Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-wang-secure-access-of-iot-terminals-03
Published: 21 March 2022
Intended Status: Standards Track
Expires: 22 September 2022
Authors: B. Wang, Ed. Hikvision
S. Liu, Ed. Hikvision
L. Wan, Ed. Hikvision
J. Li, Ed. CICS-CERT
X. Wang, Ed. Hikvision

Technical Requirements for Secure Access and Management of IoT Smart Terminals

Abstract

It is difficult to supervise the great deal of Internet of Things (IoT) smart terminals which are widely distributed. Furthermore, a large number of smart terminals (such as IP cameras, access control terminals, traffic cameras, etc.) running on the network have high security risks in access control. This draft introduces the technical requirements for access management and control of IoT smart terminals, which is used to solve the problem of personate and illegal connection in the access process, and enables users to strengthen the control of devices and discover devices that is offline in time, so as to ensure the safety and stability of smart terminals in the access process.

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 September 2022.

Table of Contents

1. Introduction

With the rapid development of the IoT and the IP-based communication system, a large number of terminals have been interconnected through the network. Due to numerous branches of IoT network and the scattered distribution of smart terminals,it is difficult for human to supervise. Therefore, how to ensure the full-time control and available of IoT network becomes a new problem. A large number of smart terminals (such as IP cameras, access control terminals, traffic cameras and other dumb terminals), which running in the network, have a large security risk in terms of security access control. With the further development of the convergence of IoT systems and information network, if IoT smart terminals are once used by hackers, it is easy for hackers to penetrate the whole

network through IoT smart terminals, causing core business systems unable to work and a large amount of confidential information to leak, which will bring huge loss. Therefore, the establishment of a perfect access control mechanism and application control mechanism of smart terminals is an important part of the IoT security system.

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.

