하면서, 동시에 데이터의 관리, 분석, 장기 저장하는 것은 클라우드상에서 계속 처리할 수 있습니다.

보안 기능: AWS IoT Greengrass는 디바이스 인증 및 암화화 기능을 사용하여 로컬 디바이스와 클라우드 간의 보안 통신이 설정되므로, 검증된 ID 없이는 디바이스와 클라우드 간에 데이터 교환이 발생되지 않습니다. 이 서비스는 AWS IoT Core에서 흔히 사용되는 것과 유사한 보안/액세스 관리 기능을 사용하므로, 상호 디바이스 인증 및 권한 부여 기능을 통해 클라우드에 보안 연결합니다.

조금 더 구체적으로 살펴보면 AWS IoT Greengrass는 X.509[8] 인증서, 관리형 구독, AWS IoT 정책 및 IAM(AWS Identity and Access Management) 정책과 (각 객체의) 역할을 사용하여 AWS IoT Greengrass 앱의 보안을 확인합니다. AWS IoT 디바이스를 AWS IoT Greengrass 에 연결하려면 AWS IoT 사물, 디바이스 인증 및 AWS IoT 보안 정책이 필요합니다. 이를 통해 AWS IoT Greengrass Core 디바이스를 AWS IoT 클라우드 서비스에 안전하게 연결할 수 있습니다. 뿐만 아니라 AWS IoT Greengrass 클라우드 서비스가 구성 정보, AWS Lambda 함수, AWS IoT Greengrass Core 디바이스에 대한 관리형 구독과 배포도 가능합니다. 이 외에도 AWS IoT Greengrass는 엣지 디바이스용 하드웨어 RoT(신뢰할 수 있는 루트) 프라이빗 키 스토리지도 제공합니다.

또다른 주요 보안 기능으로는 모니터링 및 로깅 기능입니다. 예를 들어, 이 서비스의 핵심 소프트웨어는 Amazon CloudWatch[9] (AWS IoT Core에서도 작동)를 비롯해 고객의 핵심 디바이스 내 로컬 파일 시스템에서도 로그 작성이 가능합니다. 이러한 로깅 기능은 그룹 레벨에서 구성되며, 모든 AWS IoT Greengrass 로그 항목에는 타임 스탬프, 로그 레벨 및 관련 이벤트 정보가 포함됩니다. AWS IoT Greengrass의 사용자, 역할 또는 AWS 서비스에서 수행한 작업 기록을 제공하는 서비스인 AWS CloudTrail[10]과 AWS IoT Greengrass는 통합되어 있으므로 고객이 활성화할 경우, AWS IoT Greengrass에 대한 모든 API(애플리케이션 프로그래밍 인터페이스) 호출을 이벤트로 캡처합니다. 여기에는 AWS IoT Greengrass 콘솔에서의 호출과 AWS IoT Greengrass API 작업에 대한 코드 호출을 포함합니다. 예로 사용자에 의해 트레일이 생성되고, AWS IoT Greengrass 관련 이벤트까지 포함하여, 호출을 통해 AWS CloudTrail 이벤트를 Amazon Simple Storage Service(Amazon S3) 버킷에 계속 전송하게 됩니다. 트레일 생성을 원치 않는 사용자는 이벤트 기록(활성화된 경우) 중, AWS CloudTrail 콘솔에서 가장 최근 이벤트 기록만 확인할 수도 있습니다. 이 정보는 여러 작업에서 요긴하게 사용될 수 있는데, 예를 들어 AWS IoT Greengrass로 요청이 들어온 시점과 어느 IP 주소에서 요청되었는지 확인할 수 있습니다.

---

7 AWS IoT Greengrass를 시작하려면 AWS IoT Greengrass Core를 실행할 수 있는 디바이스가 필요하다. 여기 링크를 클릭하면, 디바이스 관련 요건을 비롯한 기술적인 요건을 확인할 수 있다. 실제로 시작해 볼 수 있는 관련 안내서를 원하면 여기를 클릭한다. 이 링크에서 개발자를 위한 상세 정보를 확인한다.

8 X.509 인증서는 공개 키 인프라 표준을 사용하는 디지털 인증로, 공개 키를 인증서에 포함된 ID와 연결한다. X.509 인증서는 신로할 수 있는 기관인 CA(인증기관)에서 발급한다. CA는 스페셜 인증서(CA 인증서)를 1개 이상 유지 관리하여, X.509 인증서 발급 시 사용한다. CA 기관만이 CA 인증서에 액세스할 수 있다. 자세한 내용은 https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html 참조.

9 https://aws.amazon.com/cloudwatch 참조.

10 https://aws.amazon.com/cloudtrail 참조.

디바이스에서 고객의 데이터를 보호하기 위한, 사용 가능한 모범 사례들은 최대한 활용해야 합니다. AWS IoT Greengrass의 경우, 모든 IoT 디바이스에서 전체 디스크를 암호화하는 기능을 사용하고, 키관리를 위한 모범 사례를 따라야 합니다. 사용자는 NIST FIPS 140-2 검증 알고리즘[11]을 기반으로 한 AES 256-비트 키를 사용하여 전체 디스크 암호화하고 키 관리를 위한 모범 사례를 적용하면 됩니다. Amazon FreeRTOS에 사용되는 디바이스처럼 저전력 디바이스인 경우, 사용자는 NIST 8114 경량 암호화를 위한 [12] 권장 사항을 적용하면 됩니다.

