Application Report

Wi-Fi® Enabled Electronic Smart Lock

Michelle Tate – SimpleLink™ Product Marketing Engineer
Benjamin Moore – SimpleLink™ Wi-Fi® Applications Manager
Bhargavi Nisarga – SimpleLink™ Systems Engineer

SimpleLink

ABSTRACT

This security application brief provides an example security analysis for Wi-Fi enabled electronic smart locks. The intent is to highlight various potential threat scenarios and corresponding steps to help combat them. This process includes the identification and ranking of potential threats and exploring relevant TI security enablers.

This brief leverages the first.org CVSS 3.1 calculator. All scoring in this brief is based on TI's assessment. Readers should adjust each parameter according to their targeted applications and system designs.

Table of Contents

Trademarks

1 Introduction

Traditional locks have been around for thousands of years, controlling who can access homes and buildings and acting as the first line of defense in a security system. As locks evolved into more complex systems with integrated electronic controls and wireless interfaces, they gained a new name: electronic smart locks (e-locks). In today's world, badges, fobs, pin numbers, mobile devices and even fingerprints are popular mediums to authenticate to a lock, in many cases eliminating the need for a physical key.

The growing need to protect assets by remotely monitoring and controlling entryways has increased the number of connected e-locks on the market.

Common use-cases for remotely accessing and controlling e-locks include:

- Granting temporary access for a home owner's guests
- Granting temporary access to delivery service personnel to drop off packages within facilities
- Managing central access at facilities with multiple access points and privilege levels

Adding connectivity such as Wi-Fi to an e-lock makes it easy to create and manage access keys at any time and from any place, while also providing a direct connection to the internet without the need for a gateway or hub. In addition to all of the benefits that connected e-locks bring, this connectivity also increases the number of exposure points vulnerable to security attacks.

E-locks must be designed with security in mind, providing access to an asset by locking out unauthorized users while remaining available for authorized users. Performing threat and risk assessments and identifying necessary security enablers can help mitigate the risk of a successful e-lock attack. Specifically, in this security application brief, the goal is to guide you in performing a security threat and risk assessment during your e-lock system design.

2 Residential and commercial e-locks

Residential e-lock system designs often place the e-lock on the exterior of a building to prevent initial entry. These exterior e-locks wirelessly connect back to the home gateway, which connects the e-lock to remote internet access as illustrated in Figure 2-1.

