Understanding security features for SimpleLink™ Wi-Fi® CC32xx MCUs

Texas Instruments

Device/Family description

The **CC3220x** and **CC3235x** devices are part of the **SimpleLink™ microcontroller (MCU) platform**, which consists of a 32-bit Arm® Cortex®-M4 standalone MCU, or wireless MCUs with Wi-Fi®, *Bluetooth*® low energy or Sub-1 GHz. All devices in the platform share a common, easy-to-use development environment, software development kit (SDK), and rich tool set. Using the SimpleLink platform enables developers to add any combination of the portfolio's devices into their design, allowing maximum code reuse when design requirements change.

The SimpleLink Wi-Fi CC3220x and CC3235x wireless MCU is a single-chip solution with two physically separate execution environments: a user application Arm Cortex-M4 MCU and a network processor MCU running all Wi-Fi and Internet logical layers.

The device offers a wide range of multilayer built-in security features to help developers address a variety of security needs, which is achieved without any processing burden on the main MCU.

TI Embedded Security Portfolio –

Security is hard, TI makes it easier

Security problem targeted: Typical threats / security measures

A network-connected Internet of Things (IoT) device is commonly connected to a cloud server. An interaction with a cloud server typically requires uploading or downloading sensitive information to / from the cloud. An example of data sent to the cloud might be sensitive device or user information such as identity, passwords, keys, billing information, sensors data used by the device and more.

Examples of data received from the cloud comprise mainly software updates and new certificate files. With the device connected to the network, it is at risk to be targeted by malicious users who want to use the network access of the device and some possible vulnerability to access the type of sensitive data mentioned above or to take control of actuators (for example, a door lock). Last but not least, the device's assets are also at risk. The application code running on the device and any data related to it can be the target of malicious activities aiming at stealing proprietary information or cloning the device.

All of this sensitive data can be considered an "asset" and should be protected throughout its life cycle, when the data is in storage, in run-time or in transfer over the Wi-Fi medium. When examining the possible exposure points of a Wi-Fi connected device, designers try to address the key ones, being network threats, covering both external Internet network and the local Wi-Fi network, as well as protect against hardware tampering threats for attackers with physical proximity to the device.

The main "exposure points" of a Wi-Fi-connected device comprise network threats and hardware tampering threats. On the network threats, it is worth mentioning that an attacker could target the device from a remote access or from the local Wi-Fi network, targeting the lower level of the OSI protocol. On the hardware tampering threats, an attacker with physical access to the device could carry out an attack that may cost more but allow the attacker access to an essential secret potentially shared with several devices.

Validated for FIPS 140-2 level 1 certification

In our increasingly connected and complex world security and cyber security have become top concerns. While many devices claim security, the SimpleLink Wi-Fi CC3235x devices are tested and certified for security. The Federal Information Processing Standard (FIPS) Publication 140-2, being one of the most known and credible security certification offers a strong security assurance of the security level provided by the SimpleLink Wi-Fi devices.The CC3235x was validated by the U.S. National institute of standards and technology (NIST) to be FIPS validated. All the SimpleLink's Wi-Fi Security claims and crypto modules were reviewed and tested to perform to standards.

Security features details

- **FIPS certification** – The CC3235x devices are certified by U.S. NIST for FIPS140-2 level 1
- **Secure boot** – Validate the integrity and authenticity of the run-time binary during boot
- **Device identity** – Unmodifiable unique 128-bit number that TI stores in the device during production. It may serve as a unique device identity (UDID)
- **Secure key storage** – asymmetric key-pair storage with built-in crypto acceleration and crypto services
- **Trusted root-certificate catalog** – Built-in secure mechanism to ensure a certificate authority (CA) is trusted as root of certificate chain for the purpose of TLS and for file signing
- **TI root-of-trust public key** – Hardware-based mechanism that allows authenticating TI as the genuine origin of a given content (e.g., software service pack, trusted root-certificate catalog) using asymmetric keys
- **Hardware accelerators** – AES, DES / TDES / 3DES, SHA-1/ SHA-2/ MD5 hardware accelerators are used to offload the intense arithmetic calculations involved in the cryptographic algorithms
- **Debug security** – Blocking the access to debug capabilities such as JTAG interface and file-by-file access from external tools
- **File system security** – File system security for confidentiality and integrity of data
- **Personal and enterprise Wi-Fi security** – 802.11 standard-compliant security support (WPA / WPA2-PSK / WPA2-EAP)
- **Secure sockets** – Transport layer security complies with SSLv3, TLS1.0/1.1/1.2. Support up to 16 secure sockets concurrently (CC3220x devices supports 6 secure sockets)

