

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

SCTE STANDARD

SCTE 256 2019

**IoT Security Considerations and Recommendations
for Operators**

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Table of Contents

Title	Page Number
NOTICE	2
Table of Contents	3
1. Introduction	6
1.1. Executive Summary	6
1.2. Scope	6
1.3. Benefits	7
1.4. Intended Audience	7
1.5. Areas for Further Investigation or to be Added in Future Versions	7
2. Normative References	7
2.1. SCTE References	7
2.2. Standards from Other Organizations	7
2.3. Published Materials	7
3. Informative References	7
3.1. SCTE References	7
3.2. Standards from Other Organizations	7
3.3. Published Materials	8
4. Compliance Notation	8
5. Abbreviations and Definitions	8
5.1. Abbreviations	8
5.2. Definitions	10
6. Product Selection	10
6.1. Cybersecurity Responsibilities	10
6.1.1. Vendor	10
6.1.2. Service Provider Internal	11
6.1.3. Customer	11
6.2. Hardware Security Recommendations	11
6.2.1. Persistent Memory	11
6.2.2. Non-Persistent Memory	12
6.2.3. Secure Cryptographic Operations	13
6.2.4. Communication Ports	13
6.2.5. Physical Security	13
6.2.6. Power Supply	14
6.2.7. Development vs Production	15
6.3. Firmware Security Recommendations	15
6.3.1. Coding Security Practices	15
6.3.2. Bootloader	16
6.3.3. Firmware Download	19
6.3.4. Network Protocols	20
6.3.5. Passwords	21
6.3.6. User Interface (UI) Security	22
6.3.7. Certificate and Key Management	22
6.3.8. Miscellaneous	23
6.4. Recommended Vendor Responsibilities for the Life of the Product	25
6.4.1. Point of Contact	25
6.4.2. Public Disclosure	25
6.4.3. Vulnerability Notification	26
6.4.4. Attack Notification	26
6.4.5. Firmware Updates for Security Vulnerabilities and Attacks	27
6.5. Branding	27
6.6. Security Qualification	27
7. Retail Products	28

7.1.	Branding	28
7.2.	Qualification Process	28
7.3.	Retail Firmware	28
8.	Provisioning	29
8.1.	Security Onboarding	29
8.2.	Secure Delivery of Provisioning Transactions	29
8.3.	Secure Provisioning Database	29
8.4.	Confirmation of Provisioning	30
8.5.	Whitelisting/Blacklisting	30
8.5.1.	Whitelist System	30
8.5.2.	Blacklist System	31
9.	Cybersecurity Maintenance	32
9.1.	Firmware Upgrades	32
9.2.	Device and Platform Auditing	32
10.	Diagnostics	32
10.1.	Logs	32
10.2.	Alerts	33
11.	Attack Management Planning	33
11.1.	Vendor	33
11.2.	Service Provider Internal	33
11.3.	Customer Notification	33

List of Tables

Title	Page Number
Table 1 - Persistent Memory Recommendations	12
Table 2 - Non-Persistent Memory Recommendations	13
Table 3 - Secure Storage/Processing Recommendations	13
Table 4 - Communication Ports Recommendations	13
Table 5 - Physical Security Recommendations	14
Table 6 - Power Supply Recommendations	15
Table 7 - Development vs Production Recommendations	15
Table 8 - Development vs Production Recommendations	16
Table 9 - Bootloader Memory Storage Recommendations	17
Table 10 - Bootloader and Firmware Validation Recommendations	18
Table 11 - Bootloader Secondary Functions Recommendations	18
Table 12 - Firmware Download Security Recommendations	20
Table 13 - Network Protocol Security Recommendations	21
Table 14 - Password Security Recommendations	22
Table 15 - User Interface Security Recommendations	22
Table 16 - Certificate and Key Management Security Recommendations	23
Table 17 - Documentation Security Recommendations	24
Table 18 - Point of Contact Recommendations	25
Table 19 - Public Disclosure Recommendations	25

Table 20 - Vulnerability Notification Recommendations	26
Table 21 - Attack Recommendations	26
Table 22 - Firmware Update for Security Vulnerabilities and Attacks Recommendations	27
Table 23 - Service Provider Purchased Product Branding Recommendations	27
Table 24 - Security Qualification Recommendations	28
Table 25 - Retail IoT Devices Branding Recommendations	28
Table 26 - Retail IoT Devices Qualification Recommendations	28
Table 27 - Retail Firmware Recommendations	29
Table 28 - Secure Delivery of Provisioning Transactions Recommendations	29
Table 29 - Secure Provisioning Database Recommendations	29
Table 30 - Confirmation of Provisioning Recommendations	30
Table 31 - Whitelist System Recommendations	30
Table 32 - Blacklist System Recommendations	31
Table 33 - Firmware Upgrade Recommendations	32
Table 34 - Device & Platform Auditing Recommendations	32
Table 35 - Logs Recommendations	32
Table 36 - Alerts Recommendations	33
Table 37 - Vendor Attack Management Recommendations	33
Table 38 - Service Provider Internal Attack Management Recommendations	33
Table 39 - Customer Notification Attack Management Recommendations	34

1. Introduction

1.1. Executive Summary

This document contains considerations and recommendations for operators with regards to the security aspects of deploying hardware/software/services in the IoT space. It is the result of the SCTE DSS IoT Working Group – Security Subgroup.

