Dahua Product Security White Paper

V3.0

Zhejiang Dahua Technology Co., Ltd

Legal Notice

Copyright Statement

Without the prior written permission of Zhejiang Dahua Technology Co., Ltd. (hereinafter referred to as "Dahua"), no one may copy, transmit, distribute or store any content of this document in any form.

The products described in this document may contain software copyrighted by Dahua and other third parties. No one shall copy, distribute, modify, extract, decompile, disassemble, decrypt, reverse engineer, lease, transfer, sublicense or otherwise infringe the copyright of the software in any form except with the permission of the relevant owner.

Trademark Statement

- alhua、alhua、alhua TECHNOLOGY、alhua TECHNOLOGY、HDCVI are trademarks or registered trademarks of Zhejiang Dahua Technology Co., Ltd.
- HDMI HIGH-DEFINITION MULTIMEDIA INTERFACE: This statement applies to all products. If products use HDMI technology, the terms HDMI, HDMI High-Definition Multimedia Interface, HDMI commercial appearance and HDMI logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. The product in this document has been authorized by HDMI Licensing Administrator, Inc. to use the HDMI technology.
- VGA are trademarks of IBM.
- The Windows logo and Windows are trademarks or registered trademarks of Microsoft Corporation.
- Other trademarks or company names that may be mentioned in this document are the property of their respective owners.

Responsibility Statement

- To the extent permitted by applicable laws, in no case will the company compensate for any special, attached, indirect and secondary damages caused by the relevant contents and products described in this document, nor for any loss of profits, data, goodwill, documents or expected savings.
- The products described in this document are provided "in accordance with the status quo". Unless required by applicable laws, the company does not provide any express or implied warranties for all contents in the document.

Export Control Compliance Statement

Dahua complies with applicable export control laws and regulations and implements requirements related to the export, re-export and transfer of hardware, software, and technology. With regard to the products described in this manual, please kindly fully understand and strictly abide the applicable domestic and foreign export control laws and regulations.

About This Document

- The products, services or features you purchase shall be subjected to Dahua's commercial contracts and terms. All or part of the products, services or features described in this document may not be within the scope of your purchase or use.
- If the operation is not carried out according to the instructions in this document, any loss caused thereby shall be borne by the user.
- If the obtained PDF document cannot be opened, please upgrade the document reader software being used to its latest version or use other mainstream reading tools.
- Dahua reserves the right to modify any information in this document at any time, and the modified information will be added to the new version of this document. Please pay close attention to it.
- This document may contain technical inaccuracies, inconsistencies with product functions and operations, or typographical errors, which are all subject to Dahua's final interpretation.

Foreword

Overview

With the maturity of Internet of Things, Artificial Intelligence, Big Data and other technologies, more and more enterprises have regarded Artificial Intelligence & Internet of Things (AIoT) as one of their main development directions. Responsible, open, professional and systematic cybersecurity and privacy protection have become the guarantee and foundation for promoting the long-term healthy development of the industry. Dahua attaches great importance to cybersecurity and privacy protection, and continues to set up special funds to ensure the R&D and delivery of secured products, research on key security technologies, security compliance and incident response system construction. At present, Dahua has made fruitful achievements in security technology fields such as trusted computing, data security, privacy protection, and penetration test, which have been applied in a wide range of products.

Scope

This document applies to Dahua hardware products. It aims to describe the exploration and practice in security field, and to let users, partners, industry organizations, and government agencies know Dahua security capabilities from an open and transparent perspective.

This document will comprehensively elaborate on the security measures for hardware products from the perspectives of security engineering practice, security technology applications, security compliance, and security incidence response.

Glossary

Abbreviation	Explanation
AIoT	The Artificial Intelligence of Things
ARP	Address Resolution Protocol
ESD	Electrostatic Discharge
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
I2C	Inter-Integrated Circuit
KMS	Key Management Service
KDF	Key Derivation Function
OTP	One Time Programmable
PKI	Public Key Infrastructure
PSIRT	Product Security Incident Response Team
RBAC	Role-Based Access Control
SPI	Serial Peripheral Interface

sSDLC	secure Software Development Life Cycle
TLS	Transport Layer Security
TEE	Trusted Execution Environment

Revision History

No.	Version	Revised Contents	Release Date
1	V1.0	First Release	2017.6.30
2	V2.0	Added the new security baseline V1.3/V2.0/V2.1 iterative integration and the latest results of security technology research.	2020.2.28
3	V3.0	Added the latest research and application results of security technology and features.	2023.5.1

Table of Contents

1 Security Risk

Artificial Intelligence & Internet of Things (AIoT) collects data from different dimensions through the Internet of Things, stores them in the cloud and on the edge, and achieves digitalized and intelligent of everything based on big data analysis, AI or other technologies.

With the interconnectivity and intelligent development of all kinds of devices, the traditional cybersecurity boundary is constantly broken, thus posing greater challenges to cybersecurity:

- **Heterogeneity of devices**: There are many kinds of devices, different hardware and software architectures, and uneven performance, which make the implementation of security protection measures difficult.
- **Diversity of communication protocols:** Devices have a large number of transmission protocols. The security features of these protocols vary greatly, resulting in uneven transmission protection capabilities.
- **Openness of network:** The traditional network environment of hardware device is relatively closed, and its security boundary is relatively controllable. However, in the AIoT environment, a large number of devices are directly exposed to the network, and its security boundary has been greatly extended.

The development of technology has led to the diversification of attack methods, the security threats faced by AIoT devices are becoming more and more severe, including but not limited to the following:

- **Weak password:** A password that is easy to guess or crack, usually contains only simple numbers or letters, and may cause the device to be illegally controlled.
- **Spoofing:** The threat actor impersonates legitimate device identities and access networks to carry out malicious activities.
- **Malware:** An unauthorized program or code that interferes or damages the functionality of a device or network.
- **Data breach:** Unauthorized access, to steal user's data.
- **Privacy invasion:** Users' personal information is collected and used insecurely, improperly, or without authorization.
- **Security vulnerability:** Flaws in the specific implementation or security policies of software and hardware, allowing a threat actor to access or compromise the system without authorization.

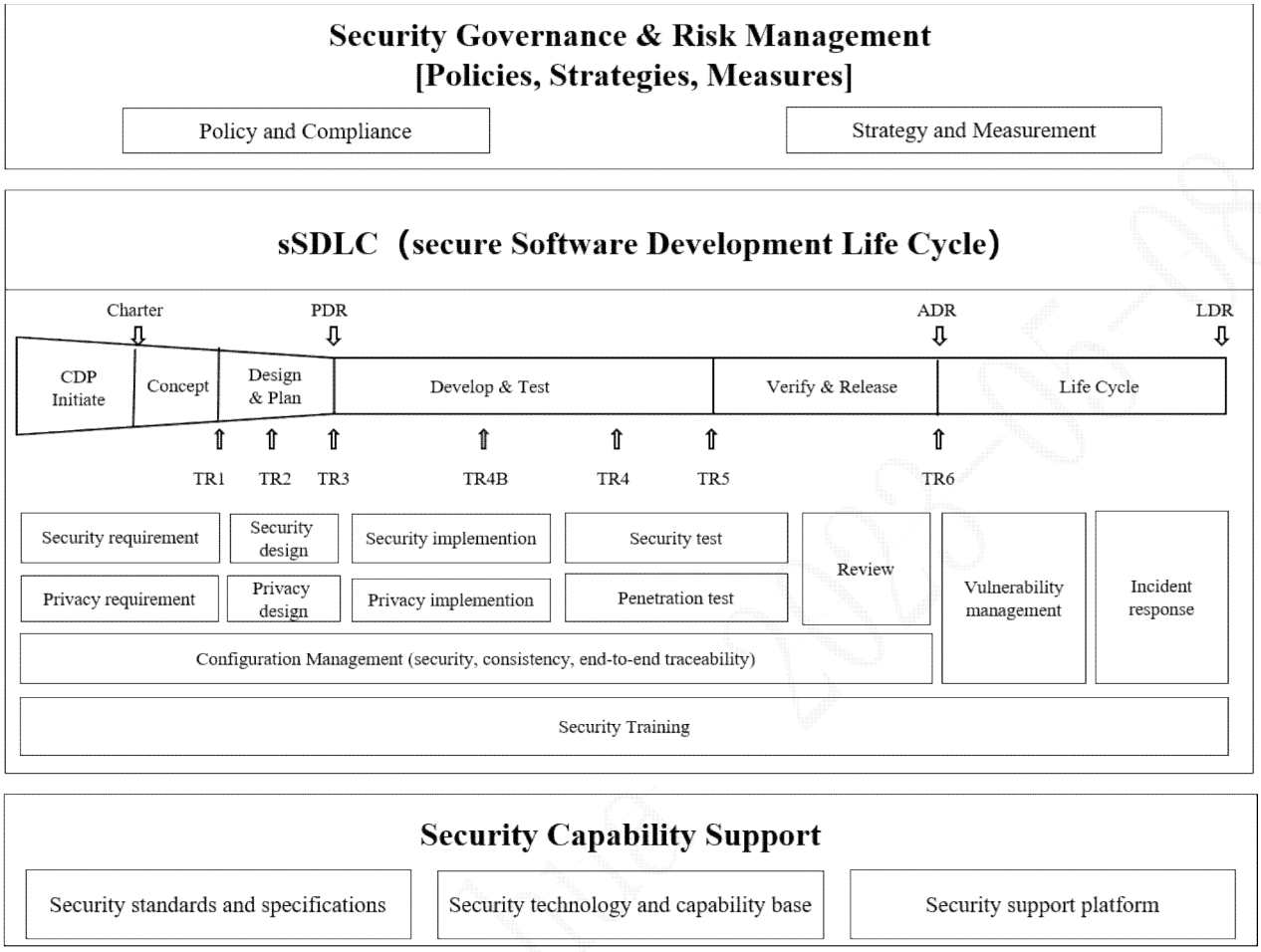

Figure 2-1 secure Software Development Life Cycle

Dahua continues to promote the construction of secure Software Development Life Cycle (sSDLC), regulates and controls the software development process, and further improves and optimizes the security software development process suitable for Dahua through comprehensive and in-depth assessment of the maturity of security activities.

- In the product definition phase, take security and privacy baseline as the most fundamental product requirements, carry out security and privacy risk assessment, and formulate the corresponding requirements and strategies based on the risk assessment results.
- In the product design phase, strictly adhere to the core principles of security design including minimizing attack surface and permission, implementing default security, in-depth defense etc. Collaborate with cyber security experts and product business experts to implement the concepts of "Security by Design", "Security by Default", "Privacy by Design", and "Privacy by Default", conduct threat modeling, and develop mitigation measures.
- In the product development phase, strictly adhere to secure coding specifications. Under the premise of code cross-inspection, static code security detection and defect repair are performed in a standardized manner. Meanwhile, the referenced open source software strictly complies with the

control requirements of Dahua Open Source Software.

