Application Note

SimpleLink CC33xx Security Features

Shlomi Itzhak

ABSTRACT

The CC33xx family of devices are the next generation of the Simplelink™ embedded solutions. The main role of these devices is to meet the requirements of the new emerging Internet of Things (IoT) use cases while being compatible with the latest cutting-edge technologies like Wi-Fi™ 6 and *Bluetooth*® Low Energy 5.4.

These next generation devices enable affordable, reliable and secure connectivity in embedded applications with a host processor running Linux® or an MCU host running RTOS. The CC33xx family of devices offer a wide range of built-in security features to help developers address a variety of security needs.

Table of Contents

List of Figures

List of Tables

Trademarks

1 Introduction

Internet of Things (IoT) products and systems hold information that can be sensitive and private, thus stressing the importance of securing the data. This data can include passwords, keys, credentials, configurations, personal information, vendor intellectual property (IP), and more. The growing number of published exploited weaknesses in security and the requirements that keep coming from governments and standards organizations, mandate building robust cybersecurity measures for every new IoT device.

This document describes these security related features, which are made available to vendors through an ecosystem that incorporates simple and concise APIs, tools, and documentation. This document does not address the security related features on network layers or application layers and cover only the features that resides in the Wi-Fi and Bluetooth Low Energy peripherals.

1.1 Terminology and Abbreviations

Table 1-1. Terminology and Abbreviations

Abbreviations	Meaning
Asset	An asset is any piece of information (security-relevant elements) that has value to the owner. An asset therefore must be protected by the measures of the target system (by means of confidentiality, integrity, authenticity). Assets can be proprietary information, personal data, or intellectual property.
Authenticity	Maintains that assets or entities are genuine and authorized to perform a task or used as intended. The verification process usually involves cryptographic algorithms, which check that the entities are who they claim to be. Some predefined trust mechanism is always part of an authentication scheme.
Certificates	Certificates are standard-formatted files. Certificates typically contain the public key of the subject, and a CA signature of the header and public key. Anyone provided with the CA public key (or sub-CA in case of certificate chain) can verify the subject's identity.
Certificate authority (CA)	A trusted entity that issues certificates used to verify identities.
Certificate chain, Chain of trust	A certificate chain consists of a hierarchy of certificates that allows anyone to verify the identity of any certificate issuer, down to the root certificate.
Confidentiality	Confidentiality maintains that an asset is not made available or disclosed to unauthorized entities. In most cases, confidentiality translates into encryption, while in other cases, obfuscation techniques are used to maintain confidentiality.
Integrity	Attribute describing an object that remains intact entirely, compared to the original version.
Root CA	The topmost certificate provided by a certificate authority, against which the certificate chain is eventually verified. The certificate is always self-signed and publicly available.

2 Internet of Things (IoT) Products and Security

An IoT device is by nature a network-connected device, and therefore can serve as a gateway to malicious access to sensitive data, such as surveillance videos, or control over actuators, such as door locks. To achieve good security for an internet-enabled product, a security assessment must be performed on the specific product and the system-level requirements. This assessment identifies the involved assets, analyzes the environment as well as intended and unintended potential usages of the product, and thereby detects potential vulnerabilities of the product.

This assessment helps the developer define the best protection scheme using the available security capabilities.

The environment, the assets, and the processes are different from one product to another, but generally for IoT devices there are some common exposure points:

- Physical access (with or without the ability to manipulate hardware interfaces)
- Local network connectivity
- Internet (or intranet) network connectivity – **not covered in this document**

Figure 2-1 illustrates the common exposure points of an IoT-connected product.

