Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 22 November 2025

B. Wang, Ed.
X. Wang, Ed.
L. Wan, Ed.
Hikvision
W.Y. Xu, Ed.
Zhejiang University
C.H. Wang, Ed.
IIE, CAS
H.N. Yan, Ed.
Xidian University
Y.H. Xie, Ed.
Hikvision

21 May 2025

Security Technical Specification for Smart Devices of IoT
draft-wang-iot-devices-security-07

Abstract

As IoT adoption accelerates, securing smart devices emerges as a critical priority. This proposal outlines a comprehensive security framework spanning hardware integrity, system reliability, data protection, network safeguards, and management controls. The framework mandates secure hardware interfaces, firmware validation mechanisms, robust data encryption protocols, encrypted communication channels, and systematic security auditing processes to ensure end-to-end protection across device ecosystems.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 22 November 2025.

Table of Contents

1. Preface

The new paradigm of IoT is recognized as one of the most important actors in the Information and Communication Technology industry for next years [Miorandi2012]. The introduction of IPv6 [RFC6568] and CoAP [RFC7252] as fundamental building blocks for IoT applications allow connecting IoT hosts to the internet. [RFC7744] provides an overview of relevant IoT use cases. With the development of IoT in recent years, the industry of smart devices gains great momentum, resulting in a large-scale production and application of smart devices. However, the absence of unified security standards leads to various security defense measures, which imposes huge threats on IoT security. Until today, smart devices have become favored targets for hackers, which leads to frequent security incidents. [Qiu2020] and [Neshenko2019] conducted a detailed survey on the security issues of IoT.

This draft proposes detailed security requirements to ensure smart devices can work in a security condition.

2. Scope

This draft proposes some basic security requirements that should be met by smart devices in the IoT."

This draft aims to specify the security functions of smart devices in the IoT, with the goal of improving device security. By implementing these functions, devices can be protected from malicious exploitation by attackers, safeguarding users' sensitive data.

This draft also serves as a guide for instructing the design and implementation of security functions in smart devices within the IoT.

3. Terms and Definitions

3.1. Smart device

A smart device is a type of device that can perceive and process various types of data, including video data, image data, and other forms of data. Examples of smart devices include video cameras, laser radar, and identity gateways. These smart devices can be directly connected to the IoT platform or can function as sub-devices connected through a gateway.

3.2. Smart Video Surveillance Device

A video surveillance device is a common example of a smart device that can capture and process video images while communicating with other devices through the internet.

3.3. Sensitive Information

A video surveillance device is a common example of a smart device that can capture and process video images while communicating with other devices through the internet.

3.4. Vulnerability

A flaw in the specific implementation of a software (hardware or protocol) or the security strategy of a system, leaving it open to the potential for exploitation in the form of unauthorized access or malicious behaviors.

3.5. Brute Force Attack

Check all possible passwords systematically to find the correct one.

3.6. Network Port

Network port is an endpoint of communication in an operating system, which identifies a specific process or a type of network service running on that system, such as service ports in TCP/IP with port numbers ranging from 0 to 65535.

3.7. Video Stream

The data stream of video information in network transmission.

3.8. Device Activation

To set the administrator’s password when the user uses the device for the first time, and the password must meet the requirements of password security policy.

4. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this draft: Abbreviations and Acronyms | Full Name --------|-----: JTAG | Joint Test Action Group IP | Internet Protocol TLS | The Transport Layer Security Protocol HTTPS | Hypertext Transfer Protocol Secure SSH | The Secure Shell Protocol SFTP | Secure File Transfer Protocol OTP | One Time Programmable Read Only Memory TEE | Trusted Execution Environment Table: Abbreviations and Acronyms

5. Overview

The framework of IoT consists of three layers. From bottom to top, they are the perception layer, the network layer and the application layer. Smart devices reside in the perception layer, aim to sense physical phenomena and translate them into a stream of information data. Furthermore, they interact with IoT platform through communication modules. The framework of smart devices is shown as follow:

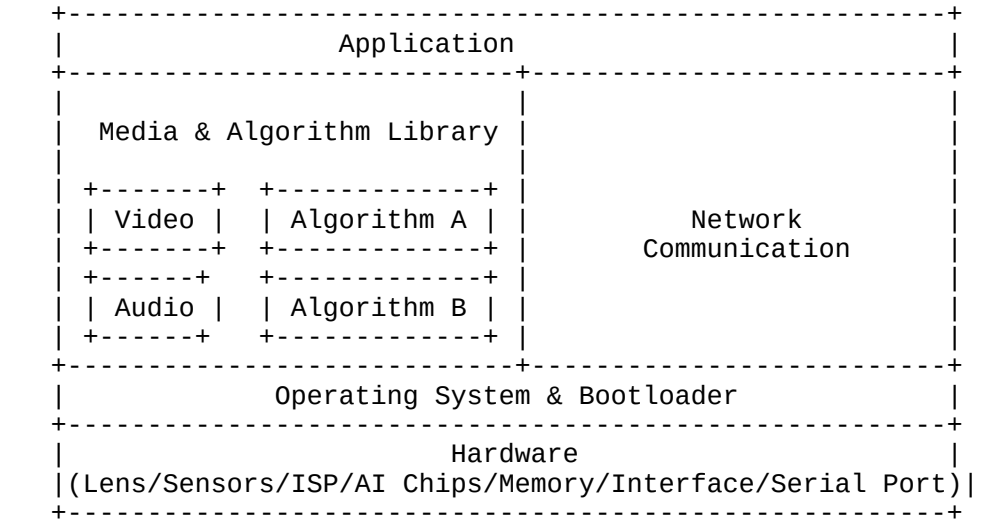

Figure 1: Framework of smart devices

The draft adopts the strategy of layered security and multi-level defense, and proposes a security function framework of smart devices, shown as follow:

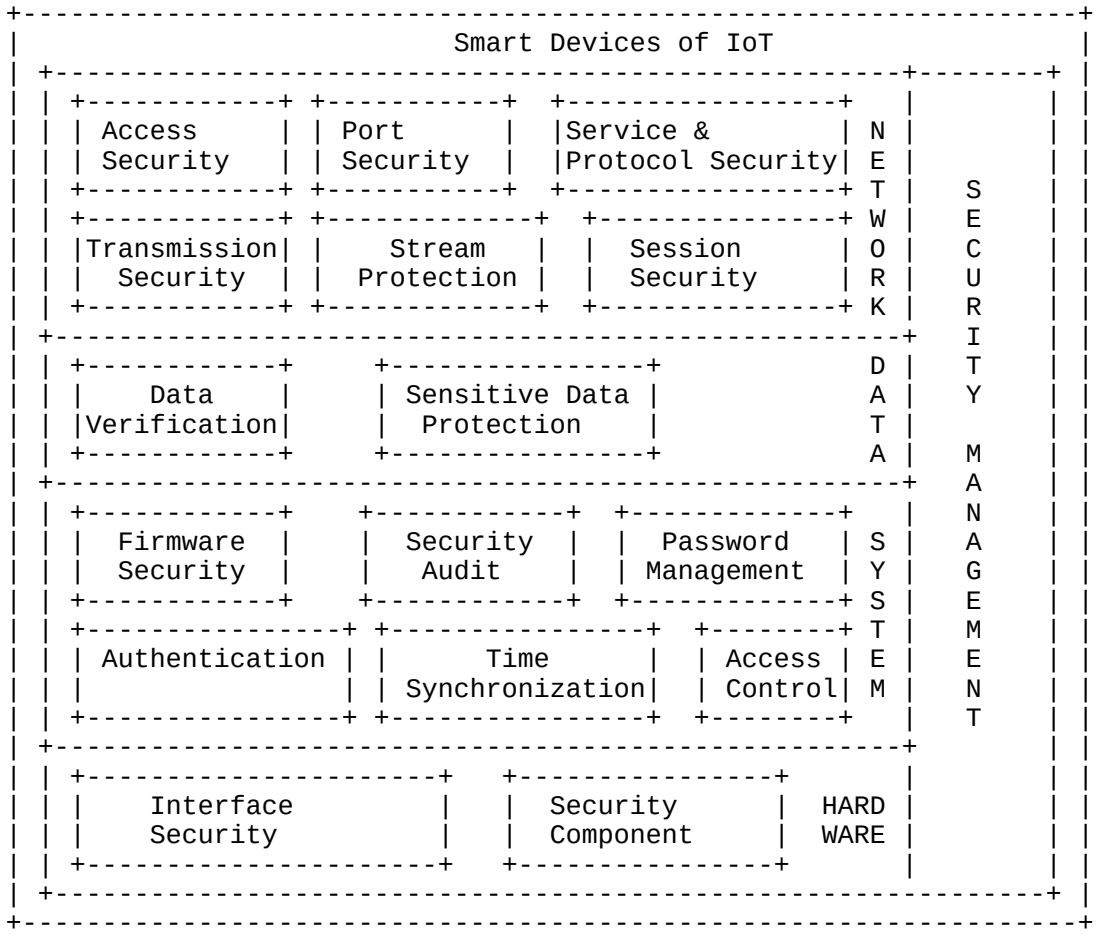

Figure 2: Security function framework

Hardware security mainly focuses on the hardware features of the device, including two aspects: 1.Whether there are any unused hardware interfaces on the device. 2.Whether the device can provide better security support due to the security components.

System security refers to the secure application of the device’s software resources, including the bootloader, operating system, and applications.

