Electronic Design

By ERNEST WORTHMAN, Contributing Editor

Meet the Latest Cybersecurity Standards with New, Integrated Wireless MCUs

Sponsored by Texas Instruments: More sophisticated cyberthreats have prioritized security measures in wireless electronics design. Thanks to the latest standards, one of the best solutions to help enhance cybersecurity is the microcontroller.

In today's global, high-threat-level environment, designers and engineers no longer have the luxury of considering security as an afterthought. The security requirement is right up there, with safety as a design priority. Few wireless designs or devices leave the factory without some sort of security layer in place.

Fortunately, advances in microcontrollers (MCUs), software, and wireless technology have made integrating a security layer or protocol a less ominous and expensive process. That's largely due to the evolution of cybersecurity standards.

In fact, 2024 legislation mandates stricter cybersecurity requirements on everything from consumer IoT devices to critical infrastructure. Standards such as ISO 26262 for functional safety and ISO/SAE 21434 for cybersecurity are examples available on MCUs.

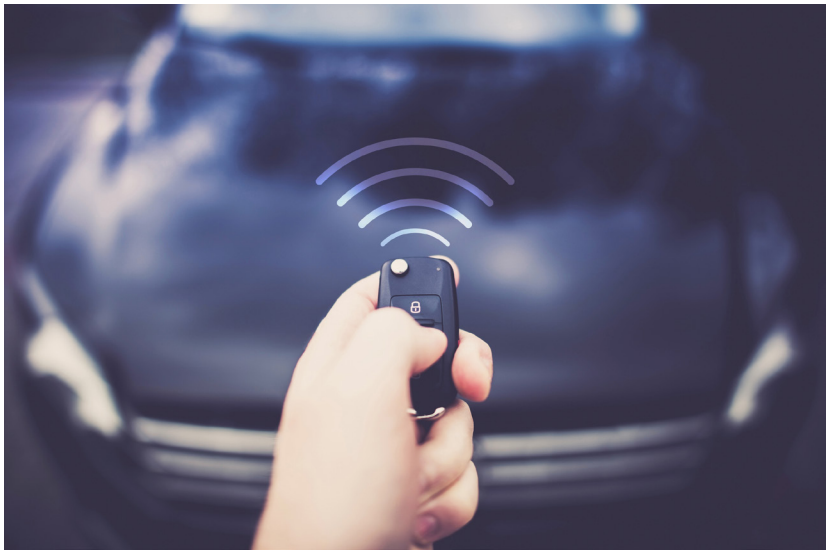
With the proliferation of wireless protocols like Wi-Fi and Bluetooth (BT), as well as myriad others both open and proprietary, keeping communications between and among devices and systems secure is imperative.

Wireless Security for Wi-Fi and Bluetooth

In the evolving Wi-Fi ecosystem, the almost final Wi-Fi 7 and ultra-high-reliable (UHR) Wi-Fi 8 will realign the deployment base of this platform. No longer will it be an unlicensed, red-headed stepchild with loose security. And, since nearly all internet servers run on Linux (a Unix derivative), it's just as important that MCUs support it. MCUs will become a pivotal device in these next-generation networks and be the launching point for the required high levels of security.

First, let's take a look at the BT platform.

The CC2755x10 SimpleLink Family of 2.4 GHz High Performance Wireless MCUs incorporates the BT core specification version 6.0 as an integrated algorithm processing unit (APU). This new feature enables extremely accurate channel sounding by providing much better distance estimation between devices, which enhances wireless security.



limits communications to a specific fixed distance and inactive states based on their distance from a smartphone, or other device. Such measures ensure more precise control of device-to-device communication links by better distance analysis and control.

And Bluetooth is only one protocol. Security spans the gamut from all wireless platforms. Each face similar challenges in offering security. It doesn't matter what wireless device is accessing a vehicle, or a smart-home device, or even an electrical grid. The challenges are similar, and solutions vary from protocol to protocol, but all have the same desired outcome: higher security.

Existing protocols such as received signal strength indication (RSSI) and direction findings (DF) work reasonably well. But current ranging protocols enable significant opportunity for compromise. By adding the version 6.0 standards—round trip timing (RTT) packet exchanges and normalized attack detector metric (NADM)-based mitigations—opportunities for signal compromise are lessened.

