Technical Article

Strengthening Wi-Fi Security at the Hardware Level

Noa Chorev

If you're an Internet of Things (IoT) designer, you're probably often challenged to do more with less when it comes to security, constantly looking for new ways to protect your products against an ever-growing list of threats with lean system resources and perhaps limited experience.

Knowing that these struggles are very real, in this post I'll outline a few top IoT security risks and common misconceptions on how to address them. I will also provide an overview of how new SimpleLink™ Wi-Fi® products give you more tools to help address security challenges through a novel architecture and rich set of integrated security features.

Are there IoT applications that don't need to implement security measures?

Any device that connects to the internet may be vulnerable to local or remote attacks. Attackers can target almost any connected device to try and steal manufacturer intellectual property stored in the system, gain access to user data, or even maliciously manipulate the system to compromise users or attack third parties online.

As demonstrated by the major distributed denial of service (DDoS) attack late last year, labeled by experts as the largest of its kind in history, even seemingly harmless products such as home digital video recorders (DVRs) can be maliciously infected and used as "botnets" to halt operations for third-party entities. The attack last year affected services such as Twitter and PayPal, but similar attacks could potentially target large smart infrastructure technologies such as electric grid systems. According to a 2016 study conducted by Kapersky Lab, a single DDoS attack can cost an organization more than $1.6 million to resolve.

Recognizing these threats, TI's SimpleLink™ Wi-Fi® CC3220 wireless microcontroller (MCU) integrates a host of powerful, multilayered and hardware-based security features to provide you with powerful tools to help protect products from attacks such as local or remote packet sniffing, man-in-the-middle (MITM) server emulation, hostile takeovers via over-the-air updates, remote file manipulation, data and software theft, intellectual property (IP) cloning, and many more.

Should IoT security features primarily focus on Wi-Fi and internet-level encryption of packets sent over the air?

Having strong Wi-Fi (Advanced Encryption Standard [AES]/Wired Equivalent Privacy [WEP]) and internet-level (Transport Layer Security [TLS]/Secure Sockets Layer [SSL]) encryption is critical to help prevent local and remote network-packet sniffing, respectively. But these measures alone may not be enough to fend off hostile takeover attempts or provide full protection against theft of IP, code, data, keys and identity information stored and used in a connected system. Figure 1 illustrates these measures in action.

