Dahua Product Security White Paper

V2.0

Zhejiang Dahua Technology Co., Ltd

Legal Notice

Copyright Statement

© 2020 Zhejiang Dahua Technology Co., Ltd. All rights reserved.

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 in 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 TECHNOLOGY, alhua, alhua, alhua TECHNOLOGY, HDCVI are trademarks or registered trademarks of Zhejiang Dahua Technology Co., Ltd.
- The names of other trademarks or companies 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, 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 the company'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.
- The company reserves the right to modify any information in this document at any time, and the modified content will be added in the new version of this document without notice.
- This document may contain technical inaccuracies, inconsistencies with product functions and operations, or typographical errors, subject to the company's final interpretation.

Foreword

Overview

The continuous and in-depth development of AIoT needs to be established on the basis of responsible, open, professional, and systematic cyber security and privacy protection. Dahua has always regarded cyber security and privacy protection as one of the company's highest programs, and has continued to set up special funds to ensure that the research & development and delivery of product security, research on key security technologies, and construction of security incident response system are steadily promoted. Before releasing the products, all of them must pass rigorous testing conducted by the attack and defense laboratory. At present, Dahua has achieved fruitful results in security technology areas such as trusted computing, data encryption, privacy protection, and attack and defense testing, and has integrated applications in a full range of products.

This product security white paper aims to provide users with a deeper understanding of the security capabilities of Dahua products through a comprehensive elaboration of Dahua product security framework construction, security baseline practices, security technology applications, and security usage recommendations.

Glossary

Abbreviation	Explanation
UCD	User Centered Design，in the design process, the user experience is the center of design decisions, and the user-first design pattern is emphasized.
sSDLC	Secure Software Development Lifecycle
ESD	Electrostatic Discharge is an electrostatic discharge technology to protect the electronic components of the device from electrostatic damage.
I2C	Inter-Integrated Circuit Bus, The I2C bus was designed by Philips in the early ’80s to allow easy communication between components which reside on the same circuit board.
SPI	Serial Peripheral Interface is a high-speed, full-duplex, synchronous communication bus.
RBAC	Role-Based Access Control, allows permissions to be associated with roles, Users become members of appropriate roles and have corresponding role permissions.
PKI	Public Key Infrastructure, which is used to implement the generation, management, storage, distribution, and revocation of keys and certificates

	based on the public key cryptosystem.
KMS	Key Management Service, which provides secure and compliant key escrow services
KDF	Key Derivation Function, which is a key derivation method, uses a pseudo-random function to derive a new key based on the master key.
TLS	Transport Layer Security, an encrypted transport layer security protocol.
ARP	Address Resolution Protocol, which is the underlying network protocol for obtaining physical MAC addresses based on IP addresses.
GDPR	General Data Protection Regulation, an important law on personal data protection issued by the European Union.
CCPA	California Consumer Privacy Act, California's Privacy Act to protect consumer information.
C5	Cloud Computing Compliance Controls Catalog, The cloud security standard proposed by BSI.
BSI	The German Federal Office for Information Security.

Revision History

No.	Version	Revised Contents	Release Date
1	V1.0.0	First Release	2017.6.30
2	V2.0.0	Added the latest results of security baseline V1.3 / V2.0 /V2.1 and security technology research.	2020.2.28

Table of Contents

Legal Notice **1**

Foreword **3**

1 Security Development Lifecycle **6**

2 Security Model **8**

3 Threat Modeling **9**

4 Security Protection **10**

4.1 Security Baseline 10

4.2 Security Framework 11

4.3 Security Technology Description 12

4.3.1 Physical Security 12

4.3.2 OS Security 14

4.3.3 Application Security 18

4.3.4 Data Security 21

4.3.5 Network Security 26

4.3.6 Privacy Protection 31

5 Security Center **33**

5.1 Overview 33

5.2 Security Scan 33

5.3 Security Configuration Centralized Management 34

6 Security Compliance **35**

6.1 UL CAP Certification（UL 2900） 35

6.2 TÜV Rheinland Protected Privacy IoT Product Certification 35

6.3 TÜV Rheinland Protected Privacy IoT Service Certification 36

7 Security Suggestion **37**

7.1 Mandatory actions to be taken for basic equipment network security 37

7.2 “Nice to have” recommendations to improve your equipment network security 37

8 Security Incident Response **40**

9 Security Commitment **42**

1 Security Development Lifecycle

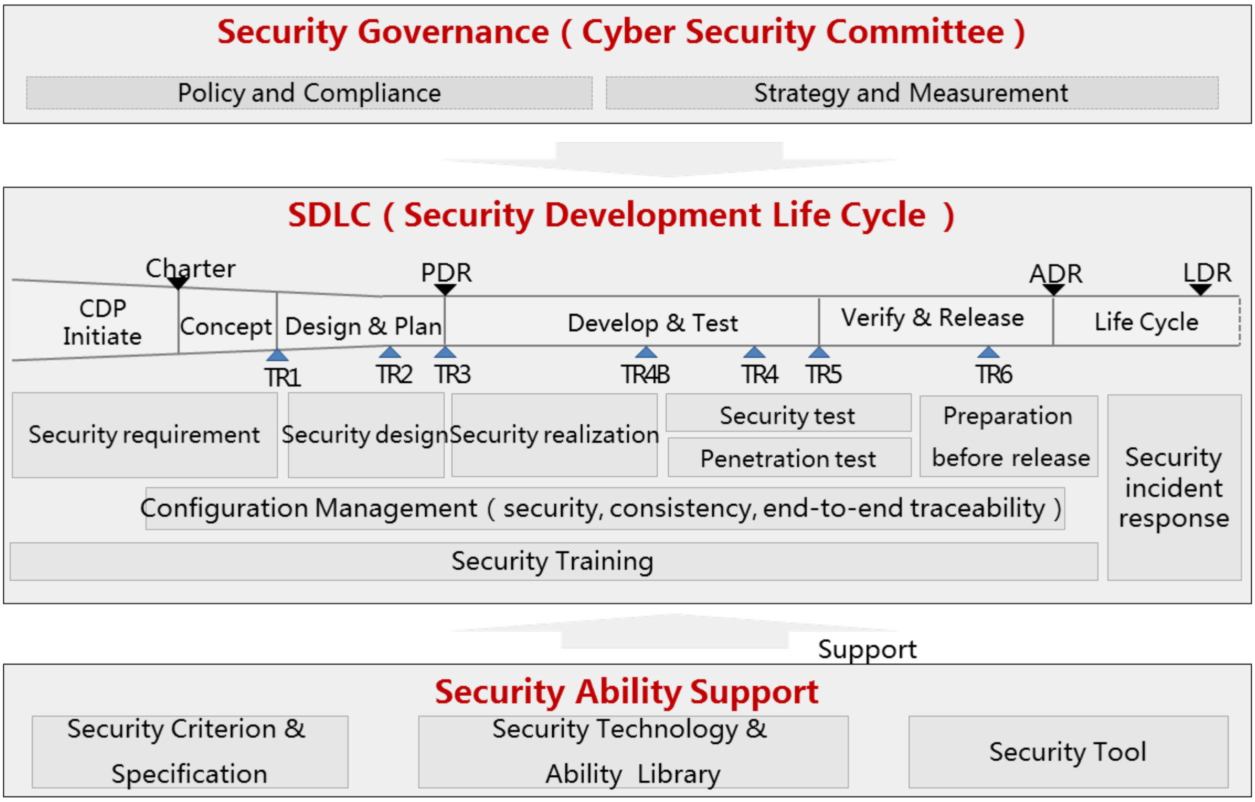


Figure 1-1 Product Security Development Process

Dahua continuously promotes the construction of sSDLC (secure Software Development Life Cycle), conducts a comprehensive and in-depth assessment of the maturity of the security activities, and further establishes a sound security R&D management and control system suitable for Dahua by standardizing the development process and controlling software engineering.

- Establish a professional security team to conduct training for all members of the R&D center, which will tackle security requirements understanding, security design methods, security coding standards, security testing methods, and the use of various security tools.
- Conduct security and privacy risk assessments in the product definition phase, taking the Security Baseline and Privacy Baseline as the most basic security requirements for the product, and formulating security activities and requirements commensurate with the risk level based on the results of the risk assessment.
- In the product design phase, strictly follow the core principles of security design such as minimum attack surface, minimum authority, default security, in-depth defense, etc., implement Threat Modeling and Threat Mitigation with combination of network security experts and product business experts, and practice "Security by Design".

- In the product development phase, strictly follow secure coding specifications. Under the premise of code cross-inspection, static code security detection and defect repair are performed in a standardized manner (such as Coverity, etc.).
- In the product verification phase, carry out comprehensive virus scan, system vulnerability scan, web vulnerability scan, verification of known vulnerability, verification of security function, verification of Penetration Testing for attacks, and Fuzzing testing.
- Conduct security check before product release, including consistency of security requirements and security design, data compliance, cleanup of code security audits, completeness check of Security Testing and Penetration Testing, product security guidance documents, etc.

