HIKVISION

Hikvision Product Security White Paper

www.hikvision.com

About this Documentation

The Hikvision Product Security White Paper is intended to give a comprehensive overview of Hikvision's current practices on product security, and make Hikvision's security capabilities open and transparent to the public.

Hikvision reserves the right to update this Documentation. Please kindly find the latest version on the company website (http://www.hikvision.com/en/).

Copyright Disclaimer

Trademarks Acknowledgement

海康威视 , HIKVISION and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTENT DESCRIBED IN THIS DOCUMENTATION IS PROVIDED "AS IS", AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, FITNESS FOR COMMERICAL USE OR A PARTICULAR PURPOSE.

HIKVISION PROVIDES NO WARRANTY ON THE ACCURACY OF THIS DOCUMENTATION CONTENT, AND RESERVES THE RIGHT TO CORRECT OR MODIFY THE CONTENT WITHOUT FURTHER NOTICE.

ANY DECISIONS RELIED ON OR BY THE USE OF THIS DOCUMENTATION TOGETHER WITH ANY CONSEQUENCES THAT IT MAY CAUSE SHALL BE UNDER YOUR OWN RESPONSILIBITY.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Revision Record

New release – May, 2019

Company Introduction

Hikvision is a provider of video-centered intelligent IoT (Internet of Things) solution and big data services.

Hikvision now has more than 34,000 employees, over 16,000 of which are R&D engineers (as of the end of 2018). The company annually invests 7 – 8% of its annual sales revenue to research and development for continued product innovation. Hikvision has established a complete, multi-level R&D system that includes every operation from research to design, development, testing, technical support, and service. Centered at its Hangzhou headquarters, the R&D teams operate globally, including R&D centers in Montreal, Canada and London in the UK, as well as five cities in China.

Hikvision advances the core technologies of audio and video encoding, video image processing, and related data storage, as well as forward-looking technologies such as cloud computing, big data, and deep learning. Over the past several years, Hikvision deepened its knowledge and experience in meeting customer needs in various vertical markets, including public security, transportation, education, healthcare, financial institutions, and energy, as well as intelligent buildings. Accordingly, the company provides professional and customized solutions to meet diverse market requirements. In addition to the video surveillance industry, Hikvision extended its business to smart home tech, industrial automation, and automotive electronics industries — all based on video intelligence technology — to explore channels for sustaining long-term development.

Hikvision has established one of the most extensive marketing networks in the industry, comprising 44 overseas regional subsidiaries and 32 provincial branches throughout China mainland (as of the end of 2018), ensuring quick responses to the needs of customers, users and partners. Hikvision products serve a diverse set of vertical markets covering more than 150 countries, such as the Philadelphia Recreation center in the USA, the safe city project in Seoul, South Korea, Dun Laoghaire Harbour in Ireland, Milan's Malpensa Airport, and the Bank of India, to name just a few.

Hikvision went public in May, 2010, and is listed on SMEs Board at Shenzhen Stock Exchange

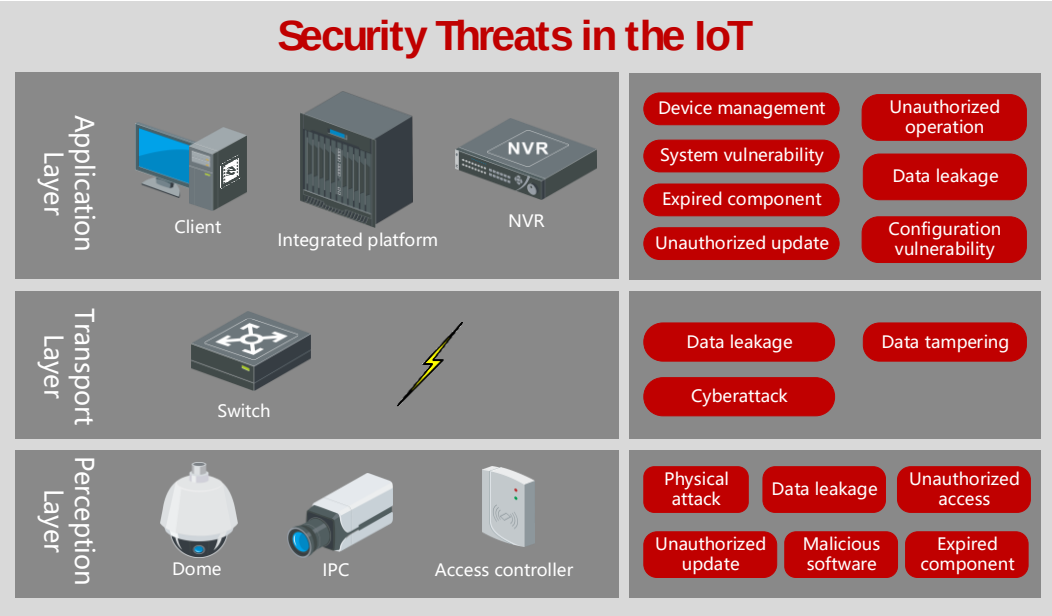
CONTENTS

1. Security Threats in the Internet of Things

The Internet of Things (IoT) connects "smart devices" from all over the world through the Internet and allows for the interaction between people and things on a global scale. The interconnection of massive devices has made networks more open, complex and diversified. However, the advent of IoT also brings security challenges.