Data security aims to protect the data in the device, including device management data and user business data. Special attention should be paid to sensitive data.

Network security ensures the security of the connection to the IoT's network layer and protects against network attacks.

Security management primarily involves securely using and managing smart devices.

6. Security Function Requirement

6.1. Hardware Security

Hardware security encompasses interface security and security components. Interface security ensures that the device does not expose any physical interfaces with security risks. Security components, on the other hand, prioritize the inclusion of hardware with security function support during the hardware design process.

6.1.1. Interface Security

Before the smart devices leave the factory

a) JTAG debugging interface should be disabled.

b) Serial ports should be disabled, or improved by developing an authentication mechanism.

6.1.2. Security Components

a) For the smart device, chips that support OTP, Secure boot and TEE are recommended. The relevant security functions should be enabled.

b) If possible, it is recommended to add a security chip with cryptography service function. The selection of security chip should follow the corresponding national cryptography management policy.

6.2. System Security

System security includes firmware security, time synchronization, cryptography management, authentication, security audit,access control, and etc.

6.2.1. Firmware Security

a) The firmware should only contain the necessary components and applications.

b) For third-party open source software, the version without known vulnerabilities (or has been patched) should be used.

c) Debug codes in the device should be deleted before device leaves the factory.

d) Administrator should have access to check the current version of the device.

e) Firmware upgrading should be available.

f) When generated, firmware upgrade packages should be digitally signed.

g) The signature information of the upgrade package should be verified when upgrading.

6.2.2. Time Synchronization

The smart device should have real-time clock and support time synchronization calibration function.

6.2.3. Cryptography Management

a) The smart device should apply publicly standard algorithms.

b) The smart device should apply industry standard cryptographic algorithm and regularly assess and update the encryption algorithm and its strength.

c) The smart device should apply secure random numbers.

d) The smart device should forbid the hard coding of secret key.

e) The smart device should apply irreversible encryption algorithm in the scenario where the recovery of the password’s plaintext is not required.

6.2.4. Authentication

a) Users’ accounts should be unique.

b) At least two user roles should be set: administrator and user.

c) When the user account is deleted, the corresponding online user should be logged out.

d) Permissions assigned to administrators and users should be different.

e) Users can manage and control the device only after successful authentication.

f) If adopted, a random password should be generated as default before device leaves the factory. The user should be prompted to change the default password.

g) If an activation mechanism is adopted, the user should set a secure password that meets security requirements when initializing the device.

h) Password complexity check should be in place, and the password should have at least 8 characters, with at least two kinds of the following types: numbers, lowercase, uppercase and special character.

i) The password entered by the user must be masked by default, and the password copying must be disabled.

j) The password should be encrypted when stored and transmitted.

k) The authentication for remote access users should be performed on the server.

l) The feedback should not include clear reasons for the authentication failure and should prompt the user with "user name or password error".

m) Illegal login lock should be applied to defend against brute force attacks during user authentication. Login attempts from the IP address or account will be rejected for a period of time if it has been failed for certain times.

6.2.5. Access Control

a) For the smart device, the access to video streams should be authenticated and authorized.

b) Only the administrator has the privilege to import (or export) the parameter profile of the device.

c) Only the administrator has the privilege to use interactive command console.

d) The command console must not provide user management commands.

6.2.6. Security Audit

a) The smart device should support security audit function. Operations that need to be audited include the following:

1. Enabling or disabling the security audit function;

2. User creation, deletion or modification;

3. User login and logout;

4. Upgrade or update of the firmware;

5. Changes of the device configuration.

b) The audit information should include account, IP address, operation time, operation type and operation result, etc.

c) The handling mechanism, such as loop coverage or warning, should be in place for scenario where the size of logs is over the preset limit.

d) Only authenticated users have the privilege to view logs.

e) Log information should be presented in a form that is easy for users to understand.

6.3. Data Security

6.3.1. Data Verification

The IoT smart device should check the validity of the input data, and this process should be carried out on the server.

6.3.2. Sensitive Data Protection

a) For the smart device, internal sensitive information, such as passwords, configuration information, should be stored as cipher text.

b) For the smart device, sensitive information should be encrypted when transmitted.

c) For the smart device, log records and information printouts should not contain any sensitive information.

d) For the smart device, user interfaces for local, remote, web, and other operations should not show sensitive information.

6.3.3. Data Storage Security:

a) Implement tiered storage strategies to segregate data according to its sensitivity, using either physical separation across different drives or logical separation through virtualization.

b) Employ redundancy for data backups to ensure availability and facilitate restoration in the event of media malfunction or data loss.

c) Enable traceability after storage to track and audit data leaks, utilizing techniques like watermarking for source identification.

d) Ensure data confidentiality and integrity during storage to prevent unauthorized data acquisition and detect alterations, applying traditional cryptographic algorithms such as encryption, hashing, and digital signatures.