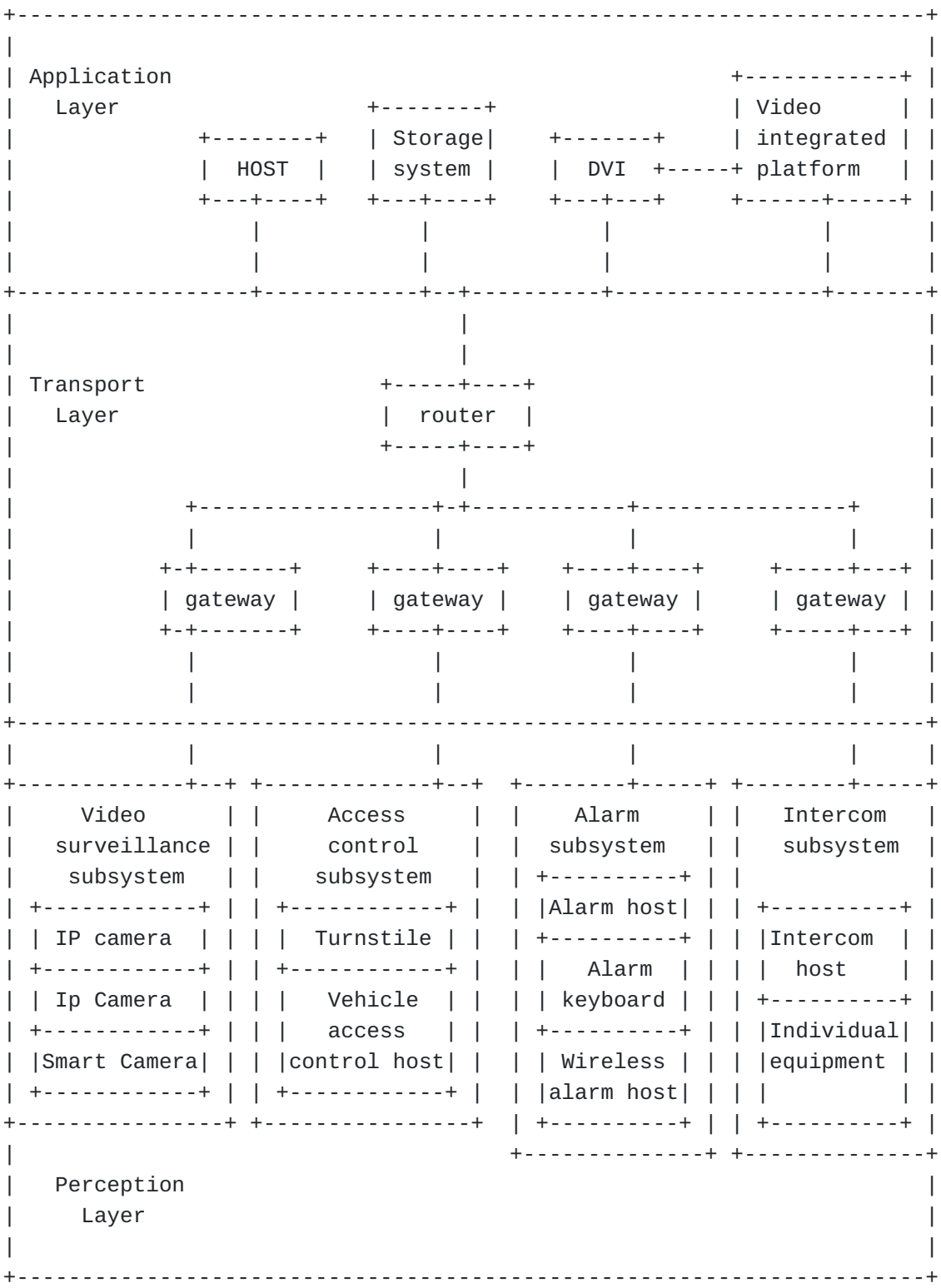

Figure 1: The Network Structure of an IoT System

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.