In addition to the traditional network security threats, there are still some special security issues in the IoT. This is due to the fact that the IoT is composed of a large number of unattended devices or perceptive nodes, which are not consistently maintained. Based on the IoT framework, security threats in the IoT can be categorized as perception-layer threats, transport-layer threats, and application-layer threats:

- The Perception Layer is the physical layer.
- The Network Layer is responsible for connecting and facilitating communications between other IoT devices, network devices and servers.
- The Application Layer is responsible for interfacing with users by accepting and providing data to those users.



Perception-layer Threats

- Physical attack:

IoT assets that lack physical protection are susceptible to theft and damage and can easily be accessed without authorization.

Outdoor devices and distributed installations must have the appropriate physical controls to prevent physical attack, tampering, and counterfeiting.

- Data leakage:

Sensitive information that is not properly encrypted and secured could be read and possibly altered. This includes data at rest (stored on the device) and data in transit (moving across a network)

- Unauthorized access:

In many IoT devices, default usernames and passwords are used for ease of installation, however if end users do not change from those defaults, it gives attackers an easy way to gain access to the device. A similar attack can be successful if the end user creates weak, easily guessed passwords.

Some IoT devices use test and debug ports in the firmware, prior to releasing to the public. If these ports are not closed, it can give an attacker a means for executing code, and potentially taking complete control of the device.

- Unauthorized update:

All computers, including all IoT devices, will require security updates and sometimes feature updates from time to time. These updates are an attractive target for attackers by either pretending to be an official update or tricking a user into installing a malicious update, or trying to embed malicious code into a valid update. To prevent this, computer and IoT vendors need to have a code verification process to ensure that only valid code from the vendor can run on that hardware. Without this verification, malware installation is possible.

- Expired components:

When an IoT device is manufactured, it is installed with the latest code. However, by the time an end user installs the device, the code may be outdated and require software updates and

patches. Unless there is a process for automated patching, many IoT devices are left vulnerable to attacks that have already been patched by the vendor because the end user did not know, or remember, to manually patch the device regularly

- Malicious software:

If an attacker is successful in gaining access to an IoT device, it is likely that they will install malicious software, or malware, on that system. The type of malware that is typically installed on IoT devices is called Trojan Horse malware and it gives the attacker a remote control of the IoT device's computing resources. Once the attacker has access to enough devices (thousands, or tens of thousands, or more) they create something called a botnet. The attacker is usually not interested in the data on the IoT device, rather, they want to use the computer in the IoT device as part of their botnet Internet weapon. When the attacker wants to attack a website or anything connected to the Internet, they can tell all of the botnet-infected devices to attack at the same time

Some famous examples of botnets include Mirai, Bashlite, Lizkebab, Torlus and Gafgyt, to name just a few, which can cause large-scale Distributed Denial of Service, or DDoS attacks. The Mirai botnet was used to take down and slow down parts of the Internet by infecting IoT devices, including home routers, video surveillance cameras and video recorders.

Transport-layer Threats

- Cyberattack:

Attackers can gain unauthorized access to a network that uses wireless networks by exploiting Wireless protocol vulnerabilities. For example, weak authentication may allow an attacker to connect to the network and watch and record all network traffic.

If an attacker can gain unauthorized access to a network, he or she can monitor that network traffic and if it is not encrypted, they can see all of the data as it traverses the network. Unencrypted communication is prone to hijacking, repeating, tampering, and eavesdropping by an attacker.

- Data leakage:

During communication between IoT devices, cloud hosting servers, and mobile devices, attackers can access sensitive data if the network traffic is not encrypted.

- Data tampering:

When a device communicates through a network, the data collected by an attacker may be altered by attackers if there is no verification mechanism. This is called a man-in-the-middle attack.

Application-layer Threats

- Device management:

There are difficulties in managing the update process and security of the various and scattered devices managed by the platform layer.

- Unauthorized access:

User accounts need to be unique for each person and account credentials must not be shared. If account credentials are shared, there is no individual accountability and may result in leakage of sensitive data, and cause a privacy and security breach.

- System vulnerabilities:

Operating systems allow humans and applications to run on hardware. Most IoT devices run Linux, Windows, Android, and iOS as their operating system. The majority of large-scale network attacks focus on exploiting known vulnerabilities in operating systems that have not been patched.

- Data leakage:

The application layer manages a large volume of data, which is prone to leakage if not encrypted.

- Expired components:

The application layer has significantly more components than IoT devices do. If those components are not updated properly in time, unpatched vulnerabilities may exist and be easily exploited.

- Configuration vulnerabilities:

Security configurations that haven't been updated or examined for a long time may have configuration issues that can be exploited by network attackers.