상기 섹션에서는 마이크로컨트롤러 및 엣지 사용 용례에 대해 살펴보았습니다. 하기 섹션에서는 클라우드에서 운영되는 IoT 서비스를 중심으로 살펴보고자 합니다.

AWS IoT Core – 클라우드 기반 IoT 게이트웨이

서비스 개요: AWS IoT Core는 연결된 디바이스들이 클라우드 애플리케이션/다른 디바이스들과 쉽고, 안전하게 상호 작용할 수 있도록 해주는 관리형 클라우드 서비스입니다. 연결된 디바이스의 다양한 종류/위치에 상관없이, 안전한 통신 및 데이터 처리 기능을 제공하기 때문에 사용자는 IoT 앱을 쉽게 구축할 수 있습니다. 사용 사례로는 산업용 솔루션과 커넥티드 홈 솔루션이 있으며, 수십억 개의 디바이스 지원과 수조 건의 메시지 처리 기능, 그리고 AWS 엔드포인트와 다른 디바이스로 안정적이고 안전하게 라우팅할 수도 있습니다.

보안 기능: 보안 활성화 및 유지를 지원하기 위하여, AWS IoT Core는 다양한 솔루션을 고객들에게 제공합니다. AWS 클라우드 보안 메커니즘은 데이터가 AWS IoT와 다른 디바이스 또는 AWS 서비스 간에 이동할 때, 데이터를 보호해 줍니다. 보안 연결을 통해, 다양한 (접근) 자격 증명을 파악하는 기능(X.509 인증서, IAM 사용자 및 그룹, Amazon Cognito 자격 증명 또는 사용자 지정 인증 토큰)을 사용하여 안전하게 다비이스를 연결합니다. 고객이 클라이언트 측면에서의 유효성 검사(예: 신뢰 검증 체인, 호스트 이름 확인, 보안 스토리지 및 프라이빗 키 배포)를 수행하는 동안, AWS IoT Core는 TLS를 사용하여 보안 전송 채널을 제공합니다. 또한 AWS IoT 규칙 실행 엔진은 고객이 정한 규칙에 따라서 디바이스 데이터를 다른 디바이스 및 AWS 서비스에 전송합니다. AWS 액세스 관리 시스템은 데이터를 최종 수신지까지 안전하게 전송하는 데에 사용됩니다. 중요한 또다른 AWS IoT 권한 부여 기능은 AWS IoT 정책 변수로 디바이스에 대한 지나친 권한이 설정되는 것을 예방합니다. AWS의 이런 보안 기능들은 통상적인 사이버보안의 모범 사례를 적용하는 것과 함께 고객의 데이터를 보호하는 데 적극 사용됩니다.

---

[11] NIST FIPS 140-2 승인 암호화 알고리즘: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/ 문서/fips1402별장 .pdf.

[12] NIST 8114 - 경량 암호화: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

AWS IoT Device Management – 클라우드 기반 IoT 디바이스 관리 서비스

서비스 개요: AWS IoT Device Management는 고객이 IoT 디바이스를 온보딩, 구성, 모니터링 및 대규모로 원격 관리할 수 있도록 해줍니다. 이 디바이스 관리 서비스는 AWS IoT Core와 통합되어 디바이스를 클라우드 및 그 외 다른 디바이스에 쉽게 연결하고, 사용자가 여러 디바이스를 원격으로 관리할 수 있게 해줍니다. 이 관리 서비스를 활용할 경우, 고객은 AWS Management Console 내 AWS IoT를 사용하거나, API를 활용하여 디바이스 제조업체, 일련번호, X.509 자격 증명 인증서 또는 보안 정책 등의 정보가 자동으로 채워지는 탬플릿을 업로드하는 방식으로 새로운 디바이스를 쉽게 온보딩할 수 있게 됩니다. 그런 다음에는 콘솔 내 AWS IoT에서 몇 번의 클릭만으로, 이 정보를 그대로 사용하여 디바이스의 전체 플릿을 구성할 수도 있습니다.

보안 기능: AWS고객은 디바이스의 기능, 보안 요구 사항 또는 유사 카타고리별 계층 구조로 디바이스 플릿을 각 그룹별로 분류할 수 있습니다. 같은 방에 있는 하나의 디바이스, 같은 층에서 운영되는 디바이스들, 한 건물 내에서 운영되는 모든 디바이스들에 대해 각각 그룹별로 분류할 수 있습니다. 그런 다음, 이런 그룹을 기준으로 한 액세스 정책을 작성, 관리하거나, 운영 메트릭스를 확인하거나, 또는 전체 그룹에 해당되는 작업을 실행할 수도 있습니다. 또한 "Dynamic Things"로 알려진 기능을 사용할 경우, 고객이 정한 기준을 충족한 디바이스를 자동 추가하거나, 요구 사항을 더 이상 충족하지 못한 디바이스는 제거할 수도 있습니다. 이를 통해, 운영 시 데이터의 무결성을 유지하면서 프로세스도 안전하게 간소화할 수 있습니다. 또한 Dynamic Things를 사용하면 각 디바이스의 특성 조합을 기반으로, 해당 디바이스 기록을 쉽게 찾을 수 있고, 한 번에 대량 업데이트도 할 수 있습니다.

