사물인터넷

자동차 IoT 보안

대표적 공격 형태에 대한 대응 방안

자동차 IoT 보안

대표적 공격 형태에 대한 대응 방안

진화하는 공격자

지난 수십 년 사이 정보 보안에는 한 가지 패턴이 등장했습니다. 즉 공격자들이 이기고 있다는 것입니다. 그것도 더 빨리. 요즘에는 컴퓨터 시스템에 침투할 수 있는 도구와 정보, 기술이 그 어느 때보다도 많습니다. 동시에, 쉼 없는 감시와 회복력 좋은 하드웨어 아키텍처, 숙련 엔지니어가 필요한 컴퓨터 시스템의 방어는 부족할 때가 많습니다.

5 년 전, Lab Mouse Security 의 Don A. Baley 가 라스베가스에서 열린 Black Hat Briefings 에서 원격으로 자동차 해킹을 처음 선보였습니다. 요즘에는 세계 최대 규모의 해커 컨벤션인 DEF CON 에서 자동차 해킹 워크숍을 열어 복잡한 보안 장치를 우회하는 하드웨어 툴과 무료 소프트웨어 기술, 전략을 제시하기도 합니다.

해킹에 대한 관심이 커지면, 전문 정보보안 연구자에게 요구되는 윤리를 지키지 않는 사람도 생겨날 것입니다. 개중에는 선을 넘는 이도 있을 것입니다. 약점이 심각하다면 범죄자들이 모여 통제권을 넘겨받으려 할 것입니다.

일부 공격자들은 피해자가 돈을 지불할 때까지 중요한 시스템을 무력화하는, 일명 "랜섬웨어"라고 하는 신종 멀웨어를 이용하고 있습니다. 이 같은 공격은 심각한 피해를 유발할 때가 많습니다.

예컨대 2015 년 12 월 우크라이나에서는 한 지역의 전력망을 운용하는 전기회사에 설치된 맬웨어가 3 주 동안 정전을 유발하기도 했습니다.

이 맬웨어는 2007 년부터 인터넷에 돌아다니고 있었지만 얼마 전에 산업용 제어 시스템의 하드웨어를 장악하고 파괴하도록 업데이트된 것으로 드러났습니다. 이번 사건은 해커 집단이 의도적으로 정전을 유발한 첫 사례였습니다.

사물 인터넷(IoT)이 발전하고 산업 시스템의 상호 연결 수준이 높아지면서 이 같은 공격은 늘어날 가능성이 큽니다. 엔지니어 그룹과 경영진에서는 언제 자사의 IoT 솔루션을 상대로 공격이 발생할지 자문해 봐야 합니다. 이 같은 공격에 효과적으로 대응하고 기술 전반의 복원력을 확보하는 길은 개념 정립 단계부터 보안을 솔루션에 구현하는 것뿐입니다.

공격 패턴

공격자들은 여러 산업과 기술에서 파생된 다수의 방법을 조합해 사용하는 IoT 솔루션을 타깃으로 삼는 경향이 있습니다.

IoT 는 서로 연결된 컴퓨팅 시스템이 클라우드와 네트워크 지속성, 임베디드 기술의 조합을 통해 혁신적이고 새로운 서비스를 제공하는 상태를 가리킵니다. 다시 말하면 IoT 는 기존 기술을 동원해 양방향성과 자동화를 구현하는 것입니다.

따라서 공격자는 잘 짜인 전략과 기존 툴을 이용해서 IoT 솔루션의 취약점을 찾아낼 수 있습니다.

그림 1 은 자동차 IoT 솔루션을 무력화할 수도 있는 구성요소를 일부 보여주고 있습니다.