- In the product acceptance phase, carry out comprehensive security activities such as virus scanning, host scanning, Web security scanning, known vulnerability scanning, mitigation measures verification, penetration testing and fuzzing testing.
- In the product release phase, review the consistency of security requirements and security design, check the satisfaction of the implementation of security measures and the completeness of security data.
- Throughout whole life cycle of product development, carry out trainings on security design principles, security coding specifications, security testing methods and the use of various security tools to enhance the security awareness and capabilities of all staff.

3 Security Techniques

3.1 Security Baseline

Since launching the "Security Baseline" program, Dahua has been adhering to the core concepts of "Secure by Design", "Secure by Default", "Privacy by Design" and "Privacy by Default", and has been deeply researching on cybersecurity and privacy protection technologies to provide users with adequate security and privacy protection.

The security baseline is based on (and implements) the security and privacy design principles, with authentication, authorization, audit, confidentiality, integrity, availability, and privacy as security elements for architecture design, forming a systematic AIoT product security framework that covers physical security, system security, application security, data security, network security, and privacy protection.

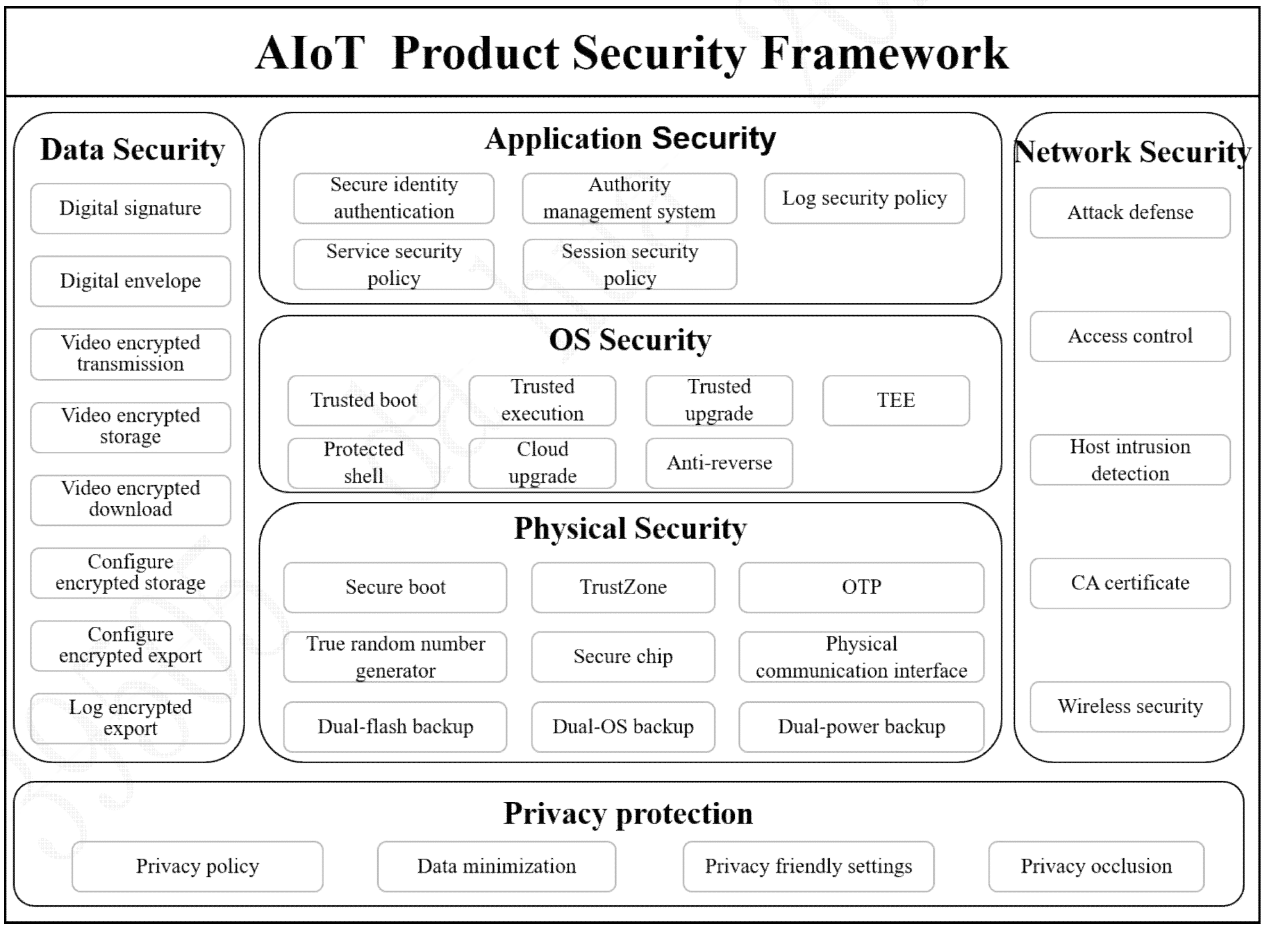

Figure 3-1 AIoT Product Security Framework

- **Physical Security**: From the perspective of physical protection of the product itself, using actual physical structural means as a protective measure to provide a secure and reliable physical framework for the product.

- **OS Security**: The operating system is the manager of resources, provides the basic operation environment for services, and constructs a secure and reliable fundamental operation environment through trusted computing, virtual technology, permission control and other technologies.
- **Application Security**: Form a closed-loop security protection structure based on authentication, authorization and auditing to strengthen the self-security capabilities of the service function at the application layer.
- **Data Security**: Based on cryptographic technology, the whole life cycle of data collection, transmission, storage, usage, sharing, display, copy, deletion and other security protection is built to avoid data leakage, tampering and destruction。
- **Network Security**: Introduce host intrusion detection, firewall and other defense technologies to improve the active awareness and defense capabilities against cyberattacks.
- **Privacy Protection**: Based on privacy function design, providing users with better privacy protection capabilities.

Dahua further solidifies its overall security framework into an enterprise standard and implements it into products through a security engineering support system, ensuring that users obtain the technical guarantee of factory default security.

With the development of the industry, iteration of technology and variation of attack methods, Dahua has continued to carry out a series of activities including “legal and regulatory compliance”, “standards and specifications analysis”, “industry dynamic tracking”, “pre-research of key technologies”, “security demand research” and “threat modeling analysis”, constantly iterating the security baseline standards, upgrading the security framework of AIoT products, to ensure the adequacy and cutting-edge of security protection.

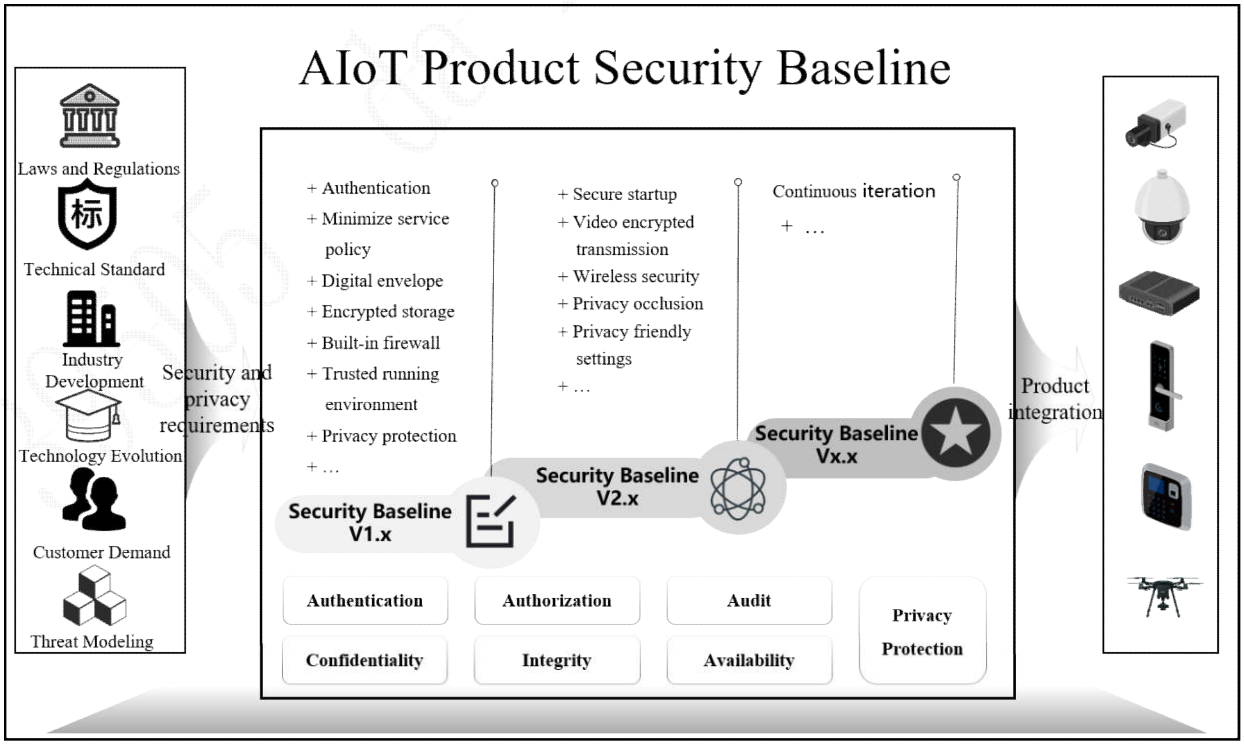

Figure 3-2 Constantly Update Security Baseline Standards

3.2 Technology Description

3.2.1 Physical Security

3.2.1.1 Secure Boot

Based on the Secure Boot of the master chip, build a physical chip-based startup trust chain to effectively guarantee the integrity and legality of the device startup process, and avoid loading untrusted firmware programs.

3.2.1.2 TrustZone

TrustZone technology is an important security feature provided by ARM master chip. This technology can implement physically isolated secure operating area and secure storage area, and provide a secure foundation for the upper application service.

3.2.1.3 OTP

OTP is short for One Time Programmable, data (such as the unique identification information of the device) cannot be modified after being written, which can effectively ensure the integrity of the written data.

3.2.1.4 True Random Number Generator

True Random Number Generator (TRNG) converts unpredictable physical phenomena into electrical signals, and obtain a series of random numbers by repeatedly collecting random signals. Theoretically, these random numbers are completely unpredictable.

3.2.1.5 Secure Chip

The secure chip provides mainstream secure encryption algorithm and supports the secure storage of the key, which effectively protects its confidentiality.

