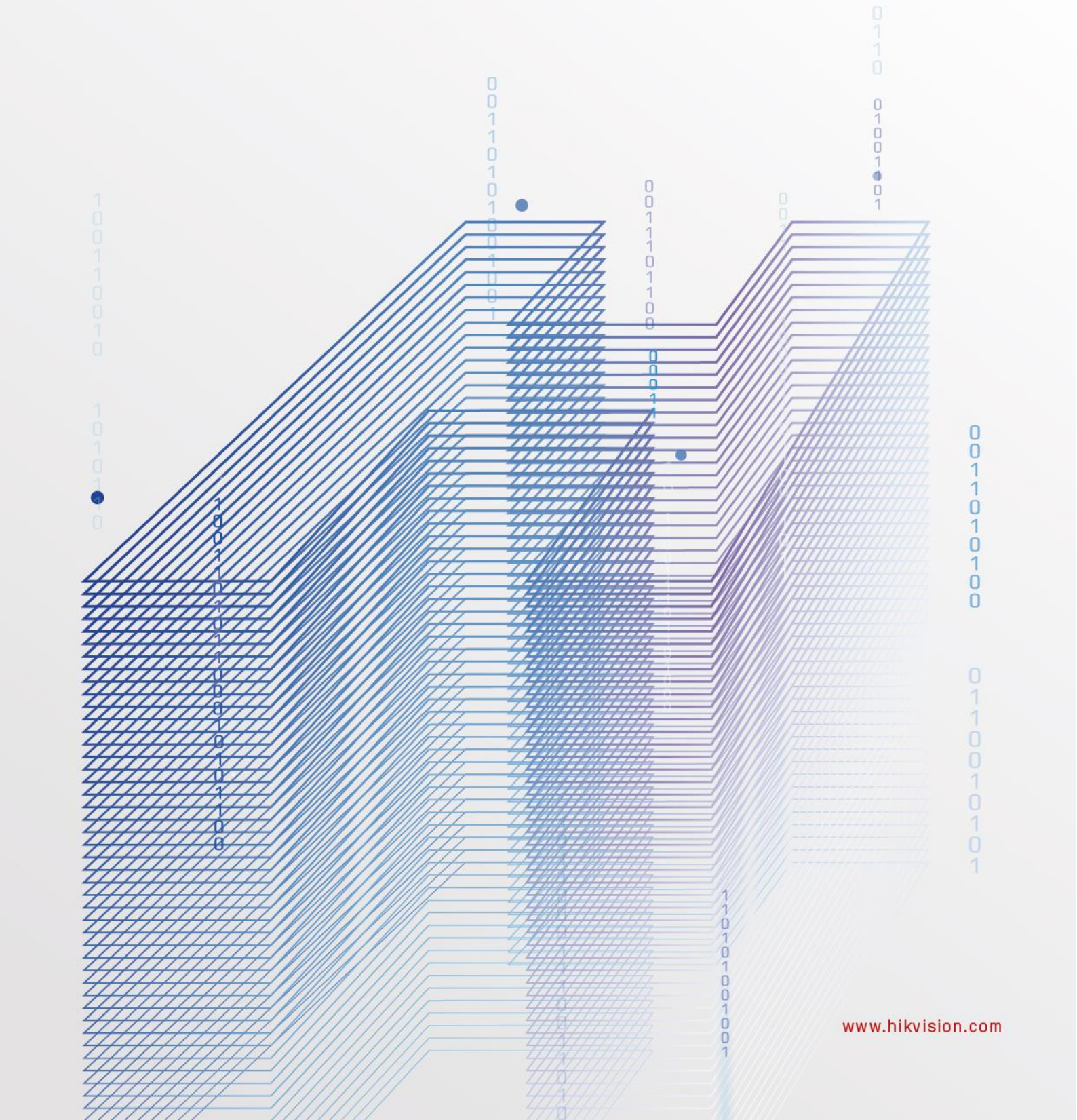
HIKVISION

Hikvision Product Security White Paper



www.hikvision.com

About this Documentation

Offering an overview of our current practice on product security, the Hikvision Product Security White Paper provides users with the company's product security capabilities in an open and transparent manner.

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's 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 RIGHTS 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 RESPONSIBILITY.

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

Revision Record

First published in January 2018 and revised in December 2023.

Company Introduction

Founded in 2001, Hikvision is a technology company focusing on technological innovation.

We adhere to the business philosophy of "Professionalism, Reliability, and Integrity," and fulfill the company's core values: dedicated to customers' continual success, adding value to companies and communities, acting with honesty and integrity, pursuing excellence in every endeavor. Hikvision is committed to serving various industries through its cutting-edge technologies of machine perception, artificial intelligence, and big data, leading the future of AIoT:

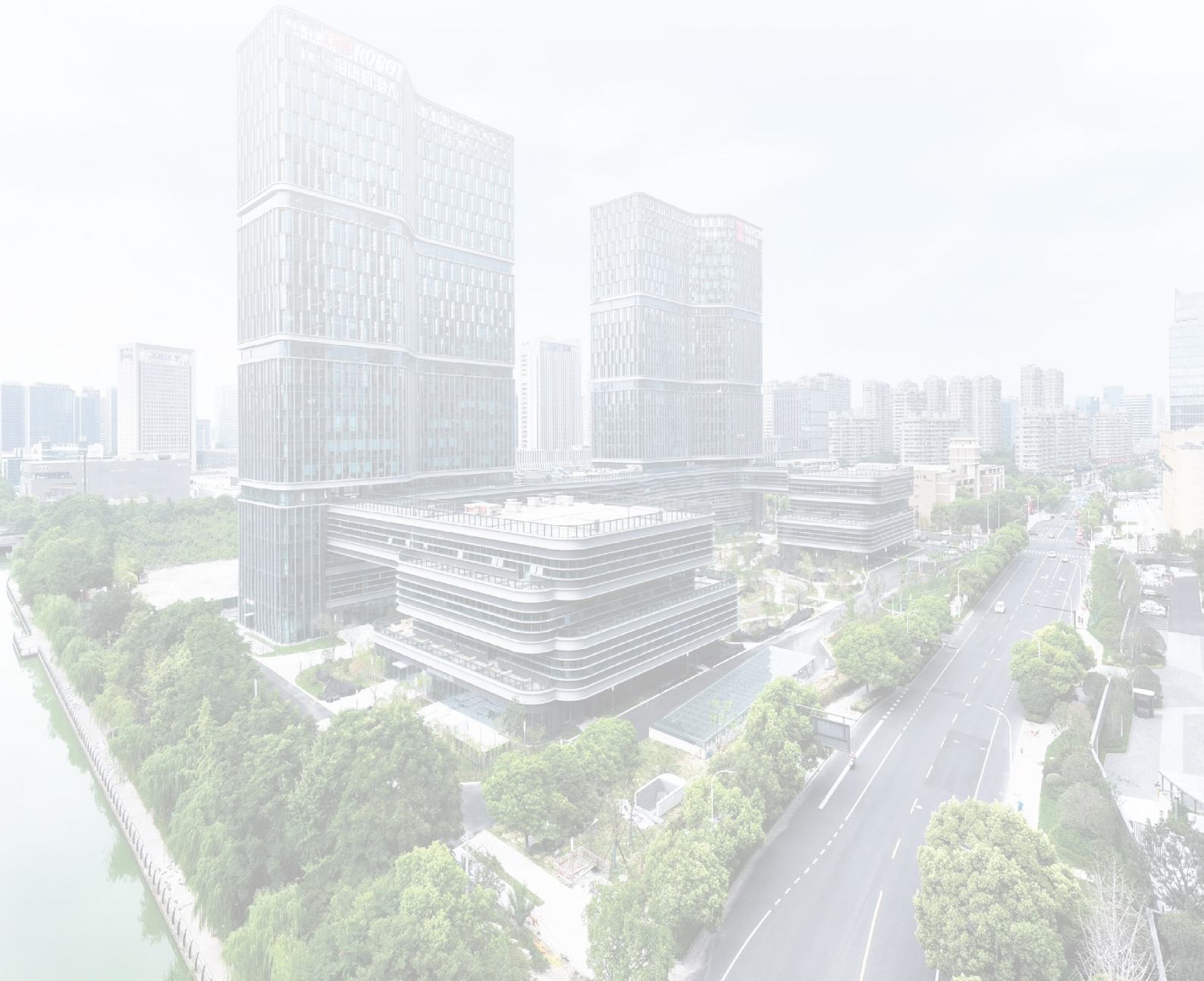
- Through comprehensive machine perception technologies, we aim to help people better connect with the world around them.
- With a wealth of intelligent products, we strive to identify diverse demands by delivering intelligence at your fingertips.
- Through innovative AIoT applications, we are dedicated to empowering every individual to enjoy a better future by building an intelligent world that is more convenient, efficient, and secure.

