Electronic
Design

RICK NELSON, Contributing Editor

MCUs, Companion Chips Enable Wireless Connectivity While Boosting Cybersecurity

Sponsored by Texas Instruments: As everyday electronic products gain intelligence and wireless connectivity, designers must choose components that can maintain security.

Our vehicles and consumer-electronics devices are increasingly able to communicate wirelessly. A smart thermostat can communicate with your Wi-Fi router, allowing you to adjust your home's temperature remotely. Your car can talk to your phone over a Bluetooth Low Energy (LE) link to facilitate vehicle access. In these cases, wireless MCUs or wireless companion ICs used with standard MCUs are able to help you implement such functionality and take advantage of features like Bluetooth channel sounding.

Unfortunately, each wireless link provides a potential path for malicious intrusion that can compromise private

1. Smart-home networks can connect to multiple smart devices using mesh technology, possibly creating security risks. (Credit: TI)

personal information or endanger safety, so make sure the components you choose have comprehensive security features built in to help minimize the risk. These features include anti-rollback protection, which ensures the use of the most recent and secure firmware; firewall authentication, which prevents unauthorized persons from gaining access; and support for Wi-Fi Protected Access 3 (WPA3), the latest security protocol standard for Wi-Fi.

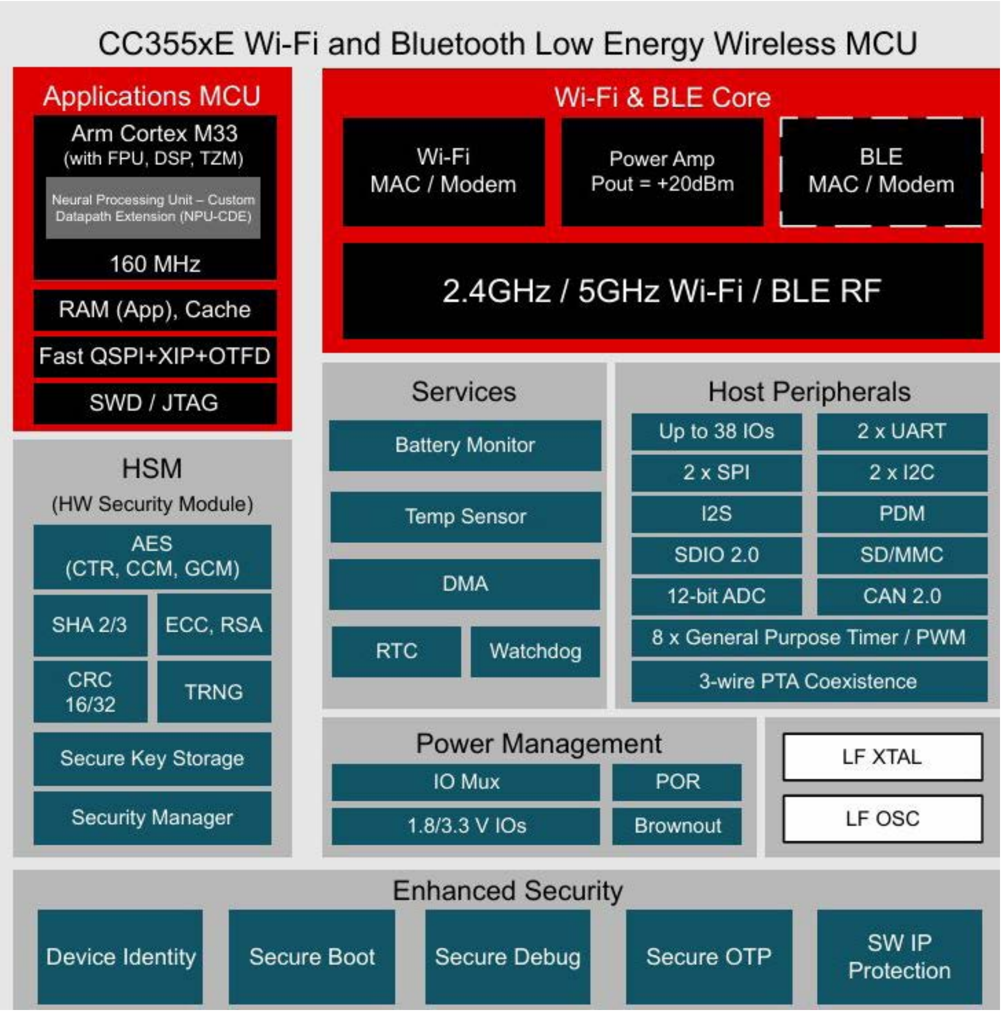
Smart-Device Security Details

Consider a potential vulnerability of the smart thermostat connected to a Wi-Fi router. A hacker could send malicious transmissions over the air to knock the thermostat off the network and then monitor the reconnection process in an attempt to steal passwords or other authentication information. If successful, the hacker can obtain data that lets him judge the likelihood of your being away from home.