These are recommendations and should not be considered to be requirements. The final design is the responsibility of the implementer.

1.2. Scope

The following areas are covered within this document:

1. Cybersecurity Responsibilities
 - a. Vendor
 - b. Service provider
 - c. Customer
2. Product selection (for Service Provider equipment)
 - a. Hardware security recommendations
 - b. Firmware security recommendations
 - c. Suggested vendor responsibilities for the life of the product
 - i. Vulnerability notification
 - ii. Attack notification
 - iii. Mitigation
 - iv. Firmware updates for security vulnerabilities
 - d. Branding
 - e. Qualification
3. Retail Products [customer owned and managed (COAM)]
 - a. Qualification process
4. Provisioning
 - a. Security onboarding
 - b. Secure delivery of provisioning data
 - c. Secure provisioning database
 - d. Confirmation of provisioning
 - e. Secure confirmation management and storage
 - f. Blacklisting
5. Maintenance
 - a. Firmware upgrade
 - b. Device and platform auditing
6. Diagnostics
 - a. Logs
 - b. Alerts
7. Attack management planning
 - a. Vendor
 - b. Service provider internal
 - c. Customer notification

1.3. Benefits

This document will be used to provide the following benefits:

- Educate the service providers on the infrastructure required to support IoT security
- Develop a common baseline architecture for IoT security such that different operators can use the same or similar tools and platforms

1.4. Intended Audience

The intended audience are the engineering and security teams for service providers.

1.5. Areas for Further Investigation or to be Added in Future Versions

As technology in the IoT space evolves, this document should be reviewed and updated and/or revised where necessary per SCTE policy.

2. Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1. SCTE References

- No normative references are applicable.

2.2. Standards from Other Organizations

- No normative references are applicable.

2.3. Published Materials

- No normative references are applicable.

3. Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

3.1. SCTE References

- No informative references are applicable.

3.2. Standards from Other Organizations

- OCF Core Framework (https://openconnectivity.org/specs/OCF_Core_Specification_v2.0.2.pdf)
- OCF Security (https://openconnectivity.org/specs/OCF_Security_Specification_v2.0.2.pdf)

- OCF Bridging (https://openconnectivity.org/specs/OCF_Bridging_Specification_v2.0.2.pdf)
- OCF Smart Home Device (https://openconnectivity.org/specs/OCF_Smart_Home_Device_Specification-v2.0.2.pdf)
- OCF Wi-Fi Easy Setup (https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification_v2.0.2.pdf)
- OCF Cloud (https://openconnectivity.org/specs/OCF_Cloud_Specification_v2.0.2.pdf)
- RDK Security Guidelines (<https://wiki.rdkcentral.com/display/RDK/Security+Guidelines?preview=/8388899/8390789/Security%20Coding%20for%20RDKV2.pdf>)
- The Update Framework (<https://theupdateframework.github.io>)

3.3. Published Materials

- National Institute of Standards Security Framework
<https://www.nist.gov/cyberframework>

4. Compliance Notation

<i>shall</i>	This word or the adjective “ <i>required</i> ” means that the item is an absolute requirement of this document.
<i>shall not</i>	This phrase means that the item is an absolute prohibition of this document.
<i>forbidden</i>	This word means the value specified shall never be used.
<i>should</i>	This word or the adjective “ <i>recommended</i> ” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighted before choosing a different course.
<i>should not</i>	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
<i>may</i>	This word or the adjective “ <i>optional</i> ” means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.
<i>deprecated</i>	Use is permissible for legacy purposes only. Deprecated features may be removed from future versions of this document. Implementations should avoid use of deprecated features.

5. Abbreviations and Definitions

5.1. Abbreviations

Acronym	Definition
AAA	authentication, authorization, and administration
AC	alternating current
bps	bits per second
CA	certificate authority
COAM	customer owned and managed

Acronym	Definition
CPE	customer premise equipment
CPU	central processing unit
CRC	cyclic redundancy code
DC	direct current
DHCP	Dynamic Host Configuration Protocol
DNS	domain name system
DNS RPZ	domain name service response policy zones
DNSSEC	domain name system security extensions
DOCSIS	Data-Over-Cable Service Interface Specifications
DRAM	dynamic random access memory
DSM-CC	digital storage media – command & control
DSS	Data Standards Subcommittee (of the SCTE)
EEROM	electrically erasable read only memory
FIPS	Federal Information Processing Standard
FLUTE	file delivery over unidirectional transport
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HDD	hard disk drive
HFC	hybrid fiber/coax
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
IV	initialization vector
JTAG	Joint Test Action Group (IEEE Standard 1149.1-1990)
LED	light emitting diode
MAC	media access control
OCF	open connectivity foundation
OS	operating system
PCB	printed circuit board
POC	point of contact
QA	quality assurance
RDKit	reference design kit
ROM	read only memory
SCTE	Society of Cable Telecommunications Engineers
SD	secure digital
SNMP	Simple Network Management Protocol
SoC	system on chip
SRAM	static random access memory
SSH	secure shell
SSM	source-specific multicast
TFTP	trivial file transfer protocol
TR	technical report
UI	user interface
URL	uniform resource locator
USB	universal serial bus

5.2. Definitions

The following are the definitions used within this document.