Security enablers:

Device	Security enablers	Detailed security features
CC3235S CC3235SF CC3220S CC3220SF	FIPS certification*	Certified by U.S. NIST for FIPS 140-2 level 1
	Secure boot	Secure boot
	Device identity/keys	Device identity Secure key storage Trusted root-certificate catalog TI root-of-trust public key
	Cryptographic acceleration	AES DES / TDES / 3DES SHA / MD5
	Debug security	Debug security
	Secure storage	File encryption File authentication File access control Factory image recovery File bundle protection Cloning protection Software tamper detection
	External memory protection	Secure storage (see detailed feature list above)
	Networking security	Personal and enterprise Wi-Fi security • WPA • WPA2-PSK • WPA2-EAP Secure sockets • SSL v3 • TLS 1.0/1.1/1.2 HTTPS server Secure content delivery Online certificate status validation (OCSP)
	Initial secure programming	Initial secure programming
	Secure firmware and software update	Personal and enterprise Wi-Fi security • WPA • WPA2-PSK • WPA2-EAP Secure sockets • SSLv3 • TLS1.0/1.1/1.2 Bundle protection Factory image recovery Online certificate status validation (OCSP)
	Software IP protection	File system security Cloning protection Software tamper detection

*Supported on CC3235x devices only

TI offers security enablers to help developers implement their security measures to protect their assets (data, code, identity and keys).

- **HTTPS server** – Internal HTTP server running on top of a TLS socket with support for client authentication
- **Secure content delivery** – Provides an end-to-end ability for delivering confidential information to the system independent of the security of the transport layer
- **Initial secure programming** – Image integrity check and image confidentiality during programming, including system configurations and user files

- **Bundle protection** – The bundle protection is a method offered by the SimpleLink device for keeping the system integrity while updating a collection of files referred to as a bundle
- **Factory image recovery** – The factory image file contains the programmed image files, which includes the service pack, host application, configuration files and user files. Once invoked, the device is formatted and reprogrammed
- **Cloning protection** – The file system is readable only by the device which first booted this image
- **Software tamper detection** – Detecting and alerting potential unauthorized manipulation of secure file content

Additional security information

While non-connected products can be taken over primarily via physical access, connected devices stand the risk of being compromised remotely. The **SimpleLink Wi-Fi CC3220x and CC3235x wireless MCUs** provide multiple layers of protection to help designers protect their system against hostile manipulation and takeover attempts.

The SimpleLink Wi-Fi device was designed with security in mind, providing several hardware and software key security building blocks, which are the foundation for all of the device's security features:

- **Separate execution environment** – By design, the architecture of the device is such that the networking processor is a physically separate process subsystem, creating a separate execution environment.
- **Hardware crypto engines** – Hardware accelerators are used to offload the intense arithmetic calculations involved in the cryptographic algorithms. The SimpleLink CC3220 wireless MCU includes a set of hardware crypto engines to enhance the performance of applications that require custom or application-level security. These engines offload the ARM Cortex-M4 MCU from the complex and time-consuming arithmetic involved in cryptographic algorithms.

Additional resources

- **CC3x20, CC3x35 SimpleLink™ Wi-Fi® Internet-on-a chip™ solution built-in security featuress** application report – Describes the security-related features of CC3120 and CC3220R/S/SF wireless MCUs and provides guidance for leveraging each feature in the context of practical system implementation.
- **Strengthening Wi-Fi security at the hardware level** blog – Outlines a few top IoT security risks and common misconceptions on how to address them.
- **SimpleLink™ Wi-Fi® integrated security features** video – Describes how the SimpleLink Wi-Fi CC3220 wireless MCUs are making it easier for customers to design a more secure product.

www.ti.com/security

Security is hard, TI makes it easier

For more information about TI's Embedded Security Solutions, visit **www.ti.com/security**

Texas Instruments

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (www.ti.com/legal/termsofsale.html) 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.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265