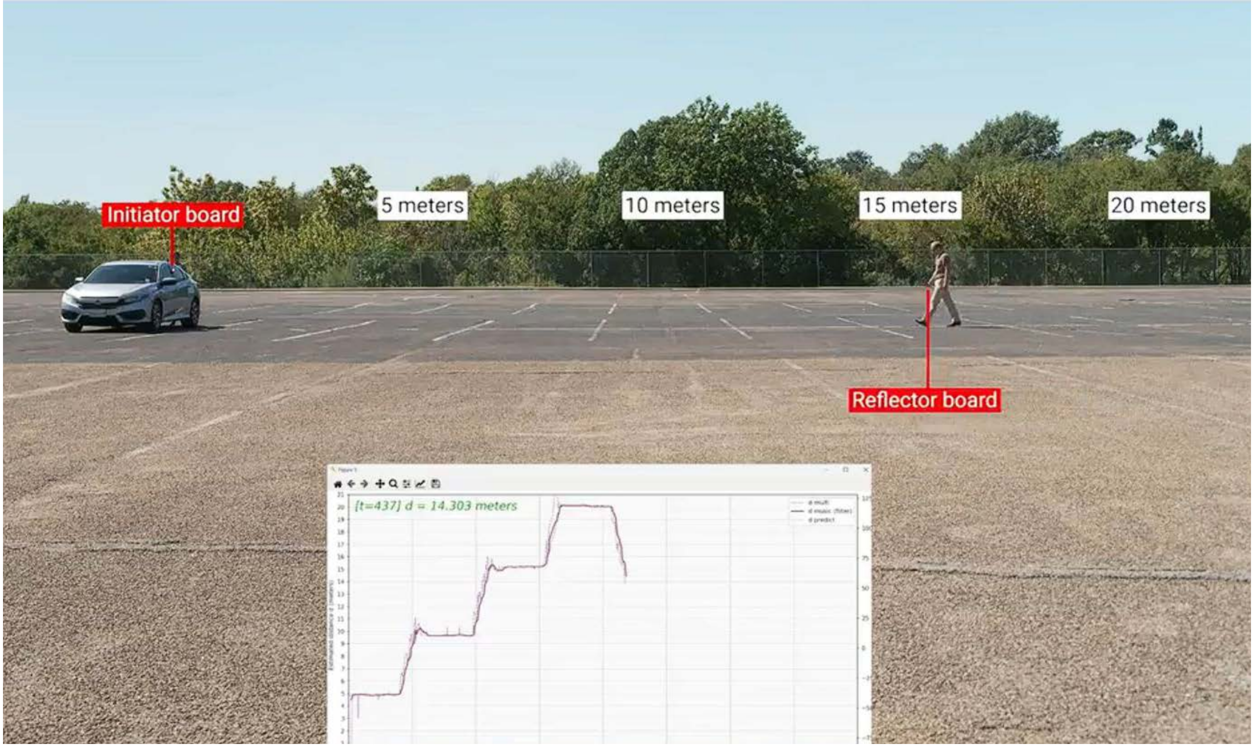
The problem becomes even more challenging when augmenting your home network with more smart devices: e-locks, motion sensors, smart appliances, and so on *(Fig. 1)*. Such devices are increasingly communicating using a mesh technology like the one defined in Matter, an interoperable, open, secure, and royalty-free standard for interconnecting compatible devices. In turn, the devices could communicate with the cloud via Wi-Fi through a smart home hub.

Any single device may jeopardize the entire network, though, compromising private information by allowing access to your home. To enhance security, Matter supports strong cryptographic suites such as the Advanced Encryption Standard (AES), secure hash algorithms, and elliptic-curve cryptography for key exchange and digital signatures to ensure that only legitimate products can join the network.

Texas Instruments offers several wireless MCUs that facilitate secure key exchange and storage as well as secure firmware updates and boot operations. For example, the CC3551E Wi-Fi and Bluetooth LE wireless MCU *(Fig. 2)* includes a hardware-security module (HSM) that can accelerate AES and other encryption operations. Other enhanced



2. The CC355xE wireless MCU includes a hardware security module and various enhanced-security features. (Credit: TI)



3. A channel-sounding demonstration plots distance (inset) between an initiator and reflector with minimal latency. (Credit: TI)

security features include secure boot, secure debug, and secure one-time password (OTP) use.

Bluetooth Channel Sounding

A key feature of the latest Bluetooth specification—Version 6—is a channel-sounding feature that enables accurate measurement of the distance between two devices: your computer, for example, and the cellphone you have misplaced. In addition to helping consumers find lost items, this technology can be used for asset tracking in industrial environments.

Channel sounding employs a one-to-one topology, where one device acts as an initiator and the other acts as a reflector. Distance between the devices is determined through phase measurements, the round-trip timing (RTT) of packet exchanges, or both.