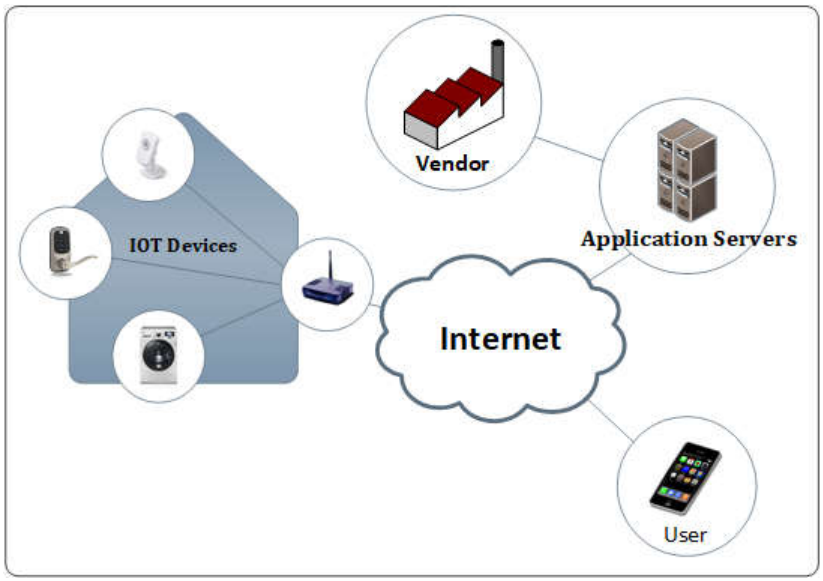

Figure 2-1. IoT Device Exposure Points

2.1 Physical Access

In the case of a physical access attack, the exposure is at the product level and there are a couple factors to consider. Physical access can result in attack vectors such as product-level manipulation and printed circuit board (PCB) manipulation. The product-level manipulation vector refers to attacks in which the attacker can control the way the device operates by using the external interfaces that the final product offers (such as power line, buttons, and so forth). The second vector relates to the ability of the attacker to access the actual board (PCB) and to monitor the lines or the hardware interfaces. In more serious cases, an attacker can even attempt to manipulate the wires, replace devices on the PCB, connect to the main controller, and inject signals to trigger certain actions.

2.2 Local Network Connectivity

The general nature of a local network leads to a specific set of attack vectors. For example, monitoring of the wireless network or injecting malicious or abusive traffic on the Wi-Fi or Local Area Network (LAN).

One vector is based on passive monitoring of traffic over the wireless network, without the attacker being connected. A wireless network can be passively monitored, because some of the headers of communication packets are not encrypted even in secured wireless networks. These headers can reveal information such as the MAC addresses of the devices on this network or the temporal properties of the traffic generated.

The Wi-Fi Alliance has regulated security and compliance tests as part of the standards. The CC33xx companion IC is tested with Wi-Fi Alliance testbeds, and complies with all these security requirements.

The second vector relates to attacks generated from another device that is part of the local area network (LAN). This provides additional opportunity for executing an attack vector that involves network access, and the ability to legitimately inject traffic over the network and abuse ports and protocols available on the target device.

3 Main Features

The CC33xx companion IC offers a wide range of built-in security features. These security features can enable and assist designers with addressing a variety of security requirements and reducing the security risk with the intended application.

Table 3-1 lists high-level descriptions of the main security features.

Table 3-1. Main Security Features

Feature	Description
Personal and Enterprise Wi-Fi security	802.11 standard-compliant security support (WPA, WPA2-PSK, WPA2-EAP, WPA3, PMF, WPA3-EAP).
Accelerators	On-chip cryptographic engine (HW accelerator) to offload data encryption/decryption.
TI root-of-trust public key	The hardware-based mechanism that allows authenticating Texas Instruments as the genuine origin of certain content (such as firmware binary, RAM bootloader binary or other containers) using asymmetric keys.
Secure boot	Validate the integrity and authenticity of the runtime binary during boot to verify that the downloaded firmware is signed by Texas Instruments and has not been tampered with.
Secured host interface	Prevent physically sniffing SDIO/SPI to maintain data integrity.
Rollback protection	Built-in HW mechanism to make sure that earlier versions of firmware cannot be reinstalled and used maliciously.

3.1 Secured Boot

Secure boot main purpose is to validate the integrity and authenticity of the runtime binary during boot to verify that the downloaded RAM bootloader and firmware is signed by TI and has not been tampered with. Authorized firmware is firmware that came from the right entity, has the right attributes (for example, the right version), or is intended for the specific device. The secure boot is always the first code that runs on the device no matter what is the life cycle state. Implementing a secure boot process is critical to device integrity throughout the life cycle. A compromised boot process allows an attacker to inject malware, access assets or entirely replace the firmware running on the device. A secure boot process is essential to make other security features possible by providing the necessary degree of trust.

3.1.1 Secured Boot Container

To better understand how authentication is implemented, the concept of container is introduced. The container is a file that contains all the information and objects required to authenticate, verify, and install the update. This include the following:

- Binaries – RAM bootloader, MAC/PHY firmware of Wi-Fi/Bluetooth Low Energy
- Certificates – can be chained
- Signatures – tested against the root-of-trust-public-key
  - Version Information
  - Dependencies

Figure 3-1 illustrates a high-level container structure.

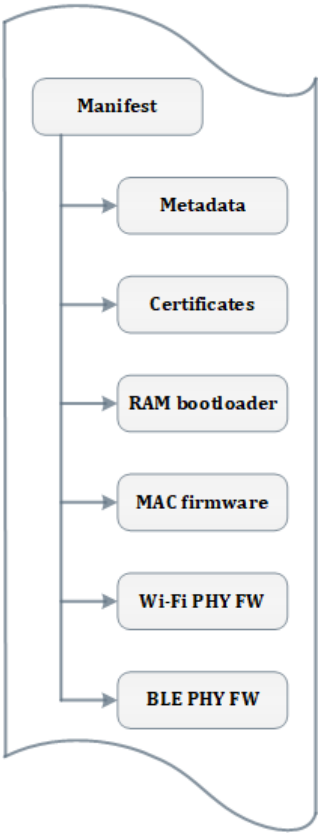

Figure 3-1. CC33xx Container

The container is released by Texas Instruments when an update is available and is used during device initialization either in operational mode through SDIO/SPI from the host or in debug mode through SWD lines from the toolbox utility.

