

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

B. Wang, Ed.  
S. Liu, Ed.  
L. Wan, Ed.  
Hikvision  
J. Li, Ed.  
CICS-CERT  
X. Wang, Ed.  
Hikvision  
H.N. Yan, Ed.  
Xidian University  
Y.H. Xie, Ed.  
Hikvision  
21 May 2025

Technical Requirements for Secure Access and Management of IoT Smart  
Terminals  
draft-wang-secure-access-of-iot-terminals-08

Abstract

This specification outlines technical requirements for IoT smart terminal access management to address critical security challenges. The widely dispersed nature of IoT devices (including IP cameras, access control systems, and traffic monitoring units) complicates effective oversight while creating significant vulnerabilities during network authentication. The proposed framework combats unauthorized access and device impersonation through enhanced access control mechanisms, enabling real-time device monitoring and prompt detection of offline status - essential capabilities for maintaining secure and stable IoT network operations.

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.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. The Network Structure of IoT System . . . . .	3
3. Security Threats and Challenges . . . . .	5
4. Current Technology Level . . . . .	5
5. Secure Access and Management of IoT Smart Terminals . . . . .	6
5.1. Framework of Secure Access Management . . . . .	6
5.1.1. *Sensing & Controlling Domain* . . . . .	8
5.1.2. *Access & Management Domain* . . . . .	8
5.1.3. *Application & Service Domain* . . . . .	9
5.1.4. *User Domain* . . . . .	9
5.2. *Requirements for Device Security Access* . . . . .	9
5.2.1. *Requirements for Devices Access Authentication Identity Information* . . . . .	9
5.2.2. *Requirements for Access Status of Devices* . . . . .	9
5.2.3. *Recommendation of Access Policy* . . . . .	9
5.3. *Requirements for Management of Terminals* . . . . .	10
5.4. *Requirements for Device Protocol Access* . . . . .	10
5.4.1. *Requirements for Access Log Audit* . . . . .	10
6. Security Considerations . . . . .	11
7. IANA Considerations . . . . .	11
8. Informative References . . . . .	11
Authors' Addresses . . . . .	12

## 1. Introduction

The rapid advancement of IoT and IP-based communication systems has interconnected massive smart terminals across extensive and decentralized networks. This proliferation creates security vulnerabilities, as human oversight struggles to manage dispersed devices like IP cameras, access control systems, and other connected endpoints. The integration of IoT with core information networks amplifies risks - compromised terminals could enable network-wide

breaches, paralyzing critical operations and exposing sensitive data. Implementing robust terminal access control and application governance mechanisms therefore forms a critical component in safeguarding IoT ecosystems, ensuring continuous security and availability amidst evolving cyber threats.

This draft outlines the technical requirements for secure access and management of smart terminals in the IoT to address the security threats and challenges that exist in the access process of terminals. We discuss the networking structure of common IoT smart terminals in Section 2. Security threats and challenges faced in the access process of IoT smart terminals in will be clarified in Section 3. In Section 4, we review the guidelines and regulations related to the access of IoT terminals. In Section 5, we present the requirements for secure access and management of IoT smart terminals and describes in detail. This draft provides a reference for IoT security access and management .

## 2. The Network Structure of IoT System

Under normal circumstances, IoT smart terminals are connected to the network through IoT gateway, and then the data of terminals is reported to the application center through IoT gateway, which builds the complete network.

The diagram of an IoT system is shown in the figure below. In the perception layer, four types of IoT smart terminals form four subsystems, which are video monitoring subsystem, access control subsystem, alarm subsystem and intercom subsystem. The smart terminals in each subsystem are different. In the video monitoring subsystem, the main terminals are IP cameras and intelligent cameras for collecting video and image data. In the access control subsystem, the main terminals are turnstiles and vehicle access control hosts for collecting vehicle information. In the alarm subsystem, the main terminals are alarm hosts, alarm keyboards and wireless alarm hosts, which are used to set alarm policies, issue alarm warnings and report alarm events, etc. In the intercom subsystem, its main terminals are intercom hosts and individual equipment, which are used to collect voice data. Through this figure, we can know that in the IoT system, smart terminals are heterogeneous and complex, and the data are aggregated into the application layer through the transport layer, which greatly increases the difficulty of the application layer to control the terminals in the sensing layer.