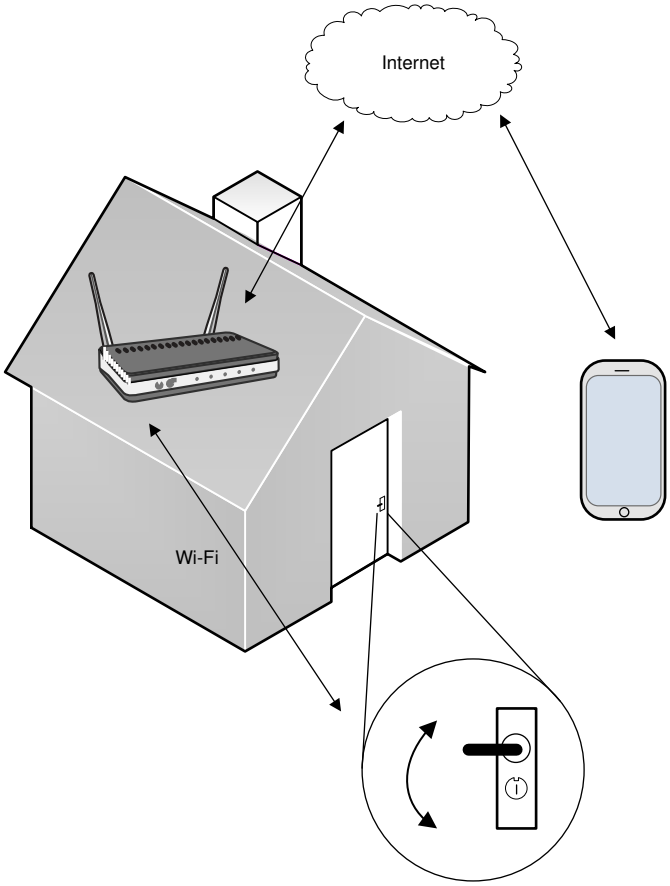

Figure 2-1. Residential e-lock system example

In commercial applications, locks are often located on both the exterior of a building to prevent initial entry and within the interior to restrict access to specific personnel. Depending on the size of the commercial building, interior e-locks may use multiple hops to connect from the initial entry location to a central building security system server. For example, in smaller hotels, each e-lock can wirelessly connect back to the central server in a single hop. In a large hotel, each floor will have a gateway supporting both wireless and wired communication, such as Wi-Fi and Ethernet. The e-locks on a particular floor connect to the corresponding gateway through wireless communication, with the gateway wired back to the central server. The addition of a central server in a commercial system enables building managers to quickly and easily push updates such as key changes to e-locks over the air.

Figure 2-2 showcases a common commercial e-lock system.

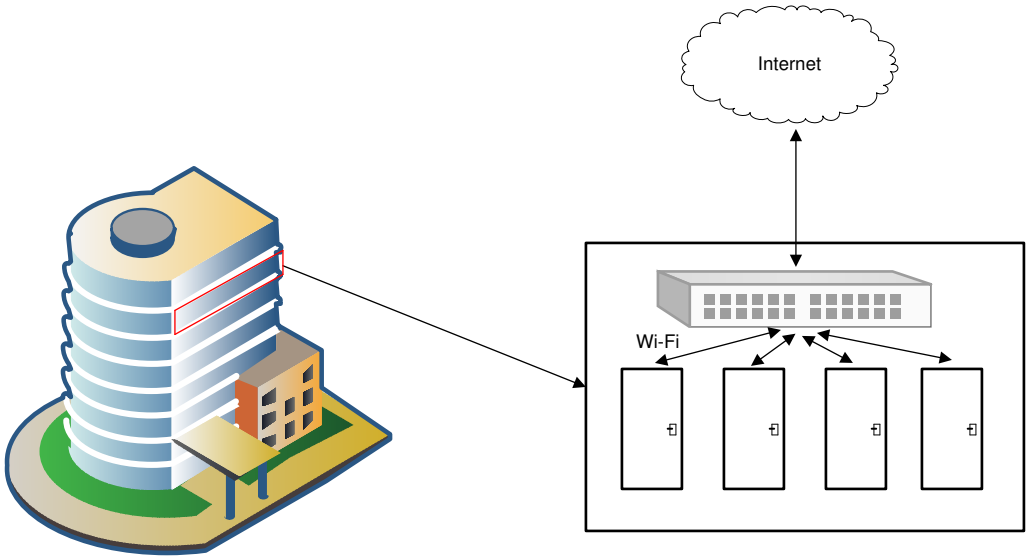

Figure 2-2. Commercial e-lock system example

3 Why would e-locks be the target of attacks?

Here are some typical examples of why e-locks would be the target of attacks:

- To access the assets that the e-lock is protecting
- To clone an e-lock product and sell it on the black market
- To use ransomware that causes the e-lock to be nonfunctional unless a ransom is paid to the attacker
- To compromise an e-lock and use it as a proxy to attack other nodes in a local area network (LAN) or central internet server, with a denial-of-service (DoS) attack, for example.
- To monitor consumer habits via e-lock usage and determine when to burglarize a house or facility

In the case of network-connected e-locks, the motivation for attacks can be much broader than just accessing assets protected by a single lock. The return on investment for the attacker(s) can also be greater. Attackers can exploit a security vulnerability in an e-lock or in other components of a network to compromise multiple e-locks in the field. For example, cloned or counterfeit e-lock products with pre-programmed malware (or software with unintentional vulnerabilities) that are enrolled onto the network can be used to perform scalable remote attacks by using a counterfeit node to spread malware to other devices or cause DoS attacks in the network.