Whereas components such as TI's wireless MCUs can help ensure the security of a Bluetooth link, the channel-sounding capability itself could improve the security of your end application. Consider a vehicle wireless key fob, for example. In a common man-in-the-middle relay attack, a hacker can copy your fob's code and replay it to steal your vehicle. However, a hacker's equipment can't replicate Bluetooth channel sounding's RTT packet exchanges. With channel sounding, your key fob must physically be within a certain distance of your door lock before the lock will open, foiling the hacker's ability to falsify your key's signal with his own equipment.

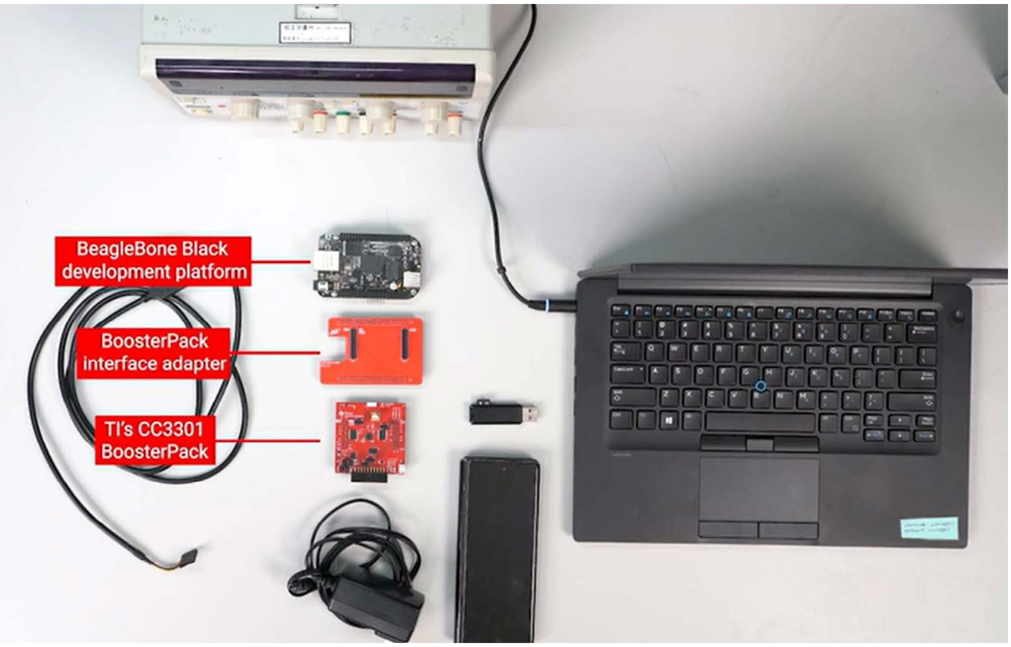
TI offers a video that shows Bluetooth channel sounding implemented using a TI CC2745 automotive SimpleLink Bluetooth 6.0 LE wireless MCU. The CC2745 includes an algorithm-processing unit (APU) that can execute distance-estimation algorithms in as little as 15 ms.

In the video demo, a CC2745 launchpad board with a multiple-antenna booster pack mounted on a car door serves as the channel-sounding initiator. An identical configuration carried by a person outside the vehicle serves as the reflector *(Fig. 3)*. The demo produces a plot showing the distance from initiator to reflector with minimal latency, as shown in the *Figure 3* inset. To help you quickly test and customize channel-sounding and other Bluetooth designs, TI offers out-of-the-box algorithms, evaluation boards, and antenna reference designs.

Companion ICs

An alternative to using a wireless MCU is the SimpleLink CC3301 single-band (2.4 GHz) or CC3351 dual-band (2.4 and 5 GHz) Wi-Fi 6 and Bluetooth LE 5.4 companion IC. Both ICs support WPA3 and provide firewall authentication and rollback protection. They work in conjunction with an external MCU that runs Linux or a real-time operating system.

A TI video demonstrates the pairing of a CC3301 with a TI AM3358 Sitara Arm-based processor running Linux. The addition of the companion IC adds Bluetooth and Wi-Fi


BeagleBone Black development platform
BoosterPack interface adapter
TI's CC3301 BoosterPack

4. A BeagleBone Black development platform and a CC3301 BoosterPack module enable a Bluetooth demonstration. (Credit: TI)

capabilities to the AM3358's wired industrial interface options, including EtherCAT and PROFIBUS.

In the demo, a BeagleBone Black development platform represents the processor. The platform connects via an interface adapter to a TI BoosterPack plug-in module that contains the CC3301 *(Fig. 4)*. A software development kit facilitates the installation of appropriate Linux drivers, firmware, and related binaries. With the hardware and software setup complete, a mobile-phone app scanning for Bluetooth devices displays the newly created connection as "CC33xx BLE."

Conclusion

Wireless technology provides a convenient method for intelligent home and automotive devices to communicate, but hackers can use communication links to compromise network security. New wireless MCUs and companion chips provide the features necessary to deal with evolving cybersecurity challenges. TI offers a variety of devices and design support to get you started developing devices for secure wireless networks.