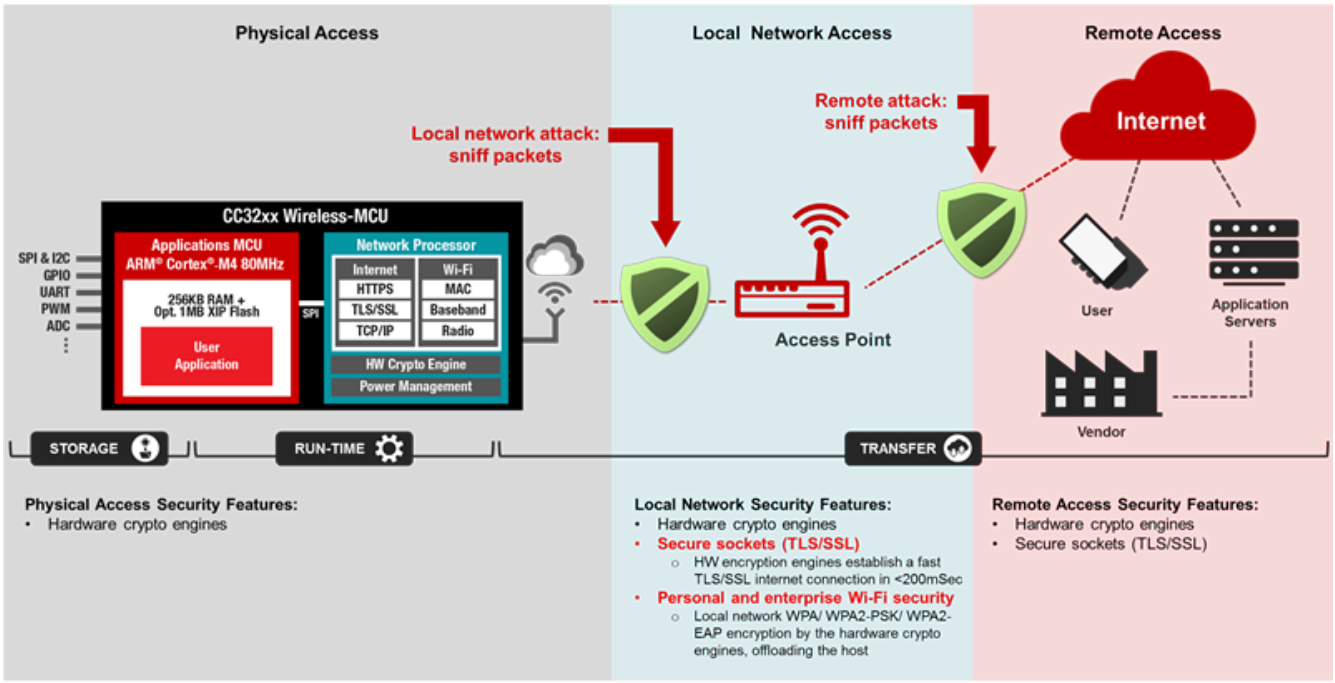


Figure 1: Local network security features in action

The CC3220 device actually integrates more than 25 additional security features to help provide tools that address potential threats from the larger end-to-end IoT landscape. Figure 2 portrays many of these features.