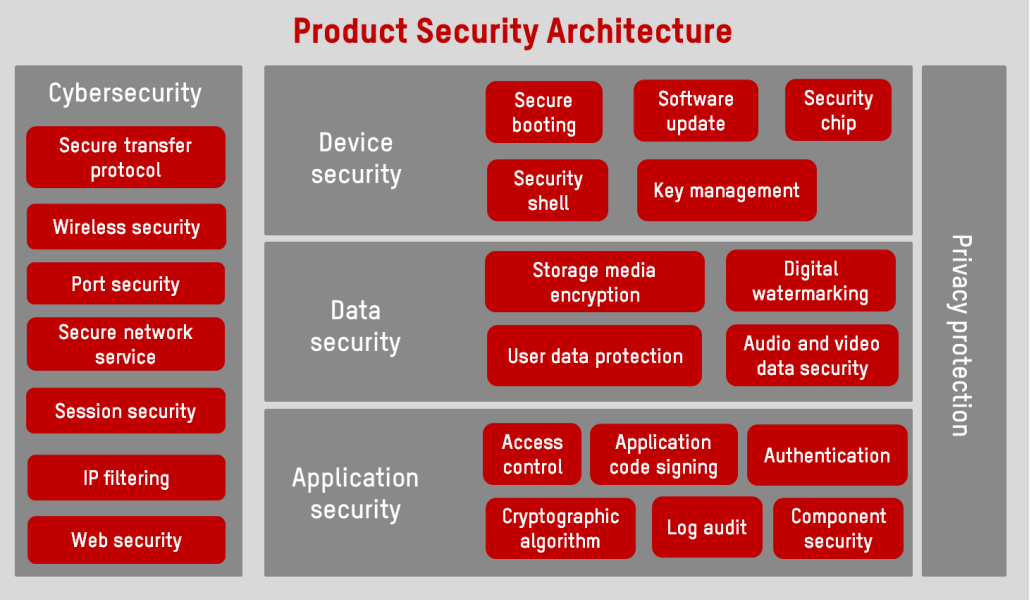
- Unauthorized update:

Unofficial software that is updated without verification may have vulnerabilities, or the software itself may be malicious.

After considering the many hidden security risks in the IoT environment, as well as the complexities of computational capabilities and the complex hardware and software environment, Hikvision created its video-centric IoT solution with an all new security framework. The goal is to establish a multidimensional security system that can ensure device, data, application, privacy, and network security, as well as security compliance. Below, six aspects of product security technology are described to explain how security technologies and functions are implemented in Hikvision's IoT solution.

2. Product Security Architecture[1]

The product security architecture guarantees product security from five aspects, namely device security, data security, application security, network security and privacy protection, in which, a large number of security technologies are used to ensure the product security.



2.1 Device Security

Device security is designed to ensure that all core components of each device provide security for both hardware and software. The tight coupling in the hardware and software of Hikvision's devices ensure each component of the system can be trusted and the whole system is robust. Security measure for each step, from initial start to software update, will be analyzed and examined in the following:

Secure Booting

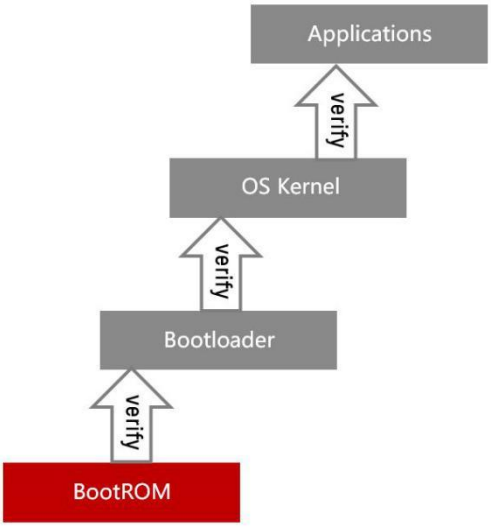
Secure booting is the cornerstone of device security.

Boot code is fused into the chip, preventing the boot process from being tampered with.

[1] Due to different hardware or software versions, some functions may be different. If there is inconsistency of the function between the actual product and the one in the guide, the actual product shall govern.

After the device is powered up, the code in Boot ROM is executed immediately and it checks whether the underlying Bootloader has been signed by Hikvision's private key. The Bootloader will only be allowed to load if verified. During the boot process, components involved in each step are digitally signed to ensure their integrity, and each step can only proceed after successful verification, forming a secure boot chain that can ensure the software is not tampered with. Programs involved in the boot process include Bootloader, the kernel, applications, etc.

If any step in the process fails to proceed or fails the verification, the boot process stops, and so does the device.