AWS IoT IoT Device Management를 통해 고객은 소프트웨어 및 펌웨어를 현장에 있는 디바이스로 푸시하여 보안 취약점을 패치하고 디바이스의 기능도 향상할 수 있습니다. 대량 업데이트를 실행하고 배포 속도를 조정하며, 실패 임계값을 설정하고, 소프트웨어의 자동 업데이트가 지속적으로 실행되도록 설정함으로써 항상 최신 버전의 소프트웨어가 운행되게 할 수 있습니다. 디바이스를 재부팅하거나 공장을 초기화하는 작업 등을 원격으로 전송해 소프트웨어 문제를 해결하거나, 디바이스를 원래 설정 상태로 복원할 수도 있습니다. 또한 디바이스로 전송되는 파일에 디지털 서명을 함으로써 디바이스의 손상을 예방할 수 있습니다.

소프트웨어 업데이트를 푸시하는 기능은 클라우드 서비스에만 국한되는 것은 아닙니다. 사실 Amazon FreeRTOS의 OTA 업데이트 작업을 통해, 고객은 AWS IoT Device Management를 활용하여 소프트웨어 업데이트 일정을 예약해 실행할 수 있습니다. 마찬가지로 보안 업데이트, 버그 수정 및 신규 AWS IoT Greengrass 기능 등을 연결된 디바이스에 배포하기 위해, AWS IoT Device Management를 사용하여, 1개 이상의 AWS IoT Greengrass 코어 디바이스에 대하여 AWS IoT Greengrass 코어 업데이트 작업을 생성할 수도 있습니다.

AWS IoT Device Defender – 클라우드 기반 IoT 디바이스 보안 서비스

서비스 개요: 전체 관리형 서비스로, 이 서비스를 사용할 경우, 전 IoT 디바이스 플릿에 설정된 보안 기능을 감사할 때 도움을 받을 수 있습니다. 이 서비스는 IoT 구성을 지속적으로 감사함으로써, 구성이 모범 사례를 따르고 있는지 확인하고, 각 디바이스의 ID, 인증 및 권한 부여, 디바이스 데이터 암호화 등과 같은 IoT 의 보안 구성이 유지, 적용되고 있는지 확인해 줍니다. 또한, 이 서비스는 고객의 IoT 구성에 보안 빈틈이 발견될 시, 경고 알람을 보냅니다. 예로 자격 증명 인증서가 다수의 디바이스에서 공유되거나, 인증이 해지된 디바이스가 AWS IoT Core에 접속을 시도할 경우, IoT 구성의 보안 위험이 될 수 있으므로 경고 알람을 보냅니다.

보안 기능: 이런 모니터링 및 감사 기능 외에도, 디바이스에서 어떤 이상 징후가 발견될 시, 이를 적시에 해결할 수 있도록 알람이 발송되게 설정할 수 있습니다. 예를 들어, 아웃바운드 트래픽이 비정상적으로 급증할 경우, 이는 디바이스가 디도스(DDoS: Dstributed Denial of Service - 분산 서비스 거부) 공격에 연류되었다는 징후일 수 있습니다. AWS IoT Greengrass 및 Amazon FreerTOS는 AWS IoT Device Defender와 자동 통합되므로, 이러한 이상 징후를 평가하는 데에 필요한 보안 메트릭스도 제공해 줍니다.

AWS IoT Device Defender를 통해, AWS IoT/ Amazon CloudWatch / Amazon SNS(Simple Notification Service)에 경고 알람을 보내고, CloudWatch 메트릭스에 경고 메시지가 게시되게 할 수 있습니다. 경고 알람에 대응하여, 고객은 AWS IoT Device Management를 사용해 보안해결책(Security fixes)를 내보내, 완화 조치를 실행할 수 있습니다.

또한, AWS IoT Device Defender는 규정된 IoT 보안 모범 사례를 기준으로 고객의 디바이스와 관련된 IoT 구성을 감사합니다. 이에 고객은 보안상의 빈틈이 어디에 있는지 확인하고, 정기적 또는 임시적으로 IoT 구성 감사를 실행할 수 있습니다. AWS IoT Device Defender 내에 포함된 보안 사례들을 선택하여 감사 작업의 일부로 실행할 수도 있습니다. 또한, 이 서비스는 다른 AWS 서비스(예: Amazon CloudWatch 및 Amazon SNS)와 통합되어 있기 때문에, 감사에 실패하거나 이상 징후가 감지된 경우, 고객이 근본 원인을 조사, 파악할 수 있도록 AWS IoT에 보안 경고 알람을 보냅니다. 예로 AWS IoT Device Defender는 어떤 디바이스 ID가 민감한 API 액세스할 경우, 고객에게 경고 알람을 보냅니다. 또한, AWS IoT Device Defender는 접근 권한 취소, 디바이스 재부팅, 공장 기본값 재설정 또는 연결된 디바이스에 보안해결책(Security fixes)를 내보낼 것을 권고하는 조치를 통해, 보안 위험의 영향이 최소화될 수 있도록 지원합니다.