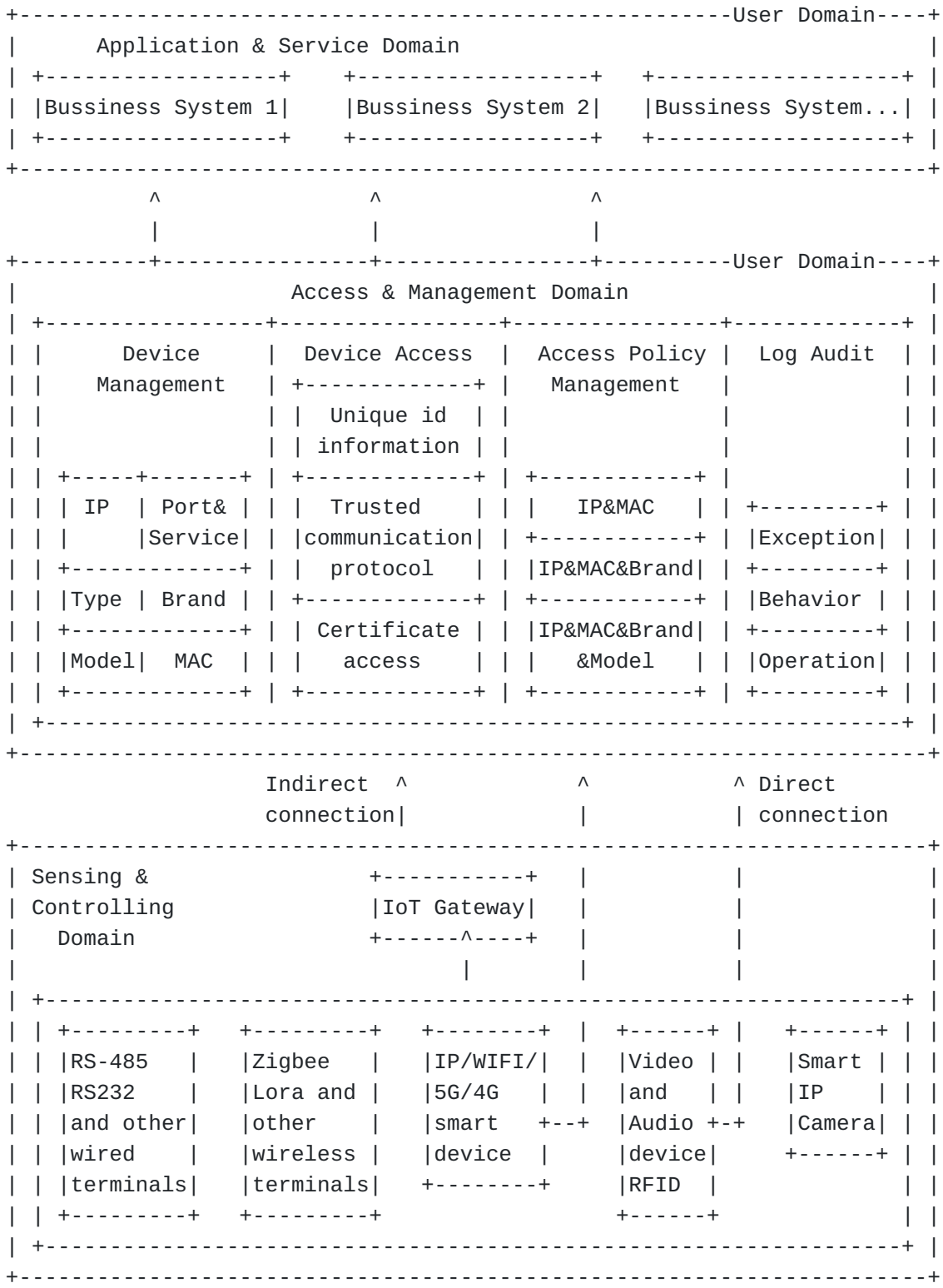

Figure 2: Framework of Secure Access Management for Smart Terminals

5.1.1. Sensing & Controlling Domain

Smart Terminals: include RS-485, RS-232 and other wired terminals, ZigBee, LoRa and other wireless terminals, smart IP, WiFi, 5G, 4G smart devcie, audio and video device and RFID, etc.

IOT Gateway: Be able to store data, compute and transform protocol, an entity used to connect smart terminals and terminals of upper layer.

Among them, smart terminals can be directly connected with the access&management domain, or indirectly connected with the access and management domain through the Internet of things gateway.

5.1.2. Access & Management Domain

Access and 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 clarified as follows:

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

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

Access Policy Management: Refers to the access policy management based on the unique identification information of smart terminals, including: IP, MAC access policy; IP, MAC, manufacturer access policy; IP, MAC, manufacturer, 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 that verified by the access & management domain to ensure security and stability of the system.

5.1.4. User Domain

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

5.2. Requirements for Device Security Access

5.2.1. Requirements for Devices Access Authentication Identity Information

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

1. IP Address
2. Address
3. Brand
4. Type
5. Model
6. Firmware Version

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 authenticated and is working well.
2. Offline: The device that has authenticated but is not connected to network.
3. Personate: A device that can not authenticate and its authentication information is the same as other authenticated device.
4. Illegal connection: A device that fails to authenticate and its authentication information is different from other authenticated device.

5.2.3. Recommendation of Access Policy

1. The device access policy can be at least five combinations:

a. IP + MAC

b. IP + MAC + Manufacturer

c. IP + MAC + Manufacturer + Model

d. IP + MAC + Manufacturer + Model + Type

e. IP + MAC + Manufacturer + Model + Type + Firmware Version

2. Quickly discover the access of personate and illegal connection, and prevent illegal control of devices.

3. The configuration of access policy can be done manually and automatically

4. Device access policy can be customized as any combination of recommendation of access policy shown in requirement 3.

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

    1. It should be able to monitor the offline and online status of smart terminals in real time

    2. It should be able to discover whether there is a weak password information of the smart terminal

    3. It should be able to discover the risky ports of smart terminals

    4. It should be able to alert offline devices or the devices with weak passwords and risky ports

2. Requirements for the management of terminal profiling

    1. It should be able to visualize information of smart terminals, including device type, IP address, open ports, etc.

3. Requirements for the management of identifying applications

    1. It should be able to automatically identify and manage the device's open services and service ports

    2. It should be able to automatically discover and identify the application system of B/S architecture or CS architecture running in the network where the IoT smart terminal is located, including: service IP, service port, application name

4. Requirements for the management of identifying asset information of the device

    1. It should be able to manage IP address, MAC address, device manufacturer, device model, device type, device firmware version number, device open port, and device online time for smart terminals

    2. It should be able to manage the communication protocol information of geographic location information of terminals

5.4. Requirements for Device Protocol Access

Device Protocol Access requires the ability to release trusted protocol data 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.

5.5. 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 to provide analysis and audit functions.

2. It should record malicious behavior log information of access in real time and to 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 can 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>.

[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>.

[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