Technical Article

Solving key wireless connectivity cybersecurity challenges with low-power wireless MCUs

Sainandan Reddy Reddy, Benjamin Moore, and Bhargavi Nisarga

With wireless connectivity innovations, the ability to connect devices has now expanded to everyday electronics, bringing intelligence to homes and vehicles (see Figure 1). More intelligence means more functionality and features: the ability to remotely monitor and control a device, augmented abilities with cloud computing, and faster software updates.

However, as our world becomes more connected, it's crucial to protect these products from intrusion. From securing stored personal or sensitive application data to protecting data in transit and physical device security, engineers implementing wireless connectivity in their designs need to address system-level security capabilities earlier in the design process, while also meeting the relevant requirements of cybersecurity standards and regulations.

Likewise, the wireless microcontrollers (MCUs) helping expand connectivity also need to meet evolving security challenges and cybersecurity standards and regulations.

In this article, we'll explore evolving wireless connectivity security challenges in connected automotive and smart home applications – specifically car access, smart thermostats, and smart sensors and e-locks – and the MCUs designed to address these challenges.

Figure 1. Vehicle access using a smart phone

Cybersecurity challenges for car access

Bluetooth® Low Energy (BLE) wireless connectivity is used in car access solutions to range and localize the vehicle keys. Security threats can lead to compromised car access security, potentially leading to the theft of a vehicle or belongings.

OEMs need to consider access security at multiple levels, including:

- **Ranging security for wireless signals:** Manipulating ranging signals can alter distance estimation results, making the vehicle key appear closer to the vehicle than it is. These threats are wireless technology-dependent and the security features in wireless physical layer and medium access control specifications typically address such threats. For example, in the latest Bluetooth channel sounding specification, the threats to phase-based ranging distance estimation operations are addressed by using round trip timing (RTT) packet exchanges and normalized attack detector metric (NADM) based mitigations.
- **Protocol-level security for the data communicated to set up ranging procedures:** Protocol- and application-level threats include sniffing, man-in-the-middle and replay attacks during wireless operations. Prescribing relevant cryptographic measures to encrypt the data being communicated and authenticate the vehicle key as a valid entity can mitigate these attacks. However, cryptographic security is only as secure as the keys used for encryption or authentication.
- **Application-level security for end-application operations (open vehicle doors, start engine):** In wireless connectivity devices, manipulated data received over the air or remotely can potentially compromise the device operation or cryptographic keys used for data communication security (through malware injection, for example). Therefore, it's important that Bluetooth LE wireless MCUs support protocol- and application-level cryptographic operations in a trusted way that secures keys. Securing the device firmware operation with secure boot, secure firmware updates and secure debugging access are all required.

Additionally, there are regulations for automotive cybersecurity in many regions, with standards such as International Organization for Standardization 21434 that require compliance with relevant cybersecurity processes during device development and maintenance.

Cybersecurity challenges for smart thermostats

A smart thermostat (see Figure 2) is a great example of the benefits and threats faced when looking at smart home technology. These devices allow homeowners to adjust the temperature of their home from anywhere and optimize energy usage through integrated Wi-Fi® connectivity.

Figure 2. A Bluetooth smart thermostat in a living room

Unfortunately, increased connectivity can expose thermostats to threats. For example, hackers could transmit maliciously crafted frames over the air to interrupt the thermostat's operation, or force it off the network. Intentionally kicking the device off the network and monitoring transmissions after reconnecting makes it possible to capture and decrypt data using a brute force or dictionary attack, resulting in the exposure of user or vendor data and credentials. Data can be captured through a remote man-in-the-middle attack by sending malicious data or code (such as malware) to the thermostat over the internet or transmitting data between it and a remote cloud server.

To mitigate, designers must follow the latest Wi-Fi security standards, which outline proven cryptographic algorithms for authentication, key agreement and encryption, and mandate protocols for protecting management frames, such as Wi-Fi Protected Access 3. These devices need to support the latest network security protocols (such as Transport Layer Security v1.3) for protecting internet-transmitted data. Furthermore, devices need to run these protocols efficiently and securely store keys used during their execution.

Cybersecurity challenges for smart sensors and e-locks

Battery-operated devices including smart sensors (motion, door, window sensors) and e-locks are increasingly using mesh technologies such as Zigbee®, Thread and Matter to meet low-power requirements while still connecting to the cloud through a smart home hub. Security threats like sniffing, man in the middle and device takeover could potentially compromise device data or secure operation (for example, e-lock access granted to a bad actor). In extreme cases, a compromised device could compromise the smart home network or ecosystem.

Securing these networks requires securing the communication channel between the sensor and hub so that only trusted devices can join the network.

Matter was designed to simplify development and provide improved protocol-level security for smart home products. In addition to securing the communication channel through a strong cryptographic suite such as Advanced Encryption Standard for confidentiality, secure hash algorithms for integrity, and elliptic-curve cryptography for key exchange and digital signatures, Matter uses certificates and passcode-based protocols to authenticate smart home devices and ensure that only genuine products join an ecosystem.

Security threat mitigation with wireless MCUs

To mitigate security risks, wireless MCUs should enable secure data communication, secure key exchange, mutual authentication, secure key storage, secure firmware updates, and secure boot operations.

Wireless MCUs such as the CC2745P10-Q1, CC2755R10, and CC3551E offer integrated security features to mitigate risks caused by malware and device takeover attacks. They support fundamental security features like secure boot and secure firmware updates with rollback protection. These MCUs feature an integrated hardware security module (HSM) with a dedicated controller for handling hardware-accelerated cryptographic operations, secure key storage, and random number generation. The HSM provides a trusted environment for cryptographic and key handling operations, thereby helping mitigate data privacy and advanced malware risks. The Arm® Cortex®-M33 core in these MCUs supports TrustZone-M, which further enables a trusted execution environment for secure software operation.

Trademarks

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