고객이 우려하는 공격의 요인은 주로 의도치 않은 사용자 오류 또는 시스템 오류, 접근 권한 보유자 중 악의적 의도를 가진 사용자입니다. 이런 요인으로 인해 보안에 악영향을 가져올 구성이 도입될 수도 있습니다. 이에 AWS IoT Core는 다른 디바이스들과 클라우드에 고객이 디바이스를 안전하게 연결할 수 있도록, 보안 빌딩 블록을 제공합니다. 이런 빌딩 블록을 사용하면 인증, 권한 부여, 감사 로깅 및 엔드투엔드(end-to-end) 암호화 등의 보안 통제 조치를 적용할 수 있습니다. 그런 다음에는 AWS IoT Device Defender가 개입하여 모범 보안 사례뿐만 아니라 고객의 자체 조직의 보안 정책이 준수되고 있는지를 확인할 수 있도록, 보안 구성에 대한 지속적 감사 서비스를 제공합니다.

IoT 보강을 위한 증명 가능한 보안 기능 활용 - 타업체와 차별화된 요소

기업의 IoT 및 엣지 디바이스의 보안을 위하여, AWS는 신규 보안 서비스 및 기술을 지속적으로 구축하고 있습니다. 특히, AWS는 최근 AWS IoT Device Defender에서 '자동 추론'으로 알려진 AI 기술에 의해 구동되는 '체크' 서비스를 론칭했습니다. 이 기술은 수학적 증명을 활용하여 소프트웨어가 바르게 작성되었는지, 디바이스에 의도치 않은 액세스 허용은 없는지 확인합니다. 따라서, AWS IoT Device Defender는 고객이 이런 '자동 추론' 기능을 직접 사용하여 자신의 디바이스를 안전하게 보호하는 좋은 사용 용례라고 할 수 있습니다. 내부적으로, AWS는 이미 Amazon FreeRTOS에서 실행되는 코드의 메모리 무결성을 확인하고, 맬웨어로부터 보호받기 위하여 '자동 추론'을 사용한 바 있습니다. 자동 추론에 투자함으로써, 대규모로 확장 가능한 안전 소프트웨어에 대한 보증(또는 "증명 가능한 보안"이라 불리는)이 제공되므로, 고객은 보안에 민감한 워크로드를 AWS에서 처리할 수 있습니다.

AWS Zelkova[13]는 자동추론을 활용하여 고객 데이터 액세스 제어가 의도한 대로 작동되는지 여부를 증명해 줍니다. Zelkova로 구동되는 AWS IoT Device Defender의 '액세스 제어 체크' 기능을 통해 고객은 본인의 데이터가 올바르게 보호되고 있는지 확인할 수 있습니다. 만약 고객이 의도한 보안 구성 이 외의 리소스에 접근 권한을 부여한다면, 해당 AWS IoT 정책은 지나치게 액세스를 허용하는 셈입니다. 따라서 AWS IoT Device Defender에 내장된 Zelkova에 의한 액세스 제어 기능은 각 보안 정책이 고객의 정한 보안 구성에 의하여, 제한된 한도에서만 작업을 허용하고, 의도한 리소스에 한해서 허가된 작업만 처리할 수 있게 설정되었는지 확인해 줍니다.

이 외에도, '자동 추론'을 기반으로 한 다른 툴도 AWS IoT 인프라의 기본 토대를 안전하게 유지하는 데에 활용되고 있습니다. 이 중 CBMC라는 오픈 소스 툴은 Amazon FreeRTOS의 정확도를 입증하는 하는 데에 사용되어, 아마존 IoT 디바이스에서 워크로드를 처리하는 고객들에게 더 큰 신뢰감을 심어주고 있습니다. 따라서 그 어떤 공격 객체도 Amazon FreeRTOS를 악용하거나 무단으로 액세스할 수 없도록 확인합니다. Amazon FreeRTOS 내 '자동 추론' 컨트롤 메커니즘은 운영체제(OS)가 업데이트될 시 '체크'하는 작업의 일부로 지속적으로 통합, 운영됩니다. 이를 통해, 코드가 변경될 때마다 AWS 개발자는 Amazon FreeRTOS 소프트웨어가 '메모리 보안성'을 갖추고 있는지를 자동 확인할 수 있습니다.

다양한 AWS 서비스 및 기능에 걸쳐 '자동 추론'을 계속 실행함으로써, AWS 클라우드의 핵심 요소에는 더욱 철저한 보안 등급이 적용되고 있습니다. AWS IoT 스택에 적용되는 인프라 검증 기술뿐만 아니라 고객을 위한 툴 개발을 위하여, AWS는 '자동 추론'을 지속 배포하고 있습니다.

IoT 보안을 위한 핵심 모범 사례에는 어떤 것이 있는가?

보안에 적용할 모범 사례들은 많습니다. 하지만, IoT 솔루션의 보안 위험을 완화하는 데에, 전체적으로 일괄 적용될 수 있는 해결책(one-size-fits-all)은 없습니다. 각각의 디바이스, 시스템, 서비스에 따라 그리고 해당 디바이스가 배포된 환경에 따라서 발생 가능한 보안 위험, 취약점, 위험 허용 범위 등이 다르기 때문에 이런 변수를 모두 고려해야 합니다. 데이터, 디바이스, 클라우드 서비스 전반에 걸친 엔드투엔드 보안을 종합 고려할 때에 권장되는 모범 사례는 다음과 같습니다.