More than 20 years ago, Hikvision began with video technology and has continued to expand and deploy visible light, millimeter wave, infrared, X-ray, sound wave, and other technologies, creating a comprehensive and multi-dimensional IoT perception technology platform. Beyond IoT perception equipment, Hikvision has five categories of software and hardware products including AIoT products that fully integrate with artificial intelligence and big data technologies, basic IT products, platform service products, data service products, and application service products. Hikvision has also expanded into integrated security to smart homes, digital enterprises, smart industries, and smart cities.

Hikvision currently has 58,284 employees (as of the end of 2022), including more than 27,951 R&D personnel and technical service personnel. R&D investment accounts for 11.80% of the annual operating income (2022), making the Company a leader in the industry. The company

has R&D centers worldwide, including in Montreal, London, and Dubai, and various Chinese cities. Hikvision has a global presence with 72 overseas subsidiaries and branch offices, serving clients in more than 150 countries and regions (2022).

Hikvision went public in May 2010, and is listed on the SME Board at Shenzhen Stock Exchange, stock code: 002415.



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 a massive number of devices has made networks more open, complex and diversified. However, the advent of IoT also brings incredible security challenges.

Figure 1-1 Characteristics of IoT

In addition to the traditional cybersecurity threats, there are still some special security issues in the IoT, because it is composed of a large number of unattended devices or perceptive nodes without effective monitoring, exacerbated by large numbers and huge concentrations. Based on the IoT framework, security threats in the IoT can be categorized as perception-layer threats, transport-layer threats, and application-layer threats.

Perception-layer threats

- Physical attack

IoT assets that are deployed remotely without physical protection are susceptible to theft or damage.

Outdoor devices are sometimes easily accessible, and not well managed, leading to physical attacks, tampering, and counterfeiting.

- Data leakage

Sensitive information leakage is caused by the lack of encryption or access control during data collection and processing by IoT devices.

- Unauthorized access

Lack of authentication requirements, weak passwords, or easily bypassed authentication mechanism leave some IoT devices susceptible to potential attacks and compromises.

Some IoT devices leave a debug interface, which could allow an attacker to obtain device operation information.

- Unauthorized update

Some IoT devices do not use a robust update verification mechanism, which could allow unofficial firmware packages that may contain vulnerabilities or malware to be installed into the devices.

- Expired components

IoT devices come with built-in components with known vulnerabilities or expired components.

- Firmware and Software Exploits

IoT devices come with built-in components with known vulnerabilities or expired components. As expired components are no longer maintained, they pose a significant security risk. Vulnerabilities in the firmware or software of IoT devices can be exploited to gain unauthorized access, control, or execute malicious code, compromising the device's security.

- Malicious software

IoT devices without security software protection are susceptible to malware infections that affect the normal operation of the device.

Transport-layer threats

- Cyberattack

Exploiting protocol vulnerabilities, such as lack of effective authentication, may lead to leaks on the access side.

- Man-in-the-Middle Attacks

Attackers intercept communication between IoT devices and manipulate data or commands exchanged, leading to unauthorized access or control over these devices.

- Denial-of-Service Attacks

Floods of data requests or commands can overwhelm IoT devices, rendering them unresponsive or causing malfunctions, disrupting regular operations.

- Data leakage

During communication between IoT devices, cloud hosting servers, and mobile devices, attackers can access sensitive data by monitoring the transmission channel.

- Data tampering

When a device communicates over a network, commands and data may be intercepted and altered by attackers if the transmission data is not checked for integrity.

Application-layer threats

- Device management

There are challenges in managing the update process and the security of the numerous devices managed by the Application-layer.

- Unauthorized access

Imperfect authorization (rights) management at the application layer may lead to unauthorized access and the risk of data leakage.

- Insecure APIs and Interfaces

Weaknesses in application programming interfaces (APIs) and communication interfaces can be exploited to manipulate device functionalities or steal data.

- System vulnerabilities

IoT device application software or operating system software has logical defects or errors in design, which can be exploited by attackers to control the entire device through network implantation of Trojan horses, viruses, and other methods, resulting in abnormal device operation.

- Data leakage

The application layer manages a large volume of data, which is prone to leakage if not encrypted or access control not properly managed.

- Outdated components

The application layer uses components with known vulnerabilities or expired components. If the components are not updated in a timely manner, the inherent vulnerabilities of the components can be easily exploited.

- Configuration vulnerabilities

In the security configuration for applications, frameworks, containers and operating systems, security vulnerabilities caused by unreasonable or improper configuration, such as using versions with security flaws, granting excessive permissions to certain accounts, and failing to control access to sensitive resources may allow attackers to access certain system data or use system functions without authorization.

After investigating the numerous hidden security risks in the IoT environment, as well as the complexities of computational capabilities and the complex hardware and software environment, Hikvision developed the video-centric IoT security solutions that promise to create a brand new security architecture, establish a multi-dimensional security system, and guarantee terminal security, data security, application security, network security, personal data protection, and security compliance.

2. Product Security Structure

Product security architecture safeguards product security across five dimensions: device security, cybersecurity, application security, data security, and secure operations. Each dimension employs a variety of security techniques. Moreover, the security techniques comply with the legal requirements of the country/region in which they are applied, meeting security and compliance requirements.

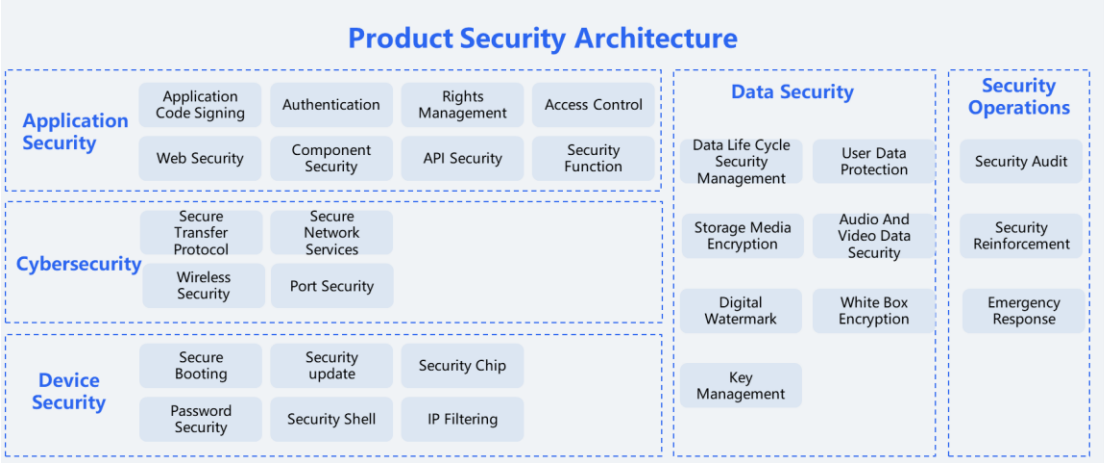


Figure 2-1 Product Security Architecture

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 Hikvision device hardware and software ensures each component of the system can be trusted and the whole system is verified. Security measures for each step, from the initial start to the software update, will be analyzed and examined.

Security Chip

To meet the high security requirements of the devices, Hikvision makes full use of the security features such as OTP and TrustZone, and combines them with the use of high-performance security chips, to realize high-intensity security at the hardware level, which provides a solid foundation for secure booting, secure upgrade, and stream encryption.