3.1.2 Secured Boot Flow

During the boot flow, the container is parsed and programmed to the device. The different binaries are checked for authenticity against a root-of-trust public key that exists in ROM, and the matching private key is located on Texas Instruments servers.

Section 3.1.2 illustrates the boot flow.

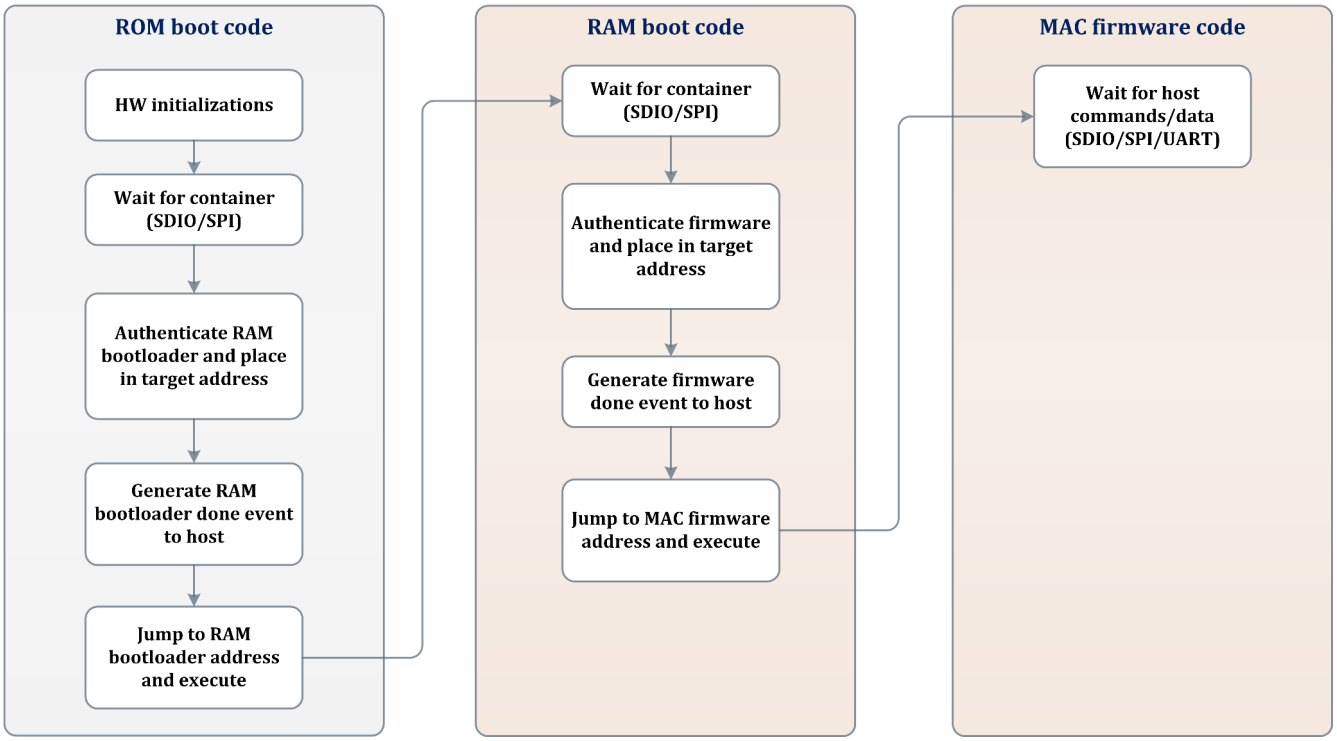

Figure 3-2. CC33xx Boot Flow

The boot flow is divided into two main phases, the ROM boot mode and the RAM boot mode. The logic behind this is to enable flexibility where the bootloader phase can be modified in case of detected bugs or added features but without compromising on security. Both bootloader sections are considered as running in privileged secure mode.

As part of the ROM bootloader phase, hardware is initialized. This step includes clock detection, PLL lock, fuse bits validation and more. Next is testing the mode or life cycle of the device. In most cases, the device are operational in functional mode but there are cases where the device can be in debug mode, test mode or some kind of failure mode. These modes are not covered in this document. Lastly on the ROM bootloader section, the RAM bootloader binary is delivered from the host processor in chunks and placed in the target location in RAM. This is done only after the binary is decrypted and authenticated against the root-of-trust public key. When this phase is over, an appropriate event is generated and propagated to the host processor.