1. **설계 단계에서부터 보안 고려**

   IoT 솔루션의 기초는 보안과 함께 시작되고 보안과 함께 끝난다고 해도 과언이 아닙니다. 디바이스에서 민감한 데이터가 대량 전송될 수 있고, IoT 앱의 최종 사용자가 디바이스를 직접 제어할 수도 있으므로, IoT 관련 "사물"의 보안은 보편적 적용이 가능한 설계여야 합니다. 보안은 정적인 공식이 아니므로, IoT 애플리케이션은 모범 사례를 지속적으로 모델링하고, 모니터링하며 반복할 수 있어야 합니다. IoT 보안이 어려운 요인에는 디바이스의 물리적인 수명주기도 있지만, 각종 센서, 마이크로컨트롤러, 구동장치, 내장 라이브러리가 장착된 하드웨어 자체의 제한성도 있습니다. 이러한 요인으로 인해, 각 디바이스에서 실행 가능한 보안 기능은 제한적일 수 있습니다. 또한, 변화하는 보안 환경에 선제적으로 대응하기 위해서는, IoT 솔루션은 아키텍처, 펌웨어, 소프트웨어에 계속 맞추어 조정될 수 있어야 합니다. 앞서 설명드린 대로 디바이스 자체가 갖고 있는 제한성 때문에 보안 리스크가 증가하고, 장애가 될 수도 있습니다. 이에 때로는, 잠재적으로 보안과 비용 중 하나를 선택해야 하는 상황이 야기될 수도 있습니다. 하지만, 어느 조직에서든 IoT 솔루션에서 보안 구축은 항상 최우선 목표가 되어야 합니다.

[13] Zelkova에 대한 상세 정보는 https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated-reasoning-zelkova에서 확인한다.

2. **널리 공인된 IT 보안 및 사이버보안 프레임워크 기반으로 구축**

AWS는 개방형, 표준(Standards) 기반의 보안 접근법을 지원함으로써, 안전한 IoT 사용을 지향해 오고 있습니다. 소비자, 산업 및 공공 부문을 포함한 모든 영역에서 강력한 IoT 생태계를 지원하려면 수십억 대의 디바이스들과 연결점을 모두 고려해야 하기 때문에, 상호운용성은 매우 중요합니다. 이에 AWS IoT 서비스는 업계 표준 프로토콜과 모범 사례를 준수합니다. 또한 AWS IoT Core는 다른 업계 표준과 사용자 지정 프로토콜도 지원하므로, 다른 프로토콜을 사용한다고 해도 디바이스들 서로 간에 통신이 가능합니다. 개발자들이 진화하는 고객의 요구 조건을 총족하고, AWS는 기존 플랫폼을 기반으로 한 빌드가 가능하도록, '상호운용성'을 적극 지원합니다. AWS는 또한 함께 번영하는 IT 생태계를 지원하기 위하여, 고객의 선택 폭과 가능성을 확대하고자 합니다. 세계적으로 공인된 모범 사례를 적용할 경우, 모든 IoT 관계자들은 다음과 같은 다양한 혜택을 누릴 수 있습니다:

- 다시 시작 / 다시 실행과 소모적인 관행 대신에, 효율적인 반복성 및 재사용 기능 활용
- 지리적 경계를 초월하는 기술적 호환성과 상호운용성을 촉진하는 일관성 및 합의 구축
- 효율성의 극대화를 통해 IT 현대화 및 혁신 가속화

3. **영향에 초점을 두고 최우선 순위 설정**

공격이나 이상 징후는 동일하게 나타나지 않으며, 각 사용자와 사업 운영, 데이터에 따라서 그 영향도 다릅니다. 고객의 IoT 생태계를 이해하고, 이 생태계 내에 어느 위치(예: 디바이스 자체 내부 위치, 또는 네트워크상의 일부 혹은 물리적 구성요소/보안)에서, 해당 디바이스가 운영되는지를 이해하면, 어디에 가장 큰 보안 위험이 존재하는지 알 수 있습니다. 그래서 보안 위험의 영향과 결과에 초점을 두는 것이 매우 중요합니다. 그렇게 해야, 보안 노력을 어디에 집중, 투입할 것인지 결정할 수 있고, 또한 IoT 생태계 내에서 누가 그러한 노력에 대해 책임질 것인지도 판단할 수 있습니다.

결론

연결된 디바이스들의 수가 기하 급수적으로 증가하면서, IoT의 각 "사물"이 서로 간에 데이터 패킷을 통신하려면 안정적 연결 상태, 스토리지, 보안이 갖추어져야 합니다. IoT 사용에 있어, 각 조직은 흩어져 있는 디바이스들의 연결성 및 방출된 대량의 데이터를 관리하고, 모니터링하며, 보안해야 하는 도전 과제를 안고 있습니다. 그러나 클라우드 기반 환경에서는 이런 도전 과제가 장애물이 되지 않습니다. 클라우드 컴퓨팅은 한 지역에 위치한 솔루션을 확장, 성장시킬 수 있을 뿐만 아니라, 전 세계 지역으로 글로벌하게 IoT 솔루션을 확장함과 동시에 ,통신 지연시간을 대폭 줄이며, 각 현장에 있는 디바이스의 응답률 또한 높일 수 있습니다. AWS는 엔드포인트, 게이트웨이, 플랫폼, 애플리케이션 그리고 이런 각 계층을 통과하는 트래픽을 운영, 보호하는 서비스를 비롯하여 엔드투엔드 보안을 갖춘 IoT 서비스 일체를 제공합니다. AWS의 이런 통합 서비스는 지속적으로 상호 작용하는 디바이스와 데이터를 안전하게 사용, 관리할 수 있도록 IT 운영을 단순화함으로써, AWS를 사용하는 기업/단체들이 IoT가 제공하는 모든 혁신과 효율성을 최대 활용하면서 동시에 '보안 제일'의 원칙을 지켜낼 수 있도록 지원하고 있습니다.