Term	Definition
asymmetric encryption	Also called public-private key cryptography. Utilizes one key to encrypt and a different key to decrypt.
attack	Any cybersecurity method which is actively being used to gain access to or control of an IoT device or the data associated with an IoT device.
authentication	Methods used to ensure that data comes from a specific user. Assumes that a trust has been established between the service provider and the vendor.
bad actor	A cybersecurity adversary that is interested in attacking information technology systems.
brownout	A reduction in the electrical voltage, either intentional or unintentional, over any period of time from 1 msec to days. Brownouts can cause unintentional behavior in digital circuits.
cybersecurity	The technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks.
downstream	Information flowing from the hub to the user
dropout	A loss of electrical voltage, either intentional or unintentional, over any period of time from 1 msec to days.
encryption	Encoding a message in a way that only authorized users can access it, usually requiring a key. Encryption is a higher order of obfuscation.
IoT	Internet of Things (IoT) devices have the ability to connect to the Internet either directly or indirectly (via a bridge) to provide greater functionality.
obfuscation	Method used to mask data except for authorized users. It can be simple, e.g., reversing the order of bits, exclusive or with a known value, etc., or complicated such as with encryption.
persistent memory	Any memory device which retains the data when there is no power.
symmetric encryption	The same key can be used for the encryption and decryption of data.
upstream	Information flowing from the user to the hub
vulnerability	Any cybersecurity method which could be used to gain access to data or control of an IoT device or the data associated with an IoT device.

6. Product Selection

6.1. Cybersecurity Responsibilities

6.1.1. Vendor

The vendor is the responsible party for implementing and maintaining the cybersecurity practices in the development and support of their products and/or services. It is expected that they will meet or exceed all guidelines mentioned in this document.

Vendors are expected to have a third party audit and review their cybersecurity practices including all hardware and software development, and support practices for products and/or services.

6.1.2. Service Provider Internal

The service provider is the responsible party for implementing and maintaining the cybersecurity practices in the deployment and support of their products and/or services in conjunction with the vendors. This includes integration of all products required for a service. It is recommended that they will meet or exceed all guidelines mentioned in this document.

Service providers should have a third party audit and review their cybersecurity practices including all product and system development, and support practices for their products and/or services.

6.1.3. Customer

It is known that there are limitations on what the vendor and service provider can provide to the customer with regards to cybersecurity. There needs to be a balance between customer privacy and customer cybersecurity. Therefore, cybersecurity is the responsibility of the vendor and service provider to determine that balance and is outside the scope of this document.

6.2. Hardware Security Recommendations

No single level of security fits all devices and deployments. The service provider and vendor are expected to work together to select a security/cost relationship that is acceptable for the deployment based upon risk and the impact of a potential exploit.

6.2.1. Persistent Memory

Persistent memory is any memory that retains the data when power is not applied. Examples include flash memory, battery backed up memory, serial electrically erasable read only memory (EEROM), and hard disk drives (HDD). It can include firmware and configuration and general data. Configuration data includes critical data such as the device ID (e.g., MAC address) and encryption keys (e.g., root of trust, certificates), and non-critical data such as customer settings and operation rules.

Persistent memory probes are a common method to locate vulnerabilities. This allows people to read the firmware programs to probe to look for vulnerabilities.

While encryption of the firmware would be ideal, this is generally not practical for some IoT devices. However, obfuscation can add enough complexity to thwart most probes and is relatively simple to implement. Some examples are to swap address lines, swap data lines, and/or logically “exclusive or” all data with known values.

Under all conditions, data integrity needs to be insured by using error detection mechanisms such as hashes or cyclic redundancy codes (CRC) as well as redundancy for critical configuration data, such as the media access control (MAC) address or encryption keys.

If there is an error detected in the firmware, then the firmware should have a mechanism that puts the device in a “safe” mode that minimizes network interaction other than to download new firmware, or if not, cease all operation and be considered as a failed unit. If there are any methods to display status to the user in the device, (e.g., light emitting diodes, or LEDs), then discovering types of problems could potentially be made easier if there is a specific pattern displayed on the LED to indicate type of failure.

If there is an error detected in the critical configuration data, then redundant entries should be validated, and if validated, utilize this value. If there is no validated configuration, then the device should cease all functionality and be considered as a failed unit. If there are any user indicators (e.g., LEDs) in the device,