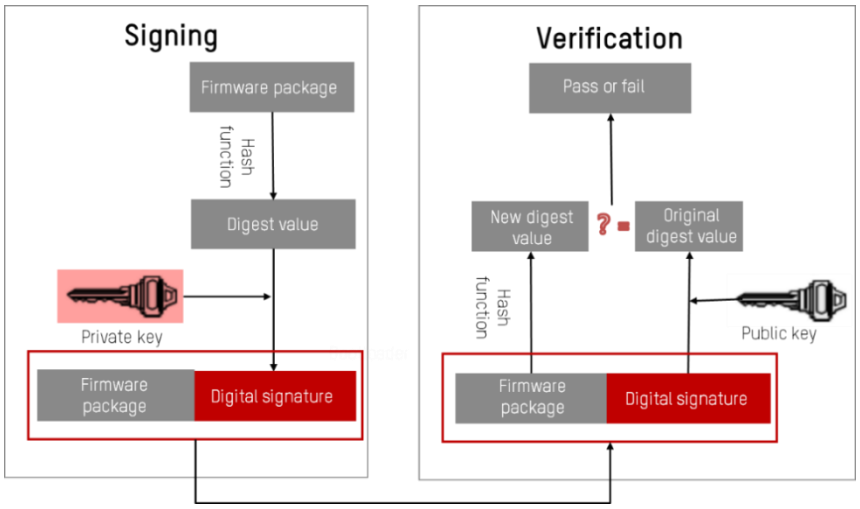


Software Update

To timely solve newly emerged security issues and provide brand-new functions in the meantime, Hikvision regularly releases software updates, which are available to all supported devices at the same time. Users are informed of firmware updates through notifications on the device and client software. Users are encouraged to quickly apply the latest firmware for security fixes.

Secure communication mechanism (e.g. HTTPS) are adopted during the transmission of update information, effectively protecting the data confidentiality and integrity of firmware update packages.

Firmware packages carry a digital signature for verification of the package's source and integrity, which can effectively prevent unauthorized firmware updates.



If a device can be downgraded, the attacker, once in control of the device, can install the earlier versions of firmware and exploit unpatched vulnerabilities. Therefore, Hikvision adopted an anti-degradation mechanism to prevent the device from being downgraded to an earlier version that could expose patched vulnerabilities.

Security Chip

To reach a high security standard on devices, Hikvision has taken advantage of security features (such as TrustZone, etc.) of device's main control chip, and has made use of high performance security chips at the same time. This is to achieve high-strength security at the hardware level, which provides a solid foundation for secure booting, secure update, stream encryption, etc.

All encryptions and decryptions are processed inside the chip, and keys will not appear outside the security chip or be exposed to other components, software, programs, or individuals in a form of plain text.

TrustZone is a security technology provided by ARM architecture on the processor level, and lays foundations for designing highly secure embedded systems. It divides hardware and software resources into two execution environments: The Secure World and Normal World. Sensitive and confidential resources reside in the physically isolated Secure World, reducing the possibility of being compromised.

Since the resource and performance are crucial to IoT devices, these two factors must be taken into consideration when designing and implementing highly complex encryption operations, otherwise, some user experience or device performance issues may occur. Therefore, Hikvision's devices are equipped with a dedicated encryption engine that can

support international encryption algorithms, capable of efficient data encryption.

The security chip has its own hardware true random number generator, which contains a high level of entropy, thus ensuring a high randomness of the key and random data in devices.

Security Shell

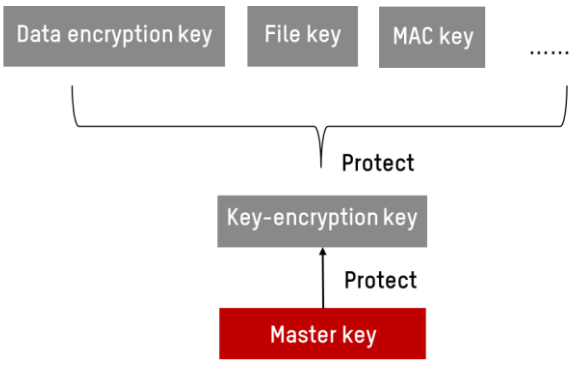
To meet the requirements for debugging and maintenance, devices support remote login through a secure SSH protocol to encrypt and protect transmitted data. The SSHv2, with better security mechanism, is adopted.

SSH services on devices are turned off by default, and only administrators have the permission to manually turn on (or off) SSH.

Shell commands via SSH are tailored and encapsulated in a secure manner by the device, and those commands are only executed after the security check is passed.

Key Management

The keys on the device are stored in the hardware security zone, and the device adopts a layered key architecture that generally is composed of the master key, the key-encryption key and the business key. The business key can be further categorized into the file key, data encryption key, etc., depending on its purpose. The master key protects the key-encryption key, which then protects the business key. The device can tailor and extend the key architecture depending on the use case, and should support at least two layers of key architecture.



2.2 Data Security

User Data Protection

With cryptographic technologies, Hikvision provides protection over user data, which includes user configuration data and user personal data. A data encryption key is randomly generated by the random number generator as the device first boots up, enabling 'Unique-key-per-device". This ensures the randomness of each device. Without a device's random key, attackers cannot decrypt any data, even if they have forcibly copied it from the device. User configuration data mainly includes user configuration parameters, usage information, etc. User personal data includes, but is not limited to, face comparison pictures, user personal information, etc.

Storage Media Encryption

For certain products, data on various storage media, especially critical data (e.g. audio and video data) on a pluggable storage medium, can be encrypted to avoid leakage. Portable storage media includes TF/SD card, USB flash disk, etc.

Digital Watermarking

Digital watermarking is a steganography technology, whose basic concept is to protect the copyright of digital products, prove the authenticity of products, and track piracy or provided additional information of products by embedding secret information in digital products, such as digital images, audio and video contents. This technology provides a method to hide digital information which then becomes invisible in the original file and can only be read with special readers. Therefore, adding digital watermarks to the video stream is an ideal solution to video tamper attacks. The state of hidden watermarks can indicate whether the video information has been tampered with or not.