부록 1 — AWS IoT 서비스 통합

AWS IoT는 하기의 AWS 서비스들과 직접적으로 통합됩니다.

- **Amazon Simple Storage Service(Amazon S3):** AWS 클라우드에서 확장 가능한 스토리지 제공. 자세한 내용은Amazon S3 참조.
- **Amazon DynamoDB:** 관리형 NoSQL 데이터베이스 제공. 자세한 내용은 Amazon DynamoDB 참조.
- **Amazon Kinesis:** 이 서비스를 사용하면 대규모 스트리밍 데이터를 실시간으로 처리할 수 있음. 자세한 내용은 Amazon Kinesis 참조.
- **AWS Lambda:** 이벤트 발생 시, 이에 대응하여 Amazon Elastic Compute Cloud(Amazon EC2)상의 가상 서버에서 고객의 코드를 실행함. 자세한 내용은 AWS Lambda 참조.
- **Amazon Simple Notification Service(Amazon SNS):** 이 서비스를 사용하면, 알람 공지를 발송/수신할 수 있음. 자세한 내용은Amazon SNS 참조.
- **Amazon Simple Queue Service (Amazon SQS):** 앱에 의하여 요청, 회수되는 데이터를 순차별로 저장하는 서비스 제공. 자세한 내용은 Amazon SQS 참조.

부록 2 — 정부 차원에서의 IoT 보안 대응 노력

미국

국립표준기술연구원(NIST, National Institute of Standards and Technology) - 상무부

미상무부는 IoT 보안 문제를 해결하기 위하여 다각도에서 총력을 기울이고 있습니다. 미국의 국립표준기술연구원(NIST)는 데이터 및 디바이스의 보안 평가 때에 일반 고객 및 정부 기관 모두가 고심하는 주제를 다룬 백서[14]를 발표했습니다. 이 백서에서는 이러한 보안 우려를 바르게 평가하고, 동시에 이런 위험을 완화하는 방법이 제시돼 있습니다. NIST는 또한 IoT 도입에 부정적인 영향을 줄 리스크를 파악하는 데 사용될 NIST 내부 보고서 (NSTIR) 8228[15] 를 발표했습니다. 이 보고서에는 보안 우려의 영향을 완화, 감소할 수 있는 권장안도 제시돼 있습니다. NIST는 또한 공공 및 민간 부분의 협업을 도모하고, 의견을 수집할 뿐만 아니라 스마트 시티, IoT 국제 표준화 등과 관련된 워크샵도 개최하고 있습니다.[16] IoT 기술이 아직은 초기 단계이고, 이와 관련한 잠재적 사이버보안 및 개인정보노출 위험은 극복해야 할 중대 과제로 남아 있지만, 그럼에도 각국 정부 및 소비자는 IoT가 부여하는 막대한 혜택을 간과할 수 없음을 지적하고 있습니다.

미국 국방부

미정부 기관 중에 또다른 사례는 국방부에서 찾아볼 수 있습니다. 2016년 미국방부(DoD)의 최고정보책임자(CFO)는 IoT에 대한 취약성 및 리스크를 해결하기 위한 정책 권고 사항을 발표했습니다.[17] 이 정책 권고에 따르면, 미국방부는 이미 DoD 시설, 차량 및 의료 디바이스에 수백만 개의 IoT 디바이스 및 센서를 프로비저닝하고 있으며, 무기 및 정보 시스템에 통합하는 것 또한 고려 중인 것으로 나타났습니다. IoT 보안이 복잡한 이유는 '디바이스의 수' 자체가 방대할 뿐만 아니라, 방화벽과 맬웨어 방지 프로그램 실행에 필요한 각 디바이스의 처리 능력에 한계가 있고, 기존의 모바일 디바이스와는 완전히 다른 차원의 복잡한 취약점에 노출되는 경우가 많기 때문입니다.

IoT 보안 위험을 해결하기 위해서 미국방부가 권장하는 접근법과 정책 조치는 1) 각 IoT 실행과 연관된 데이터 스트림을 지원하는 보안 리스크 및 개인정보보호에 대한 위험성을 분석하고, 2) 해당 위험성과 가치에 비례한 모든 지점에서 암호화하며, 3) IoT 네트워크를 모니터링하여 비정상적인 트래픽 및 새롭게 등장하는 위험 상황을 파악하는 것입니다.