6.4. Network Security

6.4.1. Access Security

a) The smart device should have unique network identifier.

b) If the device accesses the network layer via wireless networks, such as Wi-Fi, the wireless network protection mechanism, such as WPA2, should be applied.

6.4.2. Port Security

a) The smart device should only enable the necessary network port by default.

b) All available network ports of the device should be open to users.

6.4.3. Service and Protocol Security

a) The smart device should apply secure protocols, including but not limited to TLS, HTTPS, SSH, SFTP, etc.

b) The smart device should remove high-risk services, including but not limited to telnet service, FTP service, etc.

c) The on-off mechanism of the service should be provided and be off by default when protocols with imperfect security mechanism are applied. A security risk alert is required when the user apply for the service using these insecure protocols.

d) If a Web service is provided, the Web security mechanism should be implemented, including checking the validity of input and output, and taking measures to prevent code vulnerabilities such as authentication vulnerabilities, permission vulnerabilities, session vulnerabilities, injection vulnerabilities, file upload vulnerabilities, etc.

6.4.4. Session Security

a) The smart device should allow the user to initiatively end the communication.

b) The session should be ended if there is no operation for a long duration, and the duration time can be set by the administrator.

c) The smart device should restrict the address of remote connections, such as IP address filtering, etc.

d) Limit the number of concurrent network connections.

6.4.5. Transmission Security

a) The smart device should provide a trusted communication path (Such as TLS) for the remote user to protect the communication data from leakage.

b) Remote users should be allowed to initiate communication via a trusted path.

c) A trusted path is required when processing user authentication.

d) A trusted path between the device and another trusted IT product should be provided to protect communication data from modification or leakage.

6.4.6. Video Stream Protection

The smart device should use cryptographic mechanisms to protect the integrity and confidentiality of video streams during transmission.

6.5. Application Security

6.5.1. Application Signing

The smart device must employ cryptographic mechanisms to protect the integrity of applications running in it. Applications that have been tampered with or of unknown origin should be forbidden to run.

6.5.2. Third-party Component Security

In the design and development phase, it requires security reviews for any third-party components (TPCs) embedded in the applications of smart devices.

6.6. Security Management

a) The smart device should be able to be managed and configured remotely.

b) The smart device should be able to inquire and export log information.

c) The smart device should be able to upgrade firmware remotely.

d) The smart device should be able to manage activation/non-activation service remotely.

e) The smart device should follow a lifetime policy, which clarifies the security risks of overdue and declares that manufacturer will no longer update firmware of the device if overdue.

7. Security Considerations

This entire memo deals with security issues.

8. IANA Considerations

This documents has no IANA actions.

9. Informative References

[Miorandi2012]
Miorandi, D., Sicari, S., Pellegrini, F.D., and I. Chlamtac, "Internet of things: Vision, applications and research challenges", 2012, <https://doi.org/10.1016/J.ADHOC.2012.02.016>.

[Neshenko2019]
Neshenko, D., Bou-Harb, E., Crichigno, J., Kaddoum, G., and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", 2019, <https://doi.org/10.1109/COMST.2019.2910750>.

[Qiu2020] Qiu, J., Tian, Z.h., Du, C.l., Zuo, Q., Su, S., and B.x. Fang, "A Survey on Access Control in the Age of Internet of Things", 2020, <https://doi.org/10.1109/JIOT.2020.2969326>.

[RFC6568] Kim, E., Kaspar, D., and JP. Vasseur, "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", DOI 10.17487/RFC6568, April 2012, <https://www.rfc-editor.org/info/rfc6568>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7744] Seitz, L., Ed., Gerdes, S., Ed., Selander, G., Mani, M., and S. Kumar, "Use Cases for Authentication and Authorization in Constrained Environments", DOI 10.17487/RFC7744, January 2016, <https://www.rfc-editor.org/info/rfc7744>.

Authors' Addresses

Bin Wang (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China
Phone: +86 571 8847 3644
Email: wbin2006@gmail.com

Xing Wang (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China
Phone: +86 571 8847 3644
Email: xing.wang.email@gmail.com

Li Wan (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China

Phone: +86 571 8847 3644
Email: dzwanli@126.com

Wenyuan Xu (editor)
Zhejiang University
866 Yuhangtang Rd
Hangzhou
310058
China
Email: wyxu@zju.edu.cn

Chonghua Wang (editor)
IIE, CAS
Beijing
100093
China
Phone: +86 185 1894 5987
Email: chonghuaw@live.com

Haonan Yan (editor)
Xidian University
No. 8, Qiannong East Road, Xiaoshan District
Hangzhou
310051
China
Email: yanhaonan.sec@gmail.com

Yinghui Xie (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China
Phone: +86 139 5327 0326
Email: xieyinghui@hikvision.com