Recalling the earlier bullet point about attackers who demand ransoms (usually from facilities like apartments, hotels or hospitals) to return the e-locks back to normal operation, these types of attacks often incur not just financial losses but reputational losses for both end-users and product makers. Connected products are also exposed to a bigger attack surface compared to non-connected locks; therefore connected products are vulnerable to both local and remote attacks. Attackers could potentially use a security vulnerability in an e-lock end node to compromise a local network, gateway or network server, which could have a larger impact on all stakeholders. For instance, if attacker can remotely inject malware into multiple e-locks (using a vulnerability in the e-locks themselves or in other network components), he/she to take control of multiple e-locks in field and carry out distributed DoS attacks (for example, flooding the server with data packets). Therefore, it is important to consider security for all network components, including the end-nodes.

Additionally, universities, research labs or other individuals may want to hack e-locks in order to expose product vulnerabilities and bring awareness to the Internet of Things (IoT) community about the importance of security in connected products.

With multitude of motivations to attack network connected e-locks, it's essential to understand the risks and severity of each of these attacks to design essential security measures to increase protection for these products.

4 Threats description and risk assessment

Risk assessment is essential to risk prioritization. Table 4-1 lists some of the common threats for electronic smart locks with Wi-Fi connectivity. Despite its length, this table is not an exhaustive list of all of the potential ways to compromise a particular security asset.

Table 4-1. Threat analysis and CVSS scoring

Threat	Threat Description	Threat Score	CVSS Link
E-lock takeover	Attacker injects malware via LAN or WAN attacks into device to read out security credentials from memory in order to gain access to customer assets or demand ransomware.	9.0	CVSS Calculation – 9.0
Unauthorized software updates in-field	Attacker sends unauthorized software updates remotely or performs software downgrade/ rollback attack on system in order to manipulate device operation	9.0	CVSS Calculation – 9.0
Unauthorized devices in cloud network	Attacker reads device identity out of memory via malware entry point and spoofs/ impersonates a device in order connect to cloud network	9.0	CVSS Calculation – 9.0
Unauthorized access to e-lock SW IP during device programming	Attacker at untrusted programming facility steals unprotected software images and uses them to clone e-lock IP during device manufacturing process	8.8	CVSS Calculation – 8.8
E-lock software confidentiality compromised	Attacker reads firmware directly out of device memory to perform more sophisticated exploits/attacks such as remote attacks on a larger scale	7.6	CVSS Calculation – 7.6
E-lock user privacy loss	Attacker reads personal or usage information (logs) stored on e-lock device via local interfaces to understand user patterns	6.2	CVSS Calculation – 6.2
Unauthorized access to local network	Attacker reads Wi-Fi network authentication keys/passwords directly from device memory (on-chip/off-chip)	5.7	CVSS Calculation – 5.7
Unauthorized access to local network	Attacker sniffs over-the-air traffic to steal Wi-Fi network authentication keys/passwords during provisioning	5.2	CVSS Calculation – 5.2

Note

The threat scores in this table are calculated using the Common Vulnerability Scoring System (CVSS) Version 3.1 Calculator. Because Transport Layer Security (TLS) is typical for Internet Protocol-based network-connected devices, the threat score calculations assume that TLS is supported and in use between the e-lock node and the remote server for all threat scenarios.

5 Identification of relevant TI security enablers and features

Texas Instruments (TI) has defined its security framework in *Building your application with security in mind* to provide an overview of why security matters, how to evaluate which security measures you need and how to implement these measures to protect against threats. The TI security framework also includes the main security enablers that TI offers to assist you in furthering your security objectives.

Table 5-1 maps the customer asset to TI security enablers.