Audio and Video Data Security

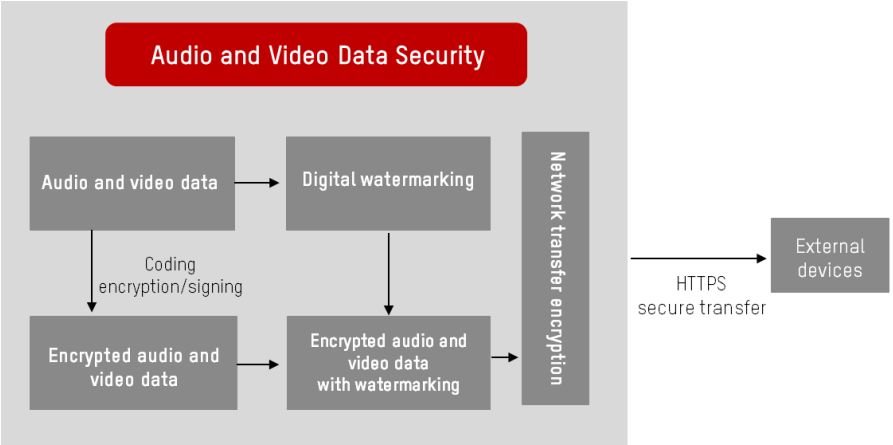
Since data is subject to unauthorized tampering or viewing at the perception layer, transport layer or application layer, audio and video data security is the priority of video surveillance systems. Accordingly, Hikvision devices support security protection during the encoding and transfer stages.

- Encoding:

Audio and video data are encrypted during the encoding process, then transmitted and stored in cipher text, which effectively prevents data from unauthorized access. Digital signing on audio and video data during the encoding stage is supported, and the data is transmitted and stored with the digital signature, effectively preventing unauthorized tampering.

➢ Transfer:

HTTPS/TLS is supported for audio and video data transmission over the network, effectively defending against all kinds of cyber-attacks.



2.3 Application Security

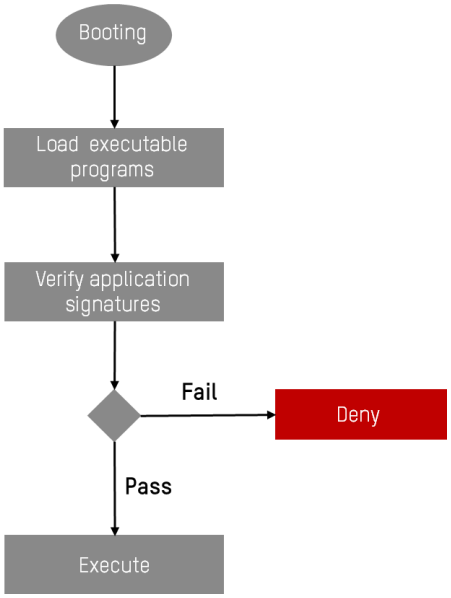
Application Code Signing

After its booting, the device kernel will determine which user processes and applications can be run. To ensure that all applications are from approved known sources and haven't been tampered with, all executable codes are required to be signed with certificates recognized by Hikvision. This mandatory code signing expands the concept of trust chain from the operating system to the application level, effectively preventing unauthorized applications from running.

With code signing, it ensures that all executed codes are authorized, preventing malicious codes from running. Different from the code signing technology over the Internet, the technology in the IoT can be applied to not only the application level, but also the firmware level. Codes running in every important device (including the sensor, the switch, etc.) need to be signed, otherwise they will not be executed.

Considering limited resources of some IoT embedded devices, e.g. limited processor capacity,

communication capacity and storage space, Hikvision has established a set of code signing mechanism that tailors to the characteristics of the IoT, balancing security, efficiency and performance.



Authentication

By implementing a series of password and access control policies, Hikvision's device account security system ensures the security of user accounts:

- Password complexity:

User passwords should comply with the password complexity policy: contain a minimum of 8 characters and use at least 2 types of characters (upper case letter, lower case letter, number, and special character).

- Access control:

User roles are restricted to certain permissions

- Activation mechanism:

Users have to set a strong password that meets the security requirements to activate the device, to avoid issues caused by having a default password.

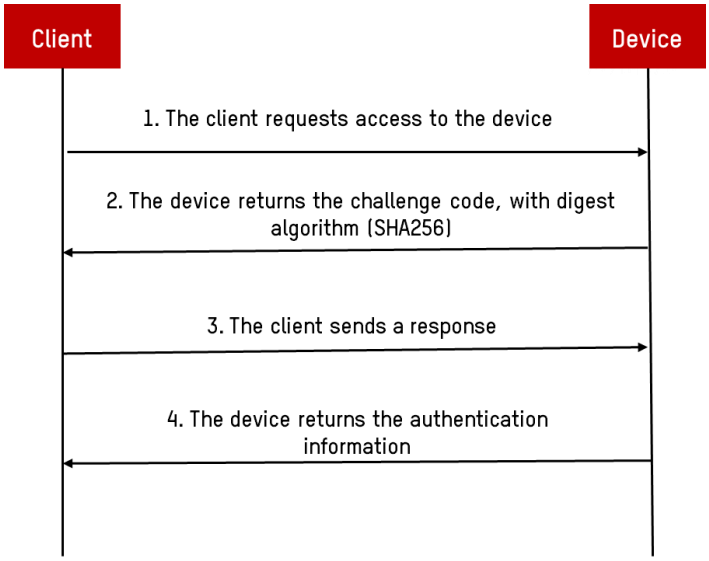
- Unauthorized login monitoring:

The system monitors unauthorized login attempts, and provides login lock to limit the number of user login attempts. The maximum number of login attempts and lockout time are configurable.