연방무역위원회(FTC)

FTC는 IoT 보안 대화에 중요한 참여자로, 보안 지침을 잘 못 전하거나 보안에 부주의한 디바이스 제조업체에 대한 관리 조치를 취해왔습니다. 또한 FTC는 "합리적인 데이터 보안"에 대한 기준을 설정했습니다. FTC에서 확인한 디바이스 제조업체의 반복되는 보안 결함은 다음과 같습니다:

---

[14] 제프리 보아스(NIST), 리처드 쿤(NIST), 필립 라플란트(펜실베이니아주립대학교), 소피아 애플바움(MITRE), "사물 인터넷(IoT) 신뢰 우려(Internet of Things (IoT) Trust Concerns)" (2018년 10월 16일, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

[15] NSTIR 8228, "IoT 사이버보안 관리 및 개인 정보 공개 시 위험 노출에 대한 고려 사항(Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment)" (2018년 9월 26일, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

[16] https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot 참조.

[17] https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440 참조.

- 디바이스에 보안 기능이 내장되어 있지 않음
- 개발자는 자사 직원들을 대상으로 '우수 보안 사례'에 대해 교육을 제공하지 않음
- (계약을 통해) 다운스트림 보안 및 규정 준수를 보장하지 않음
- 심층적인 방어 전략 부족
- 합리적인 액세스 제어 부족 (고객이 디폴트(기본) 암호를 우회하거나 추측할 수 있음)
- 데이터 보안 프로그램 부족

캘리포니아 주

캘리포니아 주는 미국 내에서 IoT에 관한 법률을 통과시킨 최초의 주 중에 하나입니다. 현행 법안은 디바이스 설계 보안, 데이터 보호 등의 문제를 다루지만, IoT 제조업체가 충족해야 하는 구체적인 요건은 마련되지 않은 상태입니다. 대신 의원들은, 데이터 보호는 "디바이스의 특성과 기능에 적합"하고 "디바이스가 수집, 포함, 전송할 수 있는 정보에 적합"해야 한다고 적시하면서, 설계 단계에서의 보안에 주력해 왔습니다.

영국

영국 디지털문화미디어스포츠부(DCMS, Department for Digital, Culture, Media and Sport) 는 2018년 10월에 소비자 IoT 보안 실무 강령의 최종 버전을 발표했습니다.[18] 이 실무 강령은 국립사이버보안센터(National Cyber Security Centre)와 공동으로 작성되었으며 소비자 협회, 산업 및 학계의 의견이 수렴되었습니다. 이 문서는 소비자 IoT 제품 개발, 제조 및 소매에 관련된 모든 조직을 대상으로, "설계를 통한 보안" 접근법을 위한 13가지 가이드라인을 제시합니다.

또한 사용자가 가장 크고 즉각적인 보안 이점을 얻을 수 있도록 지원하기 위해 아래의 세 가지 주요 실무 관련 수칙을 강조하며, IoT 관련자들에게 이러한 실무 수칙에 우선 순위를 부여할 것을 촉구합니다. 1) 기본 암호(디폴트 암호) 금지: 사용자가 많은 IoT 인 경우, 사용자들이 디폴트 암호를 변경하지 않아 보안 문제가 발생된다. 2) 취약성 공개 정책 구현: IoT 디바이스, 서비스 및 앱 개발자들은 해당 디바이스, 서비스, 앱의 취약성을 공시하고, 공개 PoC(연락 지점)을 두어, 적시에 이러한 취약점 (및 교정)이 보고될 수 있도록 한다. 3) 소프트웨어 업데이트 유지: 소프트웨어 업데이트는 적시에 구현하기 쉬우며 디바이스 기능에 지장을 주지 않아야 한다.

미국과 영국이 제시한 우려 사항과 접근법을 살펴보면, IoT의 보안은 정부의 최우선 과제가 되고 있습니다. 또한 국내외 표준 기관들의 노력 또한 진행되고 있습니다. 이들 기관은 IoT와 스마트 시티에 관한 국제표준화기구(ISO), IoT 레퍼런스 아키텍처, 국제전기통신연합(ITU) 연구 단체 등, IoT 보안[19]을 위한 표준, 가이드라인, 모범 사례를 개발하고 있습니다.[20]

---

[18] https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security 참조.

[19] IoT 보안에 대한 현재 표준 및 이니셔티브에 대한 개요는 미국 상무부, 미국통신정보관리청(NTIA, National Telecommunications and Information Administration) 카탈로그 https://www.ntia.doc.gov/files/ntia/publications/ iotsecuritystandardscatalog_draft_17.pdf에서 확인 가능.

[20] https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx 참조.

IoT 를 사용하는 고객은 기존의 "전통적인 네트워크 사이버보안" 환경, 즉 이미 어느 정도 기간 동안 사용되어 오면서 테스트된 보안 환경을 유연하게 사용할 수 있어야 합니다. 예를 들어 보안 취약점을 식별하고, 이상 징후를 감지하며, 잠재적 사고에 대해 대응하고, IoT 디바이스의 손상 또는 중단을 복구할 때, NIST 사이버보안 프레임워크(CSF)에 매핑된 사이버보안 제어를 사용할 수 있습니다.[21] 이런 기본 사이버보안 체계는 세계적으로 인정받고 있고, 정부 및 산업에서 해당 부문이나 규모에 관계없이 모든 조직에서 권장되는 기준으로 지지를 받고 있습니다. NIST CSF를 활용하는 이점은 단순히 NIST CST가 갖고 있는 명성 때문이 아니라, 물리적보안, 사이버보안, 인적 차원에 미치는 영향을 고려하면서, 동시에 사이버보안에 적용 가능한 NIST CST의 유연성에 그 이유가 있습니다. 인적 측면과 더불어, 각 조직이 주로 의존하고 있는 기술이 정보기술(IT)이든, 산업 제어 시스템이든, 사이버/물리적 시스템이든, 또는 IoT 이든 상관없이, 이 보안 프레임워크는 기술에 의존하고 있는 조직들에게 적용될 수 있습니다.