Table 5-1. Mapping of customer asset to TI security enablers

Threat	Security Asset	Measures	Device Asset	Exposure Point	TI Security Enabler	Security Enabler Usage
E-lock take-over	E-lock device operation	• Secure transport when sending commands to authenticate user with e-lock system (control commands) • Non-volatile storage with encryption, authentication, and access control for programmed user access codes	• Device identity and keys • Code	Runtime Transfer	• Secure storage • Networking security • Secure Boot • Cryptographic acceleration	• Use of secure sockets when communicating with remote network (cloud) increases protection against a man-in-the-middle attack to inject malware. • Assuming that a malware could be injected through the network interface, file system security enables user files to be stored encrypted, signed, and with access restrictions to help reduce the risk of critical information, such as credentials, from being read out of non-volatile storage. • Storing application software with a signature enables validating software during the device boot operation to prevent execution of invalid software. • Cryptographic acceleration speeds up secure socket connections to reduce latency and save power when establishing connections to the cloud and sending/receiving commands. Cryptographic acceleration also supports the secure boot process by reducing the amount of time it takes to validate signatures and decrypt the application software.
Unauthorized software and firmware updates in-field	E-lock operation and availability	• Secured communication during transfer of firmware updates • Authenticated firmware updates • Secure boot to prevent execution of unauthorized images	Code	Transfer, Storage, Runtime,	• Networking security • Secure firmware and software update • Secure storage • Secure boot • Cryptographic acceleration	• Wi-Fi networking security increases protection against man-in-the-middle attacks during over-the-air updates. • Signature verification on downloaded firmware and software image bundles helps ensure integrity of updates and verify that they originate from a trusted source. • File system security enables the creation of files that are encrypted and authenticated (secure-signed) via a signature. The signature for a secure-signed file must be provided to the device and verified each time the file is written. • Software tamper protection monitors for invalid attempts to access write firmware in non-volatile memory and can lock file system to prevent access to software IP. • Secure boot enables the device to validate SW during the device boot operation to increase protection against execution of invalid software. Cryptographic acceleration reduces the time and power consumed while decrypting firmware and validating signatures during boot operation.
Unauthorized devices in cloud network	Customer cloud network resources (availability and security of cloud)	• Client authentication when devices are enrolled to network • Secure storage of client identity on the device	Device identity and keys	Storage, Runtime	• Device identity • Secure storage	• Use of 128-bit unique device IDs and built-in unique asymmetric key pairs to identify devices as genuine manufactured products. Device identity (unique device ID and unique key pair) can be used to generate a certificate signing request (CSR) which can be signed by an authority and used to enroll device in cloud network. • File system security enables private keys to be stored encrypted with access control.

Table 5-1. Mapping of customer asset to TI security enablers (continued)

Threat	Security Asset	Measures	Device Asset	Exposure Point	TI Security Enabler	Security Enabler Usage
Unauthorized access to e-lock SW IP during device programming	Customer software IP	Secure customer software images on the production line	Code, Data, Identity and keys	Transfer Storage	• Secure initial programming • Software IP protection • Cryptographic acceleration	• Secure initial programming allows the developer to use encrypted images on the production line and restrict system activation to a trusted individual/ environment. • Cloning protection (enabled by encrypting file system with device unique keys) helps reduce the risk of software IP being copied from one device to another in order to create additional clones of the system. • Cryptographic accelerators reduce time taken to encrypt/decrypt SW images during production programming.
E-lock software confidentiality compromised	E-lock Software IP confidentiality and integrity	• Prevent access to debug port after programming • Secure SW IP on the device • Secure boot to prevent execution of unauthorized images	Code	Runtime, Storage	• Debug security • Secure Storage • Software IP protection • Secure boot	• Disabling JTAG access and file-by-file access to file system when programming systems on the production line increases protection against attacker reading software IP directly from on-chip or external memory. • File encryption increases security against attacker reading software from non-volatile memory as plain text. • Software tamper protection monitors for invalid attempts to read firmware in non-volatile memory and can lock file system to prevent access to software IP. • Secure boot enables the device to validate SW during the device boot operation to increase protection against execution of invalid software.
E-lock user privacy loss	Customer's e-lock usage data (logs) and general personal data.	Secure logs and/or personal data stored on the device Encrypt sensitive user data when transferred locally or over network	Data	Storage, Transfer	• Secure storage • Networking Security • Keys • Cryptographic Acceleration	• File encryption, authentication, and access control helps protect sensitive data stored locally on system from being read out by an attacker. • Wi-Fi security and secure sockets can be used to increase protection when transferring data over local network. • Cryptographic utilities and accelerators can be used to add protection to sensitive information when transferred over physical interfaces.
Unauthorized access to local network	Wi-Fi password or authentication keys that protect communication data over local network	Secure storage and restricted access control to network credentials stored on the device	Keys	Storage, Runtime	• Secure storage • Separate execution environments	• File system security (encryption and access control) helps prevent network passwords or authentication keys stored locally on system from being directly read out of non-volatile memory by an attacker. • Separate execution environments for applications MCU and network processor enables access to keys to be limited to network processor subsystem after provisioning.
Unauthorized access to local network	Wi-Fi password or authentication keys that protect communication data over local network	Secured transport for provisioning system with network credentials	Keys	Transfer	Networking security	• Use of Wi-Fi security and secure sockets to protect local link between e-lock and device used for provisioning helps mitigate risks of attacker gaining access to Wi-Fi credentials during setup.