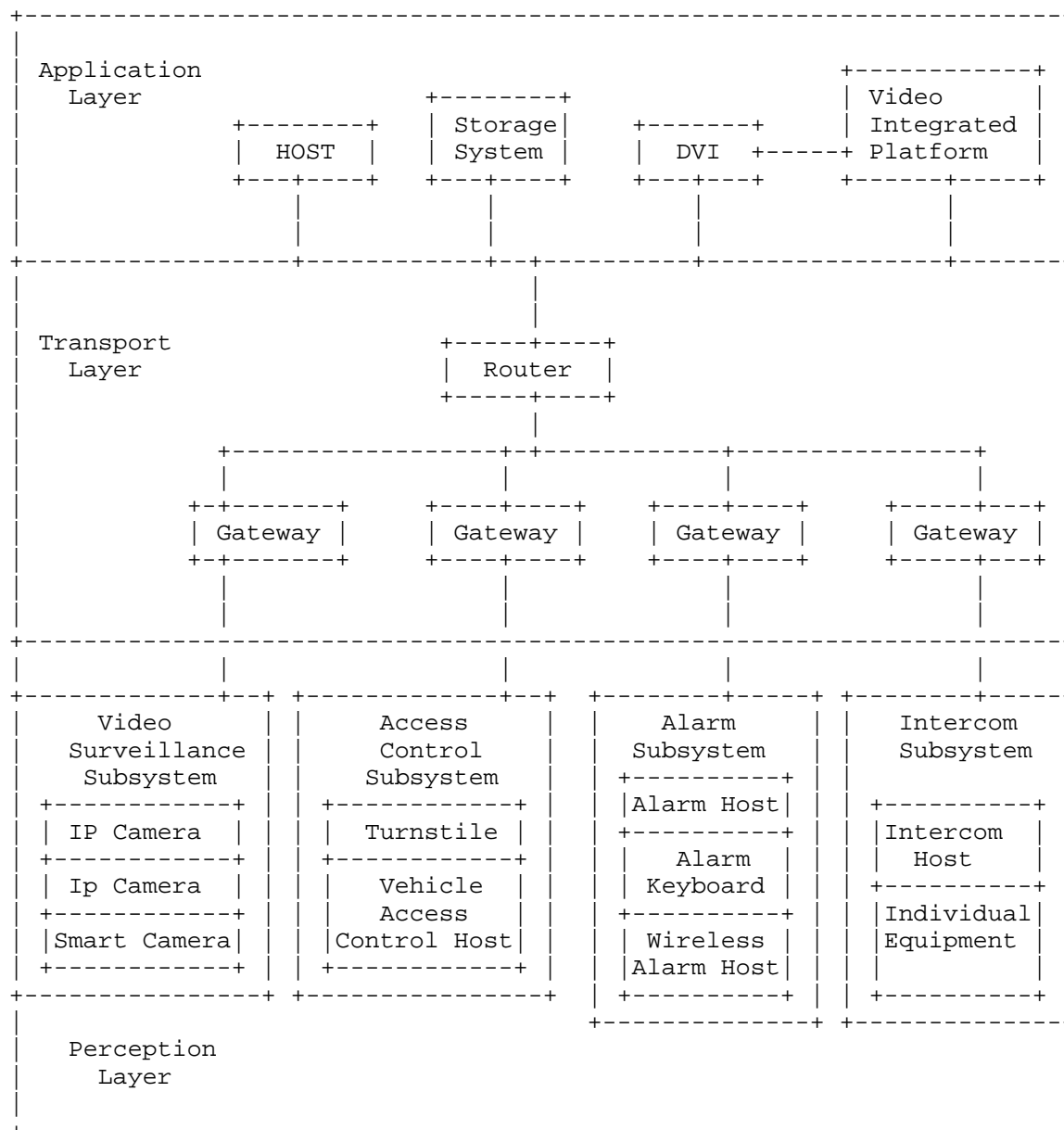


Figure: The Network Structure of an IoT System

### 3. Security Threats and Challenges

The main security threats and challenges in the process of accessing IoT smart terminals are as follows:

1. Illegal connection: By IoT smart terminals, illegal devices and hosts may access to the network for probing and attacking. The application layer network may be invaded by smart terminals, which will lead to information leakage.
2. Personate connection: Wide distribution of IoT smart terminals and the public deployment environment make it easy for malicious devices to impersonate legitimate devices and upload fake data, which will lead to abnormal function of the devices and causes great damage to the security of IoT.
3. Devices offline: IoT smart terminals are numerous and very vulnerable when they suffer from physical attacks, network anomalies, power supply anomalies, and aging of device, which leads them to work offline. However, offline devices are difficult to discover, causing the loss of some functions.
4. Devices management: There are many kinds of IoT smart terminals, and it is often not clear how many IoT smart terminals are in the whole IoT network and how many IoT smart terminals have security problems, which leads to unable to control IoT smart terminals and sort out device assets.

### 4. Current Technology Level

1. On the access control of IoT, many control protocols applied to IoT smart terminals have been proposed, such as Zigbee [ZB], DALI [DALI], BACNET [BACNET], which do not contribute to the secure access of IoT devices. The UPnP [ISOIEC23941] access protocol defines the access to IoT smart terminals, but does not consider the issue of secure access.
2. There are many specialized and generic security protocols being used in current IP-based deployments of IoT smart device applications. For example, IPsec [RFC7296], TLS [RFC8446], DTLS [RFC6347], HIP [RFC7401], Kerberos [RFC4120], SASL [RFC4422], and EAP [RFC3748], etc. However, these protocols also can not protect against illegal connection, personate connection and offline encountered during device access.