3.2.1.6 Physical Communication Interface

The physical interface of the device adopts ESD static protection to ensure the secure operation of the interface and the system. The motherboard does not reserve idle serial ports, USB, I2C, SPI and other communication interfaces on the periphery of the chip. It is directly closed inside the system to prevent unauthorized interfaces access to the system internal resources. For chip JTAG debug port, program burn port, etc., the motherboard does not reserve relevant interfaces.

3.2.1.7 Dual-Flash Backup

The idle Flash space is used to back up the firmware data in the main Flash area. When the main Flash data is destroyed, the device will automatically reboot and restore the firmware in the main Flash area based on the backup data.

3.2.1.8 Dual-OS Backup

The device adopts a dual motherboard design structure. The motherboards work together and back up each other.

When the main motherboard is damaged, the host will seamlessly switch to the standby motherboard to continue working and to ensure the continuity and robustness of the device operation.

Figure 3-3 Dual-OS Backup

3.2.1.9 Dual-Power Backup

The device adopts multi-power supply design structure to keep multiple power supplies working at the same time. When any one of the power supplies is interrupted due to a failure, the dual power supply can continue to maintain power and maintain the normal operation of the device.

Figure 3-4 Dual-Power Backup

3.2.2 OS Security

3.2.2.1 Trusted Boot

The device uses a secure master chip as the "physical trust root" for trusted boot. During the system loading process, the trust is verified step by step to implement the secure transfer of control right until the boot of the final application service. Establishing a complete trusted boot chain to construct the initial trust status of the device greatly assures the subsequent operation of the device.

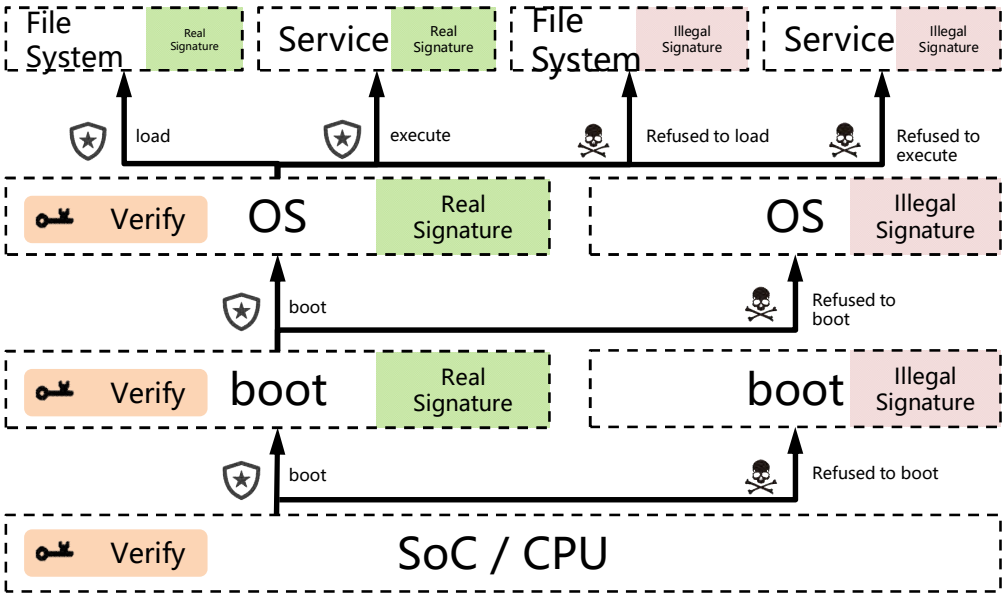

Figure 3-5 Trusted Boot

3.2.2.2 Trusted Execution

During the runtime of the device (before any executable program is loaded and operated), it must pass the trusted verification of the kernel to prevent malicious programs (e.g. virus, Trojan, etc.) from damaging the device.

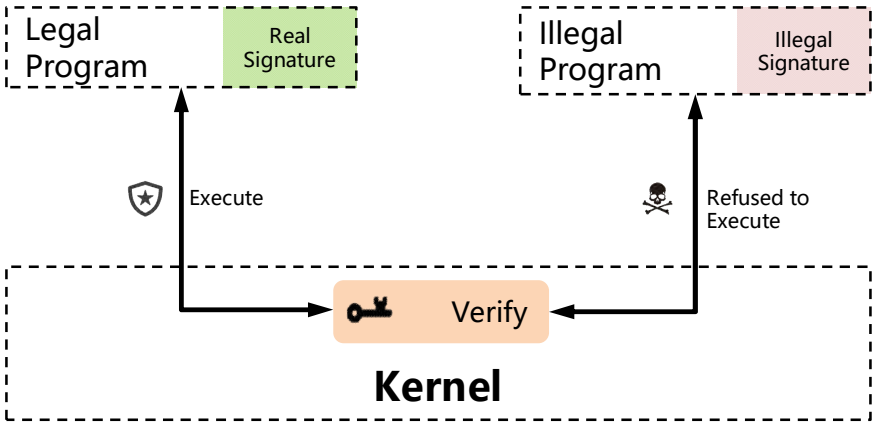

Figure 3-6 Trusted Execution

3.2.2.3 Trusted Upgrade

When a device upgrades its firmware, the upgrade service will perform trusted verification on the target firmware and refuse to write illegal or tampered firmware to the device.

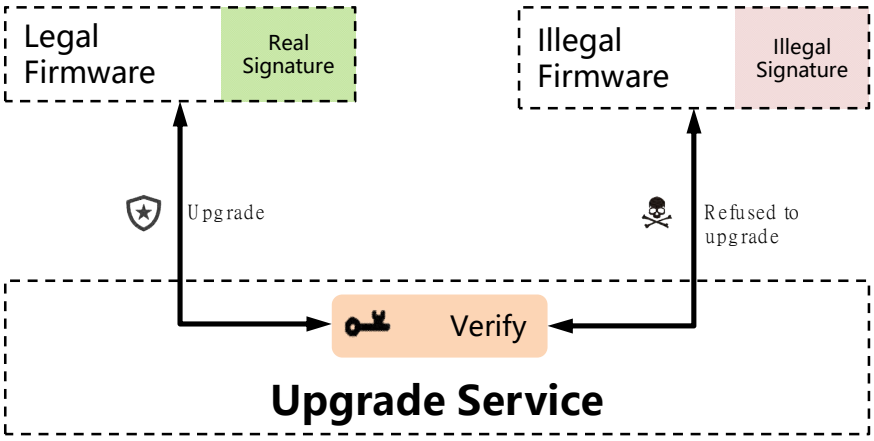

Figure 3-7 Firmware Upgrade Trusted Verification

3.2.2.4 TEE

TEE is a secure executive standard developed by the Global Platform. TEE has independent and isolated CPU, memory, IO and other resources. It only executes trusted code.

Based on TEE technology, devices achieve trusted encrypted storage of sensitive data such as account information, configuration information and key information. At the same time, in order to ensure the security of network communication between devices, the device identity certificate is built into the TEE. During the establishment of network communication, the TEE implements the signature process of the device identity, thus ensuring security against any spoofing attempts.

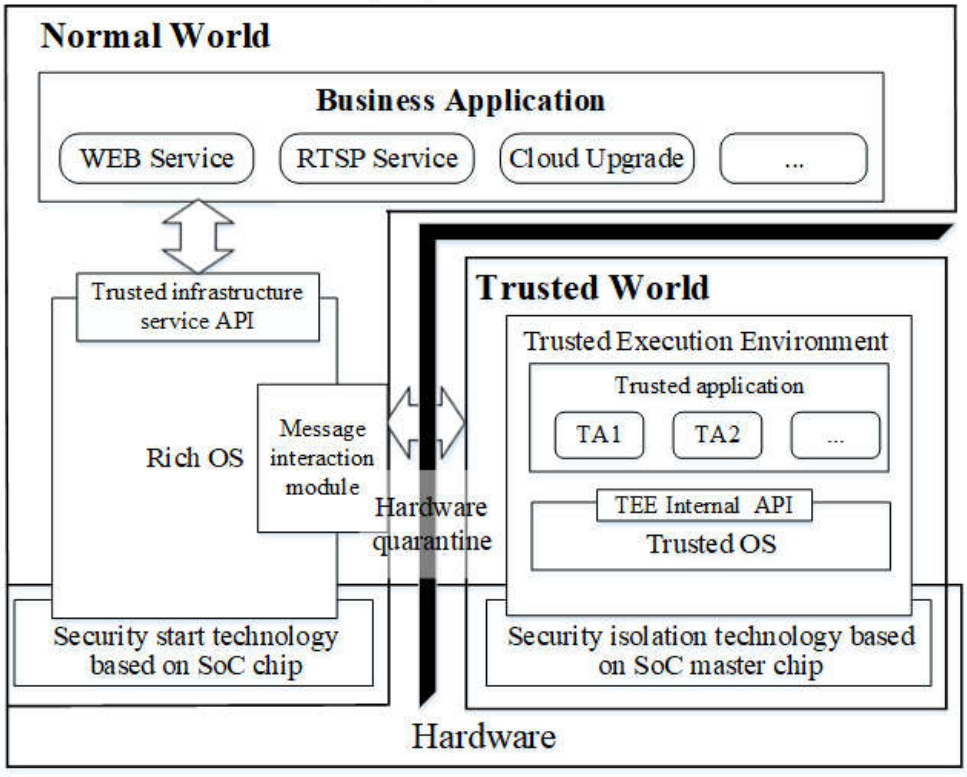

Figure 3-8 TEE Framework

3.2.2.5 Protected Shell

Shell is a command control terminal of the device, and is usually used for device debugging, detection, and problem location. The Protected Shell is a multi-factor authentication protection based on Hook technology to avoid malicious operations of devices.