6 TI devices with security enablers

The SimpleLink™ Wi-Fi CC3235x and CC3220x devices offer a wide range of built-in security features to enable and assist designers with addressing e-lock security threats. Table 6-1 lists high-level descriptions of the main security enablers.

Table 6-1. Security enablers of SimpleLink WiFi CC3235x and CC3220x devices

Enabler	Detailed security features	TI device	
		SimpleLink CC3220S/SF	SimpleLink CC3235S/SF
Secure boot	Secure boot	✓	✓
Device identity/keys	Device identity Secure storage Trusted root-certificate catalog TI root-of-trust public key	✓	✓
Cryptographic acceleration	FIPS 140-2 level 1 certification		✓
	AES / DES / TDES / 3DES SHA / MD5 PKA (RSA) TRNG	✓	✓
Debug security	Debug security (enabled by default on production images)	✓	✓
Secure storage	File encryption File authentication File access control Factory image recovery File bundle protection File system security Software tamper detection	✓	✓
External memory protection	See secure storage features above	✓	✓
Networking security	Personal and enterprise Wi-Fi security • Wi-Fi Protection Access (WPA) • WPA2-Pre-Shared Key (PSK) • WPA2-Extensible Authentication Protocol (EAP) • WPA2 + Protected Management Frames (PMF) • WPA3 Secure sockets • Secure Sockets Layer (SSL) v3 • TLS 1.0/1.1/1.2 Hypertext transfer protocol secure server	✓	✓
	Online certificate status validation (OCSP)		✓
Secure firmware and software update	Networking security Firmware/software image authentication Bundle protection Factory image recovery	✓	✓
Initial Secure Programming	Encrypted programming image	✓	✓
Software IP protection	File system security Software tamper detection	✓	✓

Note

Cryptography is a constantly changing field. As new discoveries in cryptanalysis are made, older algorithms will be found unsafe. In addition, as computing power increases, the feasibility of brute force attacks will render known cryptosystems or the use of certain key lengths unsafe. Standard bodies such as The National Institute of Standards and Technology (NIST) should be monitored for recommendations.

7 Conclusion

The increasing number of connected locks on the market increases the risk of more complex and remotely performed security attacks. As we've shown in this security application brief, the ability to exploit a connected e-lock has greater security implications than just exploiting a single unconnected lock. This danger calls for threat and risk assessments more than ever in order to determine the security measures required to protect end-equipment assets.

Per security threats analysis, the most critical attacks to consider are those instrumented with malware or those that result in unauthorized software updates, which can lead to an entire system takeover and the potential exposure of confidential assets such as software IP, device identities and keys, and personal data. It is also important to reduce the risk of unauthorized access to software IP, which could allow system cloning or reverse-engineering of software with the intent of exposing vulnerabilities and performing more sophisticated attacks on a larger scale.

Equipped with important security enablers – networking security, secure storage through the file system security, debugging security, software IP protection, built-in device identity, TI root of trust, secure boot, and support for secure software/firmware updates – the CC32xx device series can help you with designing necessary security solutions for your e-lock application and system.

8 References and related documentation

- Texas Instruments: *SimpleLink™ Wi-Fi® Enabled Electronic Smart Lock*
- Texas Instruments: *Understanding security features for SimpleLink™ Wi-Fi® CC32xx MCUs*
- Texas Instruments: *CC3x20, CC3x35 SimpleLink™ Wi-Fi® Internet-on-a Chip™ Solution Built-In Security Features*
- Common Vulnerability Scoring System Version 3.1 Calculator

9 Revision History

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

Changes from Revision * (September 2019) to Revision A (September 2020)	Page
• Updated the numbering format for tables, figures, and cross-references throughout the document	2
• Updated Table 6-1, *Security enablers of SimpleLink WiFi CC3235x and CC3220x devices*	8

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