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 the form of plain text.

TrustZone is a security technology provided by ARM architecture in the processors, and lays the foundations for designing highly secure embedded systems. It divides hardware and software resources into two execution environments: The Secure World and Normal World. Physical isolation through hardware logic reduces the likelihood of attacks on sensitive and confidential resources by placing them in a secure environment.

Resources 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 comes with a hardware true random number generator, which ensures that the keys and random data in the device function with robust randomness.

Secure Booting

Secure booting is the cornerstone of device security.

The code for secure boot is embedded within the chip, ensuring that the initial loading logic cannot be tampered with. After the device is started, it immediately executes the boot code stored in read-only memory (Boot ROM). The Boot ROM code uses Hikvision's firmware signature public key to verify whether the underlying bootloader has been signed, and determine whether it is allowed to load. Each component involved in the boot process is digitally signed to ensure its integrity. Only after successful verification, each step can proceed, forming a secure boot chain. The programs included in the boot process primarily consist of the bootloader, kernel, and applications, among others. The secure boot chain helps ensure that the software has not been tampered with.

If at any point during this boot process, a step cannot load or fails to verify, the boot process will halt, and the device will be unable to function.

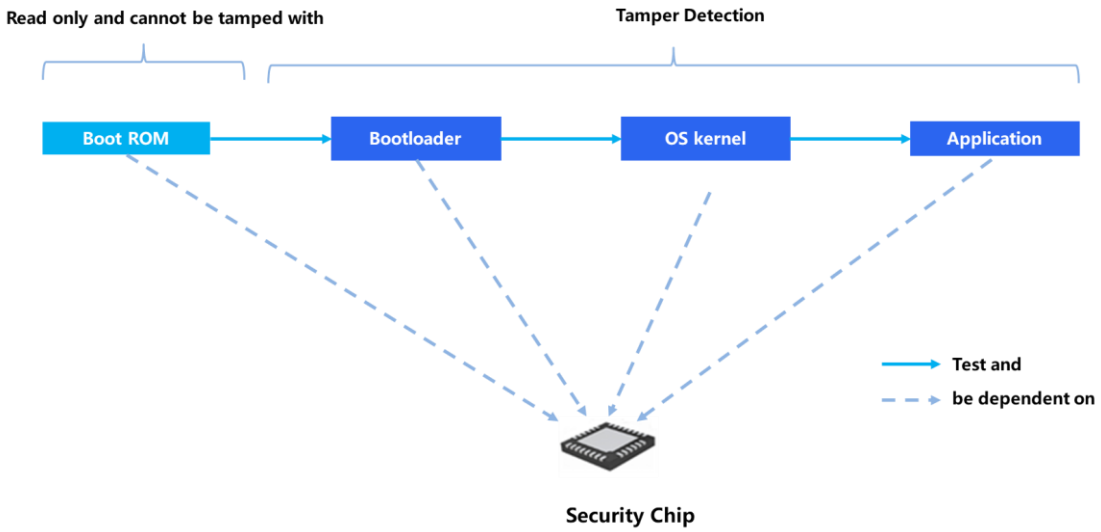


Figure 2-2 Secure Booting

Security Update

Hikvision promptly releases software updates to address emerging security issues. Users can see firmware update notifications on their devices and client software, and we encourage them to apply the latest firmware for security fixes as soon as possible.

Secure communication mechanisms (e.g., HTTPS) are adopted during the transmission of updated 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.

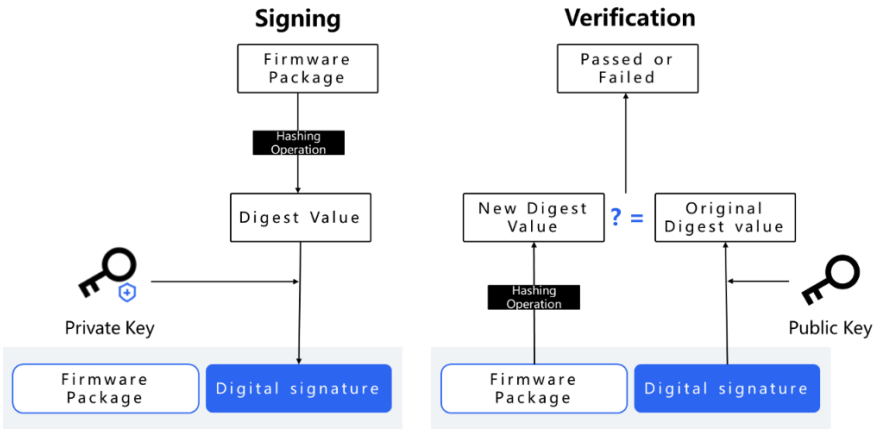


Figure 2-3 Digital Signature and Signature Verification Process

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 adopts an anti-degradation mechanism to prevent the device from being downgraded to an earlier version that could expose patched vulnerabilities.

Password Security

Hikvision's device account security system relies on a series of password and access control strategies to fully ensure user account security:

- User account password complexity requirement: The password for the user account must have a complexity requirement of at least eight characters or more, and contain two or more different character types (numbers, uppercase and lowercase letters, special symbols).
- Activation mechanism: When users first access the device, they are forced to set a new password that meets security requirements to activate the device, eliminating default password issues.
- Illegal login monitoring: The system monitors illegal login attempts and provides multiple login failure locking functions to effectively prevent brute-force attacks. The maximum number of consecutive failed login attempts and the lock time can be configured.

Secure Shell

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

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.

2.2 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 the trust chain from the operating system to the application level, effectively preventing unauthorized applications from running.

Devices can be protected from attacks by code signing, which ensures that all running codes are authorized and that malicious codes cannot run. Compared to the Internet, code signature technology in IoT can be applied not only to the applications, but also the firmware, where all important devices, including sensors, switches, etc., have to ensure that all the codes running on them are signed. It also ensures that codes that have not been signed cannot run.

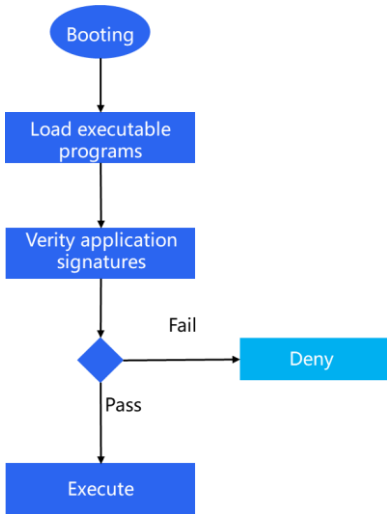


Figure 2-4 Application Code Signing Process

As some embedded devices in IoT are resource-constrained, with limited capacities in processor, communication and storage, Hikvision established a set of code signing mechanisms tailor-made for IoT, which strikes a balance of security, efficiency, and performance.

Identity Authentication

The identity management system defines and manages the access permissions of each user's identity role and required resources, and dynamically manages their required resource access

permissions based on their identity role lifecycle, achieving functions such as unified identity management, unified identity authentication, unified access control, and permission compliance management

- Ensure the uniqueness of the user identity throughout its entire lifecycle.
- Access Control: Provides the access control functions, uses roles to assign different users' rights and control the rights of logged-in users.
- Two-factor authentication: Optional support of two-factor authentication based on digital certificates to bolster security authentication.

Permission Management

Hikvision limits the access permissions of applications, categorizes and grades permissions, and configures permissions based on business relevance and minimum authorization principles. Only authorized users can log in or access applications.

Access Control

Hikvision devices all support user permission and access control management, providing multi-dimensional security guarantees for user operations and device access control:

- User permission grading: The device provides user permission role division, distinguishing between different roles such as administrators and other users, etc.
- User operation control: Access control is implemented for users' sensitive behavior (such as controlling devices, modifying device attributes, etc.) based on their device operations, which can effectively prevent sensitive information from being accessed and sensitive operational actions without authorization.
- Minimum authorization: All operation permissions are functionally specific and can be set individually for each user. Thus, it prevents security risks caused by a user's improper operations or identity theft.

