Technical Article

저전력 무선 MCU로 주요 무선 연결 사이버 보안 문제 해결

Sainandan Reddy Reddy, Benjamin Moore, Bhargavi Nisarga

무선 연결을 혁신하여 장치를 연결하는 기능이 이제 일상적으로 이용하는 전자 제품으로 확장되어 가정 용품과 차량을 지능적으로 사용할 수 있게 되었습니다(그림 1 참조). 지능이 높을수록 장치를 원격으로 모니터링하고 제어할 수 있는 기능, 클라우드 컴퓨팅을 통한 증강할 수 있는 역량, 더욱 빠른 소프트웨어 업데이트 등 더 많은 기능과 역량이 향상됩니다.

그러나 세상이 더욱 연결됨에 따라 이러한 제품들을 침입으로부터 보호하는 것이 중요합니다. 저장된 개인 또는 민감한 애플리케이션 데이터의 보호부터 전송 중인 데이터 보호와 물리적 장치 보안까지, 설계 시 무선 연결을 구현하는 엔지니어는 설계 프로세스 초기에 시스템 수준 보안 기능을 해결하고 사이버 보안 표준 및 규정의 관련 요구 사항을 충족해야 합니다.

이와 마찬가지로, 연결 확장에 도움이 되는 무선 마이크로컨트롤러(MCU)도 진화하는 보안 과제와 사이버 보안 표준 및 규정을 충족해야 합니다.

이 문서에서는 연결된 차량용 및 스마트 홈 애플리케이션과 특히 차량 액세스, 스마트 온도 조절기, 스마트 센서, 전자 잠금 장치 등의 과제를 해결하기 위해 설계된 MCU에 대해 알아봅니다.

그림 1. 스마트폰을 사용하여 차량에 액세스

차량 액세스를 위한 사이버 보안 과제

Bluetooth® 저에너지(BLE) 무선 연결은 차량 액세스 솔루션에서 차량 키의 범위를 설정하고 지역화하기 위해 사용됩니다. 보안 위협은 차량 액세스 보안을 손상시켜 차량 또는 소지품을 도난당할 수 있습니다.

OEM은 다음을 포함한 여러 수준의 액세스 보안을 고려해야 합니다.

- **무선 신호의 보안 범위 지정:** 범위 지정 신호를 조작하면 거리 측정 결과가 변경될 수 있으므로 차량 키가 차량보다 더 가까이 보일 수 있습니다. 이러한 위협은 무선 기술에 종속적이며 무선 물리 계층의 보안 기능과 중간 규모 액세스 제어 사양은 일반적으로 이러한 위협을 해결합니다. 예를 들어, 최신 Bluetooth 채널 사운딩 사양에서는 RTT(라운드 트립 타이밍) 패킷 교환 및 NADM(정규화된 공격 감지기 메트릭) 기반 완화를 사용하여 위상 기반 범위 지정 작업에 대한 위협을 해결합니다.
- **범위 설정 절차를 설정하기 위해 전달된 데이터에 대한 프로토콜 수준 보안:** 프로토콜 및 애플리케이션 수준의 위협에는 무선 작동 중 스니핑, 중간자 공격 및 재생 공격이 포함됩니다. 통신 중인 데이터를 암호화하고 차량 키를 유효한 엔터티로 인증하기 위해 관련 암호화 수단을 규정하면 이러한 공격을 완화할 수 있습니다. 그러나 암호화 보안은 암호화 또는 인증에 사용되는 키만큼 안전합니다.
- **최종 애플리케이션 작업을 위한 애플리케이션 수준 보안(개방형 차량 도어, 시동 엔진):** 무선 연결 장치에서 무선을 통해 수신되거나 원격으로 조작된 데이터는 (예: 맬웨어 주입을 통해) 데이터 통신 보안에 사용되는 장치 작동이나 암호화 키를 손상시킬 수 있습니다. 따라서 Bluetooth LE 무선 MCU는 키를 보호하는 신뢰할 수 있는 방식으로 프로토콜 및 애플리케이션 수준 암호화 작업을 지원하는 것이 중요합니다. 보안 부팅, 보안 펌웨어 업데이트 및 보안 디버깅 액세스를 통해 장치 펌웨어 작동을 보호해야 합니다.