As part of the RAM bootloader, similar procedure is done but this time with the rest of the binaries, including the Wi-Fi/Bluetooth Low Energy MAC firmware, the Wi-Fi PHY firmware and the Bluetooth Low Energy PHY firmware. When this phase is over, an appropriate event is generated and propagated to the host processor. At this point, the firmware is running and ready to get commands and data from the host processor.

3.2 Wi-Fi Network Security

The Wi-Fi layer of the CC33xx companion IC complies with 802.11 security to maintain the integrity and confidentiality of the frames (L2 data units) in transactions between AP and STA, or between two peers in the case of Wi-Fi direct mode. The security protocols are described in the IEEE 802.11 specifications and the extensions.

The Wi-Fi subsystem of the CC33xx companion IC provides support for both personal and enterprise security paradigms, including RADIUS-based authentication (802.1X).

> Wi-Fi Enterprise is not implemented inside the CC33xx companion IC but externally (for example, Wpa_supplicant and hostapd).

The CC33xx companion IC complies with Wi-Fi Alliance (WFA) security standards and test suites.

Table 3-2 lists the supported Wi-Fi security-related capabilities.

Table 3-2. Wi-Fi Security

Type	Wi-Fi Security
Personal	WPA-PSK (TKIP)
	WPA2-PSK (AES)
	WPS PBC + PIN
	WPA3 (SAE)
	PMF
Eneterprise (for station mode, GCMP long keys of 192 bits is supported)	EAP TLS
	EAP TTLS
	EAP TTLS-MSCHAP
	EAP PEAPv0-MSCHAP
	EAP PEAPv1-TLS

3.3 Rollback Protection

Rollback protection is a built-in HW mechanism to maintain that earlier versions of firmware cannot be reinstalled and used maliciously. The basic assumption is that vulnerabilities exist (typically implementation issues) and are detected over time. This is the reason the secure boot is partitioning into ROM and RAM to allow updating the secure boot code itself. The actual versions are held in fuse bits and reflect versions of the RAM bootloader, the different firmware binaries and the Texas Instruments certificate revocation list. Upon initialization, the versioned elements are tested such that the versions are equal or higher than configured.

The rollback protection mechanism contains up to 16 versions of the RAM bootloader and 32 versions of the firmware.

3.4 JTAG Protection

CC33xx companion IC also includes a 2-wires serial Wire Debug (SWD) interface. The SWD interface is not related to the host interface and can be used during boot time instead of the host interface for radio testing purposes. In general, the SWD interface is locked for development, debug and profiling of the software and hardware deployed on CC33xx, and is used by customers with the Radio Tool utility in the SimpleLink™ platform Wi-Fi Toolbox.

3.5 Secured Host Interface

> Host interface security is still under design and must be implemented in next phases. Nevertheless, host interface security is brought here for reference.

Secured host interface focuses on the traffic that is transferred from the host MCU/MPU subsystem to the CC33xx companion IC. A potential hacker can hijack the interface HW lines and use those lines to read confidential information like encryption keys, payload of data units and more. A hacker can also write to those lines and cause unwanted behavior of the device or give misleading events to the host controller as is illustrated in Figure 3-3.

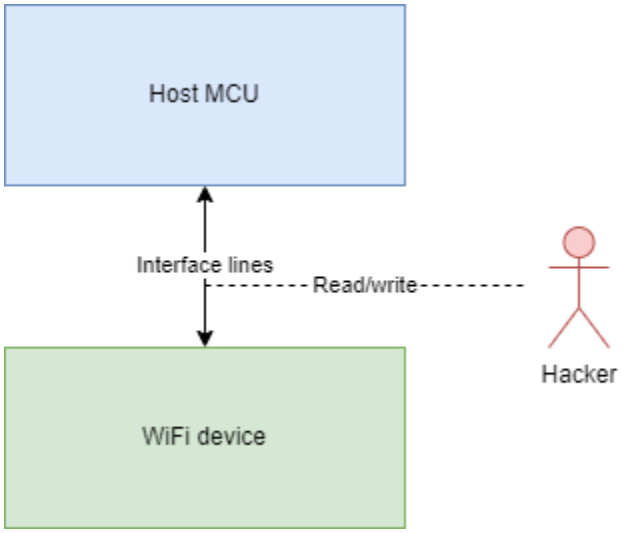

Figure 3-3. Host Interface Threat

4 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from Revision * (September 2023) to Revision A (January 2024)	Page
• Added 'JTAG Protection' feature to the main features list	1
• Moved the main features in order of importance	1
• Updated the 'Secured Host Interface" to remove misleading information	1
• Updated the 'CC33xx Boot Flow' figure to reflect the current status	1
• Updated the Wi-Fi Security suites	1
• Deleted 'Separate execution environment' feature to prevent confusion	1

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