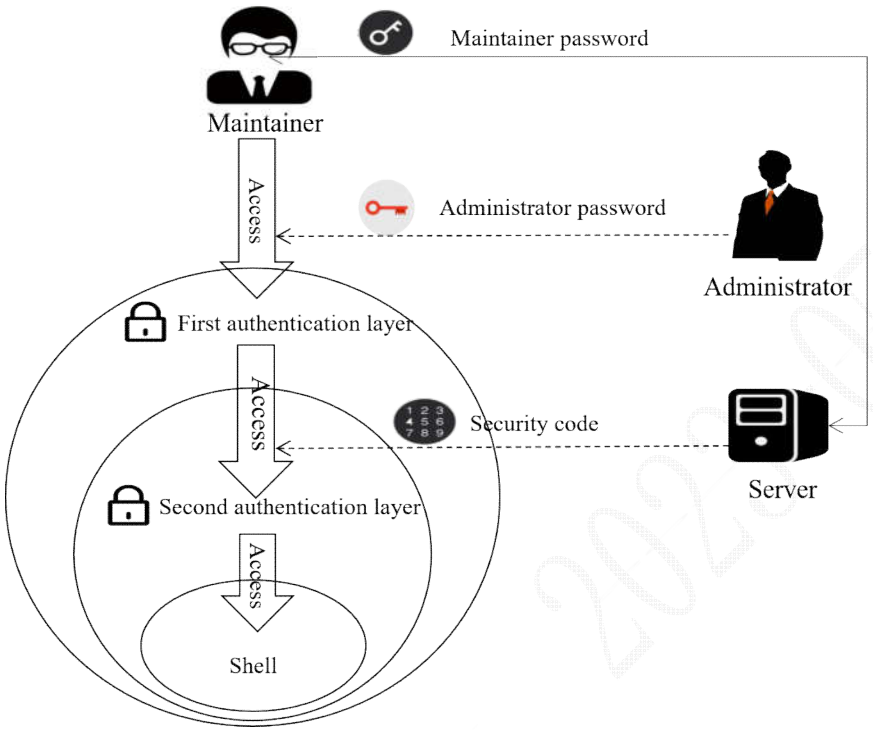

Figure 3-9 Protected Shell

Multi-factor authentication includes two levels of authorization:

- Administrator authorization: Based on the user management system of devices, the administrator is authenticated to obtain the first-level authorization of the device.
- Server authorization: Use the maintenance personnel credentials to get the security code from the authentication server and realize second-level authorization.

3.2.2.6 Cloud Upgrade

In the AIoT industry, upgrading devices has been a great challenge due to the large number of devices, complex network, and scattered installation locations. Upgrading to the latest firmware not only allows users to acquire the latest features, but also helps the device to improve its security capabilities. Dahua has proposed a cloud upgrade solution to help users conveniently and securely upgrade their device:

- Supports automatic version detection.
- Supports automated batch upgrade.

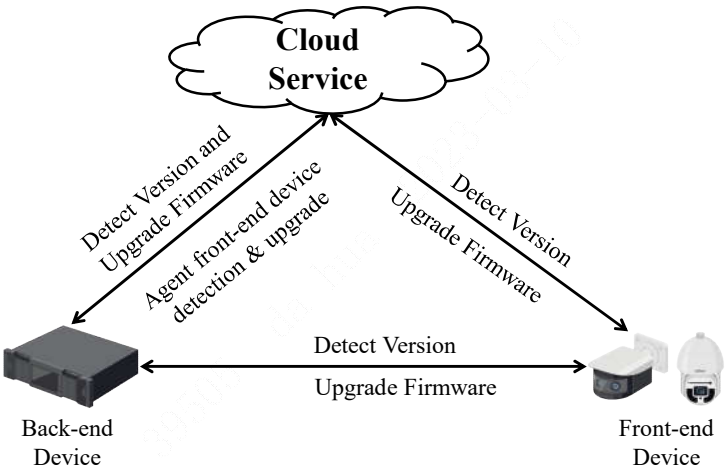

Figure 3-10 Cloud Upgrade

3.2.2.7 Anti-Reverse

In order to prevent threat actor from attacking devices through reverse firmware, Dahua has designed a firmware encryption solution to ensure that the firmware remains encrypted during the data transfer process. The basic principles are as follows:

- Create a security key based on KDF technology to encrypt the firmware;
- When the device upgrades the firmware, write the security key into a Flash in an encrypted form;
- During the device startup process, decrypt and load the Flash partition data.

3.2.3 Application Security

3.2.3.1 Secure Identity Authentication

3.2.3.1.1 Account Security Policy

The device has no default account. An account must be created by the user during deployment, and the password composition must meet the following requirements:

- At least 8 characters;
- No less than two types of characters.

To guide the user to set a strong password, the device will check the strength of the password set by the user and prompt the user when adding an account or changing a password.

In addition, the devices support password expiration reminder. When the user creates an account, the device will prompt the user to set a validity period for the account password and reminds them to modify the password in time before the expiration date in order to prevent the user from using the same password for a long time and increase the risk of password disclosure.

3.2.3.1.2 Digest Authentication Technology

Digest authentication technology is a challenging authentication method based on HASH algorithm on passwords and random numbers (valid once). It ensures the confidentiality and non-repeatability of the authentication process.

The credential calculation is as follows:

- HA1 = HASH("username:realm:password")
- HA2 = HASH("method:uri")
- DigestPassword=HASH("HA1:nouce:nc:cnonce:qop:HA2")

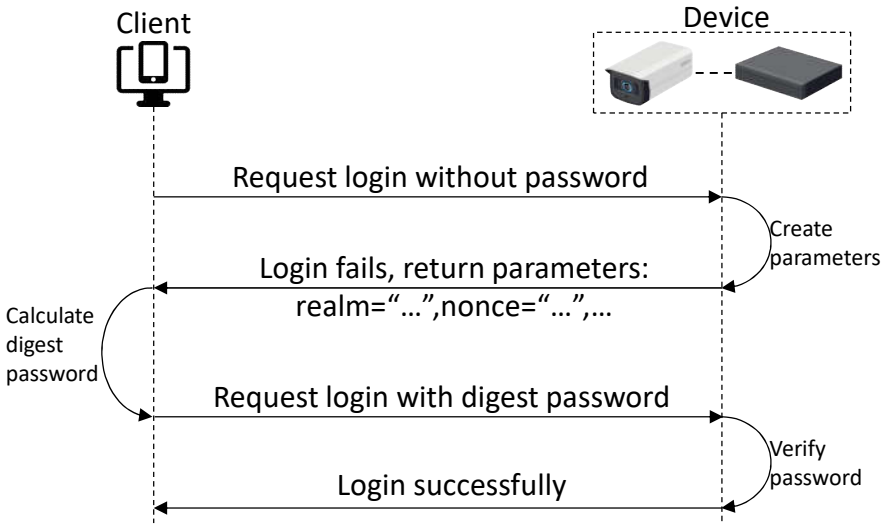

Figure 3-11 Digest Authentication Technology Interaction Process

3.2.3.1.3 WSSE Authentication Technology

WSSE authentication technology is a non-challenging authentication method. It is a HASH algorithm based on password, random number, time and other factors to ensure the confidentiality of password during transmission process. It is based on the non-repetition of random number factors in a limited time to ensure the non-repeatability of the authentication process.

The credential calculation is as follows:

- HA1 = HASH("username:realm:password")
- HA2 = HASH("method:uri")
- HA3 = HASH("HA1:nouce:nc:cnonce:qop:HA2")
- WSSEPassword = Base64(HASH(Nonce + CreationTimestamp + HA3))

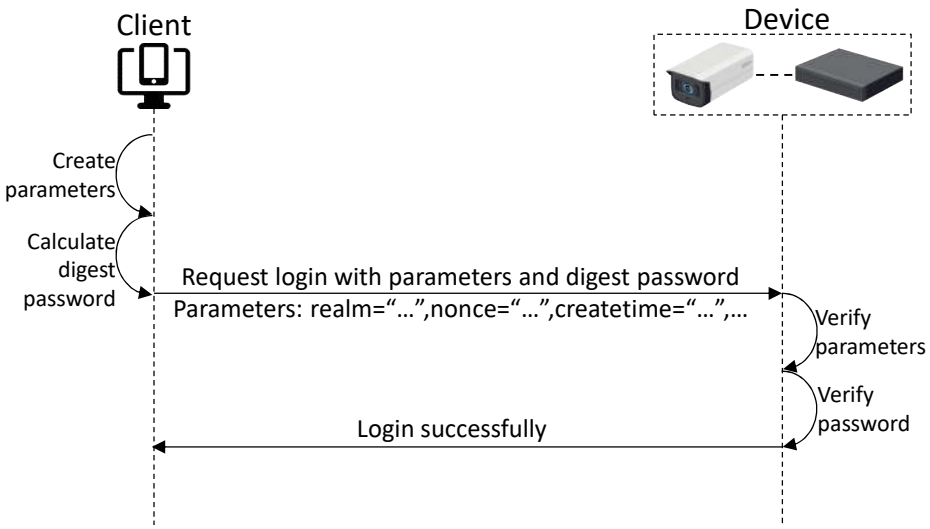

Figure 3-12 WSSE Authentication Technology Interaction Process

3.2.3.1.4 Digital Certificate Mutual Authentication Technology

Mutual identity authentication of digital certificate based on TLS technology ensures the legitimacy of the identities of both sides of the communication between the device and the platform. The private key information representing the identity of the device is generated and stored by the security module, and the identity authentication is completed within the security module, which fully ensure the authenticity of the device identity.

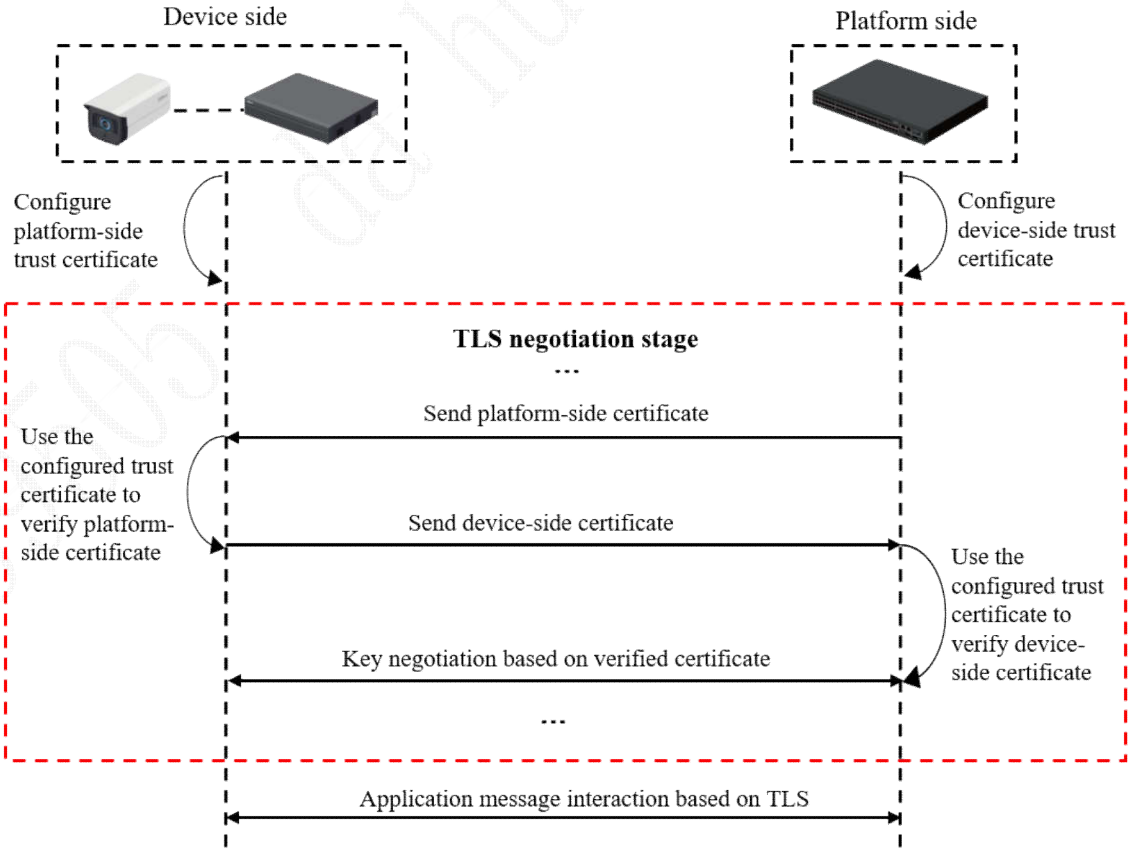

Figure 3-13 Mutual Identity Authentication

3.2.3.2 Authority Management System

Based on the RBAC model, Dahua devices have a flexible and efficient authority management and control system that meets the needs of users in different scenarios.