또한 많은 지역에 자동차 사이버 보안에 대한 규정이 있으며, 장치 개발 및 유지 보수를 하는 도중 관련 사이버 보안 프로세스를 준수해야 하는 국제 표준화 기구 21434와 같은 표준을 준수해야 합니다.

스마트 온도 조절기에 대한 사이버 보안 과제

스마트 온도 조절기(그림 2 참조)는 스마트 홈 기술에서 직면하는 장점 및 위협의 좋은 예입니다. 이러한 장치를 통해 주택 소유자는 어디에서나 가정의 온도를 조정하고 통합된 Wi-Fi® 연결을 통해 에너지 사용량을 최적화할 수 있습니다.

그림 2. 거실의 블루투스 스마트 온도 조절기

안타깝게도, 증가된 연결성은 온도 조절 장치를 위협에 노출시킬 수 있습니다. 예를 들어, 해커는 악의적으로 제작된 프레임을 무선으로 전송하여 온도 조절기의 작동을 중단하거나 네트워크를 강제로 차단할 수 있습니다. 의도적으로 네트워크와의 장치 연결을 해제하고 다시 연결한 후 전송을 모니터링하면 무차별 암호 대입 또는 사전 공격을 사용하여 데이터를 캡처하고 해독할 수 있으므로 사용자 또는 공급업체 데이터 및 자격 증명이 노출됩니다. 인터넷을 통해 온도 조절기 로 악성 데이터나 코드

(예: 맬웨어)를 전송하거나 원격 클라우드 서버 간에 데이터를 전송하여 원격 중간자 공격을 통해 데이터를 캡처할 수 있습니다.

이를 완화하기를 위해 설계자는 인증, 키 계약 및 암호화를 위한 입증된 암호화 알고리즘을 간략히 소개하고 Wi-Fi 보호 액세스 3과 같은 관리 프레임을 보호하기 위한 프로토콜을 의무화하는 최신 Wi-Fi 보안 표준을 따라야 합니다. 이러한 장치는 인터넷 전송 데이터를 보호하기 위한 최신 네트워크 보안 프로토콜(예: Transport Layer Security v1.3)을 지원해야 합니다. 또한 장치는 이러한 프로토콜을 실행하는 동안 사용되는 키를 효율적이고 안전하게 저장해야 합니다.

스마트 센서와 전자 잠금 장치에 대한 사이버 보안 과제

그림 3에 표시된 것처럼 스마트 센서(모션, 도어, 창 센서) 및 전자 잠금 장치를 비롯한 배터리 작동 장치는 Zigbee®, Thread, Matter와 같은 메시 기술을 사용하여 스마트 홈 허브를 통해 클라우드에 연결하면서 저전력 요구 사항을 충족하는 동시에 점점 더 증가하고 있습니다. 스니핑, 중간자 및 장치 인수와 같은 보안 위협은 잠재적으로 장치 데이터 또는 보안 작업(예: 악의적인 행위자에게 부여된 전자 잠금 액세스)을 손상시킬 수 있습니다. 극단적인 경우, 장치가 손상되면 스마트 홈 네트워크나 생태계가 손상될 수 있습니다.

그림 3. 전자 자물쇠 및 스마트 센서를 갖춘 스마트 홈

이러한 네트워크를 보호하려면 신뢰할 수 있는 장치만 네트워크에 연결할 수 있도록 센서와 허브 간의 통신 채널을 보호해야 합니다.