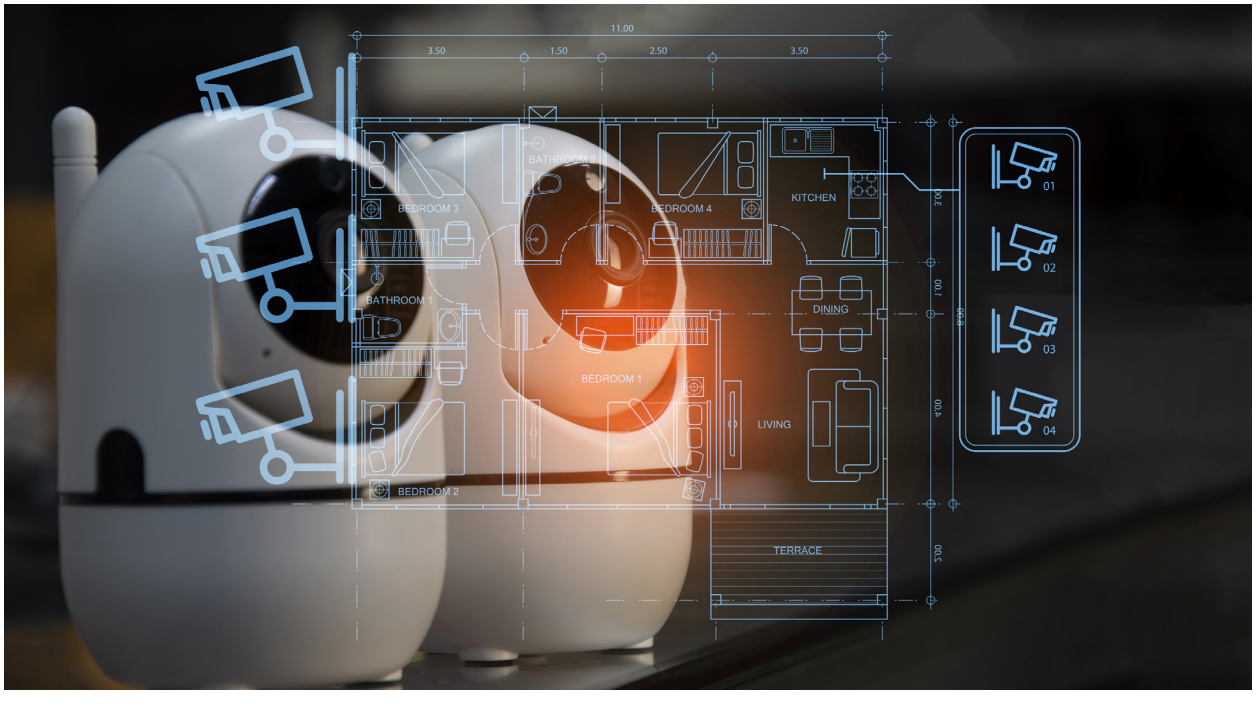
These physical-layer (PHY) and medium-access-controller (MAC) system-level integrations elevate ranging security significantly with advanced digital key solutions.

Another is the human-machine interface (HMI). This

The MCU's Cybersecurity Role

Many types of network attacks are directed across the ubiquitous wireless infrastructure. MCUs play a significant role in that they can offer protection against cyberattacks by integrating security at the system level.

The evolution of devices with system-level security measures has reached critical mass. For example, TI's CC2745P10-Q1, CC2755R10, and CC3551E offer significant system-level security options based on authentication algorithms for key agreement, encryption, and exchange. These MCUs address not only BT, but Wi-Fi, Mesh, Zigbee,



Matter, and others.

Processes within the MCUs implement security features, such as secure key storage and exchanges, mutual authentication, and secure-boot operations with an integrated hardware security module (HSM). These complex protocols are too lengthy to explore in this short piece, but a cursory discussion of some is warranted.

One of the more common security protocols is TrustZone. This mature standard developed by Arm is found in nearly all security devices based on the Arm architectures. TrustZone is a hardware security extension that includes a bus fabric and peripherals. It works by partitioning all of the hardware and software on the system-on-chip (SoC) into separate layers: the secure unsecure.

The secure layer is implemented when security is demanded (such as the boot sequence). The unsecured layer takes over once all security protocols have been vetted, and no abnormalities found. These routines run in hardware-bounded barriers to prevent unsecure layer components from accessing secure ones.

Boot Security

Perhaps the most common example of a security implementation is in the boot operation. This is an operation that runs during the MCU's startup process. Basically, it runs algorithms verifying the digital signatures of each boot component by comparing it to the public keys of the embedded system (provided by the vendors during manufacturing).

If the keys are valid, the process advances to the embedded public keys; otherwise, it returns to firmware initialization and generally runs an error or halt function. If the algorithm validates the first component's signature, it steps into the next component in the verification chain and so on until all of the code is verified and loaded. After verifying all boot components successfully, the firmware loads the operating system kernel into memory.

Another weapon is the HSM. As mentioned earlier, it's the "container"—a physical device that enhances security of sensitive data by generating cryptographic keys for essential functions. These include hardware-accelerated encryption, decryption, and authentication via stored keys.

These devices come in several forms. They can be plugin cards, or may be integrated into other hardware, i.e. the MCU. They're also available as smart cards for wireless appliances, and external devices. HSMs are agile solutions. Beyond their integration into components, they may be connected to a network server or operated independently offline. And today, they're also available as cloud services.

Conclusion

In the end, generally, the best solution is to embed security in the SoC, and make it field upgradable, either over the air, or on site. Security is no longer an afterthought and the lower in the chain it can be implemented, the more effective it is.

Thanks to standards, the MCU has taken its rightful place among the best solutions for cybersecurity.