3. There are also a number of groups that focus on IoT device security. For example, the Cloud Security Alliance (CSA) recommended that when enterprises build the IoT network, they

should strengthen IoT smart device authentication/authorization [CSA]. The Global System for Mobile communications Association (GSMA) has published a security guide for IoT systems [GSMA] to bring a set of security guidelines to the research of IoT security product. The United States Department of Homeland Security(DHS) has proposed six IoT security strategic principles [DHS] to guide IoT developers, manufacturers, service providers, and consumers in considering security issues. These teams give good advice on building security for the IoT, but there is no introduction or description of secure access to the IoT.

4. The current security standards on IoT, such as [RFC8576], introduce the security issues and solutions, but there is no mention of the problems and solutions in the access process of smart terminals.
5. In other related device access standards, there are device access and portal-based authentication based on 802.1x [ISO88021X]. However, due to IoT smart terminals are mainly dumb terminals, they are not suitable for authentication access through 802.1x or portal, and the two authentication methods cannot be used to solve the illegal and personate connection of devices.

## 5. Secure Access and Management of IoT Smart Terminals

### 5.1. Framework of Secure Access Management

Comparing to three-layer framework of IoT, a layer of access and management is added for the framework of secure access management, which is between transport layer and application layer. The framework of secure access management for IoT smart terminals is shown in the following figure. In this framework, the access process of IoT is divided into four parts, which are sensing&control domain, access&management domain, application&service domain, and user domain. Among them, access&management domain is the specific implementation of the secure access and management technical requirements to ensure secure access of smart terminals in terms of smart terminals management, access control, strategy management and access log audit.