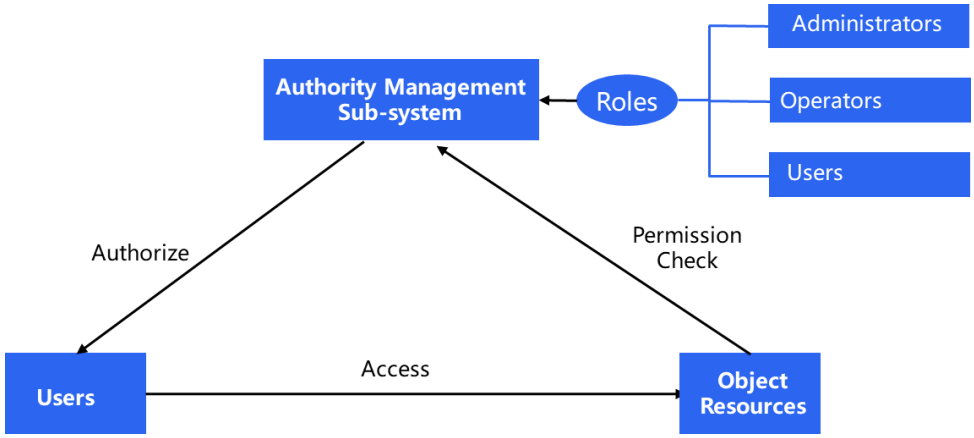


Figure 2-5 User Permission and Device Access Control Management

Web Security

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

- All data from untrusted sources is verified on the server side, and those that fail verification are rejected. If the data transmitted to the client is from an untrusted data source, the data will be encoded or converted to escape characters accordingly.
- User access/operation permission verification is enforced to prevent horizontal/vertical overreach.
- Key information of uploaded files, such as type, format, content and size, will be checked for validity to prevent malicious files.
- Unauthorized access and information leakage can be prevented with data access control and sensitive data encryption.
- Source identifications and content detections are carried out on requests received by the server side to eliminate forgery attacks.
- According to different application scenarios, web container configurations will be audited strictly to ensure the security of the configurations.
- The session ID of the web application is random and unique. After the authentication is successful, the session ID is changed to prevent the session from being fixed.
- Session timeout and auto-disconnection: the timeout period is configurable. If there is no interaction for the set period, 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 allowable can be limited to prevent unauthorized access.
- Session lock: when the number of failed authentication attempts exceeds the preset

number, the user is automatically locked from subsequent attempts, effectively preventing brute-force attacks. The number of failed attempts before activating lock-out mode is configurable.

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

Component Security

Before the design of a product architecture, Hikvision analyzes the security of the short-listed open-source and third-party software in product development, including their open-source protocols, compliance, unfixed security vulnerabilities, potential risks, etc. The Company strictly follows the principle of "security analysis before introduction".

During the testing stages, the team analyzes and verifies the source code consistency of open-source and third-party software, and conducts security scans of the software to detect the presence of old components or components with unrepaired vulnerabilities in the device, This includes components from earlier versions and components with CVE vulnerabilities. Our team also makes relevant rectifications to ensure the security of open-source and third-party software in the released version of the device is ensured.

API Security

In IoT products, there are various APIs that call and access each other, and interface abuse must be prevented. For API security, it can include but is not limited to the following functions:

- Provide an authentication mechanism when calling APIs to identify and authenticate users that access open APIs and manage access permissions.
- Use security protocols such as HTTPS, SSL/TLS, etc. for API access.
- Apply rate restrictions and set access quotas for API access.
- Use input and output verification components for API calls, restrict or filter unsafe input parameters of the interface, provide exception handling capabilities for the interface, and prevent injection attacks.
- Logs should be provided for API call access for audit purposes.

Security Function

Due to the lack of a built-in boundary checking-mechanisms in the C/C++language, many functions provided by standard function libraries do not check for overflow, such as memcpy(),

strcat(), strcpy(), sprintf(), gets(), etc. When these functions are improperly used or the parameters of the functions are maliciously input by malicious users in some form, it is highly possible to create a buffer overflow vulnerability, leading to serious security risks such as program termination or even dangerous code execution. Traditionally, such functions are referred to as dangerous functions.

To prevent vulnerabilities that may arise from the use of dangerous functions, Hikvision encapsulates based on functions of the standard library. Together with validation and mitigation measures, The Company launched the Hikvision Security Function Library. Our self-developed code static scanning platform enables comprehensive detection of dangerous functions to ensure the effective implementation of secure functions in our products.

2.3 Cybersecurity

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

In addition to the built-in security mechanism that protects stored data in devices, there are also several cybersecurity measures available to ensure the security and accuracy of the information when transmitting to and from the devices. To achieve these security objectives, Hikvision integrates proven technologies and the latest standards for data network connectivity.

Secure Protocol

The network transmission of all Hikvision products supports secure transfer protocols such as 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, TLSv1.0/1.1, SNMPv2, etc. are turned off by default;
- Private protocols all support TLS-based transmission;
- Syslog protocol supports transmission based on TLS or DTLS;
- 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 exposure to attacks:

- Telnet service is not supported;
- FTP service is not supported, SFTP service is supported;
- SSH service is disabled by default;
- SNMP service is disabled by default, and secure SNMPv3 is supported;
- NTP service is disabled by default;
- UPNP service is disabled by default.

Wireless 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: 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 products are open by default to ports only directly relevant to customers' demands, with all other ports closed. We clarify all the ports that can be opened, the business functions and authentication methods corresponding to the ports, and whether the ports are opened by default in the product communication matrix, so that customers can stay informed and make necessary changes.

2.4 Data Security

Data Life Cycle Security Management

The company's product or service team consider the protection of personal data during the requirements analysis and design phase, and use appropriate technical and management measures to ensure the security of personal data according to specific business use scenarios. A Product Personal Data Statement is included in the product interface, if the company is involved in the processing of personal information. The Statement describes the

type, purpose, processing method, retention period, risks or recommendations of all personal data generated in the product.

Data subjects have the right to be informed, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restrict processing, the right to data portability, the right to object, and the right to not be subject to automated decisions. To comply with regulations and better protect the data security, functions that support data subjects in exercising the above rights are included in the design and implementation of products and services.

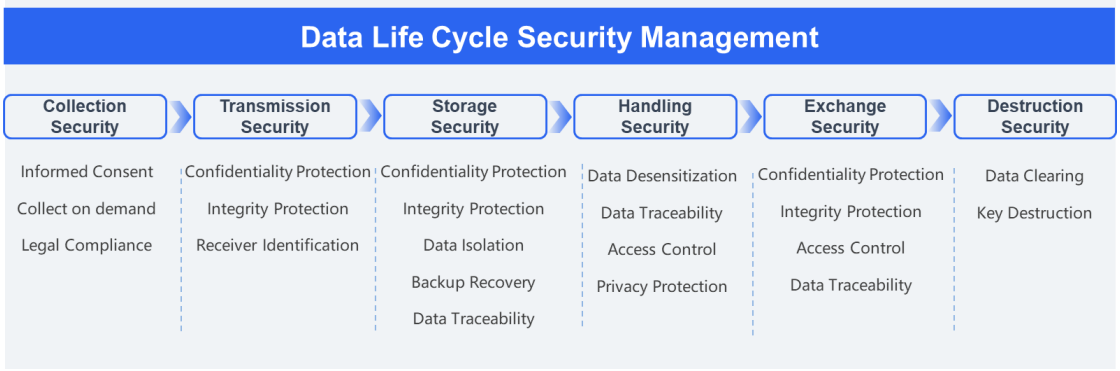


Figure 2-6 Data Life Cycle Security Management

1. Data Collection Security

Compliance with the applicable laws and regulations is a must for data collection. Users must be informed, and principles such as user consent and data minimization should be followed. Data should only be collected as needed, and the scope of collection and purposes of use should be clearly outlined in the personal data policy. When users engage with services or products that involve personal data, such as using Hikvision cloud services or IoT devices, Hikvision will inform users of the scope and purposes of data collection in accordance with applicable laws and regulations. Personal data will be collected only upon obtaining user consent.