3.2.3.3 Log Security

3.2.3.3.1 Log Security Policy

The device completely records the user's operation track, including (but not limited to) the following activities:

- Account login and logout
- Add, delete, modify user account and password
- Import and export system configuration
- Modify system configuration
- Upload file
- Restart and upgrade the device
- Modify the system time
- Abnormal events (including network disconnection, no hard disk, hard disk error, low hard disk capacity, video loss, etc.)
- Security events (such as account lockout, session blasting, etc.)

The log content recorded by the device contains the following important factors:

- Operational source, including account and source IP
- Operational content
- Operational time
- Operational result

3.2.3.3.2 Separate Security Logs

To ensure the traceability of security events, the device allocates an independent security log storage area to ensure the record of security event logs, including account crash and malicious program operation.

3.2.3.3.3 Network Logs

Devices support Syslog network log function and can synchronously save important logs to the log server. At the same time, Syslog supports TLS to ensure the security of log data during network transmission.

3.2.3.4 Service Security Policy

Based on the principle of minimization, Dahua has implemented strict management and control on all services of the device. By default, only basic services can be enabled, including:

- WEB Service
- RTSP Service
- Device Search Service

- …

Dahua devices support more secure service protocols and provide users with more secure options, including:

- Support HTTPS, to replace HTTP
- Support SFTP, to replace FTP
- Support SNMP v3, to replace SNMP v1/v2
- Support SSH, to replace Telnet
- …

3.2.3.5 Session Security Policy

Web services support session interaction based on short connection, with protection strategies including:

- Use highly complex and strongly random session credentials;
- Valid session is strongly bound to the source host, and sharing of session credentials across hosts is prohibited;
- Real-time monitoring of brute force cracking of session credentials, and actively logout all online users of risk hosts;
- Automatically logout long inactive sessions.

3.2.4 Data Security

3.2.4.1 Digital Signature Technology

Based on PKI infrastructure and signature algorithm, Dahua devices implement data signature and verification functions to ensure the integrity of target data.

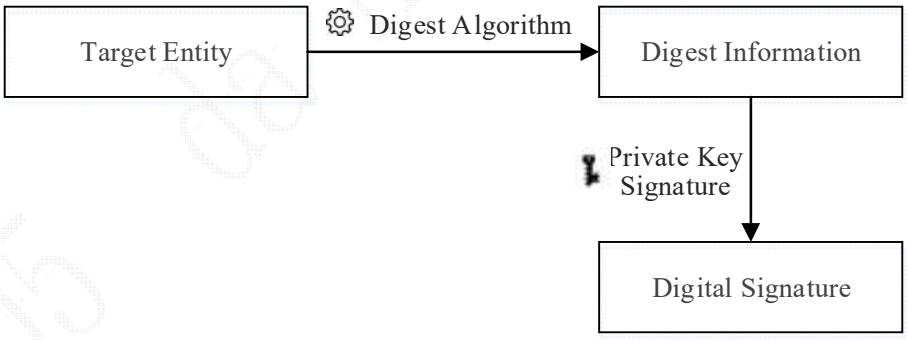

Figure 3-14 Digital Signature Process

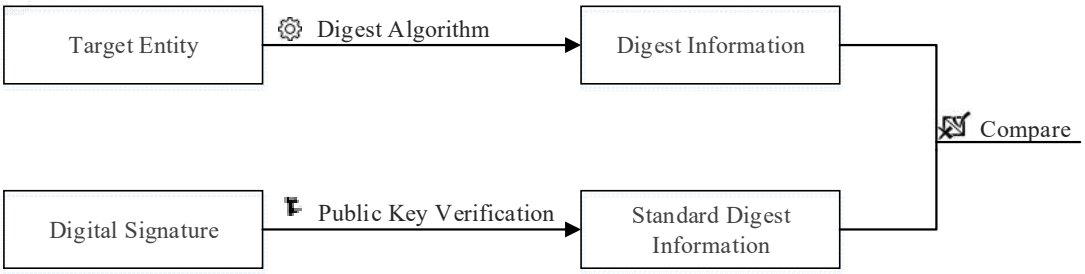

Figure 3-15 Digital Signature Verification Process

3.2.4.2 Digital Envelope Technology

Digital envelope technology is similar to our regular letters. This technology ensures that only legal users can decrypt and read the information transmitted in the network.

- The client uses a randomly generated symmetric key to encrypt the target data, and then encrypts the generated symmetric key based on the public key provided by the device;
- After the device receives the encrypted data and the symmetric key, it uses the corresponding private key to decrypt the symmetric key first, and then use the symmetric key to decrypt the ciphertext data.

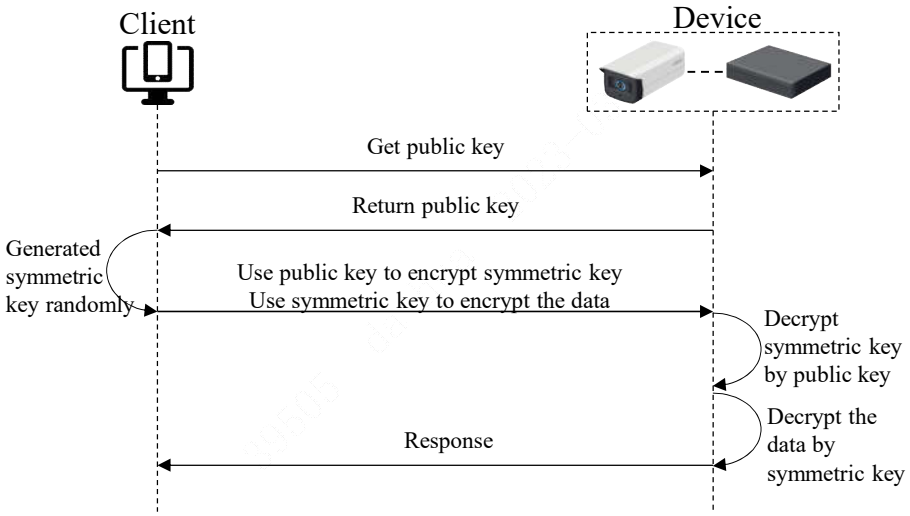

Figure 3-16 Digital Envelope Technology Interact Process

3.2.4.3 Video Transmission Encryption

3.2.4.3.1 Frame Encryption Technology

Frame encryption technology, that is, encrypted protection for media stream frame data, currently supports AES 256 encryption algorithm. Dahua's private protocol data stream transmission uses this technology. The specific process is as follows:

- Dahua device generates a random key and encrypts the frame data;
- Digital envelope technology is used to synchronize and update the key between the device and the client;
- The client decrypts the frame data based on the synchronized key.

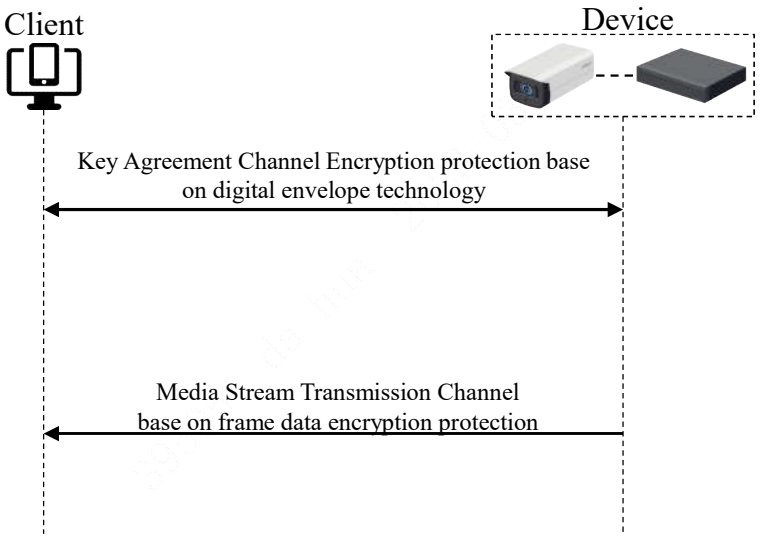

Figure 3-17 Frame Encryption Technology Interact Process

3.2.4.3.2 Channel Encryption Technology

The Dahua RTSP protocol supports TLS channel encryption. It is implemented in the standard and supports docking with third-party clients implemented in the standard. The specific process is as follows:

- Client and device establish a trusted encryption channel based on TLS protocol;
- Data stream transmission based on TLS channel.

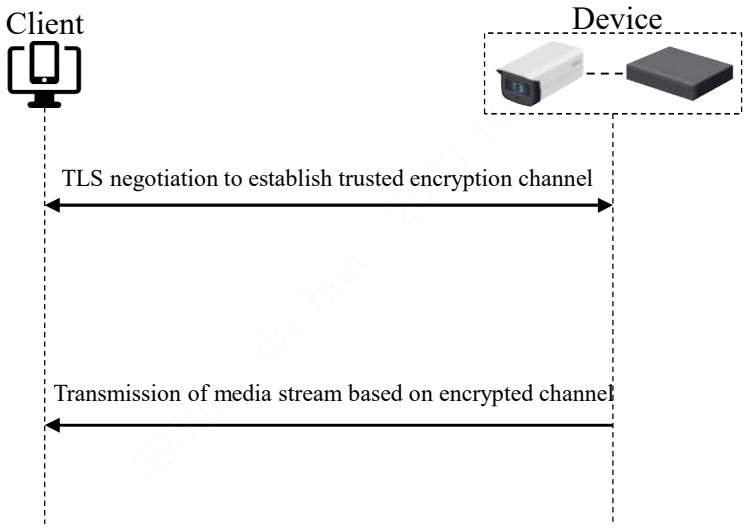

Figure 3-18 Channel Encryption Technology Interact Process

3.2.4.4 Video Storage Encryption

3.2.4.4.1 Encrypted Storage Based on KMS

KMS is a professional key management server that helps devices in the network, performing unified key management to ensure the stability and security of keys. The specific process is as follows:

- Use randomly generated keys to encrypt video data (supports AES 256 encryption algorithm);

- Connect the KMS system to protect random keys, and use industry standard protocols KMIP and HTTPS to connect the KMS system;
- Regularly update keys.