Matter는 스마트 홈 제품에 대한 개발을 간소화하고 향상된 프로토콜 수준의 보안을 제공하도록 설계되었습니다. Matter는 기밀성을 위한 고급 암호화 표준, 무결성을 위한 보안 해시 알고리즘, 키 교환 및 디지털 서명을 위한 타원 곡선 암호화와 같은 강력한 암호화 제품군을 통해 통신 채널을 보호하는 것 외에도 인증서와 암호 기반 프로토콜을 사용하여 스마트 홈 장치를 인증하고 에코시스템에서 정품 제품만 사용하도록 합니다.

무선 MCU를 사용한 보안 위협 완화

보안 위험을 완화하기 위해 무선 MCU는 안전한 데이터 통신, 보안 키 교환, 상호 인증, 보안 키 스토리지, 보안 펌웨어 업데이트 및 보안 부팅 작업을 지원합니다.

CC2745P10-Q1, CC2755R10, CC3551E와 같은 무선 MCU는 맬웨어 및 장치 탈취 공격으로 인한 위험을 완화하는 통합 보안 기능을 제공합니다. 롤백 보호 기능을 갖춘 보안 부팅 및 보안 펌웨어 업데이트와 같은 기본 보안 기능을 지원합니다. 이러한 MCU는 하드웨어 가속 암호화 작업, 보안 키 스토리지 및 난수 생성을 처리하는 전용 컨트롤러가 포함된 통합 HSM(하

드웨어 보안 모듈)을 제공합니다. HSM은 암호화 및 키 처리 작업을 위한 신뢰할 수 있는 환경을 제공하기 때문에 데이터 개인 정보 보호 및 고급 맬웨어 위험을 완화할 수 있습니다. 이러한 MCU의 Arm® Cortex®-M33 코어는 TrustZone-M을 지원하며, 이는 더욱 안전한 소프트웨어 작동을 위해 신뢰할 수 있는 실행 환경을 지원합니다.

상표

중요 알림 및 고지 사항

TI는 기술 및 신뢰성 데이터(데이터시트 포함), 디자인 리소스(레퍼런스 디자인 포함), 애플리케이션 또는 기타 디자인 조언, 웹 도구, 안전 정보 및 기타 리소스를 "있는 그대로" 제공하며 상업성, 특정 목적 적합성 또는 제3자 지적 재산권 비침해에 대한 묵시적 보증을 포함하여(그러나 이에 국한되지 않음) 모든 명시적 또는 묵시적으로 모든 보증을 부인합니다.

이러한 리소스는 TI 제품을 사용하는 숙련된 개발자에게 적합합니다. (1) 애플리케이션에 대해 적절한 TI 제품을 선택하고, (2) 애플리케이션을 설계, 검증, 테스트하고, (3) 애플리케이션이 해당 표준 및 기타 안전, 보안, 규정 또는 기타 요구 사항을 충족하도록 보장하는 것은 전적으로 귀하의 책임입니다.

이러한 리소스는 예고 없이 변경될 수 있습니다. TI는 리소스에 설명된 TI 제품을 사용하는 애플리케이션의 개발에만 이러한 리소스를 사용할 수 있는 권한을 부여합니다. 이러한 리소스의 기타 복제 및 표시는 금지됩니다. 다른 모든 TI 지적 재산권 또는 타사 지적 재산권에 대한 라이선스가 부여되지 않습니다. TI는 이러한 리소스의 사용으로 인해 발생하는 모든 청구, 손해, 비용, 손실 및 책임에 대해 책임을 지지 않으며 귀하는 TI와 그 대리인을 완전히 면책해야 합니다.

TI의 제품은 ti.com에서 확인하거나 이러한 TI 제품과 함께 제공되는 TI의 판매 약관 또는 기타 해당 약관의 적용을 받습니다. TI가 이러한 리소스를 제공한다고 해서 TI 제품에 대한 TI의 해당 보증 또는 보증 부인 정보가 확장 또는 기타의 방법으로 변경되지 않습니다.

TI는 사용자가 제안했을 수 있는 추가 또는 기타 조건을 반대하거나 거부합니다.

주소: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265