2. Data Transmission Security

When transmitting collected data, it's crucial to authenticate the identities of both communication parties to ensure that the entity receiving or sending data is a legitimate user. This is primarily achieved through cryptographic techniques like message digests and digital signatures. During transmission, it's essential to prevent data leakage and to detect any tampering with the data. This involves ensuring the confidentiality and integrity of the

transmitted data, which can be achieved using encryption, hashing, and digital signatures, among other traditional cryptographic algorithms. Hikvision product transmission security is ensured by utilizing the SSL/TLS protocol to guarantee the confidentiality and integrity of the data.

3. Data Storage Security

When storing data, data can be segregated and stored based on different levels of sensitivity. This can be achieved through various techniques such as physical isolation, logical isolation, or virtualization to create separation between areas containing data of different security levels.

Data storage media can potentially experience malfunctions or data loss. To ensure the availability of stored data, redundancy mechanisms are employed to back up the data. When the data storage media becomes available again, data recovery and restoration are carried out to bring the data back to its original state.

After data is stored, it's important to establish data traceability mechanisms. This ensures that if data is illicitly leaked, it can still be traced, allowing identification of the source of the leak and enabling relevant audits. Digital watermarking technologies can be employed to achieve data traceability in such cases.

When storing data, it's also essential to ensure data confidentiality and integrity. This means that even if attackers manage to access the data, they should not be able to retrieve meaningful information, and any unauthorized modifications should be detectable. To achieve this, traditional cryptographic techniques such as encryption, hashing, and digital signatures can be used. These techniques play a vital role in safeguarding data from unauthorized access and tampering.

Data storage security is ensured by employing standard cryptographic algorithms to ensure data confidentiality and integrity. The cryptographic algorithm calculation module provided by the vendor utilizes cryptographic cards that comply with commercial cryptography specifications.

4. Data Processing Security

When processing and computing data, it is essential to ensure that users have the corresponding permissions. When data is used, sensitive information should be anonymized based on business relevance and the principle of least privilege. In data calculations, it is crucial to prevent the extraction of additional personal information from intermediate results. Privacy-preserving technologies such as secure multi-party computation, homomorphic encryption, and differential privacy computing can be employed to protect personal information during the data usage process. Hikvision employs techniques such as data anonymization, encryption, and privacy-preserving computing to safeguard personal information during the data processing.

5. Data Exchange Security

Security control on data exchange channels is necessary for data transmission and sharing, with measures such as mandatory identity authentication and strict access control. Data watermarking and other methods are used for traceability in the process of data exchange. Hikvision adopts password technology to ensure data confidentiality, integrity and access control in interacting with data, and employs digital watermarking technology for data traceability.

6. Data Destruction Security

Logical deletion and physical destruction are to be employed for data destruction to prevent the data from being recovered or retrieved after erasure, especially sensitive data such as passwords and keys.

User Data Protection

With cryptographic technologies, Hikvision protects user data, which includes user configuration data and sensitive personal data. A data encryption key is randomly generated by the random number generator as the device first boots up, enabling "one key for one device". This ensures the randomness of each device. The device's random key prevents attackers from decrypting any data, even if they have forcibly copied it from the device. User configuration data mainly includes user configuration parameters, usage information, etc. Sensitive personal data includes, but is not limited to user password, key, etc.

Storage Media Encryption

Encryption of all kinds of data on all kinds of storage media is supported to avoid data leakage. In particular, key data (such as audio and video data) on portable storage media are encrypted. Portable storage media include TF/SD cards and hard disks.

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 security 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.

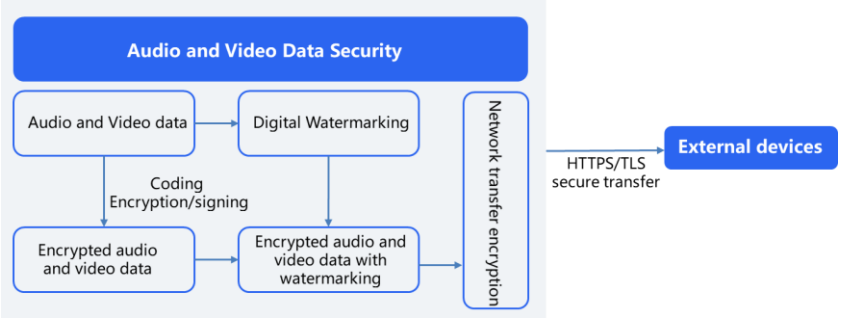


Figure 2-7 Audio and video encryption transmission process

Digital Watermark

Data watermarking refers to the embedding or implicit marking of data files (such as videos, audio, images, documents, databases, models, etc.) based on information security,

information hiding, data encryption, and other technologies, to cope with traceability and copyright declaration after data leakage.

The digital watermarking system mainly includes two stages: embedding and extraction. In the embedding stage, the main goal of the embedding algorithm is to find a better compromise between the invisibility and robustness of the digital watermark. The extraction stage includes an extraction algorithm corresponding to the embedding process. At present, to prevent attackers from removing the watermark, most watermarking schemes use keys in embedding and extraction, and only those who have the key can read the watermark.

Data watermarking is the last line of defense against data leakage. Therefore, from the perspective of watermarking technology itself, it has broad application prospects and huge economic value.

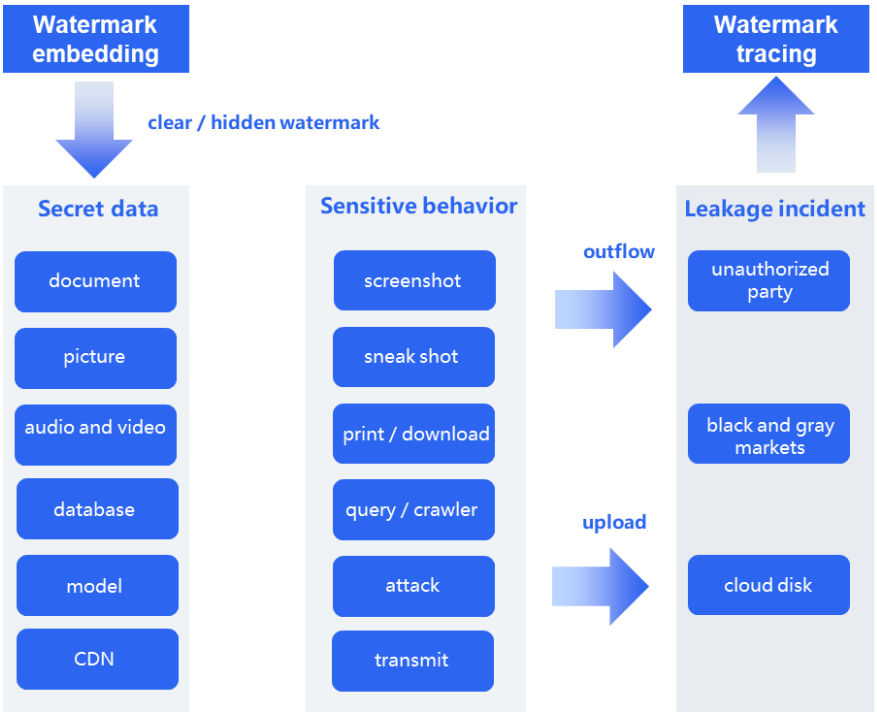


Figure 2-8 Digital watermark

White Box Encryption

White box encryption is a technology that resists white box attacks and protects the security of keys, by making it difficult for attackers to analyze keys from intermediate data. White box encryption can be divided into static white box and dynamic white box according to implementation methods.

Static white box: The key is processed and obfuscated to generate a lookup table and finally a static white box library. The static white box library is directly called for encryption and decryption. Since the operations in the static white-box library are implemented by way of lookup tables, the attacker cannot deduce the key by analyzing the intermediate data, and the user does not need to maintain the key. However, if the key is changed, the static library needs to be recompiled.