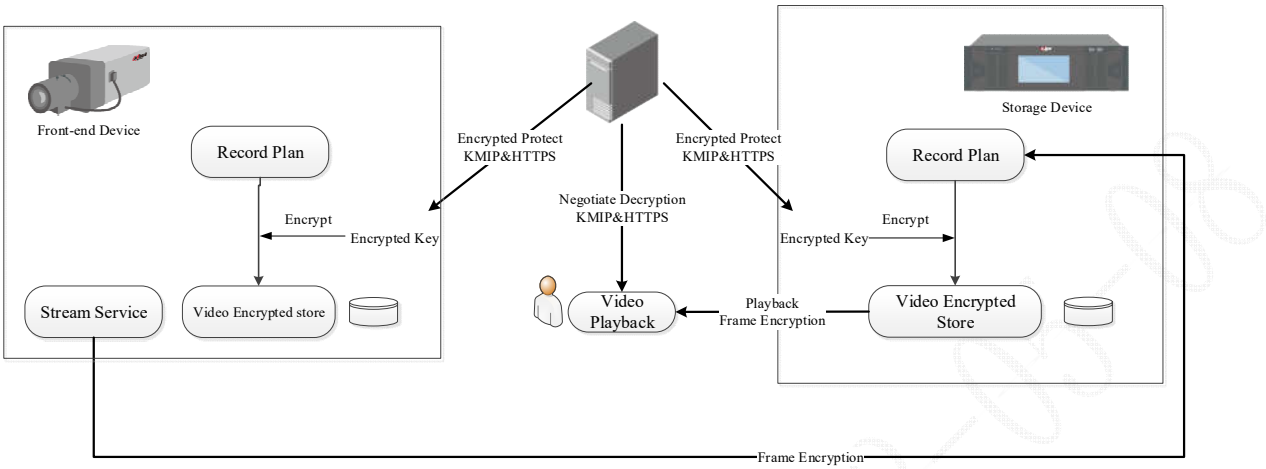

Figure 3-19 Video Encryption Protection Based on KMS

3.2.4.4.2 Encrypted Storage Based on Password Derivation

To simplify the deployment of the key management server, Dahua device implements secure storage of video data based on the password set by users. The basic principles are as follows:

- Obtain derived key through KDF calculation based on user-configured password.
- Use derived key to store the randomly generated key with AES 256 encryption.
- Use randomly generated key to store the video data with AES 256 encryption.

3.2.4.5 Video Download Encryption

Dahua device implements security protection for downloaded video data based on passwords set by users. The basic principles are as follows:

- When downloading, the digital envelope technology is used to send the password entered by the user to the device securely;
- Perform KDF calculation on the user's password to obtain the derived key;
- Use derived key to encrypt randomly generated key with AES 256 encryption;
- Use randomly generated key to encrypt download video data with AES 256 encryption.

3.2.4.6 Encrypted Storage Configuration

Based on the different capabilities of devices, the encrypted storage configuration function uses different encryption algorithms, including:

- If the device supports secure chip, then utilize the secure chip for encrypted storage;
- If the device does not support secure chip, a key will be generated based on KDF technology that can be used to encrypt data.

3.2.4.7 Encrypted Export Configuration

The export configuration function is mainly used for backup and synchronization of device configuration data. The exported configuration file may contain sensitive information such as account and password. To protect the confidentiality and integrity of configuration data, the Dahua device creates a security key based on KDF technology and fully encrypts the exported configuration data.

3.2.4.8 Log Export Security

The log export function is mainly used for the backup and analysis of the device log data. The exported log file contains important information such as user operation. In order to protect the confidentiality and integrity of the log data, the exported log data is protected by standard ZIP encryption.

3.2.5 Network Security

3.2.5.1 Attack Defense

3.2.5.1.1 Anti-ARP Spoofing Technology

ARP spoofing implants the fake IP-MAC map into network devices or hosts by continuously sending ARP spoofing messages, thus intercepting the data sent to the target host. The spoofed IP-MAC mapping refers to the mapping relationship formed by the combination of attack target's host IP and attacker's host MAC.

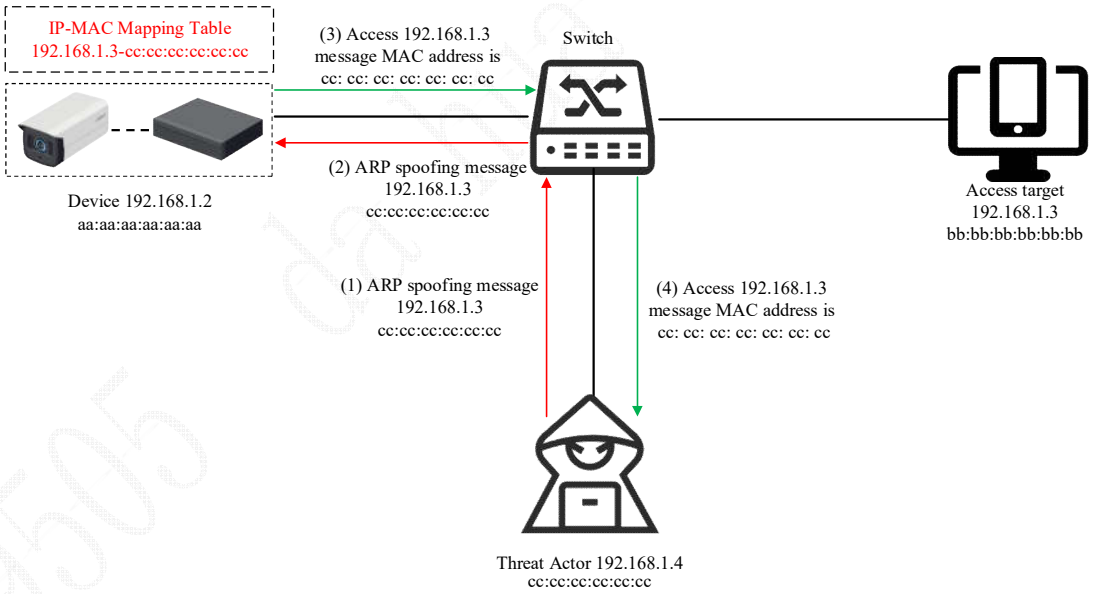

Figure 3-20 ARP Spoofing

The anti-ARP spoofing is used to shield the ARP spoofing message by fixing the IP-MAC mapping list of the source host and avoid the implantation of spoofed IP-MAC mapping relationship.

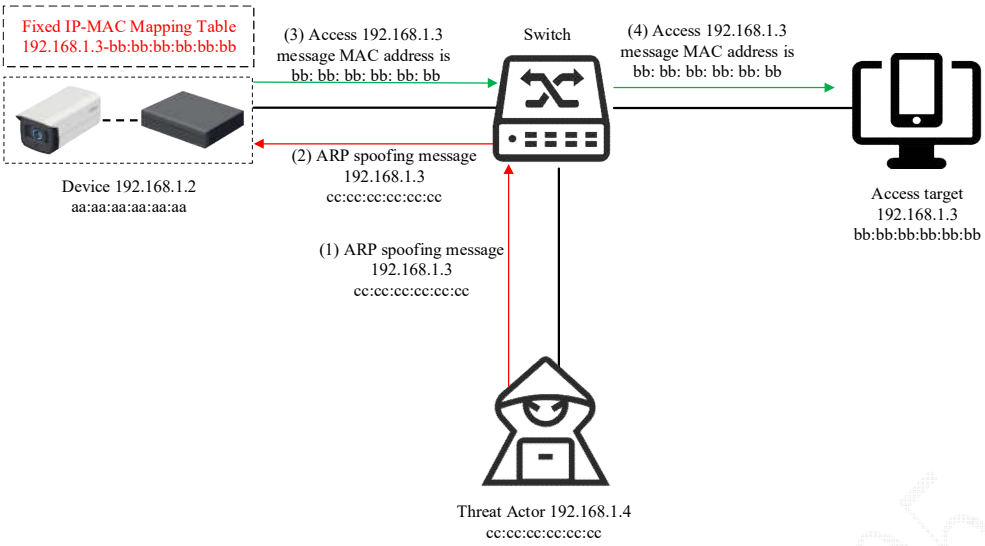

Figure 3-21 Anti-ARP Spoofing

3.2.5.1.2 Anti-DoS Attack Technology

In a DoS attack, the threat actor exhausts the target host's service resources by sending malicious network packets, resulting in the target host being unable to provide normal services to legitimate users. Dahua device provides the following two DoS defense capabilities:

- ICMP Flood Defense: Using firewall protocol filtering technology to intercept ICMP packets.
- SYN Flood Defense: Adopting SYN Cookie technology to optimize TCP resource allocation strategy and achieve defense against SYN Flood.

3.2.5.1.3 Anti-Cracking Password Technology

Password brute-force refers to using a high-performance host to make high-frequency password guesses on the target device until successfully logged in to obtain the correct password of the target device.

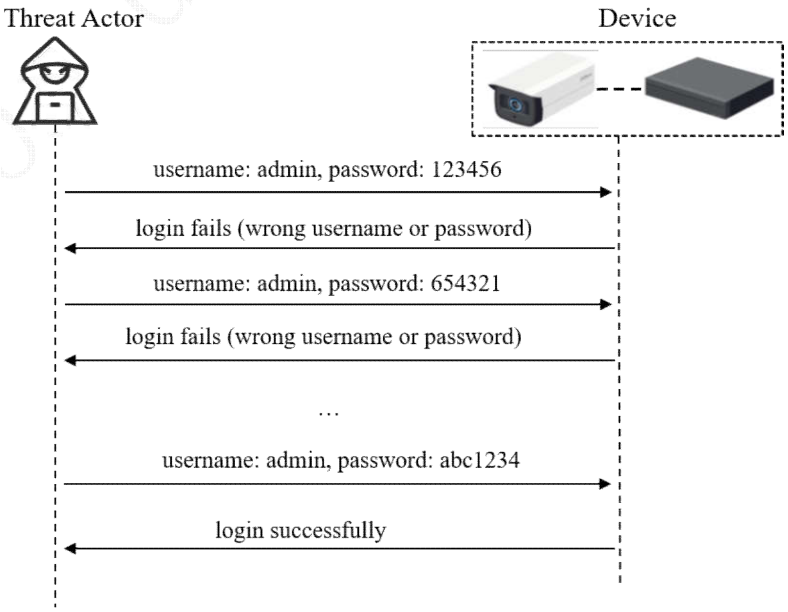

Figure 3-22 Password Brute-force Attack Technology

Based on the above-mentioned attack characteristics, when the device recognizes a password cracking attack, it will automatically lock the account and prohibit logging in for a period of time.

