Technical Article

Use Validated Security with FIPS 140-2 on SimpleLink™ Wi-Fi® Devices

Mason Berhenke

As more and more devices connect to the Internet of Things (IoT), higher security standards have become a necessity. The threat from using unsecure IoT devices poses a risk to infrastructures as big as connected cities all the way down to connected fish tanks.

Governments are taking notice that IoT devices need to be secure before integrating these devices into their infrastructures. In 2017, the U.S. Senate introduced legislation requiring that devices that connect to the internet have no security defects listed by the National Institute of Standards and Technology (NIST). In 2018, California passed a law requiring manufacturers to implement “reasonable” security against unauthorized access. This law goes into effect Jan. 1, 2020.

Security remains a priority for businesses looking to implement IoT products into their infrastructures. According to a 2018 survey by Bain and Co., security is the top barrier to adopting enterprise IoT solutions, and has been the top concern since 2016. In the same survey, enterprise customers said they would actually pay more if their security concerns were addressed. This is especially true for markets that handle highly sensitive data like health records.

So it’s clear that manufacturers need to implement secure products. Unfortunately, the term “secure” is a bit unclear. Several third parties claim to have a secure solution, but nothing on the market provides a whole system approach.

This ambiguity indicates a clear need for manufacturers to use silicon that implements industry standards for secure algorithms; however, since any silicon company can claim to have implemented these standards, it then becomes even more important to have third-party verification.

TI has decided to follow an industry standard for security, a standard that outlines secure algorithms that requires validation by approved third-party test labs and is reviewed for accuracy by an agency dedicated to security. In the third generation of SimpleLink™ Wi-Fi devices, we validated our security through Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard.

What is FIPS 140-2?

FIPS 140-2 is a standard for certifying the security of electronic hardware.

Implementing security can be a long, expensive and rigorous process; validating for FIPS is no exception. The first step involves creating and implementing an approved security algorithm. Any manufacturer knows that whether it is implementing algorithms like the Advanced Encryption Standard or Secure Hash Algorithm, development requires planning from the physical to application layer. As you can see in Figure 3, TI’s SimpleLink MCUs have been developed to cover security from the physical to the application layers in both of our separate execution environments.