2 Security Model

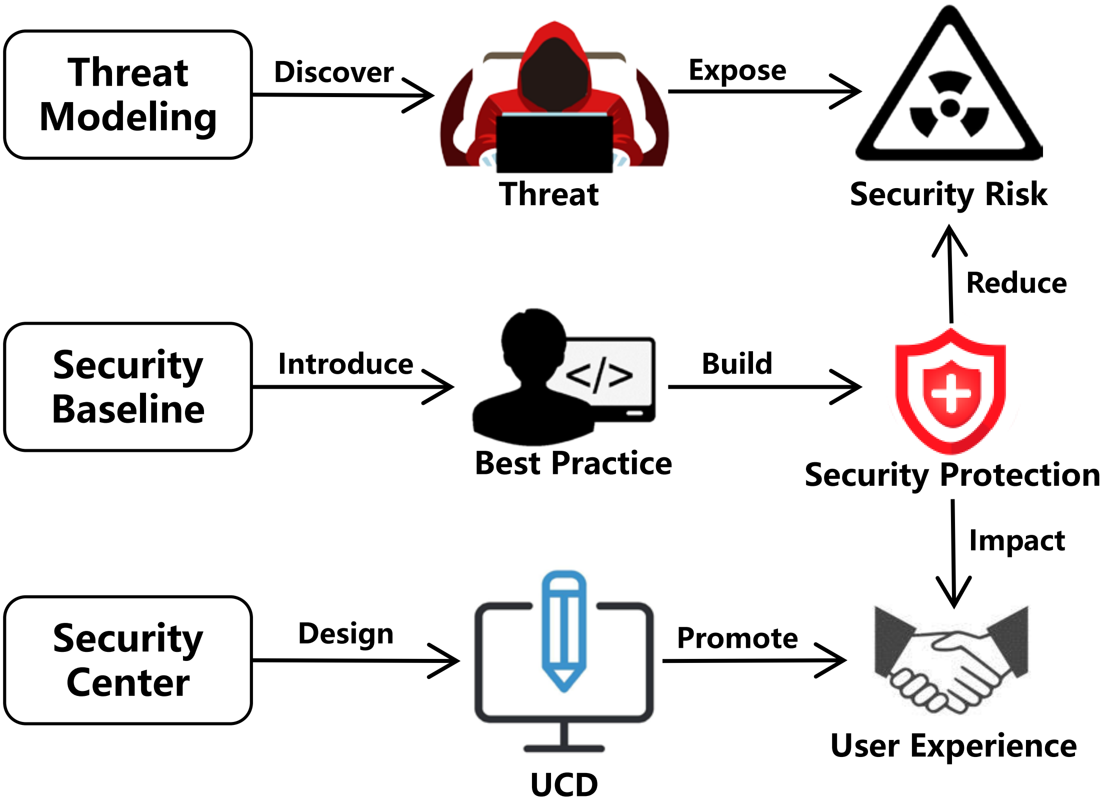


Figure 2-1 Product Security Model

The stage of product security requirements and design involves: threat modeling based on deep mining that exposes potential security risks; hierarchical and systematic security protection based on continuous iterative security baseline standard; user experience based on user-centric security center with convenient security management and visible security status. These three security activities work together to continuously improve the technical iterative model of security protection.

3 Threat Modeling

Threat modeling is a process based on a structured method that systematically identifies and assesses product security risks and develops targeted mitigation measures. Dahua introduces the threat modeling method, which aims to think about product security weakness and flaws from the perspective of an attacker, in order to continuously improve product security measures and reduce security risks.

Dahua adopts the industry's popular threat modeling method based on the STRIDE model. The basic idea is to conduct assessment and analysis based on the following six types of core threats:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

At the same time, the attack tree model was introduced to effectively improve the implementation of STRIDE threat modeling and deepen product security risk analysis. With the development of technology and the continuous enrichment of attack methods, the introduction of the attack tree models helps to identify the threats posed by new attack methods as early as possible.

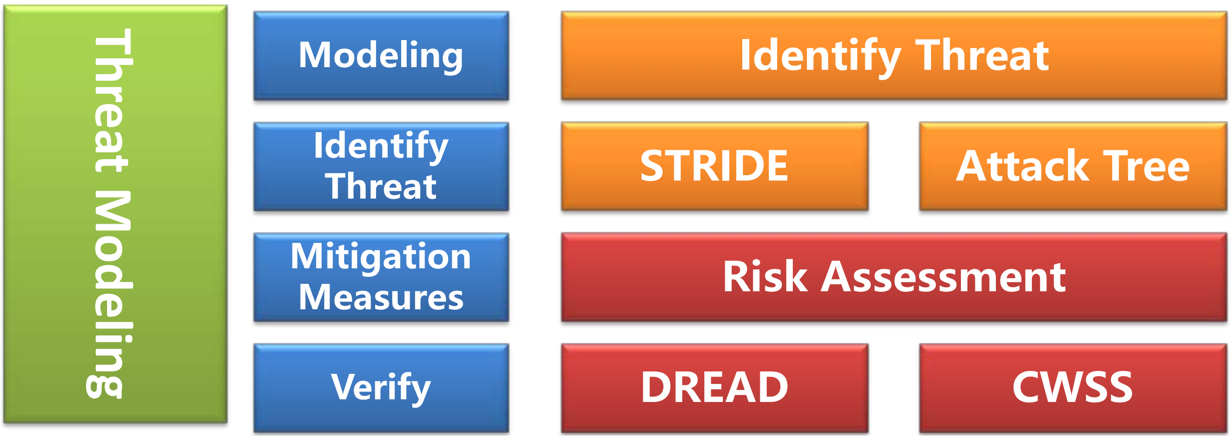
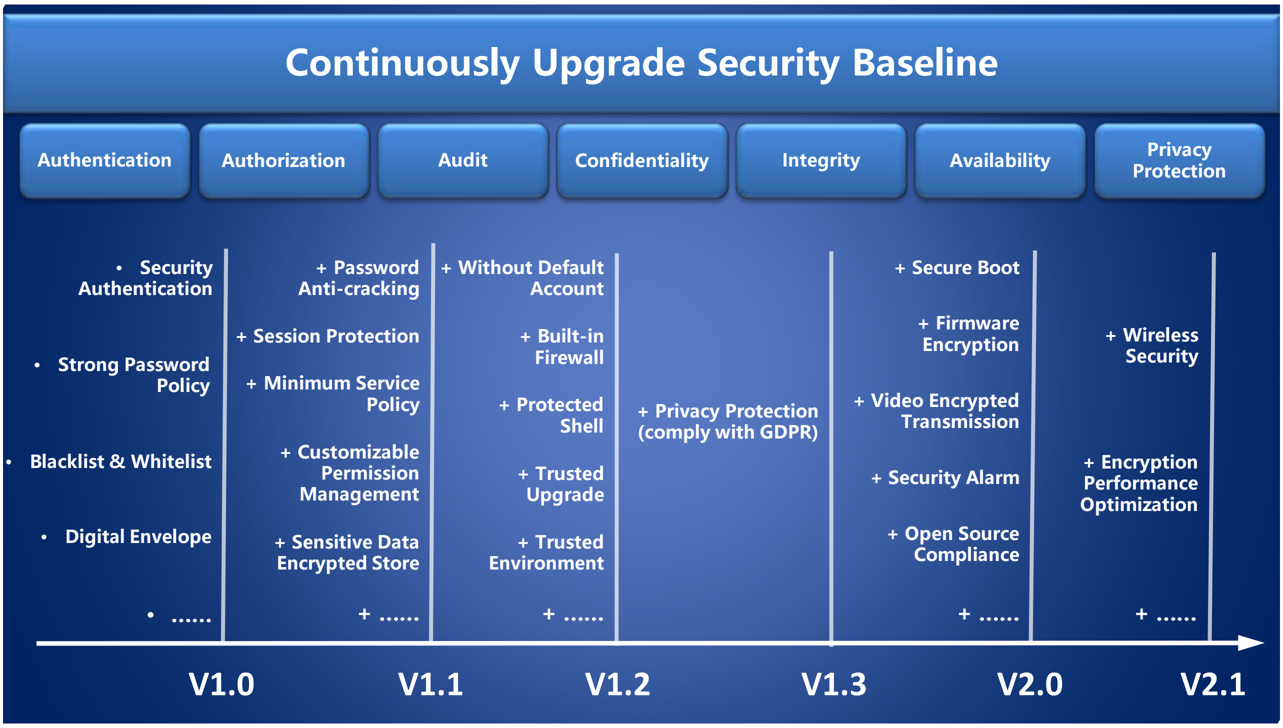


Figure 3-1 Threat Modeling

4 Security Protection

4.1 Security Baseline



Continuously Upgrade Security Baseline

Authentication | Authorization | Audit | Confidentiality | Integrity | Availability | Privacy Protection

V1.0
- Security Authentication
- Strong Password Policy
- Blacklist & Whitelist
- Digital Envelope
- ......