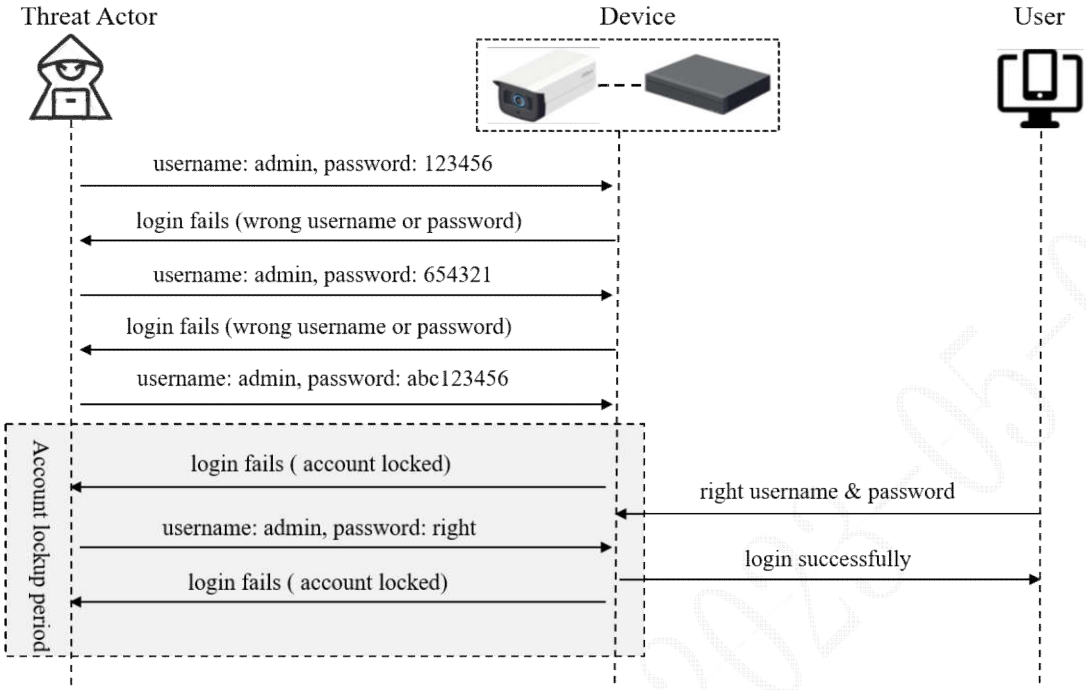

Figure 3-23 Password Anti-Cracking Technology

3.2.5.2 Access Control

3.2.5.2.1 Firewall

The firewall uses network packet filtering technology, checks the characteristics of the received or sent network packets based on the pre-configured filtering rules, and decides whether to allow them to pass, thus reducing the network risk. Its network packet characteristic information mainly includes the following:

- Source host IP address
- Target host IP address
- Source host MAC address
- Target host MAC address
- Source host port
- Target host port
- Network protocol

3.2.5.2.2 Time Calibration Allow List

Many business functions in devices rely on the accuracy of system time, including login, recording time, and so on. Dahua device supports time calibration allow list function. Based on the pre-configured rules, only specified hosts are allowed to calibrate the time of the device to avoid malicious tampering.

3.2.5.2.3 802.1x

802.1x is a standard protocol for network access control. It can restrict unauthorized devices or hosts from accessing the private network. The basic principles are as follows:

- In the initial state of the physical network port of the network switch, only 802.1x authentication messages are allowed to communicate;
- The device or host connected to the switch initiates identity authentication through the 802.1x protocol;
- After passing the authentication, the network switch opens the communication of its business data.

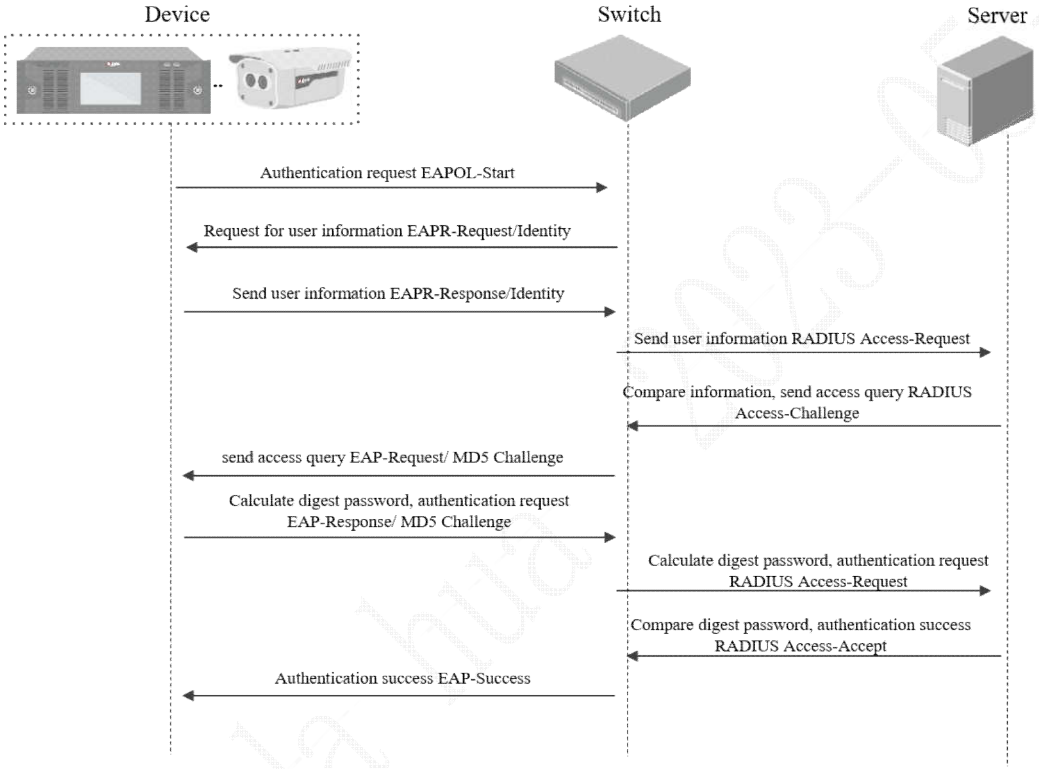

Figure 3-24 802.1x Authentication Process

3.2.5.3 CA Certificate

Dahua device supports the standard digital certificate of x.509, supports importing of digital certificate issued by third-party CA organization, and supports generation of Certificate Signing Request in PKCS#10 format. You can apply and import a digital certificate from a third-party CA organization. At the same time, users can manage the service certificates in the device uniformly.

3.2.5.4 Wireless Security

Dahua supports enterprise-level WPA/WPA2 encryption authentication method based on Radius authentication, as well as public-level WPA-PSK/WPA2-PSK encryption authentication method.

3.2.5.5 Host-based Intrusion Detection

HIDS identifies suspicious behavior by analyzing critical information during device operation. After detecting suspicious attack behavior, the device will notify users in real-time through email, mobile push, beep, and other

methods to help them handle security incidents in a timely manner.

The supported threat monitoring capabilities mainly include the following：

- Rootkit detection
- Hidden process detection
- Illegal IP access detection
- Illegal time attempt to log in detection
- User name and password crack
- Session crack
- The number of session connections exceeds the limit
- Web path crack

3.2.6 Privacy Protection

3.2.6.1 Privacy Policy

The privacy policy includes the types of data collection, usage purposes, processing methods, storage periods, user rights, and responses related to personal information, to ensure the transparency and openness of the personal information processing process.

Guide users to carefully read the privacy policy when using the device for the first time, and support users to check it at any time during subsequent use, so that users can fully understand privacy protection related information.

3.2.6.2 Privacy Occlusion

Based on intelligent recognition technology, in the image encoding stage, identify the areas that need to be occluded in the collected image, and perform intelligent matting. During playback, only users with administrator rights can restore the image, while other users without administrator rights cannot restore it.

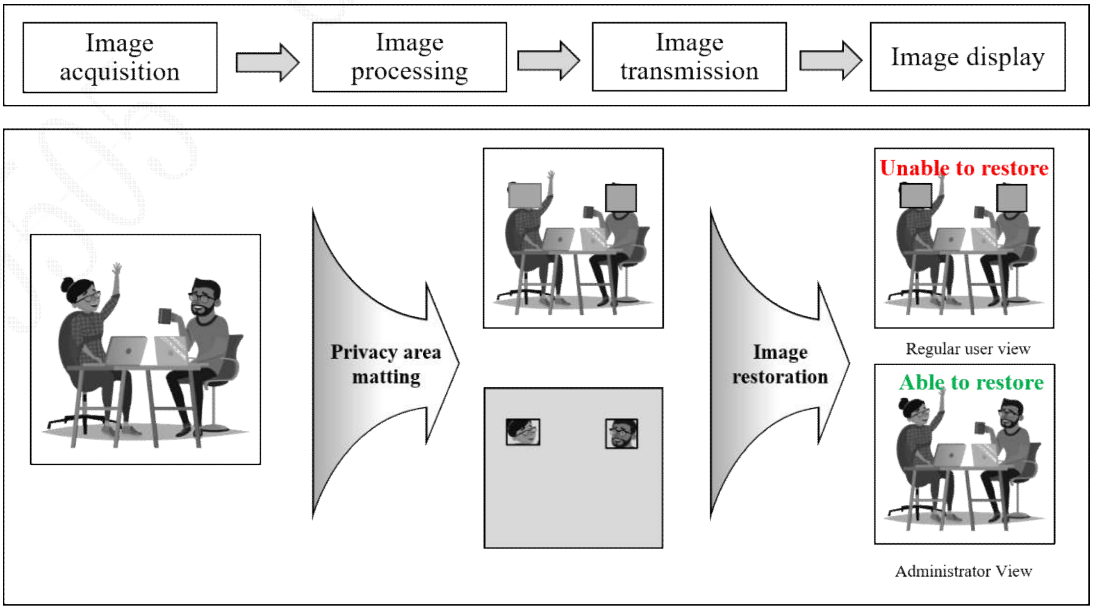

Figure 3-25 Privacy Occlusion Technology

4 Security Center

The Dahua Product Security Center is a secure brain integrated with the product. It integrates four major capabilities: internal state self-check, external threat monitoring, real-time risk alarm, and in-depth defense management. It aims to provide users with a clear and convenient security control experience and strengthen the in-depth defense capability of Dahua devices, and passed information security testing of China Electronic Product Reliability and Environmental Testing Research Institute (CEPREI) in 2022.