그림 1 - 일반적인 자동차 IoT 구성요소와 기능

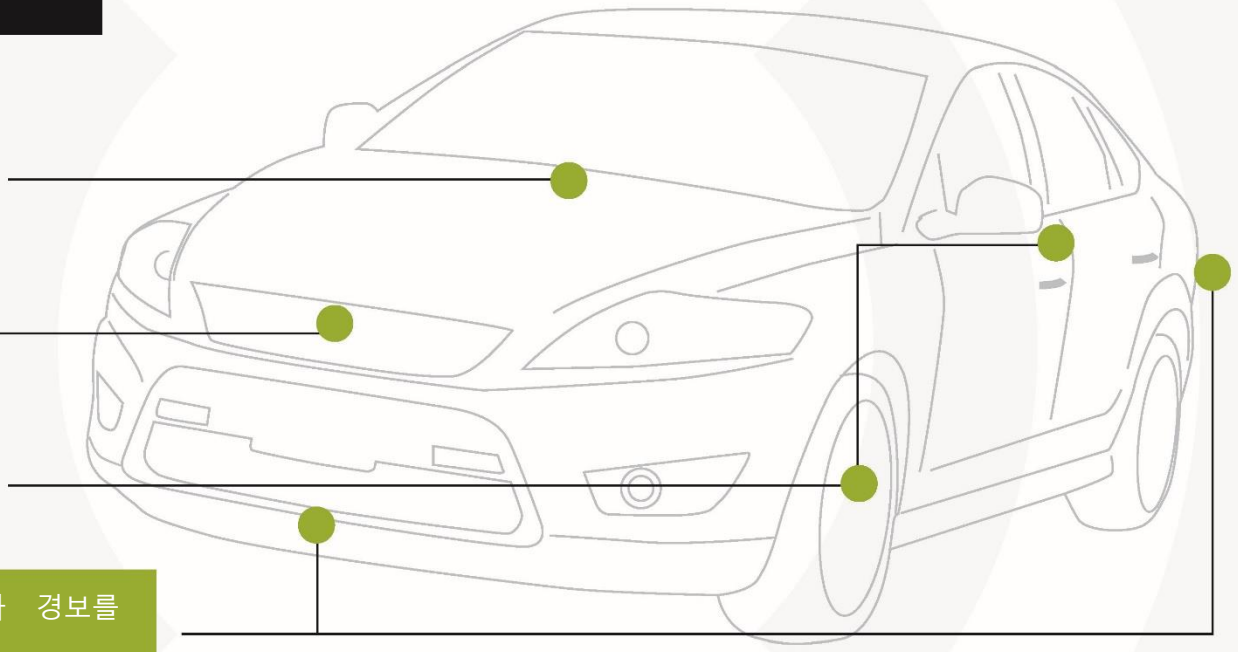
요즘 자동차의 IoT 기능

데이터와 엔터테인먼트, 시각화, 진단 기능이 합쳐진 텔레매틱스 시스템

실시간 의사결정을 주도하는 중앙 컴퓨팅 시스템

도로의 상태에 맞춰 운전자를 안전하게 유도하는 센서

가까운 동료를 찾아 안전 관련 지표와 경보를 전달하는 무선 통신 시스템



IoT 기술의 공격에 자주 쓰이는 방법은 다음과 같습니다.

- 동료(peer) 인증의 취약점
- 실질적인 암호화 탬퍼링
- 엔드포인트 무결성의 허점
- 핵심 애플리케이션과 비핵심 애플리케이션 간의 세그먼트화 결여
- 소프트웨어 애플리케이션의 결함
- 비즈니스 로직 취약점

실력 있는 공격자라면 어떤 격리된 통신망이든 물리적 디바이스가 가장 취약한 침투 지점임을 알고 있습니다. 물리적 디바이스의 보안은 까다로우므로, IoT 생태계를 와해시키는 가장 손쉬운 방법은 네트워크 통신의 약점이나 물리적 엔드포인트의 약점을 파고드는 것입니다.

핵심이 되는 텔레매틱스 시스템은 정교한 엔지니어링을 통해 보호할 수도 있겠지만 자동차 컴퓨팅 네트워크의 나머지를 이루는 센서나 ECU(electronic control unit) 엔드포인트는 비용과 복잡성 때문에 보안을 확보하기가 쉽지 않습니다.

그림 2 는 자동차 IoT 솔루션이 공격을 받는 방식을 몇 가지 보여주고 있습니다.