Cryptographic Algorithm

Hikvision's use of cryptographic algorithms is in line with international standards, such as FIPS. Unless required to be compatible with third-party systems or historical standard protocols, cryptographic algorithms all support secure algorithms and use secure modes.

During authentication, a large number of standard protocols, including HTTP, ONVIF, RTSP, etc., still use insecure algorithms, such as MD5, as their default digest authentication algorithms. Hikvision's devices support cryptographic algorithms with higher security levels, such as SHA256.



Access Control

Hikvision manages user permission and devices' access control uniformly, providing multidimensional security assurance.

- User roles restriction:

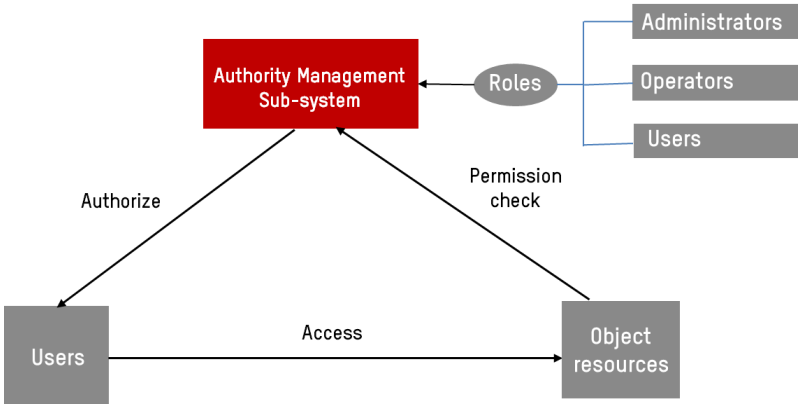
The device provides role-based access control: the administrator, common user, etc.

- User operation control:

Sensitive behaviors (such as controlling the device, modifying device properties, etc.) are controlled on the device, effectively preventing unauthorized operations and unauthorized access to sensitive information.

- Minimum privilege:

All operation permissions are fine-grained and can be set individually for each user. Thus, the security risk caused by a user's incorrect operations or identity theft can be prevented.

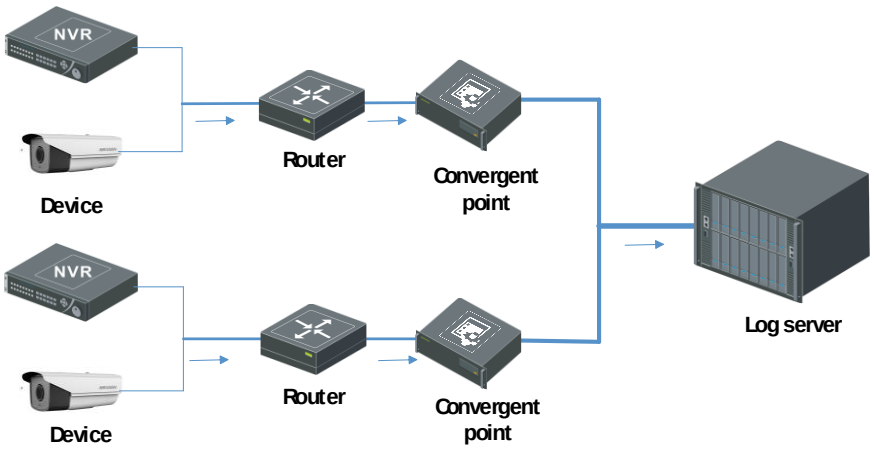


Log Audit

Hikvision's security audit maintains detailed track records of all data activities, realizing active monitoring of user access behaviors. All kinds of abnormal events could be identified in the process. The generated report can provide details of all data activities, e.g. login failure, configuration changes, user management, device update & maintenance, access failure, etc., and ensures all user operations are traceable.

Besides, the audit process is guaranteed to be uninterrupted and audit records intact. Abnormal events alarm will be triggered if risks are detected.

Local log is stored securely, protected with cryptographic technology to prevent unauthorized viewing and tampering. The device supports the syslog protocol to ensure secure upload of the log data to the log sever in real time. The log server can support log audit, automatic analysis, early warning and permanent log archive for tens of thousands devices.



Encryption and authentication on the transport layer is supported for log transmission over the network through the TLS protocol.

Component Security.

Before the design of a product architecture, Hikvision will analyze the security level of open source and third-party software involved in product development (including their open source protocols, compliance, unfixed vulnerabilities, potential risks, etc.), strictly following the principle of "security analysis before introduction".