V1.1
+ Password Anti-cracking
+ Session Protection
+ Minimum Service Policy
+ Customizable Permission Management
+ Sensitive Data Encrypted Store
+ ......

V1.2
+ Without Default Account
+ Built-in Firewall
+ Protected Shell
+ Trusted Upgrade
+ Trusted Environment
+ ......

V1.3
+ Privacy Protection (comply with GDPR)

V2.0
+ Secure Boot
+ Firmware Encryption
+ Video Encrypted Transmission
+ Security Alarm
+ Open Source Compliance
+ ......

V2.1
+ Wireless Security
+ Encryption Performance Optimization
+ ......

Figure 4-1 Security Baseline

Since the launch of the "Security Baseline" plan, Dahua adheres to the core principles of "Security by Design" and "Security by Default", deeply research product security technology, and provides users with sufficient security protections.

The security baseline is based on and implements the principles of security and privacy design, constructs the layout of "AAA + CIA + P" security elements, and forms a systematic protection framework covering Physical Security, OS Security, Application Security, Data Security, Network Security and Privacy Protection..

The layout of "AAA + CIA + P" security elements is as follows:

- AAA：Authentication, Authorization, Audit
- CIA：Confidentiality, Integrity, Availability
- P：Privacy Protection

In order to ensure the adequacy of the Security Baseline, Dahua has carried out a series of activities like: "legal and regulatory compliance", "standards and specifications study", "industry dynamic tracking", "threat modeling analysis", "pre-research on key technologies", "security requirements research" to continuously output effective and high-value security requirements for the Security Baseline.

As one of Dahua's important enterprise standards, the Security Baseline is an important part of Dahua's sSDLC. It has been deeply integrated into the product quality assurance system to ensure that Dahua's entire series of products enjoy the factory default security.

4.2 Security Framework

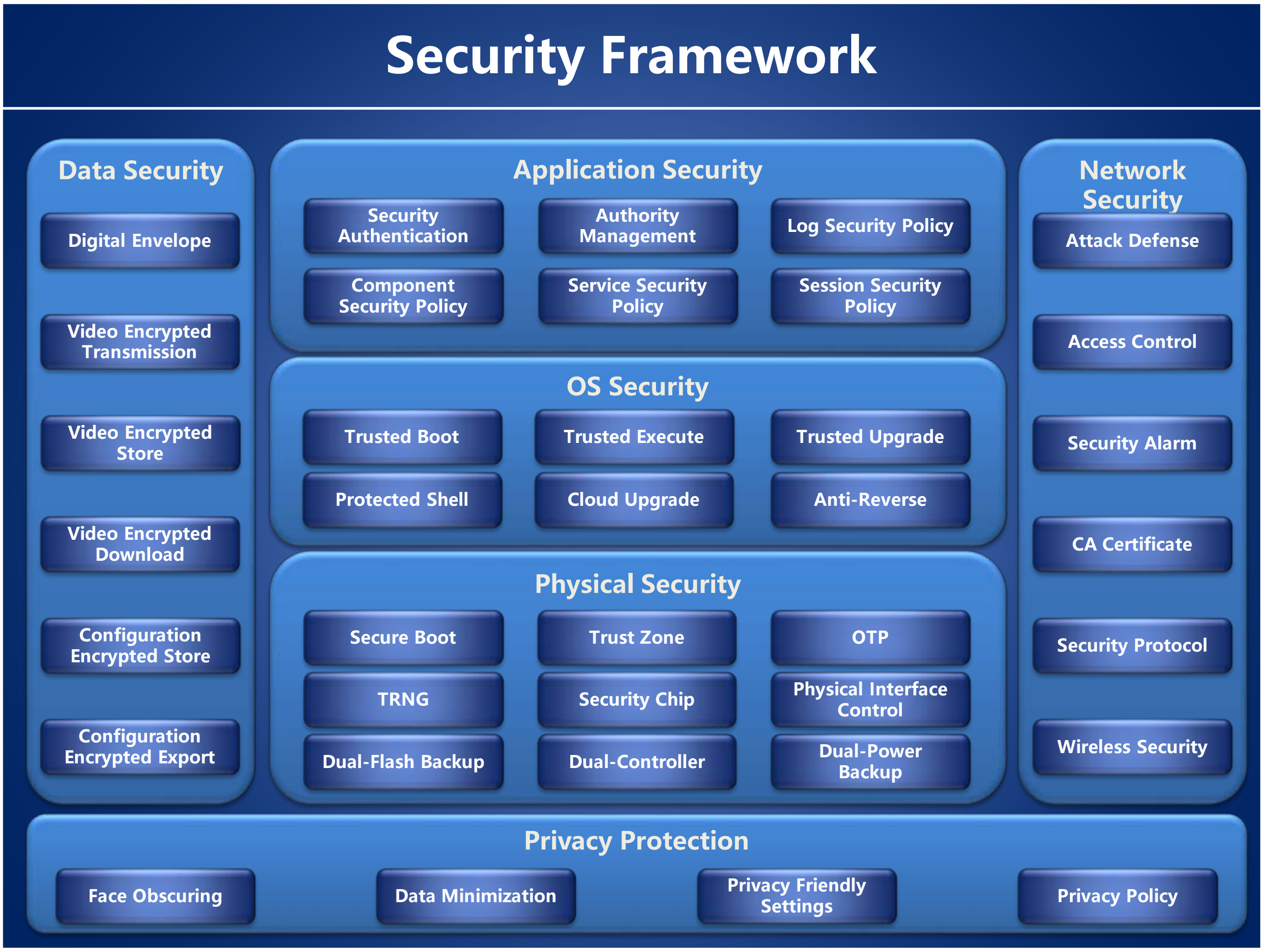


Figure 4-2 Product Security Framework

The product security framework protects product security from six dimensions: Physical Security, OS Security, Application Security, Data Security, Network Security, and Privacy Protection:

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

- OS Security: the operating system is the manager of resources, provides the basic execution environment for services, and constructs the secure and reliable basic execution environment through trusted computing, virtual technology, permission control and other technologies.
- Application Security: forming a closed-loop security protection structure based on authentication, authorization, and auditing to strengthen the self-security capabilities of application-layer service.
- Data Security: based on cryptography, digital signature and other technologies, constructs the whole life cycle security protection of data storage, transmission, sharing and destruction to avoid data leakage, tampering and destruction.
- Network Security: introducing security alarm, firewall and other attack defense technologies to improve the detect and defense capabilities of network attacks.
- Privacy Protection: providing privacy protection measures covering the whole life cycle of data collection, transmission, storage, use, sharing, display, copying, and deletion etc.

4.3 Security Technology Description

4.3.1 Physical Security

4.3.1.1 Secure Boot

Based on the Secure Boot of the SoC, a booting trust chain based on the physical chip is built, which can effectively guarantee the integrity and legality of the device boot process and avoid loading untrusted firmware.

4.3.1.2 Trust Zone

Trust Zone technology is an important security feature provided by ARM. Based on this technology, it is possible to implement physically separated secure operating area and secure storage area, and provide a secure foundation for upper-layer application services.

4.3.1.3 OTP

OTP (One Time Programmable) is a one-time programmable storage area. 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.

4.3.1.4 TRNG

TRNG (True Random Number Generator) is to convert 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.

4.3.1.5 Security Chip

The security chip provides security encryption algorithm, and supports the secure storage of sensitive data such as key, which effectively protects the confidentiality of data.

4.3.1.6 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, and it is directly closed inside the system to prevent unauthorized interfaces access to the system internal resources; for JTAG debug port, program burn port, etc., the motherboard does not reserve relevant interfaces.

4.3.1.7 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.

4.3.1.8 Dual-Controller Technology

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 to ensure the continuity and robustness of the device business.

Figure 4-3 Dual-Controller Technology

4.3.1.9 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.

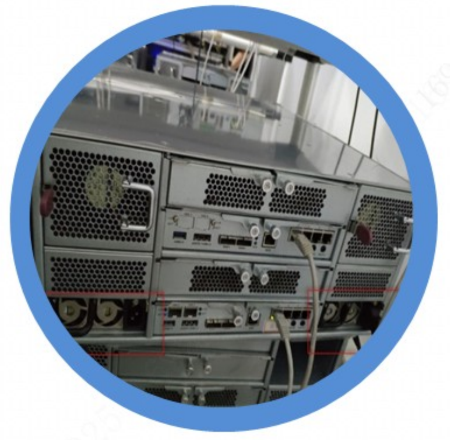


Figure 4-4 Dual-Power Backup Technology

4.3.2 OS Security

4.3.2.1 Trusted Boot

The device uses SoC/CPU as the "physical trust root" for trusted boot. During the system boot process, the trust is verified step by step to realize the secure transfer of control right until the boot of the final application service. By establishing a complete trusted boot chain to construct the initial trust status of the device, it is a reliable basic guarantee for the subsequent operation of the device.