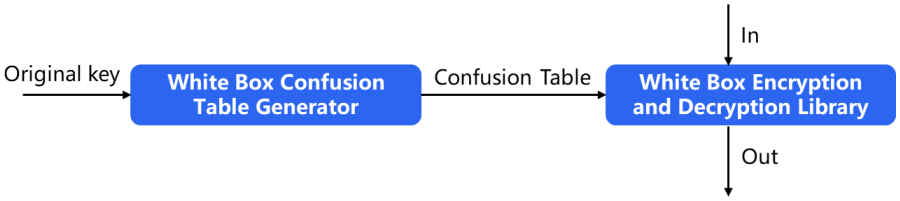


Figure 2-9 Static white box usage process

Dynamic white box: If the key is modified during use, there is no need to regenerate the white box library. Firstly, a non-linear obfuscation lookup table needs to be generated, which is used by the white box key generation tool and white box library. The original key is generated by a key generation tool to generate a white box key, and users only need to use the white box key and white box library to encrypt and decrypt. Generating a new white-box key on the server would replace the key without replacing the white-box library.

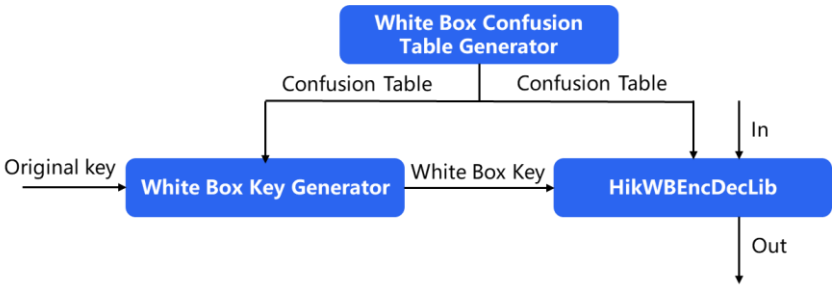


Figure 2-10 Dynamic white box usage process

Key Management

The keys stored on the device are kept in a hardware secure zone and employ a layered key architecture. Typically, the key architecture consists of three layers for protection: the master key, the key encryption key, and the business key. The business key can be further categorized based on usage, such as file keys or data encryption keys. The device allows customization and expansion of the key architecture according to the scenarios of the business application. At a minimum, the device must support a two-layer key architecture.

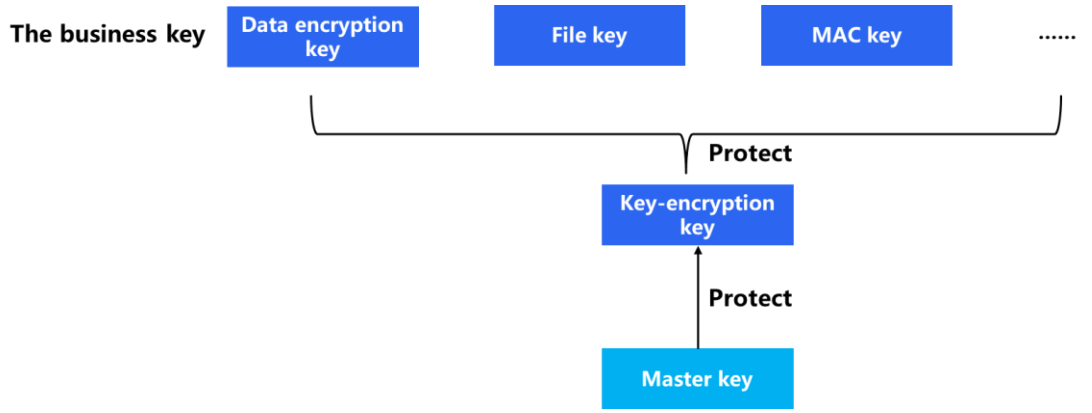


Figure 2-11 Key Layered Management

2.5 Security Operations

Security Audit

Hikvision's security audit logs list the detailed records related to product security activities, including the information required for audits and the identification of various anomalies. The report generated with the audit results detail all data activities, such as login failures, configuration changes, user management, device upgrades and maintenance, and access failures, with all user operation records available.

In addition, the logs ensure that the audit process shall not be interrupted, and audit records not be deleted, modified, or overwritten. Anomaly alarms will be triggered if risks are detected.

Local logs are stored securely and 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 server in real time.

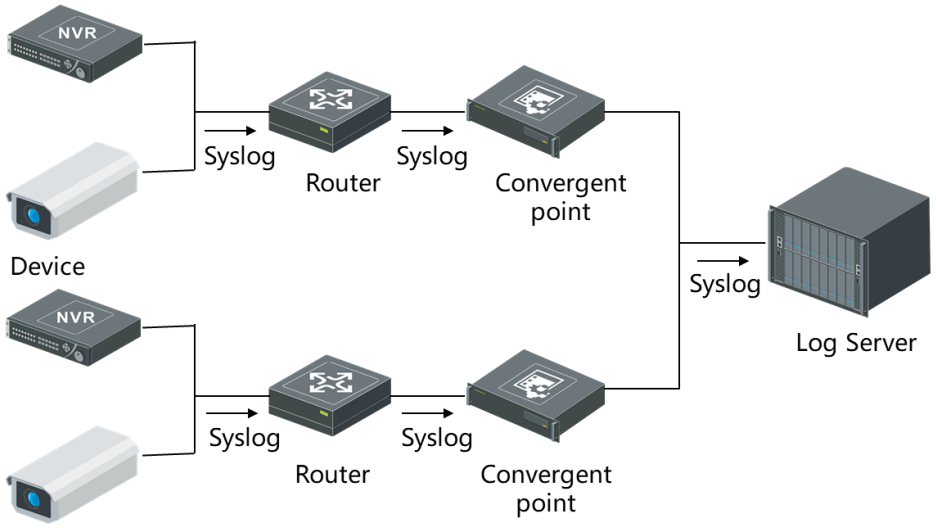


Figure 2-12 Syslog Log Management Service

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

Security Harden

Regular security hardening should be carried out on various devices or systems, such as updating configurations, installing security patches, etc. In case of an emergency, hardening measures should be taken immediately to repair the loopholes. Vulnerability scanning can provide comprehensive vulnerability detection services such as operating systems, software, weak passwords, ports, etc., to check and evaluate the security status of systems and applications running in various stages of the system, and for timely discovery of potential security vulnerabilities.

For example, the basic security hardening of the operating system can include the following items:

- Minimize services: Disable unnecessary or dangerous system backend processes and services, such as email agents, graphical desktops, Telnet, compilation tools, etc.
- Service hardening: Secure commonly used services such as SSH and web.
- Kernel parameter adjustment: Modify kernel parameters to enhance operating system security, such as disabling IP forwarding, prohibiting response to broadcast requests, and prohibiting acceptance/forwarding of ICMP redirect messages.

- File directory permission setting: Hardening standards and application requirements in the industry are referenced to ensure that file permissions are minimized.
- Account and password security: Start password complexity check, password validity period, number of login failures and retries, etc.
- System authentication and authorization: Prohibit root remote login. It is recommended not to use a root account to install or run processes.
- Logging and auditing: Record the running logs of services and kernel processes, which can be connected to the logging server.

Emergency Response

Hikvision established the Hikvision Security Response Center (HSRC), which is responsible for receiving, addressing, disclosing, and resolving security-related vulnerability issues with Hikvision's products and solutions. Responsibilities include:

- Responding to and handling customer-submitted security incidents.
- Responding to and handling security matters reported by industrial associations.
- Formulating the company's information security incident management strategy and procedures for handling security incidents.
- Analyzing the vulnerabilities and patches announced and released by system software providers and professional security companies.

The company also specifies each department's responsibilities and the procedures for product security incident management to ensure the quality and efficiency of security incident management. The scope of the Security Response Center's management responsibility covers product security during the pre-sales, sales, and after-sales processes, and includes customers' security-related interactions, cooperation with security organizations, emergency response management, security information announcement, and the process and implementation of legal compliance.