During the testing stages, the testing team will analyze and verify source code consistency of open source and third-party software, and conduct security scanning on that software. This is to detect the presence of old components or components with unfixed vulnerabilities in devices, such as components of earlier versions, components with CVE vulnerabilities, etc. Necessary rectifications are made. In this way, the security of open source and third-party software in released version can be ensured.

2.4 Network Security

In the early days of the IoT, devices and networks were mostly designed to operate in an isolated environment, and the security mechanism was relatively immature. With the rapid development of the IoT, these devices and networks have gradually become connected to the Internet, which introduces new security issues.

In addition to the built-in security mechanism that protects stored date in devices, there are also a number of network security measures available to ensure the security and accuracy of the information when transmitting to and from the device. To achieve these security

objectives, Hikvision has integrated proven technologies and the latest standards for data network connectivity. Hikvision has removed unnecessary network services (such as Telnet or FTP servers) to reduce the scope of attacks.

Secure Protocol

The network transmission of all Hikvision products supports secure transfer protocols: e.g. HTTPS, TLS, and DTLS.

A variety of security protocols will be applied in a secure manner, including:

- Secure certificate management and verification mechanism;
- Insecure protocols, such as SSLv3.0, TLSv1.0, SNMPv2, etc. are turned off by default;
- Private protocols all support TLS-based transmission, and no clear text data is transmitted directly;
- HTTPS access is supported by default to ensure network transfer security;
- Syslog protocol supports transmission based on TLS or DTLS, and no sensitive data is leaked;
- Secure algorithm suites are used.

Secure Network Services

Management protocols are disabled by default on all Hikvision's products, and secure versions of these protocols are adopted to reduce the exposure to attacks:

- Telnet service is not supported;
- FTP service is not supported, while SFTP service is supported and is turned off by default;
- SSH service is turned off by default;
- SNMP service is turned off by default, and secure SNMPv3 is supported;
- NTP service is turned off by default;

- UPNP service is turned off by default.

Session Security

Hikvision devices have unified security measures for all sessions:

- Session timeout and auto-disconnection: the timeout period is configurable; if there is no interaction for the set period of time, the system will automatically return to the login page, and re-authentication will be required.

- Limit on the number of sessions: the maximum number of sessions is configurable; the number of simultaneous access can be limited to prevent unauthorized access.

- Session lock: after the number of failed authentication attempts exceeds the preset number, the user is automatically locked from subsequent attempts, thus effectively preventing brute-force attacks. The number of failed attempts before activating lock out mode is configurable.

- Session lock time: the session lock time is settable. Users can configure the lock time for authentication failures that exceed the preset number, to provide a good user experience while ensuring security.

WLAN (Wireless Local Area Network) Security

Hikvision devices support industry-standard WLAN protocols, including "WPA2 Enterprise", providing access authentication services for the company's wireless networks. The "WPA2 Enterprise" protocol uses secure AES encryption algorithm to provide users with the highest level of security, which is, user's data will always be protected when communicating via WLAN. With the support of 802.1x, Hikvision's devices can be integrated into a variety of RADIUS authenticated environments.

Port Security

Hikvision can guarantee that all default open ports in released products are relevant to the business, and ports that are not needed will be closed. Details of all open-ended ports can be found in the product communication matrix, including corresponding business function descriptions, corresponding authentication modes, whether is open by default, etc.

IP Filtering

Hikvision devices support IP filtering:

- The technology can filter out unauthorized client objects, thus reducing the threat to the host.

- When devices are under attack, the IP filtering technology can complete specific defensive actions to enhance the device's ability to handle risks.

Web Security

Hikvision provides a comprehensive security defense for all Web systems, providing users with high-quality and all-round security protection, including but not limited to:

- All data from untrusted sources is verified on the server side, and those that fail verification will be rejected. If the data output to the client is from an untrusted data source, the data will be encoded or escaped accordingly.

- User access/operation permission verification will be enforced to prevent horizontal/vertical overreach.

- Key information of the uploaded file, such as type, format, content and size, will be checked for validity to avoid uploading malicious files.

- Unauthorized access and information leakage can be prevented by access control on data and encryption of sensitive data.

- Source identifications and content detections are carried out on requests received by the server side to eliminate request forgery attacks

- According to different application scenarios, the WebServer configurations will be audited strictly in line with the "CIS" specification, to ensure the security of the configurations.

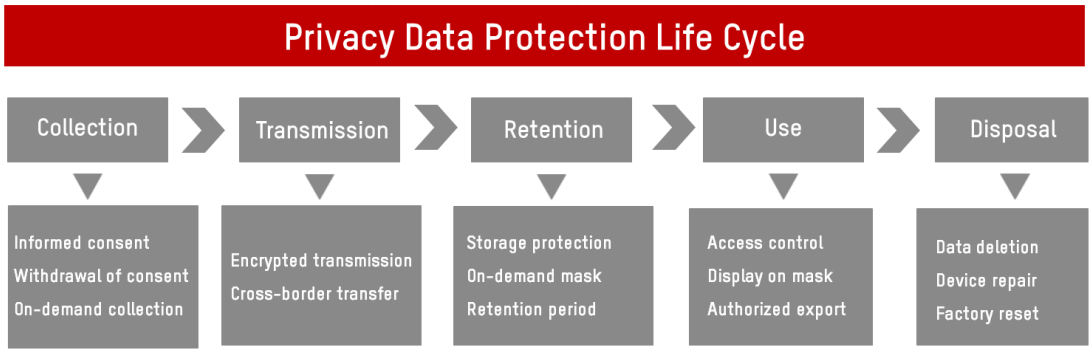
Session identity of the Web application is random and unique. After each successful authentication, the session identity will be changed to prevent the session fixation.