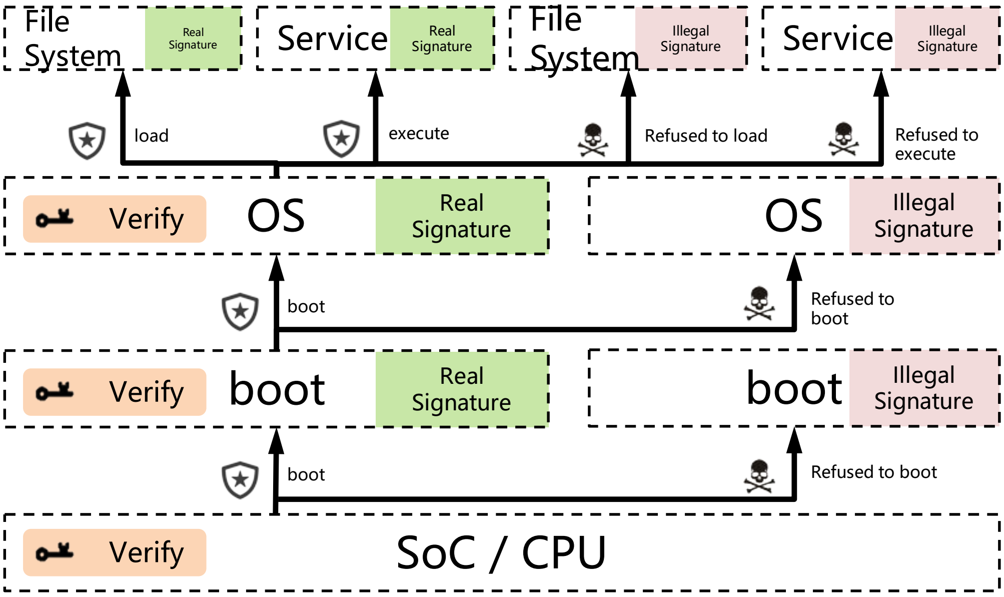


Figure 4-5 Principle of Trusted Boot

4.3.2.2 Trusted Execution

During the running of the device, before any executable program is loaded and run, it must pass the trusted verification of the kernel to prevent malicious programs (such as viruses, Trojans, etc.) from invading the device.

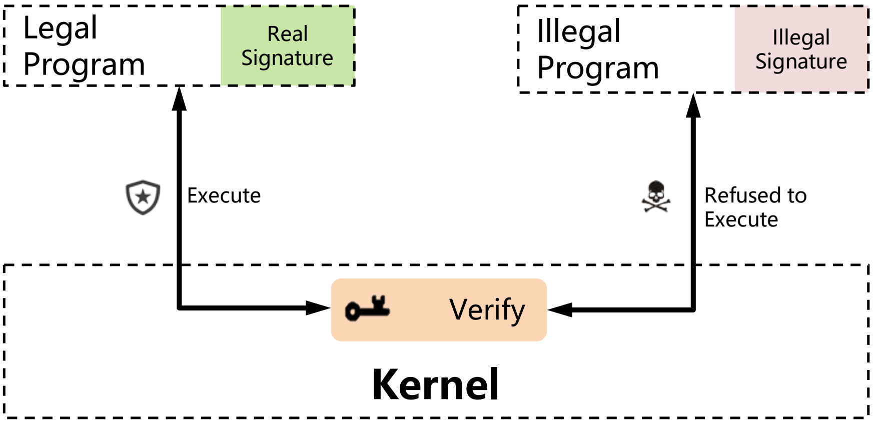


Figure 4-6 Principle of Trusted Execution

4.3.2.3 Trusted Upgrade

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

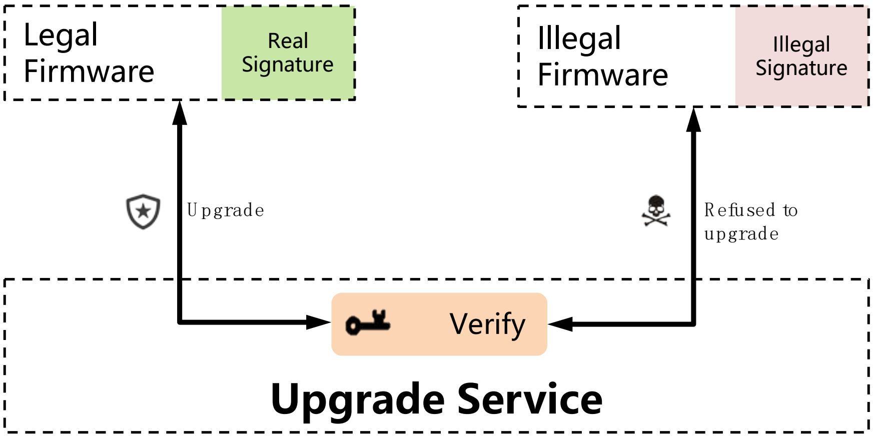


Figure 4-7 Firmware Upgrade Trusted Verification

4.3.2.4 Protected Shell

Shell is the 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 prevent malicious operations from damaging the device.

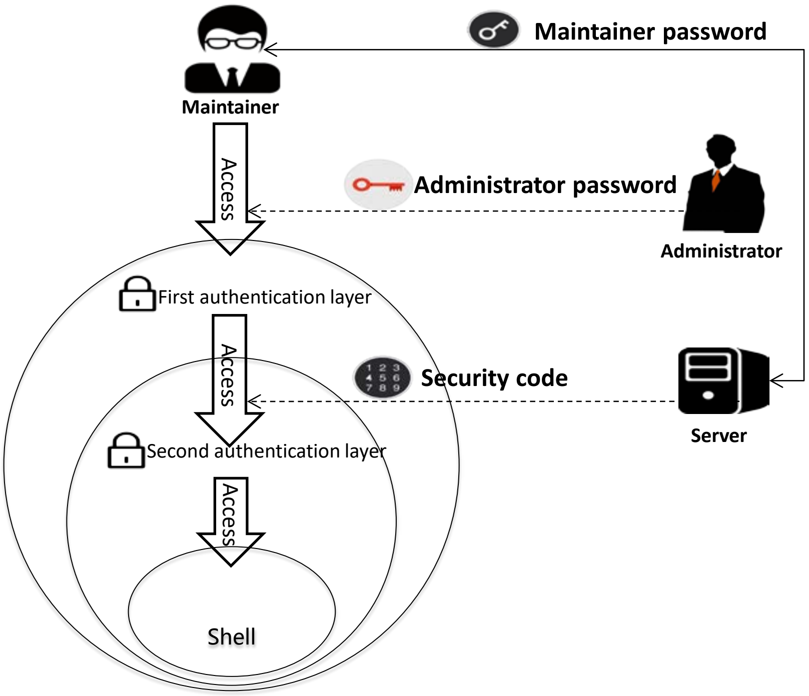


Figure 4-8 Principle of Protected Shell

Multi-factor authentication includes two levels of authorization:

- Administrator authorization：Based on the user management system of the device, 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 achieving the second-level authorization.

4.3.2.5 Cloud Upgrade

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

- Supports automatic version detection
- Supports automated batch upgrades

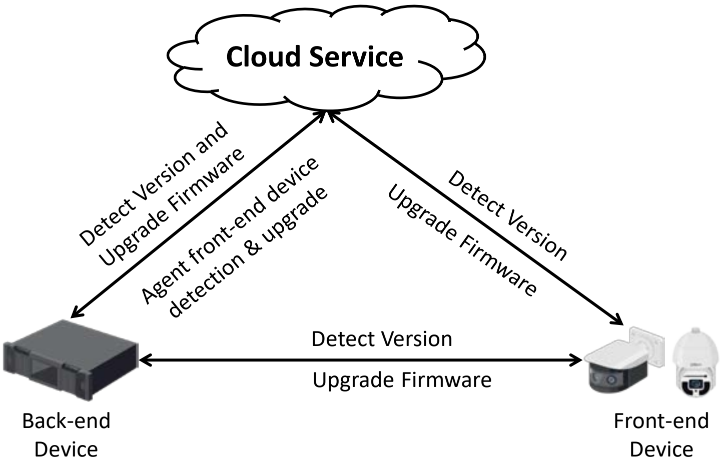


Figure 4-9 Cloud Upgrade Diagram

4.3.2.6 Anti-Reverse

Firmware is one of the important assets of the device. In order to prevent reverse attacks by hackers, Dahua has designed a firmware encryption scheme to ensure that the firmware remains encrypted during the data transfer process. The basic principle is as follows:

- Create a security key based on KDF technology and encrypt the firmware data;
- When the device upgrades the firmware, write it to Flash in encrypted form;
- During the device startup process, the Flash partition data is decrypted and loaded.