그림 2 - 자동차 환경에서 흔한 공격 패턴

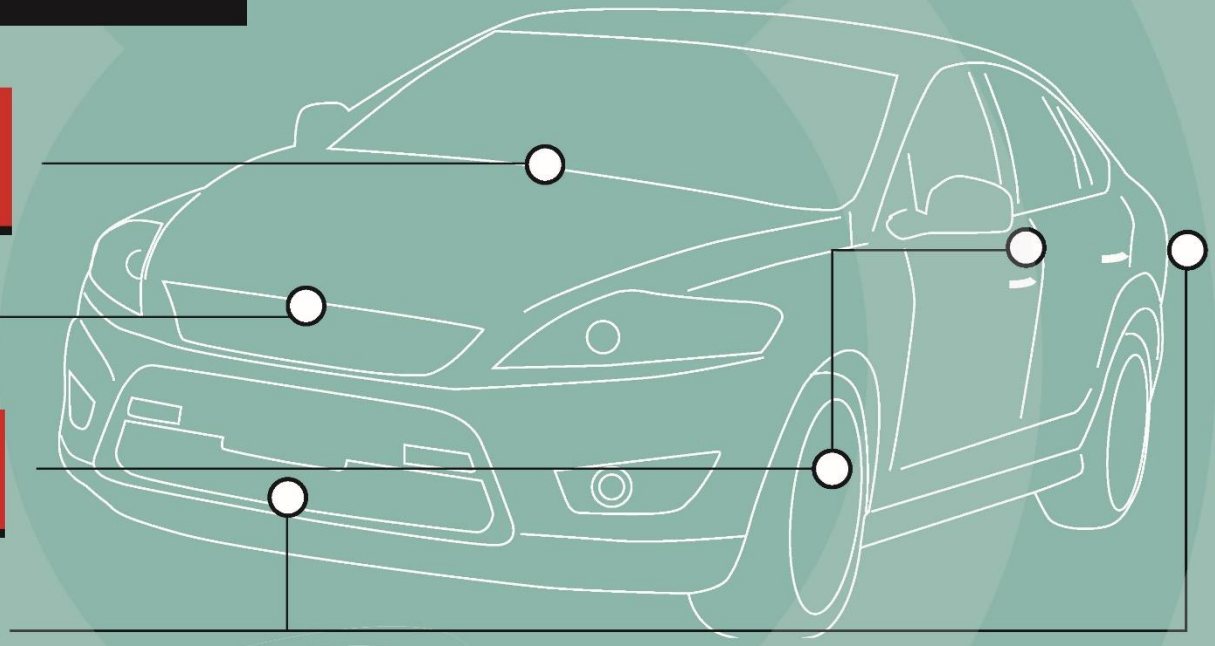
자동차 IoT 기능에 대한 공격 패턴

텔레매틱스 백엔드 서비스 가장, 펌웨어 업데이트 조작, 통신 보안 결함, 3 자 애플리케이션 "탈옥"

ECU 의사결정을 통제하는 로컬 또는 원격

표준 무선 포로토콜의 취약점을 이용한 원격 코드 실행 또는 센서 데이터 가장

보안 인증서 또는 핵심 계층의 남용을 통한 주요 통신 채널의 조작



경제적인 해결책

위에서 소개한 문제들은 체계적이지도, 해결이 불가능한 것도 아닙니다. 사실, 아주 경제적으로 IoT 솔루션에 대한 공격을 무마하는 방법이 있습니다.

관리 인터페이스의 보안은 대개 제품이나 서비스 아키텍처와 분리해 해결해야 하지만, 다음 네 가지 조치면 엔드포인트의 관리 인터페이스에 보안을 확보할 수 있습니다.

- **네트워크와 애플리케이션 보안에 TCB(Trusted Computing Base)의 사용 의무화**
- **모든 네트워크 통신이 기밀성과 무결성 부여**
- **애플리케이션의 거동 제한**
- **탬퍼 내성 강제**

1. TCB 의 적용

TCB(Trusted Computing Base)는 암호화와 애플리케이션 기반 토큰의 사용과 보안을 강제하는 일단의 정책과 절차, 기술을 말합니다. 어떤 플랫폼의 신뢰도를 정의하는 기반이기도 합니다. 잘 설계된 TCB 를 제품의 핵심에 적용하면 현장에서 그 제품의 신뢰도는 높아집니다. TCB 활용의 효과는 다음과 같습니다.

- 하드웨어 클로닝 또는 스푸핑(spoofing) 가능성을 낮추거나 아예 없애버릴 수도 있음
- 서비스 내에서 정품 구성요소의 사용을 의무화할 수 있음
- 현장 또는 원격 OTA(over-the-air) 애플리케이션 업데이트의 비용 대비 효과가 개선됨
- 서비스 구성요소 간 상호운용성과 신뢰가 높아짐
- 제품의 수명이 늘어남

SMA IoT 보안 지침에서 TCB 에 관해 더 자세히 설명합니다. **http://www.gsma.com/iot/iot-security-guidelines** 에서 내려받을 수 있습니다.

2. 네트워크 통신 보안 확보

IoT 보안에서 두 번째로 중요한 속성은 네트워크 통신입니다. 네트워크를 구성하는 요소는 모두 서로 인증을 할 수 있고 필요하다면 데이터를 기밀로서 주고 받을 수 있어야 합니다. 이 요소들은 검증 가능한 무결성을 바탕으로 통신을 하여 데이터가 가로채기를 당하거나 변경되거나 가장을 할 수 없도록 해야 합니다.