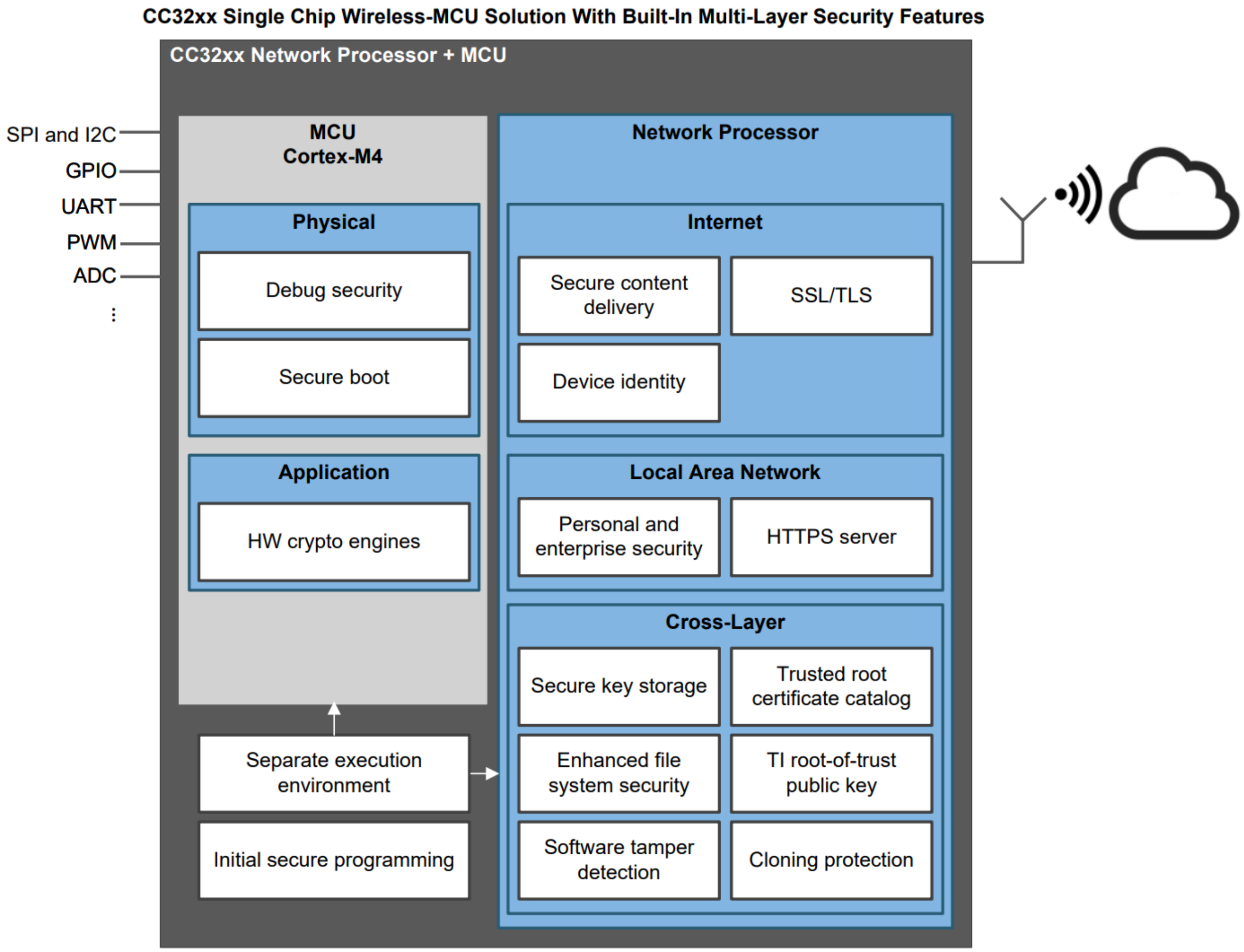
CC32xx Single Chip Wireless-MCU Solution With Built-In Multi-Layer Security Features
CC32xx Network Processor + MCU
SPI and I2C
GPIO
UART
PWM
ADC
⋮
MCU
Cortex-M4
Physical
Debug security
Secure boot
Application
HW crypto engines
Separate execution environment
Initial secure programming
Network Processor
Internet
Secure content delivery
SSL/TLS
Device identity
Local Area Network
Personal and enterprise security
HTTPS server
Cross-Layer
Secure key storage
Trusted root certificate catalog
Enhanced file system security
TI root-of-trust public key
Software tamper detection
Cloning protection

Figure 3. CC3220/CC3235x Device Security Features

The next step involves selecting a NIST-approved third-party testing lab to verify the algorithms. This process can take several months to even over a year. TI had to go back and forth constantly with the test lab, implementing fixes and verifying our design until we got it right. Each algorithm requires its own testing and verification. This was true when we validated our WiLink™ WL1837MOD module for FIPS, and it continued to be true for SimpleLink devices, where we validated 12 algorithms for FIPS.

All test reports must be submitted to NIST for review and approval. While the third-party labs are reputable and approved, NIST takes it a step further to verify the test reports themselves before giving the final validation. This entire process ensures three levels of verification for SimpleLink Wi-Fi devices: manufacturer, third-party lab and government agency.

What Does FIPS 140-2 Validation Mean?

In TI SimpleLink Wi-Fi devices, we've always claimed to have comprehensive end-to-end security. We've taken it a step further to validate that security with FIPS. When you implement SimpleLink Wi-Fi devices in your applications, you'll be implementing far more than just "reasonable" security. You'll be implementing security that the U.S. government has validated – security that organizations swear by to ensure their safety and privacy.

If your end product uses our third-generation devices, you can use the phrase "FIPS Inside" to show your customers that you only use components with the highest standard of security. You can even take it a step further to FIPS-validate your own devices. Our validation can be reused, and you will save time and money.

If you'd like to learn more about FIPS, visit our page about the SimpleLink platform.

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