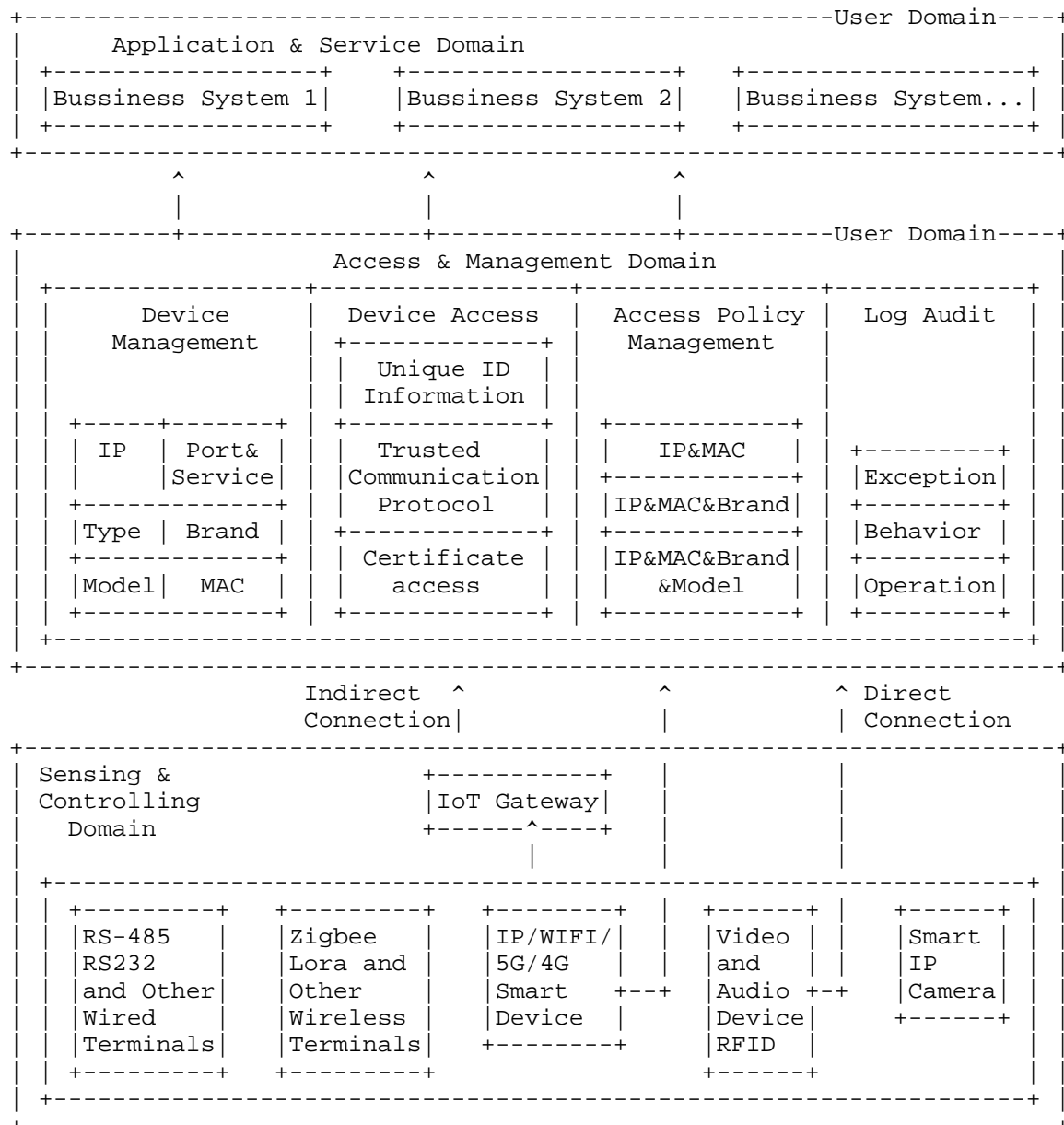


Figure: Framework of Secure Access Management for Smart Terminals

#### 5.1.1.1. \*Sensing & Controlling Domain\*

Smart Terminals: Include wired terminals like RS-485, RS-232 and other devices, wireless terminals such as ZigBee, LoRa and other devices, smart devices like smart IP, WiFi, 5G, 4G, audio and video device and RFID, etc.