[21] AWS 서비스를 사용하여 NIST CSF와 조율하는 방법에 대한 자세한 내용은 이 백서 및 고객 워크북 (https://do.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf) 참조.

부록 3 — AWS IoT 서비스 및 규정 준수

우수한 확장성을 갖춘 글로벌 클라우드 서비스 공급 업체인, AWS는 IoT 서비스의 보안과 고객 데이터 보호를 위하여 엄격한 기준을 갖고 보안 문제를 다룹니다. AWS는 모든 클라우드 서비스에 내부 보안 프로세스를 필수적으로 적용하여 보안 및 복원력에 영향을 미치는 현 보안 이슈 또는 새롭게 등장하는 보안 위협으로부터 보호하는 데 필요한 관리, 기술 및 운영 제어의 효과성을 평가합니다. 이런 필수 보안 보증 프로세스는 AWS의 다양한 규정 준수 프레임워크의 구축을 입증할 뿐만 아니라, 전 서비스의 수명주기 내에 개발과 운영 절차 전 단계에 걸쳐 보안을 보증하고자 하는 AWS의 강한 의지를 보여줍니다. AWS는 여러 글로벌, 각 국가별, 그리고 전문 분야별 인증 중, 국제표준기구(ISO, International Standards Organization) 27001,[22] 결제카드산업데이터보안표준(PCI, Payment Card Industry Data Security Standard)[23] 및 서비스조직통제보고(SOC, Service Organization Control Report)[24]와 같이 국제적으로 인정된 주요 표준에 대해 인증된, 확장성이 뛰어난 상용 클라우드 서비스를 제공합니다. 또한 AWS는 특정 정보 기관의 기밀 환경을 지원하는 데 필요한 엄격한 보안 요구 사항을 충족합니다. AWS는 서비스에 "하이 워터마크(high watermark)"를 적용하기 때문에, 조직 규모에 상관없이 어느 기업/공공 단체이든 AWS 클라우드 서비스를 사용하는 모든 고객들은 AWS가 대리로 취득한 보안 인증의 혜택을 받을 수 있습니다.

AWS는 고객에게는 증명 가능하고, 준수해야 하는 특정 보안 요구 사항이 있을 수 있음을 잘 이해하고 있습니다. 이를 고려하여, AWS는 고객 수요에 기반한 규정 준수 프로그램과 연계된 서비스를 지속적으로 추가하고 있습니다. AWS 적용 범위 내에 있는 IoT 서비스 정보는 AWS 웹 사이트의 규정 준수 프로그램별로 수록되어 있습니다.[25]

---

[22] ISO 27001/27002는 널리 채택된 글로벌 보안 표준으로, 끊임없이 변화하는 보안 위협 시나리오에 적합한 정기적인 위험 평가를 기반으로, 회사 및 고객 정보를 관리하는 체계적인 접근 방식에 대한 요구 소항과 모범 사례를 제시하고 있다. ISO 27018은 클라우드의 개인 정보 보호에 초점을 맞춘 실행 코드다. ISO 정보 보안 표준 27002를 기반으로 하며 공용 클라우드 개인 식별 정보(PII, Personally Identifiable Information)에 적용할 수 있는 ISO 27002 컨트롤에 대한 구현 지침을 제공한다. 또한 기존 ISO 27002 제어 세트에서 다루지 않는 공용 클라우드 PII 보호 요구 사항을 다루기 위해 일련의 추가 제어 및 관련 지침되 제시되어 있다.

[23] 신용카드산업 데이터보안표준(PCI DSS, Payment Card Industry Data Security Standard)은 PCI 보안 표준 위원회 (https://www.pcisecuritystandards.org)에서 관리하는 독점 정보 보안 표준으로, American Express, Discover Financial Services, JCB International, MasterCard Worldwide 및 Visa Inc. 에 의해 창립된 표준 위원회이다. PCI DSS는 판매자, 프로세서, 취득자, 발급자 및 서비스 공급자를 포함하여 카드 소지자 데이터(CHD) 및/또는 중요한 인증 데이터(SAD)를 저장, 처리 또는 전송하는 모든 기관/조직에 적용된다.

[24] 서비스 조직 관리(Service Organization Controls) 보고서(SOC 1, 2, 3)는 미국 및 국제 감사 기관에 대한 광범위한 재무 감사 요구 사항을 충족하기 위한 것이다. 이 보고서에 대한 감사는 국제 보증 계약 번호 3402(ISAE 3402) 및 미국공인회계사협회(AICPA, American Institute of Certified Public Accountants): AT 801(이전 SSAE 16)에 따라 실행된다.

[25] https://aws.amazon.com/compliance/services-in-scope 참조.