Hikvision is a member of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Security Emergency Service Support Organization of the Industrial Information Security Industry Development Alliance. It shares

best practices and experience in security emergencies with other excellent members worldwide, promotes reliable communication and cooperation, and enhances the effectiveness and timeliness of the company's response to security incidents.

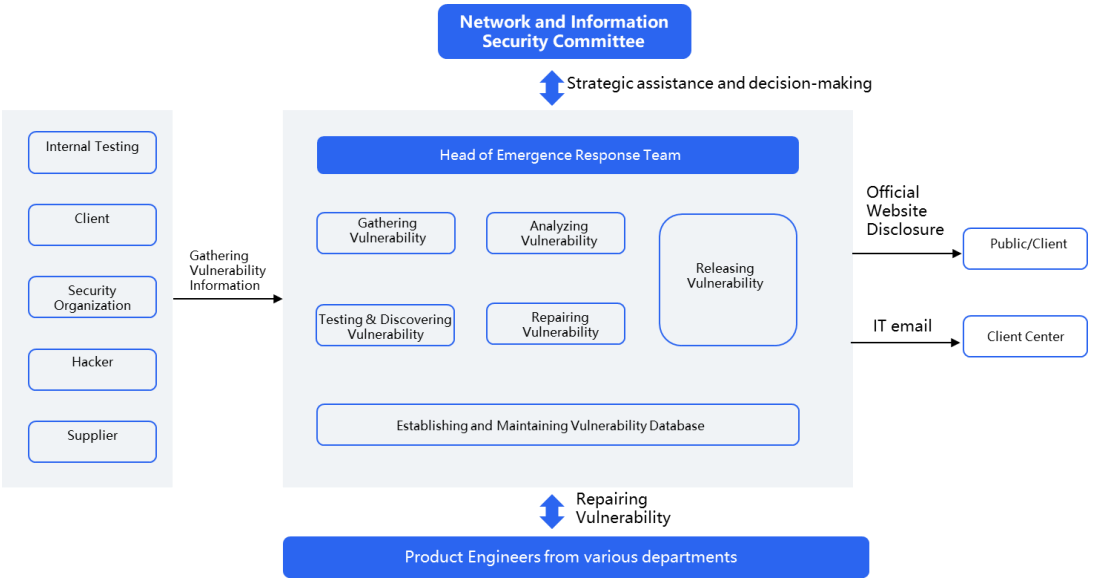


Figure 2-13 Security Emergency Response

3. Security Commitment

Common Criteria / ISO 15408

The Common Criteria (CC) certification is one of the most widely recognized international certifications in the field of information technology security. It is endorsed by the United States National Information Assurance Partnership (NIAP), which operates under the oversight of the National Institute of Standards and Technology (NIST). It is also recognized by countries such as the United Kingdom, Canada, and other nations. Currently, security certification organizations from 31 countries around the world have joined the CC Recognition Arrangement (CCRA). Since CCRA members are either government agencies or third-party authoritative organizations in their respective countries, CC certification has high acceptance and credibility on a global scale. It has become an important foundation for security assessments.

CC certification is primarily used to evaluate the security, reliability, and privacy protection of information technology products or solutions. The certification is divided into seven levels based on the Evaluation Assurance Levels (EAL), ranging from EAL1 to EAL7, with increasing levels of verification requirements.

In September 2018, two series of Hikvision cameras were certified with EAL2+[1], and another three series of cameras with EAL3+ in June 2022. Hikvision is committed to making all products up to the EAL3+ standards, thus improving the company's security practices and setting a great example within the industry.

Cybersecurity Labelling Scheme

In response to the growing threat of cybersecurity, the Singapore Cybersecurity Agency (CSA) launched the Cybersecurity Labeling Scheme (CLS) in 2020. CLS rates consumer-grade IoT devices based on their ability to withstand network attacks, and divides them into four security levels. The corresponding verification requirements increase from Level 1 to Level 4.

In September 2023, four series of Hikvision cameras were certified with CLS Level 4.

[1] CC certificate query: https://www.commoncriteriaportal.org/

4. Typical Security Practices

4.1 IoT Product Security Design Practice

Hikvision manufactures a wide range of products. Take the smart IP Camera (IPC) as an example. Smart IPCs serve as the video data collection ends of data services. From front-end security protection to cloud storage data security control, we always adhere to the principle of defense in depth to ensure the security and compliance of the product, prevent data loss and information leakage, and enable traceability.

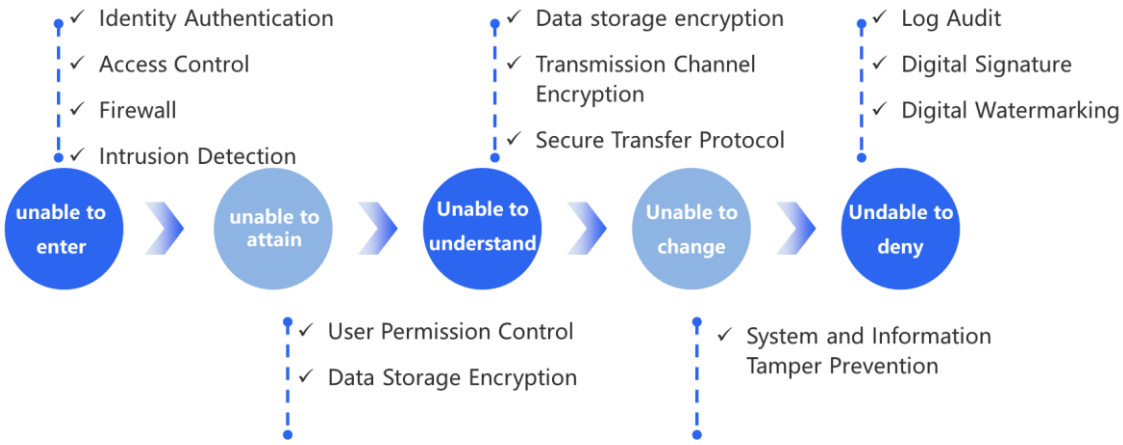


Figure 4-1 IoT Product Security Design Practices Reference Guide

4.2 AIoT Security Management and Control Practice

With the rapid development of the Internet of Things, its security issues have become increasingly prominent:

- IoT devices are prone to risks of weak passwords and vulnerabilities, leading to security issues such as illegal intrusion and data theft.
- A large number of widely-distributed IoT devices make it hard to verify the configurations.
- It is difficult to manage the security policy and password maintenance of IoT devices
- Scattered deployment of IoT devices are prone to replacements and counterfeits, making itself vulnerable to hackers.
- IoT devices are easily exploited by hackers, malicious codes and illegal intrusions.

- Elusive security situations, and delayed responses to abnormal operations and threats may result in frequent security risks.

- Crypto equipment, keys, etc. cannot be monitored in real time, and password security events cannot be displayed in a centralized manner.

Hikvision AIoT security management solution includes: IoT situational awareness platform, IoT traffic threat probe, video firewall, security access control system, device security management system, host security detection and response system.