IOT Gateway: An entity used to connect smart terminals and upper layer, which is able to store data, compute data and transform protocol.

Among them, smart terminals can be directly connected to the access &-management domain, or indirectly connected to the access & management domain through the IoT gateway.

#### 5.1.1.2. \*Access & Management Domain\*

Access & management domain is the core, which is used to manage and control the access of smart terminals, including four parts: device management, device access, access policy management and log audit.

The contents of each part are clarified as follows:

Device Management: It mainly manages device asset information, including status, IP address, MAC address, type, brand, model, firmware version, open port and service of smart terminals.

Device Access: It refers to the device access mode supported by smart terminals, including access based on unique identification information of smart terminals (the composition of it can be one or more sets of device asset information), access based on trusted communication protocol of smart terminals and access based on certificate authentication.

Access Policy Management: It refers to the access policy management based on the unique identification information of smart terminals. The access policy includes IP&MAC access policy, IP&MAC&brand access policy, IP&MAC&brand&model access policy.

Log Audit: Used to record, store and audit the log information generated in the access process of smart terminals, including exception log audit, behavior log audit and operation log audit.



### 5.1.3. \*Application & Service Domain\*

Application & service domain is the core business system, which provides informational application services for information collecting, exchanging and processing. The information provided by the smart terminals is verified by the access & management domain to ensure security and stability of the system.

### 5.1.4. \*User Domain\*

User domain refers to the users of smart terminals who can directly access the core business system in application & service domain, and view the access condition of smart terminals and manage them in access & management domain.

## 5.2. \*Requirements for Device Security Access\*

### 5.2.1. \*Requirements for Devices Access Authentication Identity Information\*

The identity information of devices should include one or more of the following characteristics:

1.IP Address 2.MAC Address 3.Brand 4.Type 5.Model 6.Firmware Version  
7.Port & Service

### 5.2.2. \*Requirements for Access Status of Devices\*

There should be at least four types of access status:

1.Online: The device that has been authenticated and is still working well. 2.Offline: The device that has been authenticated whereas is not connected to network. 3.Replacement: The device that has not been authenticated whereas its authentication information is as the same as other authenticated device. 4.Illegal connection: The device that has not been authenticated and its information is different from other authenticated device.

### 5.2.3. \*Recommendation of Access Policy\*

1.The device access policy should have at least five combinations:  
a. IP + MAC  
b. IP + MAC + Brand  
c. IP + MAC + Brand + Model  
d. IP + MAC + Brand + Model + Type  
e. IP + MAC + Brand + Model + Type + Firmware Version  
2.The illegal access of replacement device and illegal connection device can be quickly discovered and prevented. 3.The configuration of access

policy can be done manually and automatically. 4.The access policy can be customized by any combination of recommendation of access policy shown in requirement 1.

### 5.3. \*Requirements for Management of Terminals\*

Device management requires to monitor status of terminals in real time, to profile terminals, to identify and manage applications running on terminals, to identify and manage asset information of terminals, and to manage IP addresses of terminals.