Internal state self-check： Provides one-click, centralized and visual internal state self-check and display capabilities. The user can detect the device login authentication method and password complexity. They can also check whether the device service meets the recommended requirements and configuration through its internal state self-check capability, display the scanning results, and provide “directional jump” or one-click repair function.

External threat monitoring: Provides real-time awareness, centralized and visual external threat monitoring, and display capabilities. Users can monitor and be aware of "malicious programs", "brute-force cracking", "malicious scanning" and other attacks in real time through the external threat monitoring capabilities, enabling them to analyze and handle the situation.

Real-time risk alarm: Allows setting of real-time risk alarm linkage in a centralized manner. When a risk is detected, Dahua device supports timely notification of users through e-mail or predefined alarm channels.

In-depth defense management: Offers convenient, centralized and visual in-depth defense management and display capabilities. Users can easily and quickly configure access control policies, account lockout policies, audio and video encryption policies and digital certificate.

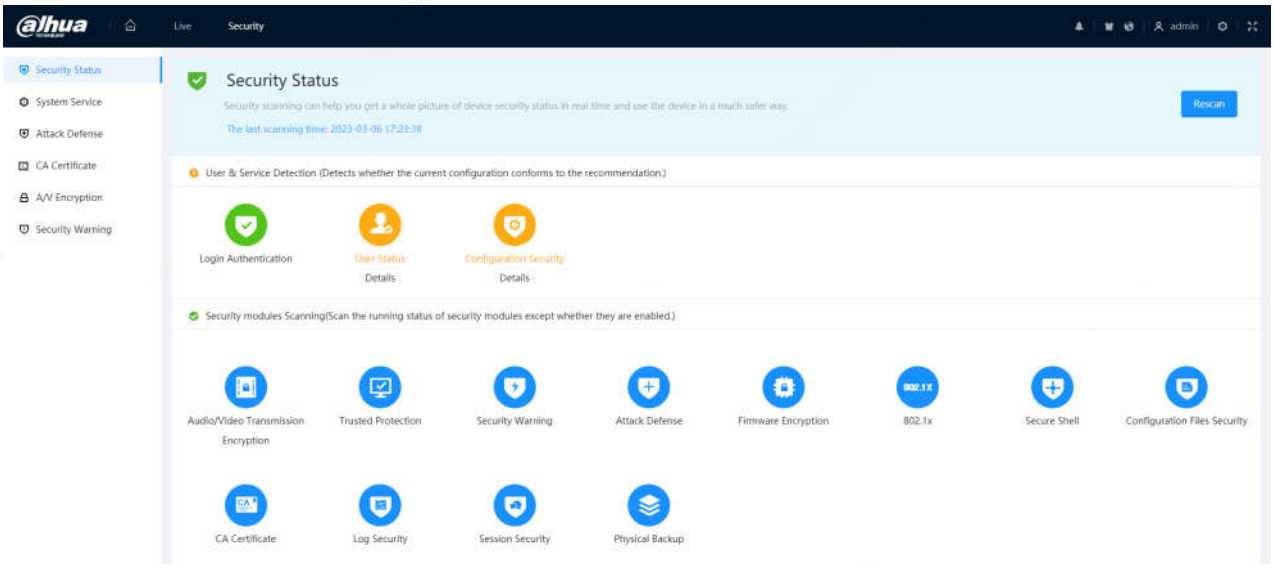

Figure 4-1 Security Center

5 Security Compliance

5.1 Legal and Regulatory Compliance

With the promulgation of laws and regulations such as the <Cybersecurity Law of the People's Republic of China> and the EU's <General Data Protection Regulation>, the regulatory and compliance requirements for cybersecurity, data security and privacy protection have become increasingly stringent worldwide. Dahua has always responded positively with a pragmatic attitude and strategies.

Dahua attaches great importance to the compliance construction of cybersecurity and privacy protection. Adhering to the concept of "active, open, cooperative and responsible", Dahua has formulated a comprehensive security and privacy management system, and relies on mature security engineering capabilities to strictly implement the system during product planning, design, development, delivery, and other stages to ensure product security and privacy compliance.

5.2 Testing and Certification

- **CC Certificate**

Common Criteria (CC) certificate is one of the widely recognized international certification standards in the field of information security. CC certificate is recognized by the National Information Assurance Partnership (NIAP) of the United States as well. At present, government departments or government agencies from 28 countries, including the United States, United Kingdom and Canada, have joined the CC Recognition Agreement (CCRA).

In 2023, a series of Dahua product passed the testing of SGS（Brightsight）and obtained the CC certificate.

- **ETSI EN 303645 Certificate**

The promulgation of General Data Protection Regulation (GDPR), the "strictest" data protection regulation in history, has set strict, high-level and wide-range protection requirements for data security and privacy protection. Based on the GDPR Act, the European Telecommunication Standards Institute (ETSI), together with product manufacturers, academia and government agencies, released the ETSI EN 303645 standard, aiming to solve the significant and widespread cybersecurity defects and protecting user privacy.

Based on GDPR, Personal Information Protection Law and other laws and regulations, and in combination with ETSI EN 303645, Personal Information Protection Specifications and other standards, Dahua has developed and continuously improved the <Dahua Personal Data and Privacy Protection Standard>, which is strictly implemented in Dahua products.

In 2022, a series of Dahua product passed France Bureau Veritas (BV) testing and evaluation, and obtained ETSI EN 303645 certificate.

- **FIPS 140-2 Certificate**

The FIPS 140-2 standard is jointly established by the National Institute of Standards and Technology (NIST) of the United States and the Canadian Communications Security Agency (CSE), aiming to evaluate, verify and authenticate the security of cryptographic modules. It is recognized as the "practical standard of cryptographic modules". Its security requirements cover the security design and implementation of cryptographic modules, including physical security, operating environment, key management, etc.

In 2022, the Dahua cryptographic software module passed Canada EWA test, and was reviewed and issued FIPS 140-2 certificate by NIST.

- **IoT Secure Product Evaluation Certificate**

Secure Product Certificate is a certification for camera products initiated by the IoT Terminal Security Alliance and tested by the China Academy of Information and Communications Technology (CAICT) Telecommunication Technology Labs (TTL). Its testing scope includes hardware security, operating system security, application software security, data security, and other aspects. Based on the enterprise's capabilities, Secure Product Label is awarded after comprehensive evaluation.

In 2022, a series of Dahua product passed the testing of TTL, and obtained the IoT secure product evaluation certificate.

- **Product Information Security Assessment Certificate**

Product information security assessment follows the GB/T 38626-2020 " Information security technology -Guide to password protection for intelligent connected device " and GB/T 38632-2020 " Information security technology -Security requirements for application of intelligent audio-video recording device ". The assessment categories include 68 aspects such as account security, password security, device security, server security, log security, and security vulnerabilities.

In 2021, a series of Dahua product passed the testing of China Electronic Product Reliability and Environmental Testing Research Institute (CEPREI) and obtained the product information security assessment certificate.

6 Security Incident Response

The Dahua Product Security Incident Response Team (hereinafter referred to as "Dahua PSIRT") is responsible for receiving, handling and publicly disclosing security vulnerabilities related to Dahua products and solutions. It is the only designated window to disclose vulnerability information.

Dahua attaches great importance to vulnerability management, and establishes a complete vulnerability management process with reference to ISO/IEC 30111, ISO/IEC 29147 and other standards, ensuring that vulnerabilities can be fixed in time and improving product security.

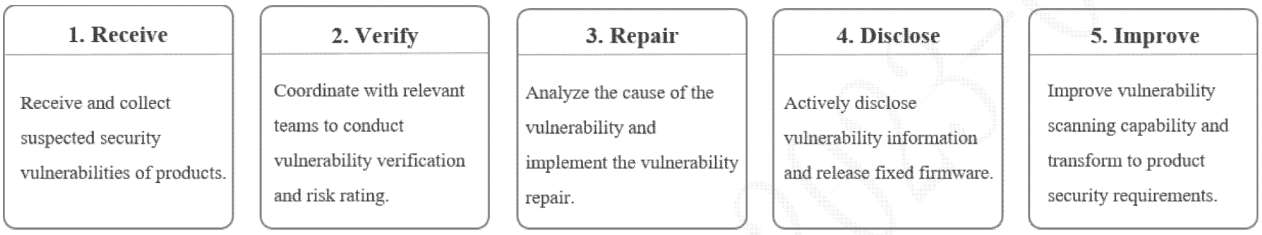

Figure 6-1 Vulnerability Management Process

Dahua follows the principle of openness and transparency and releases vulnerability information in the following two forms:

- Security Advisory (SA): Releases security vulnerability information related to Dahua products and solutions, including but not limited to vulnerability description, fixes and patches, etc.;
- Security Notice (SN): Releases information to respond to security topics related to Dahua products and solutions, including but not limited to vulnerabilities, security incidents, etc.

The Dahua PSIRT has participated in the activities of the industry and the public with an active and open attitude. By the end of 2022, Dahua PSIRT has joined many authority vulnerability organizations, including the international CVE Numbering Authority (CNAs), China National Vulnerability Database (CNVD), China National Vulnerability Database of Information Security (CNNVD), China National App Vulnerability Database (CAPPVD), and China National Industrial Cyber Security Vulnerability Database (CICSVD). In addition, the Dahua PSIRT greatly utilized the role of member units in the organization, established a cooperative cybersecurity threat information sharing mechanism, and received "Outstanding Unit of Vulnerability Emergency Work" awarded by CNVD, as well as the "Advanced Enterprise of Vulnerability Management Practice" jointly awarded by CAPPVD and CICSVD.

7 Security Commitment and Recommendation

Dahua attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

1. Account Management

1.1 Use complex passwords

Please refer to the following suggestions to set passwords：

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

1.2 Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

1.3 Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

1.4 Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be

locked.

1.5 Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

2. Service Configuration

2.1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2.2 Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

2.3 Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP：Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP：Choose TLS to access mailbox server.
- FTP：Choose SFTP, and set up complex passwords.
- AP hotspot：Choose WPA2-PSK encryption mode, and set up complex passwords.

2.4 Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

3. Network Configuration

3.1 Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

3.2 MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3.3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the

network to achieve network isolation;

- stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

It is recommended to check online users regularly to identify illegal users.

4.2 Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

4.3 Configure network log

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

5. Software Security

5.1 Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. Physical protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

【让社会更安全 让生活更智能】
ENABLING A SAFER SOCIETY AND SMARTER LIVING