정교하게 설계된 TCB 가 없다면 네트워크 통신의 보안에 문제가 생길 수 있고 생산 환경에서 예상치 못한 거동이 발생할 수도 있습니다. 예를 들면, 새로 나온 IoT 제품 중에 BLE(Bluetooth Low Energy)나 Zigbee, Thread 같은 개인통신망(PAN) 통신 기술을 이용하는 것이 많습니다.

이들 프로토콜에는 신뢰하지 않는 네트워크에서 서로 연결된 피어 간에 보안 세션을 만들 수 있는 새로운 보안 기능이 들어 있습니다.

이들 프로토콜이 세션의 보안 확보를 위해 사용하는 암호화 알고리즘(Elliptic Curve Diffie-Hellman 등)은 수학적으로 문제는 없지만 데이터 기밀성과 무결성은 보장하지 못합니다.

이는 이들 기술에 RoT 가 없고 탬퍼링 내성이 있는 메모리 영역에 키값을 저장하지 않으며 완전한 세션 보안을 위해 필요한 처리 기능 중 일부가 없을 수도 있기 때문입니다.

공격자의 제일 목표는 네트워트 통신의 분석이므로, 네트워크 통신의 보안을 IoT 제품이나 서비스의 핵심 측면으로 검토해야 합니다.

3. 애플리케이션의 거동 제한

애플리케이션 보안은 매우 까다롭습니다. 매일이 전투인 기업에게는 더욱 더 그러합니다. 제조사의 엔지니어링팀에서 설계한 핵심 애플리케이션은 속속들이 감사할 수 있지만, 요즘 애플리케이션에서는 IoT 엔드포인트에 3 자 애플리케이션의 로드를 허용하는 경우도 많습니다. 앱 스토어를 통해 사용자가 줄잡아 수십 만 가지 3 자 앱에 접근할 수 있게 되면서, 그들 모두를 속속들이 감사하기는 불가능에 가깝습니다.

애플리케이션의 보안을 확보하는 올바른 방법은 그것을 감옥이나 가상 기기, 컨테이너, 기타 추상화 안으로 격리해 그것의 기능과 주요 시스템 디바이스 또는 자원에 대한 접근을 모두 제한하는 것입니다.

이렇게 하면 소프트웨어의 결함 때문에 공격자가 애플리케이션을 빠져나와 CANbus 등 핵심 자원에 접근하는 사태가 벌어지지 않습니다. 특히, 애플리케이션에 대해 다음을 확보하는 것이 중요합니다.

- 애플리케이션이 스스로 권한을 높여 호스트 운영체제에 영향을 주지 못해야 함
- 애플리케이션이 낮은 수준의 드라이버나 디바이스에 접속할 수 있는 능력을 갖지 못해야 함
- 애플리케이션이 다른 주요 애플리케이션의 거동에 영향을 미치지 못해야 함
- 다른 애플리케이션의 메모리나 자원에 읽고 쓰기를 하지 못해야 함

이 같은 규칙을 의무화하면, 공격자가 설령 3 자 애플리케이션을 이용해 코드 실행을 하거나 애플리케이션에 '숨은 뒷문'이 있더라도 그 영향은 가늠할 수 있고 무력화된 애플리케이션에 한정됩니다. 다른 애플리케이션이나 서브시스템, 호스트 운영체제는 어떤 식으로도 영향을 받지 아니합니다.

4. 탬퍼링 내성 의무화

IoT 공격 대부분이 물리적 디바이스를 통해 일어나므로 이들 디바이스의 분석을 차단하는 것이 공격의 가능성을 낮추는 현실적인 방법이 될 수 있습니다.

공격자의 손에 있는 물리적 디바이스는 항상 무력화의 위험에 처하게 되지만, 물리적인 탬퍼링 내성으로 공격 과정을 복잡하게 만들고 공격의 실용성이나 경제성이 없어질 정도로 비용을 늘릴 수 있습니다.

예컨대, 광감지 퓨즈를 넣으면 디바이스의 케이스가 열렸을 때 메모리가 삭제됩니다. 또, 디바이스의 케이스에 회로를 내장하면, 디바이스가 열렸을 때 동전 셀 배터리가 분리되고 주요 메모리 구성요소가 지워집니다.

이 밖에도 낮은 비용으로 공격자가 역설계를 하거나 디바이스의 보안을 무력화하기 위해 들여야 하는 시간과 전문성, 장비를 크게 늘리는 방법은 많습니다.