1.Requirements for condition monitoring and management of terminals  
a.It should be able to monitor the offline and online status of smart terminals in real time. b.It should be able to discover whether there is a weak password information of the smart terminal. c.It should be able to discover the risky ports of smart terminals. d.It should be able to alert offline devices or the devices with weak passwords and risky ports. 2.Requirements for management of terminal profiling a.It should be able to visualize the information of smart terminals, including IP address, brand, type, model, etc.  
3.Requirements for management of identifying applications a.It should be able to automatically identify and manage the devices' open services and service ports. b.It should be able to automatically discover and identify the application system of B/S architecture or C/S architecture running in the network where the IoT smart terminal located, including IP, service port, application name. 4.Requirements for management of identifying asset information of the device a.It should be able to manage IP address, MAC address, brand, model, type, firmware version, open port, and online time of smart terminals. b.It should be able to manage the communication protocol information. c.It should be able to manage the geographic location information of terminals

### 5.4. \*Requirements for Device Protocol Access\*

Device Protocol Access requires the ability to release trusted protocol of IoT smart terminals and block untrusted protocols.

1.It should release IoT protocols, such as http, mqtt, onvif, coap, etc. 2.It should block illegal protocols in real time, such as ssh, ftp, telnet, etc. 3.It should select the corresponding protocols based on the specific business scenario, such as rtsp, onvif, and other protocols that used in the video surveillance field.

#### 5.4.1. \*Requirements for Access Log Audit\*

Access log audit requires the ability to audit all types of operations, such as abnormal and malicious behavior of access.

1.It should record abnormal behavior log information of access in real time and provide analysis and audit functions. 2.It should record malicious behavior log information of access in real time and provide analysis and audit functions. 3.It should record the management, access and blocking of access devices and other types of operations in real time, and provide analysis and audit functions.

## 6. Security Considerations

This entire memo deals with security issues.

## 7. IANA Considerations

This documents has no IANA actions.

## 8. Informative References

- [BACNET]    American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), "BACnet", <<http://www.bacnet.org>>.
- [CSA]       "Security Guidance for Early Adopters of the Internet of Things (IoT)", 2015, <[https://downloads.cloudsecurityalliance.org/whitepapers/Security\\_Guidance\\_for\\_Early\\_Adopters\\_of\\_the\\_Internet\\_of\\_Things.pdf](https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf)>.
- [DALI]      "DALI Explained", <<http://www.dalibydesign.us/dali.html>>.
- [DHS]       "Strategic Principles For Securing the Internet of Things (IoT)", 2016, <[https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL....pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf)>.
- [GSMA]      "GSMA IoT Security Guidelines and Assessment", <<http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines>>.
- [ISO88021X]    ISO/IEC/IEEE, "Telecommunications and exchange between information technology systems - Requirements for local and metropolitan area networks - Part 1X: Port-based network access control".
- [ISOIEC23941]    ISO/IEC, "IoT management and control device control protocol".

- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", DOI 10.17487/RFC3748, June 2004, <<https://www.rfc-editor.org/info/rfc3748>>.
- [RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", DOI 10.17487/RFC4120, July 2005, <<https://www.rfc-editor.org/info/rfc4120>>.
- [RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", DOI 10.17487/RFC4422, June 2006, <<https://www.rfc-editor.org/info/rfc4422>>.
- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.
- [RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", DOI 10.17487/RFC7401, April 2015, <<https://www.rfc-editor.org/info/rfc7401>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8576] Garcia-Morchon, O., Kumar, S., and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges", DOI 10.17487/RFC8576, April 2019, <<https://www.rfc-editor.org/info/rfc8576>>.
- [ZB] "Zigbee Alliance", 2020, <<http://www.zigbee.org/>>.

## Authors' Addresses

Bin Wang (editor)  
Hikvision  
555 Qianmo Road, Binjiang District  
Hangzhou  
310051  
China

Phone: +86 571 8847 3644  
Email: wbin2006@gmail.com

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

Li Wan (editor)  
Hikvision  
555 Qianmo Road, Binjiang District  
Hangzhou  
310051  
China  
Phone: +86 571 8847 3644  
Email: dzwanli@126.com

Jun Li (editor)  
CICS-CERT  
No.35, Lugu Rd., Shijingshan Dist  
Beijing  
100040  
China  
Email: lijun@cics-cert.org.cn

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