4.3.3 **Application Security**

4.3.3.1 Security Authentication Technology

4.3.3.1.1 User Security Policy

The device has no default account before leaving the factory, and 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.

4.3.3.1.2 Digest Authentication

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

HASH algorithm is as follows:

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

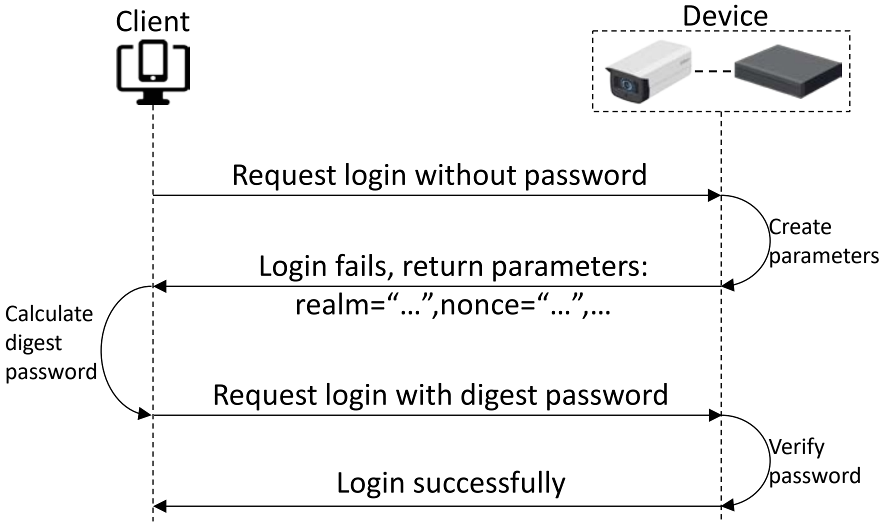

Client
Device
Request login without password
Create parameters
Login fails, return parameters:
realm="…",nonce="…",…
Calculate digest password
Request login with digest password
Verify password
Login successfully

Figure 4-10 Digest Authentication Technology

4.3.3.1.3 WSSE Authentication

WSSE authentication technology is based on HASH algorithm of password, random number, time and other factors to ensure the confidentiality of the password transmission process. Based on the non-repeating random number factor within a limited time, the non-repeatability authentication process is guaranteed.

The WSSE algorithm 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))

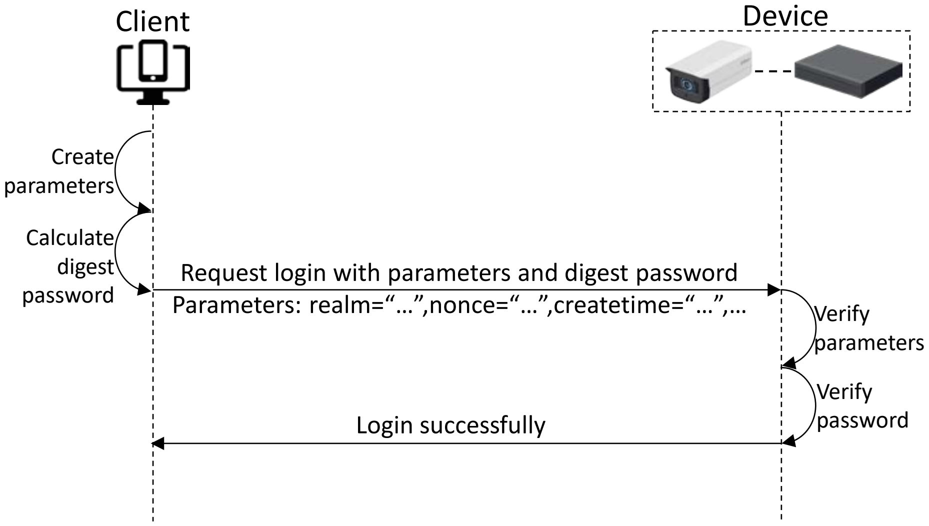

Client
Device
Create parameters
Calculate digest password
Request login with parameters and digest password
Parameters: realm="…",nonce="…",createtime="…",…
Verify parameters
Verify password
Login successfully

Figure 4-11 WSSE Authentication Technology

4.3.3.2 Authority Management System

Based on the RBAC model, the Dahua device has a flexible and efficient authority management and control system to meet the needs of users deploying devices in different scenarios.

4.3.3.3 Log Security Policy

4.3.3.3.1 Log specification record

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

- 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, or 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

4.3.3.3.2 Separate Security Logs

Based on the sensitivity of security events, and in order to further ensure the traceability of such events, the security log storage area is independently divided. While not affecting the business operation log records, the security event log records are given priority.

4.3.3.3.3 Network Logs

Dahua device supports the syslog protocol, which can save important logs to a log server simultaneously.

4.3.3.4 Component Security Policy

Dahua has established a control process for open source and third-party components. As an important part of sSDLC, it has been integrated into the product quality control system. The management of open source and third-party components in the product mainly includes:

- The components must pass security assessment and audit, including open source compliance audit, vulnerability detection, risk assessment, etc.
- After the product is released, use the latest vulnerability library regularly to detect the vulnerability status of components, and pinpoint the scope of affected products to ensure that vulnerabilities are fixed in a timely manner.

4.3.3.5 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 are allowed, including:

- WEB Service
- RTSP Service
- Device Search Service
- …

The device supports more secure service protocols and provides users with more secure options for the same functions, including:

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

4.3.3.6 Session Security Policy

Web services support session interaction based on short connect and the protection strategies are as follows:

- Use highly complex and strong 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 log out all online users of risk hosts;
- Automatically log off long inactive sessions.

4.3.4 **Data Security**

4.3.4.1 Digital Signature Technology

Based on the PKI infrastructure and signature algorithm, it implements data signature and verification functions to ensure the integrity of target data.

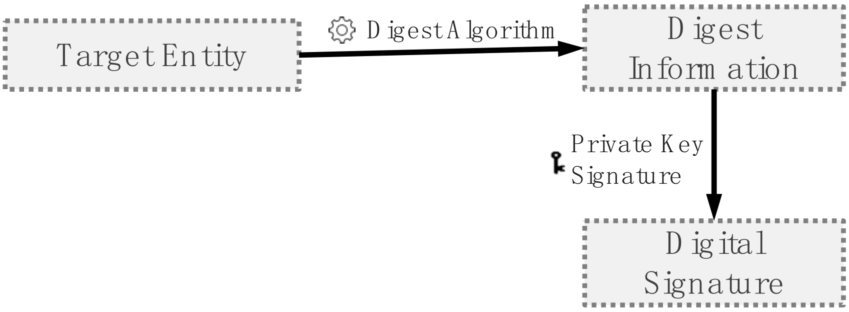


Figure 4-12 Digital Signature Process

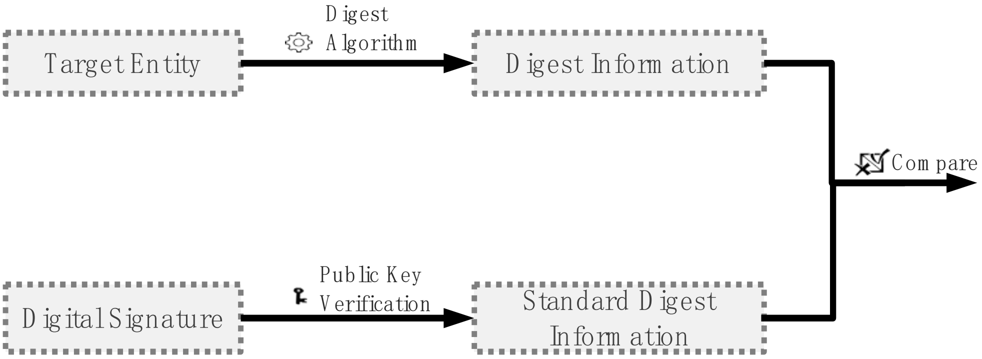


Figure 4-13 Digital Verification Process

4.3.4.2 Digital Envelope Technology

Digital envelope technology is similar to regular letters. Based on this technology, it can ensure that only the intended recipient can decrypt and read the data transmitted on 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;
- When 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.