그림 3 에 자동차 IoT 솔루션의 보안 확보를 위해 사용할 수 있는 방안이 몇 가지 제시돼 있습니다.

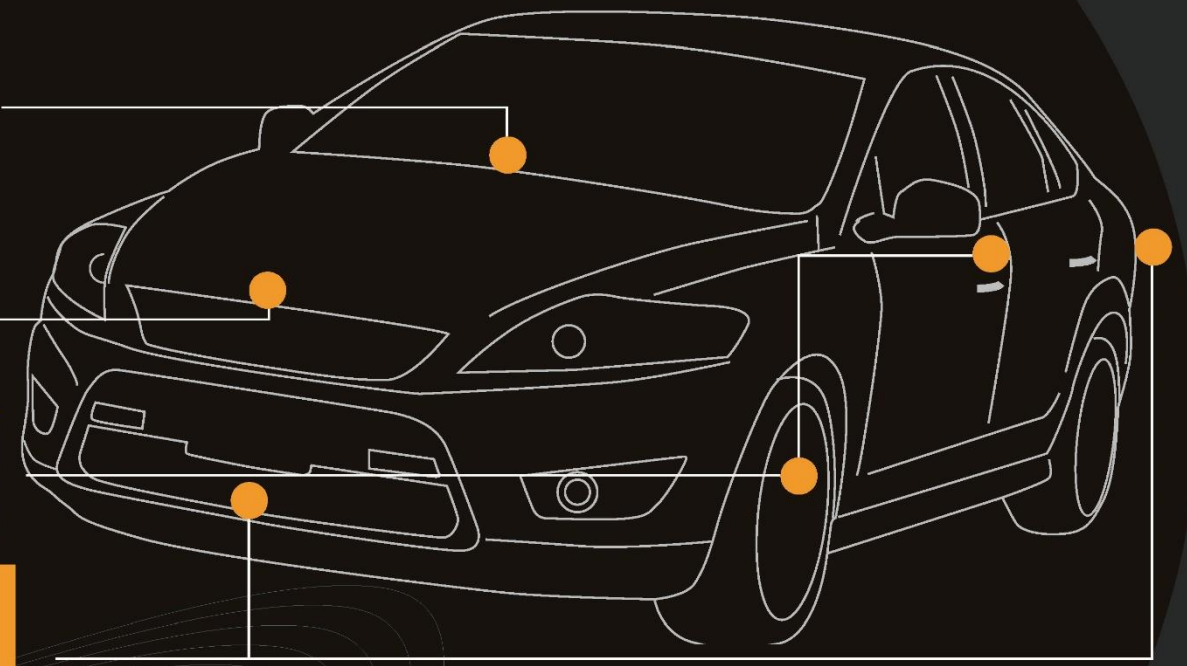
실용적인 자동차 IoT 보안 전략전

애플리케이션 차원에서 통신 보안을 의무화해 로밍이나 프로토콜 다운그레이드 때문에 모바일 네트워크 보안이 불확실할 때에도 최고 수준의 기밀성과 무결성을 확보한다.

핵심 아키텍처의 신뢰를 확보해 장기 엔지니어링 비용을 낮추고 기기의 수명을 연장한다.

경량 센서 엔드포인트에도 피어 인증과 데이터 기밀성, 메시지 무결성을 도입한다.

핵심 애플리케이션과 비핵심 애플리케이션을 서로 분리한다. 그렇지 않으면 커스텀 앱이 무력화되었을 때 공격자가 핵심 구성요소를 파고들 여지가 생긴다.



요약

여론은 호들갑을 떨고 있지만 IoT 솔루션은 보안을 확보할 수 있습니다. 비용 대비 효과가 좋은 보안은 아키텍처 수준에서 시작합니다. 작은 변화로도 IoT 제품 또는 서비스 생태계 전체가 침입으로부터 안전해질 수 있습니다. 그러나 이것을 실현하려면 엔지니어링팀이 충분한 시간을 갖고 처음부터 보안을 구축해야 합니다. IoT 솔루션의 보안은 애드온(add-on)으로 구현할 수 없습니다. 보안이 기초가 되어야 합니다.

GSMA IoT 보안 지침에 흔한 IoT 위험을 완화하는 방안이 더 자세하게 제시돼 있으므로 참고하기 바랍니다.
http://www.gsma.com/iot/iot-security-guidelines

GSMA 최신 IoT 소식

웹사이트: **www.gsma.com/IoT**

뉴스레터 구독: **http://www.gsma.com/IoT/sign-up-for-newsletter/**

LinkedIn 팔로우: **http://gsma.at/IoT**