2.5 Privacy Protection

Many IoT devices, such as cameras and smart thermostats, are used in our daily life. When

using IoT devices, users' personal data might be directly or indirectly collected, transmitted, stored and processed. Thus, data security is one of the crucial tasks in the IoT industry. Hikvision strictly complies with the applicable data protection laws and regulations, including but not limited to the Chinese Cybersecurity Law, and General Data Protection Regulation (GDPR) in EU. Referring to the best practice in the industry, Hikvision integrates the concepts of data security and privacy protection throughout the full business process from technology development, product design, development, verification, test, delivery to after-sale services.

Specific protection measures of personal data protection as a life cycle are as follows:



➢ Collection: As hardware supplier, Hikvision does not have access to users' personal data in most cases. For cloud service, Hikvision as cloud service supplier, would collect specific and necessary personal data after obtaining users' consents. And the scope and the purpose of data collection will be expressed in the privacy policy

➢ Transmission: Personal data will be encrypted during transmission by Hikvision. If there is cross-border transfer, Hikvision will only transfer the data in accordance with applicable data protection laws. For example, if personal data originating within the European Economic Area (EEA) will be transferred outside the EEA, Hikvision will take appropriate safeguards in accordance with the GDPR, including standard contractual clauses adopted by the European Commission

➢ Retention: Adequate security measures will be taken to protect personal data when stored by Hikvision, including but not limited to encrypted storage, access control, logging, etc. Personal data will be retained by Hikvision for the period necessary to fulfill the purpose outlined in corresponding privacy statement unless a longer retention period is required or permitted by applicable law. Hikvision will cease to retain personal data, or remove the means by which personal data can be associated with particular individuals, as soon as it is

reasonable to assume that the purpose for which that the personal data was collected is no longer being served by retention of the personal data

➢ Use: The product will conduct identity authentication and permission management on users who are accessing personal data. During the data use, e.g. interface display or logging, whether the data should be masked will be determined according to actual business scenarios, and all personal data will be cleaned up in time after use. For business scenarios where personal data needs to be exported from the user network, the data will be processed in accordance with applicable local laws and regulations.

➢ Disposal: In the case of equipment repair, destruction or cloud resource recovery, the product provides a sound mechanism for personal data deletion.

2.6 Security Compliance

FIPS 140-2

FIPS 140-2 establishes the Cryptographic Module Validation Program (CMVP) as a joint effort by the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, and the Communications Security Establishment (CSE) for the Government of Canada. FIPS 140-2 is used by U.S. and Canadian government agencies, and regulated industries such as finance, healthcare, legal, and utilities, as well as commercial businesses. It is used and referenced by numerous standards bodies and international testing organizations, including the ISO standard.

Hikvision has achieved FIPS 140-2 certification with certificate number 3228 in July, 2018. Cryptographic modules in all similar products of Hikvision are exactly the same and comply with FIPS requirements. For future new products, Hikvision will continue to submit modules for corresponding verification.

For FIPS 140-2 Certification, please refer to:

https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Common Criteria / ISO 15408

As one of the most widely recognized international standards (ISO/IEC 15408) in information technology security, the Common Criteria certification is mainly applicable to evaluating security and reliability of information technology products or solutions, and is also focused on the protection of private information. Government organizations or government agencies from 28 countries have participated in the Common Criteria Recognition Arrangement (CCRA), including National Information Assurance Partnership, Department of Defense of U.S. Many enterprise organizations also use CC as a requisite in relevant procurements.

Hikvision's relevant products have achieved the CC certification with assurance type EAL2 augmented with ALC_FLR.2 (EAL2+). It demonstrates Hikvision's commitment to global customers on reliability and cybersecurity.

Hikvision will actively participate in the development of currently unimplemented protection profiles (PPs), and will continue to conduct evaluation and certification based on the new and updated versions of PPs that are already implemented.

For CC Certification, please refer to:

https://www.commoncriteriaportal.org/products/

3. Commitment to Security

Hikvision strives to use leading privacy and security technologies to protect customers' personal information and data in comprehensive ways.

Hikvision uses an integrated security infrastructure for its entire Internet of Things video surveillance ecosystem. Hikvision also has a professional security team responsible for providing support for all Hikvision products. This team provides security reviews and testing of released products and products under development. The security team also provides security training and actively monitors new security issues and threat reports. To find out how to report issues to Hikvision and how to subscribe to security notifications, please visit: https://www.hikvision.com/en/Support/Cybersecurity-Center/Report-an-Issue.

Hikvision

Product Security White Paper

See Far, Go Further

HIKVISION®

Hikvision Digital Technology Co., Ltd.

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China