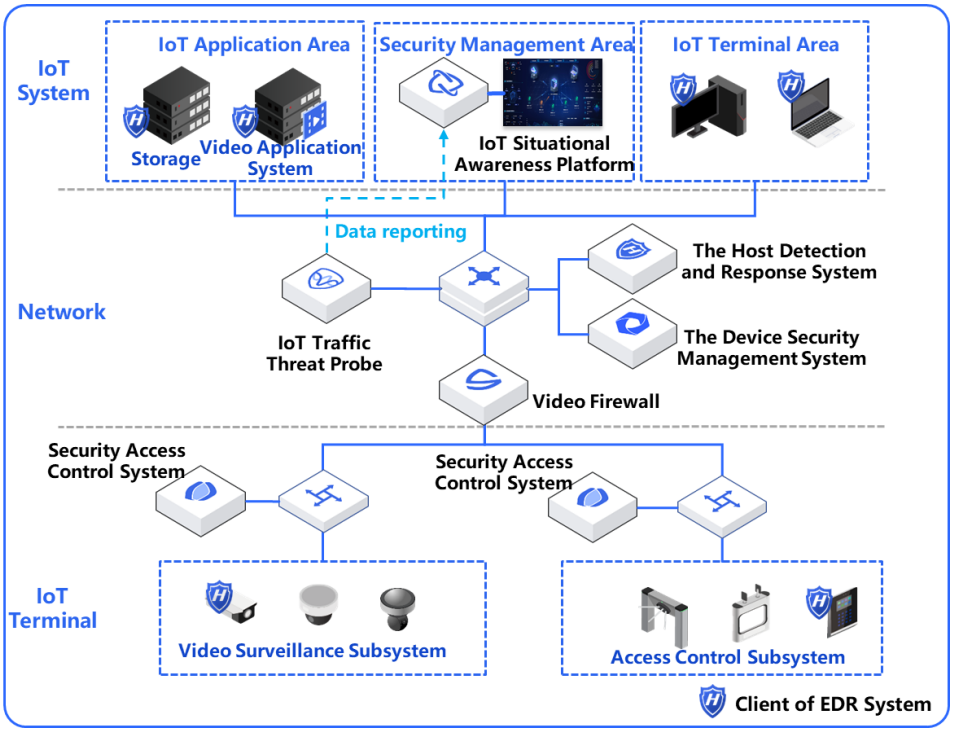


Figure 4-2 AIoT Security Management Solution

- The IoT situational awareness platform enables asset and threat visualization analysis, and security situation visualization presentation

- The IoT traffic threat probe enables refined security auditing of video traffic.

- The video firewall enables efficient detection and response to cyber threats.

- The security access control system realizes unified security management and access control of IoT terminals.

- The host detection and response system implements baseline configuration verification of IoT terminals, efficient detection and repair of terminal vulnerabilities.

- The device security management system realizes automatic operation and maintenance of terminal passwords, and remote and real-time distribution of security policies.

4.3 Hikvision Cluster Storage Security Practice

Hikvision Cluster Storage is a cloud storage device that takes video storage technology as its core and deeply integrates cloud storage technology with intelligent applications from the video security industry, to realize integrated storage of videos, pictures, files, and object data. Hikvision Cluster Storage Devices have long-term and extensive industry applications, and have currently served tens of thousands of security video storage projects. In terms of the storage security of data, Hikvision Cluster Storage ensures the storage security of transmission security, host system security, data secure storage and system access security.

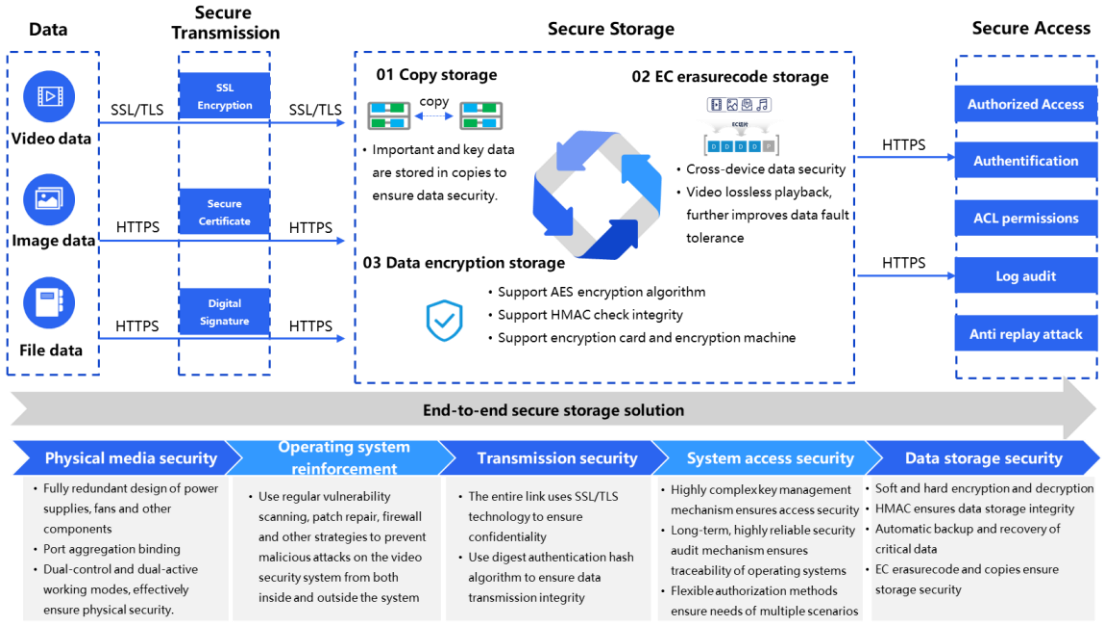


Figure 4-3 Supports Multi-level Data Security Assurance

5. Security Commitments and Recommendations

Hikvision is committed to employing cutting-edge security and personal data protection technologies to assist customers in safeguarding their personal information. Additionally, the company adopts a comprehensive approach to ensure the protection of user data.

Hikvision uses a unified and integrated security infrastructure across the entire AIoT application ecosystem. Hikvision has a professional security team responsible for providing support for all Hikvision products. The team provides security reviews and testing for both in-development and released products and also monitors and provides reports of new security issues and threats.

Product security not only requires manufacturers' continuous efforts and improvements in R&D, production, delivery and maintenance, but also requires the active participation of customers to improve the usage environment and methods of products, and ensure the safe operation of products after delivery. To this end, we recommend the secure uses of devices, including but not limited to:

1. Account security

- Complex passwords are required, the setting of which is recommended as follows:

  - ✓ The password must be no fewer than eight characters.
  - ✓ It must contain at least two types of character types (numbers, uppercase and lowercase letters, special symbols).
  - ✓ Do not use risky passwords, including but not limited to medium-length passwords that contain the username or the reverse order of the username, four consecutive or more increasing or decreasing numbers, and four consecutive or more of the same characters.
  - ✓ Avoid using default passwords.

- Update passwords regularly

  It is recommended to update passwords regularly to reduce the risk of being leaked or cracked.

- Properly allocate accounts and permissions

It is recommended to add accounts appropriately based on actual business scenarios and configure permissions based on the principle of minimum authorization.

2. Security configuration

- Use security protocols by default

  It is recommended to use HTTPS to access web services by default.

- Audio and video-encrypted transmission

  It is recommended to enable audio and video encoding encryption and network transmission encryption in scenarios with sensitive audio and video data to reduce the risk of data being tampered with and illegally viewed during the encoding or transmission stage.

- Disable unsafe services by default

  Disable various management services such as Telnet, FTP, SNMP, UPNP, etc. by default to reduce the threat surface of the device.

- Disable unnecessary functions and services

  Many IoT devices provide various functions and services, but not all are required, and disabling unnecessary functions and services can reduce the attack surface of the device.

- Port configuration security

  It is recommended that users only open ports necessary for business when configuring secure ports.

3. Update device software and firmware in a timely manner

Following industry standard operating practices, device software and firmware must be updated to the latest version in a timely manner to ensure that the device can promptly repair known security vulnerabilities and improve device security. If the device is connected to the public network, it is recommended to enable the automatic detection function for online

upgrades so that it can promptly obtain software and firmware update information released by the manufacturer.

4. Audit security

- Review online users

  It is recommended to review online users from time to time to identify whether there are illegal user logins.

- Audit device logs

  The IP information, login time, login results and key operation information of the logged-in user on the device can be obtained by reviewing the logs.

- Configure network

  Due to the limited storage capacity of the device itself, the log storage capacity is limited. It is recommended to enable the syslog log management capability to ensure that log data is safely uploaded to the log server for centralized storage in real time and to ensure that problems can be traced.

5. Physical security

It is recommended to physically protect the devices (especially storage devices), such as placing them in a dedicated computer room or cabinet, and managing access rights and keys to prevent unauthorized personnel from damaging hardware and protecting external devices from other physical attacks.

For more information on how to report risks to Hikvision, please refer to:

https://www.hikvision.com/en/support/cybersecurity/

Hikvision
Product Security White Paper

See Far, Go Further

Hangzhou Hikvision Digital Technology Co., Ltd.
No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China