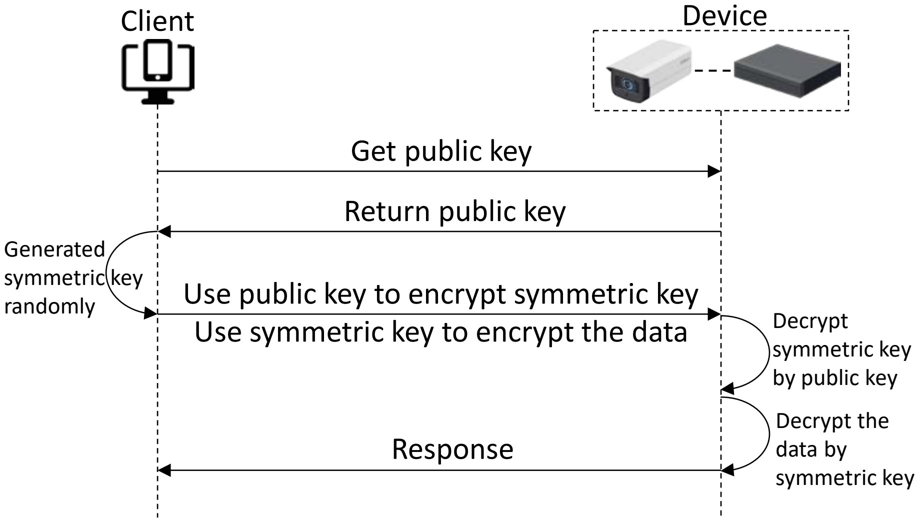

Client
Device
Get public key
Return public key
Generated symmetric key randomly
Use public key to encrypt symmetric key
Use symmetric key to encrypt the data
Decrypt symmetric key by public key
Decrypt the data by symmetric key
Response

Figure 4-14 Digital Envelope Technology

4.3.4.3 Video Encrypted Transmission

4.3.4.3.1 Frame Data Encryption Technology

Frame data encryption technology, that is, encryption and protection based on media stream frame data, currently supports AES256-OFB encryption algorithm. Dahua's private protocol RTSP uses this technology. The specific process is as follows:

- The 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.

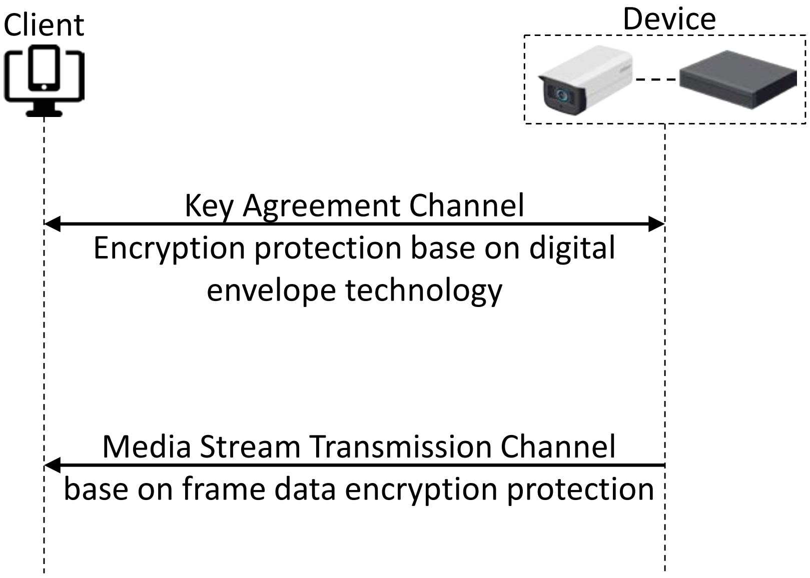

Client
Device
Key Agreement Channel
Encryption protection base on digital envelope technology
Media Stream Transmission Channel
base on frame data encryption protection

Figure 4-15 Interactive Flow of Frame Encryption Technology

4.3.4.3.2 Channel Encryption Technology

Dahua RTSP supports media stream transmission based on TLS channel encryption protection. Both RTSP and TLS are implemented using standard protocols, and support third-party client connection in standard implementation. The specific process is as follows:

- The client and the device establish a trusted encryption tunnel based on TLS protocol;
- Media stream transmission based on TLS channel.

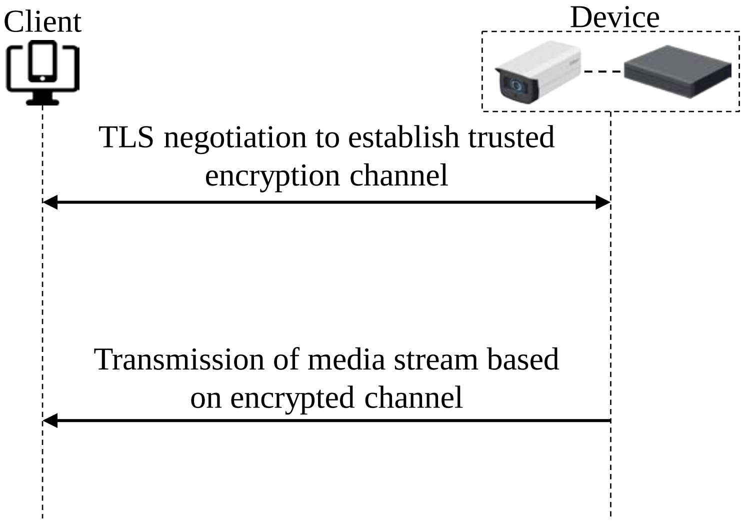

Client
Device
TLS negotiation to establish trusted encryption channel
Transmission of media stream based on encrypted channel

Figure 4-16 Channel Encryption Technology

4.3.4.4 Video Encrypted Storage

4.3.4.4.1 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, support AES256 encryption algorithm;
- Connecting KMS system to protect random key, using industry standard protocols KMIP and HTTPS to connect KMS system;
- Support key regularly update.

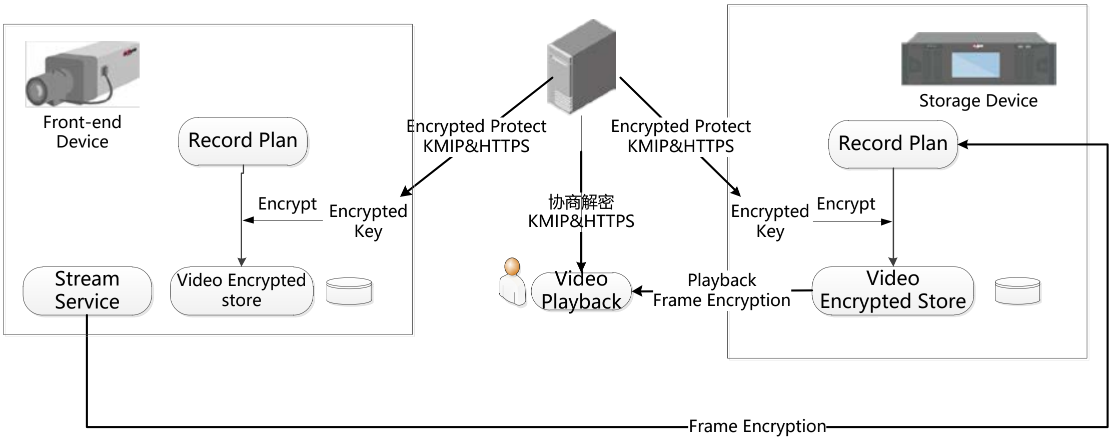


Figure 4-17 Video Encryption Protection Base on KMS

4.3.4.4.2 Encrypted Storage Based on Password Derivation

To simplify user key management deployment, Dahua device implements encrypted storage of video data based on user-set passwords. The basic principle is as follows:

- Use randomly generated keys to encrypt video data, support AES256 encryption algorithm;
- Use KDF technology to derive the key based on the password configured by the user, and encrypt and protect the video key.

4.3.4.5 Video Encrypted Download

The device supports video download function. In order to ensure the security of the video data in the portable storage, the device also supports encrypted download function to ensure confidentiality of the video data transmission process in the portable storage. The basic principle is as follows:

- Based on the video encryption download password set by the user, conducting KDF key derivation to get the key;
- Use the key to encrypt the target video and download it to the client.

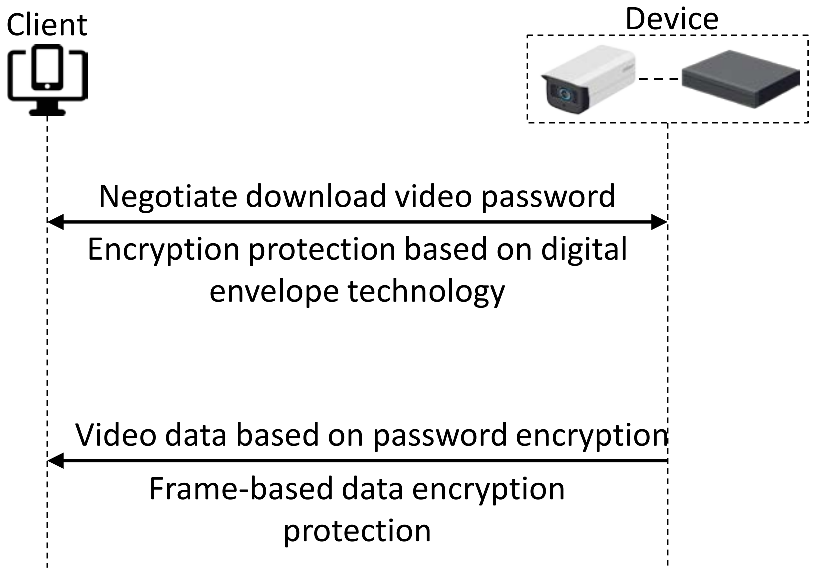

Client
Device
Negotiate download video password
Encryption protection based on digital envelope technology
Video data based on password encryption
Frame-based data encryption protection

Figure 4-18 Video Encrypted Download Principle

4.3.4.6 Configuration Encrypted Storage

Based on the different capabilities of the device, the configured encrypted storage function uses different encryption algorithms, including:

- If the device supports security chip, use the security chip for encrypted storage;
- If the device does not support security chip, a key is generated based on the KDF technology, and the data is encrypted using the key.