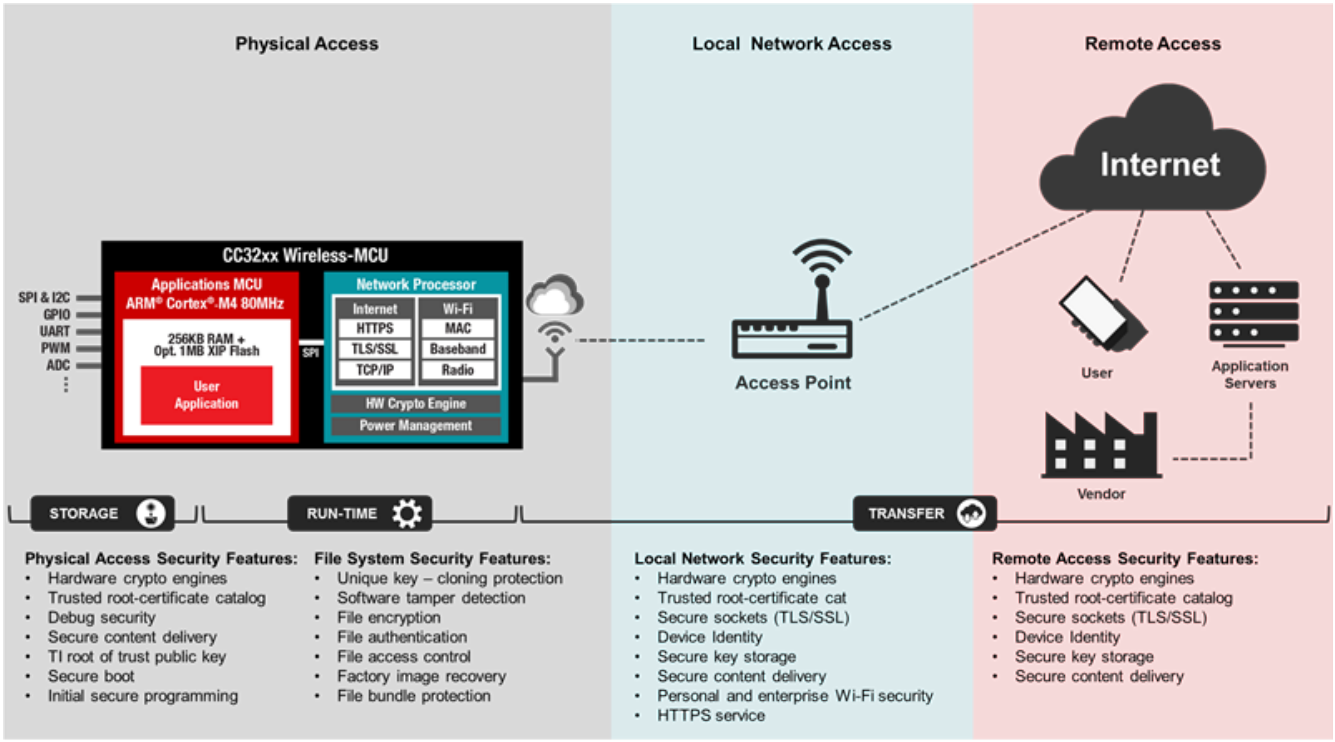


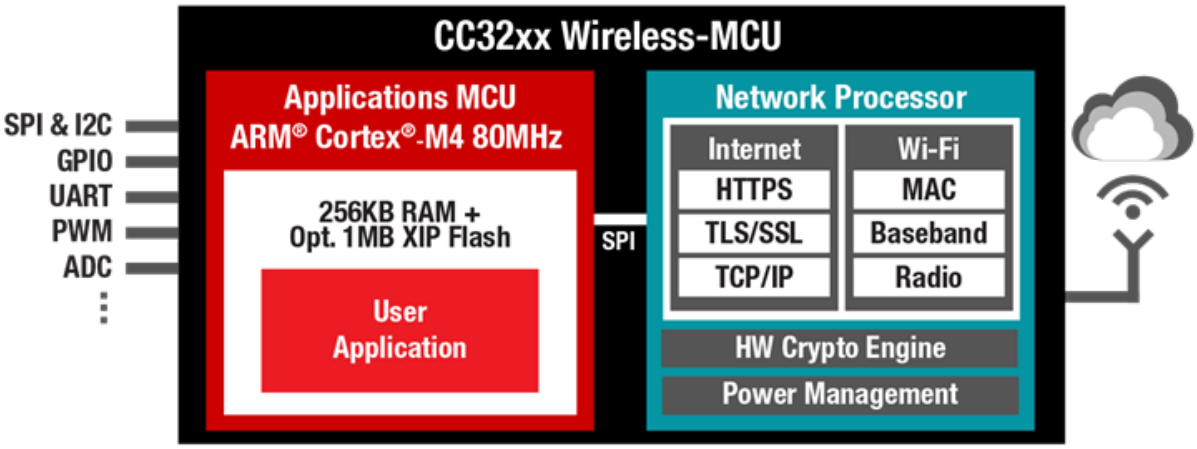
Figure 2: CC3220 security features

Do you need to use a high-end microprocessor unit (MPU) or dedicated secure element to effectively protect your products against potential risks?

While increasingly lean IoT system resources often present design challenges, you can still strive to target more robust security in MCU-based, bill of materials (BOM)-optimized systems. The first steps are to identify which system assets are at risk, where the potential exposure points exist and what threats you anticipate will put the system at risk. From there, you work to choose components that offer a wide range of integrated hardware-based security features, while offloading the host MCU.

The CC3220 wireless MCU sets out to give you these tools. The unique dual-core architecture (illustrated in Figure 3) runs both the host application and the network processing on a single chip to simplify the design. However, running these operations on two physically separate execution environments enables the chip to:

- Offload the processing of the device's security functionality (including secure file system management) to the network processor and hardware cryptographic engines. This enables the million instructions per second (MIPS) and application MCU memory to be solely dedicated to the host application.
- Help reduce the firmware and network-management vulnerability for application-related risks by physically partitioning the programmable application MCU from the read-only memory (ROM)-based network processor



For more information about the CC3220 device, be sure to check out the product page and the broader SimpleLink Wi-Fi security documentation, including the full security application note, "SimpleLink CC3120, CC3220 Wi-Fi Internet-on-a-Chip Solution Built-In Security Features."

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