4.3.4.7 Configuration Encrypted Export

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

4.3.5 **Network Security**

4.3.5.1 Attack Defense

4.3.5.1.1 Anti-ARP Spoofing Technology

ARP spoofing refers to continuous sending of ARP spoofing packets to implant spoofed IP-MAC mappings into network devices or hosts, thereby intercepting data sent to the target host. The spoofed IP-MAC mapping refers to the mapping relationship composed of the attack target host IP and the attacker host MAC

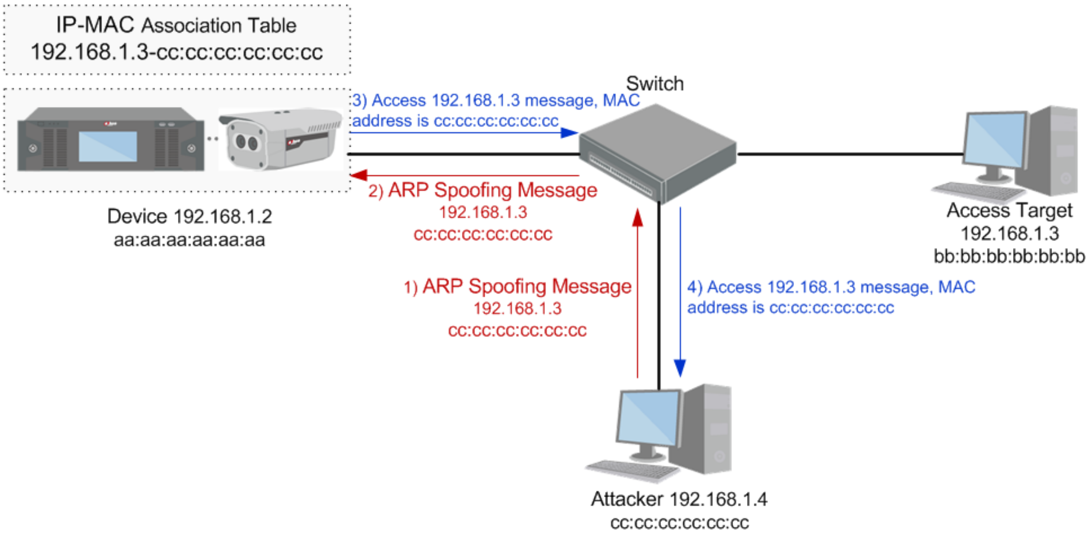


Figure 4-19 ARP Spoofing Technology

The anti-ARP spoofing technology is used to harden the source host's IP-MAC mapping list, block ARP spoofing messages, and prevent the implantation of spoofed IP-MAC mapping relationships

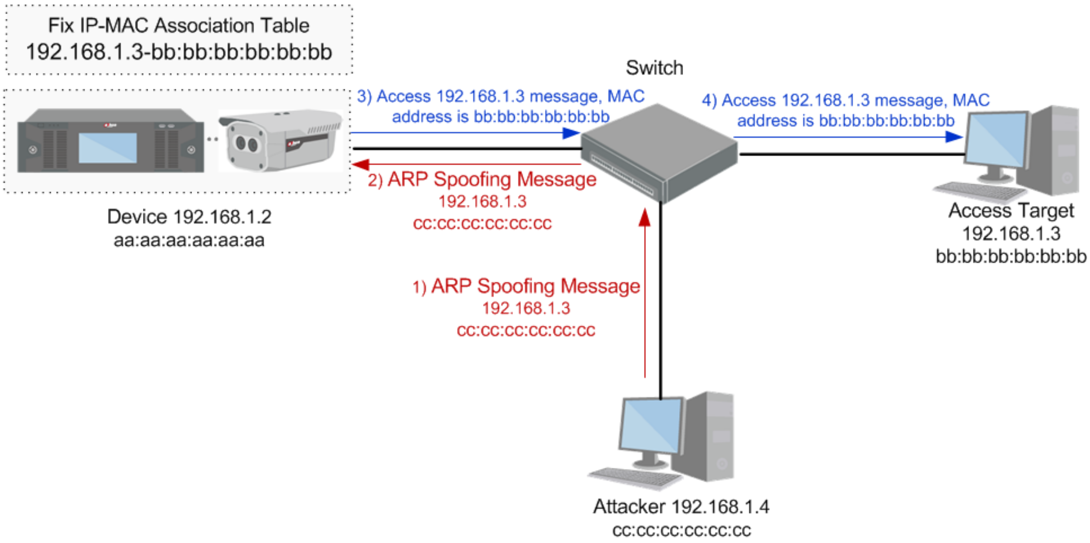


Figure 4-20 Anti-ARP Spoofing Technology

4.3.5.1.2 Anti-DoS Attack Technology

DoS attack means that the attacker exhausts the service resources of the target host by sending malicious network packets, so that the target host cannot provide normal services for legitimate users. Dahua device provides defense technologies for the following DoS attacks:

- ICMP Flood, by sending a large number of ICMP message packets to the device, the device cannot respond to legitimate service requests;
- Syn Flood, which is a TCP semi-connection attack. By continuously sending fake TCP

connection requests, the attacker causes the device to build a large number of TCP semi-connection resources, thereby exhausting the TCP protocol stack and implementing DoS attacks.

4.3.5.1.3 Password Anti-cracking Technology

Password crack attack refers to using a high-performance host to make high-frequency password guesses on the target until the device is successfully logged in to obtain the correct password for the login device.

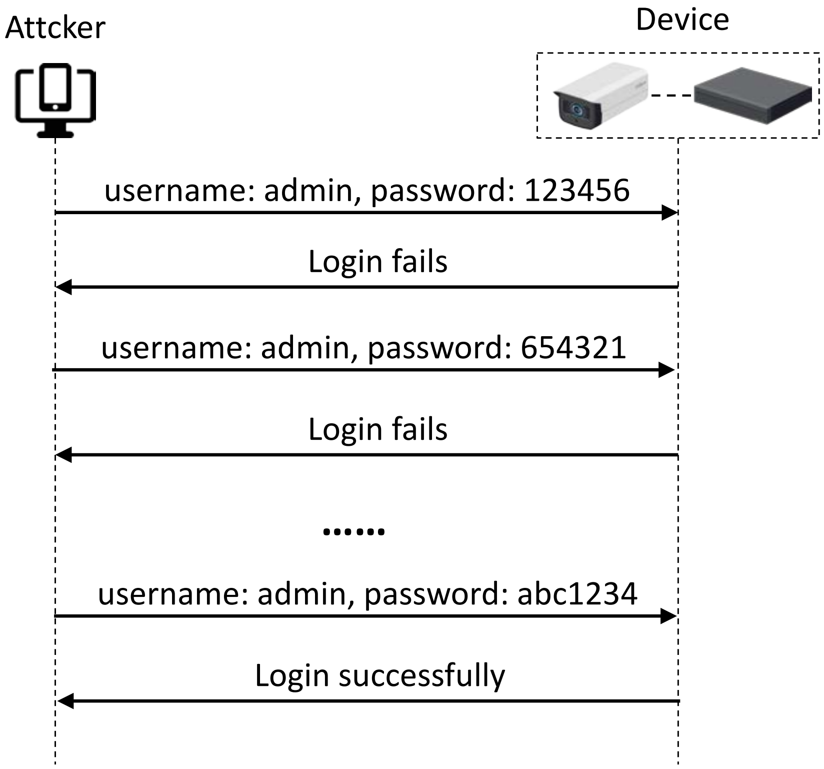

Attcker
Device
username: admin, password: 123456
Login fails
username: admin, password: 654321
Login fails
……
username: admin, password: abc1234
Login successfully

Figure 4-21 Password Crack Technology

Based on the above-mentioned attack characteristics, when the device recognizes the attack of a password crack, it will automatically lock the account and prohibit the login behavior of the host for a period of time.

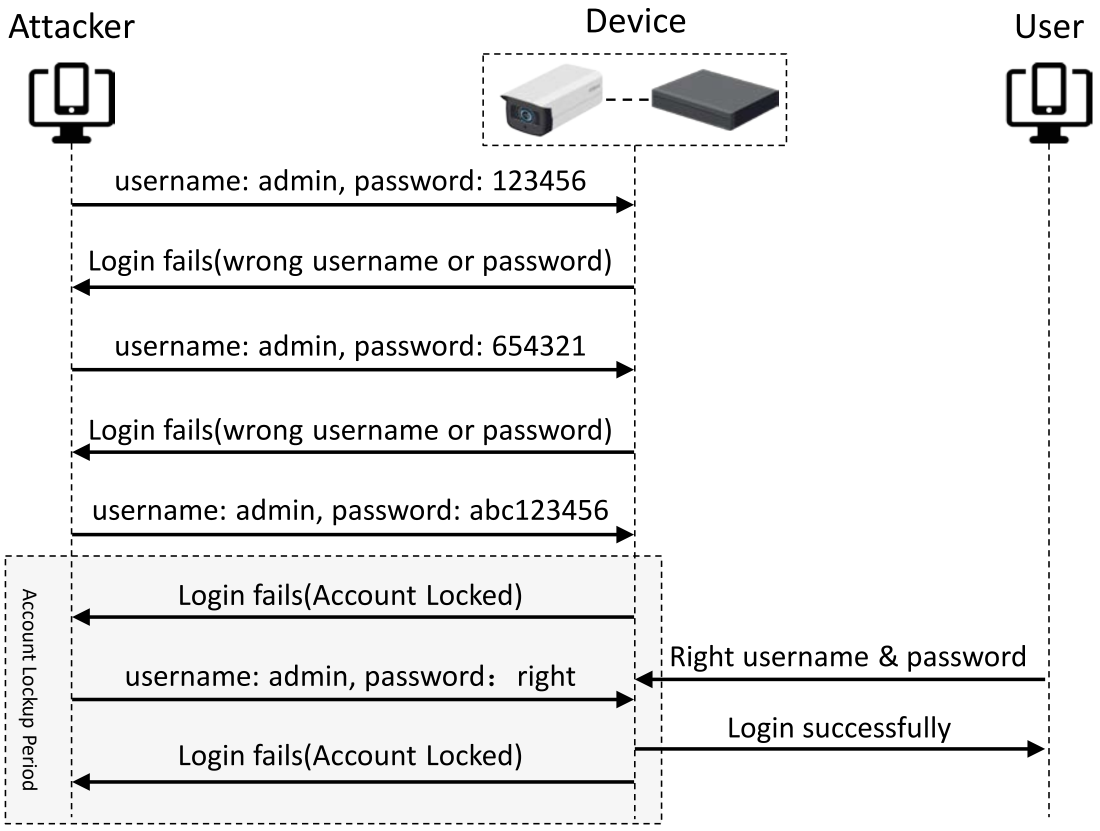

Attacker
Device
User
username: admin, password: 123456
Login fails(wrong username or password)
username: admin, password: 654321
Login fails(wrong username or password)
username: admin, password: abc123456
Account Lockup Period
Login fails(Account Locked)
username: admin, password： right
Login fails(Account Locked)
Right username & password
Login successfully

Figure 4-22 Password Anti-Cracking Technology

4.3.5.2 Access Control

4.3.5.2.1 Firewall

The firewall is implemented based on network packet filtering technology. Based on pre-configured filtering rules, it verifies the characteristics of network packets received or sent, and decides whether to pass, thus reducing the network risk. Its network data packet characteristic information mainly includes the following:

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

4.3.5.2.2 Time Calibration Whitelist

Time is one of the important assets of the device, and its accuracy affects many important functions, such as log, recording time and so on. Dahua device supports time calibration whitelist function. According to the pre-configured rules, only specified hosts are allowed to calibrate the time of the device to avoid malicious tampering with the time.

4.3.5.2.3 802.1x

802.1x is a standard protocol for network access control. It can restrict unauthorized devices or hosts from accessing the private network. The basic principle is 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 the authentication service is verified, the network switch opens the communication of its business data.

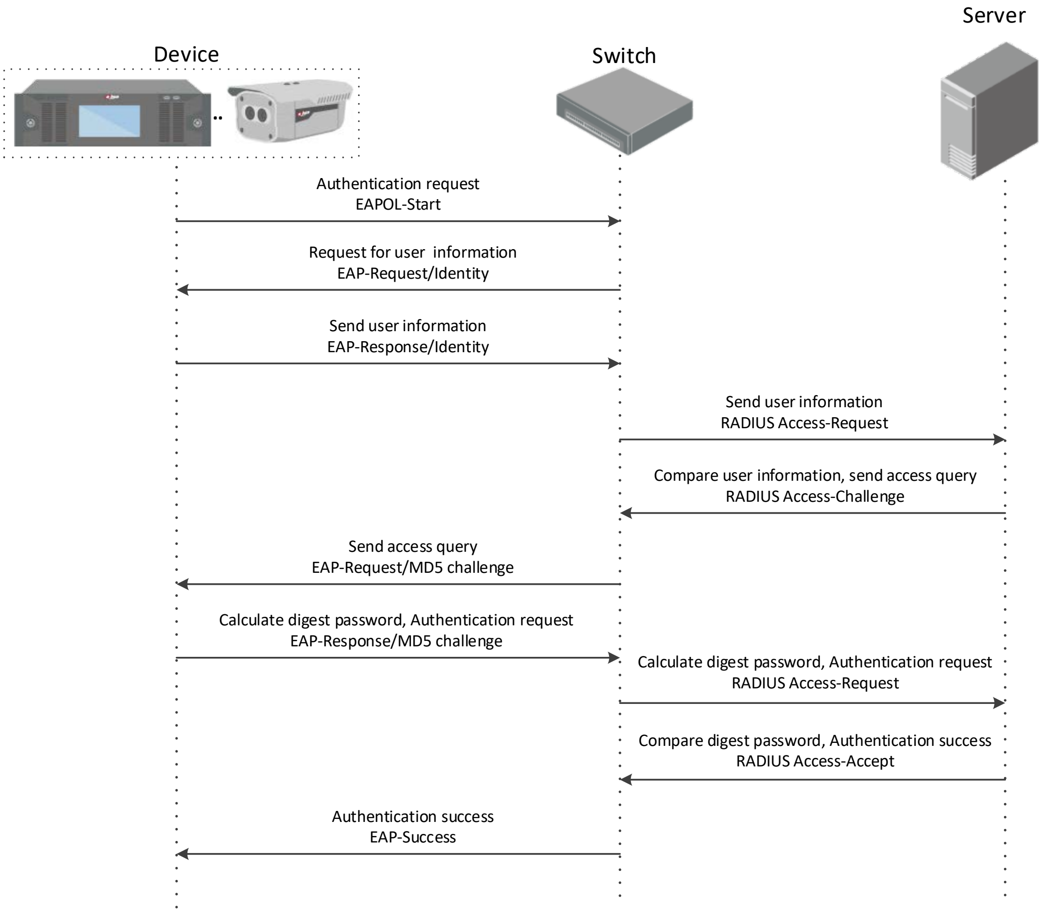


Figure 4-23   802.1x Authentication Process

4.3.5.3 Security Alarm

The device monitors abnormal attack behaviors in real time, notifies users by means of email, mobile push notification, beep, etc., and realizes real-time security alarm. The supported monitoring attack events mainly include:

- Illegal IP access
- Attempt to log in at illegal time
- User name and password cracking
- Session cracking
- Web path cracking
- The number of session connections exceeds the limit
- Illegal program attempting to run

4.3.5.4 CA Certificate

The device supports the digital Certificate of x.509 standard, supports the import of the digital Certificate issued by the third-party CA organization, and supports the generation of the Certificate Signing Request in PKCS#10 format. You can apply for the digital Certificate from the third-party CA organization and import it.

4.3.5.5 Wireless Security

Dahua supports WPA/WPA2 encryption authentication methods based on Radius authentication, and supports WPA-PSK/WPA2-PSK encryption authentication methods.

4.3.6 Privacy Protection

With the continued in-depth development of AIoT, data security and privacy protection are highly valued by countries around the world. Since the promulgation of China's "Network Security Law", "GB/T 35273-2017 Information Security Technology-Personal Information Security Regulations", “EU GDPR”, and “California CCPA”, Dahua has always adopted a proactive and pragmatic attitude and policy to respond, and establishes Data Security and Privacy Protection Special Committee paying close attention to global laws and regulations, comprehensively conducts compliance audits, and actively promotes compliance rectification and certification. In order to comprehensively improve the level of privacy protection of products and services, and better help customers achieve compliance, Dahua has formulated “Dahua personal data and privacy protection standards” in combination with internal security design principles, personal information security specifications, GDPR regulations and TÜV Rheinland standards, and introduced a privacy baseline in the product demand and design stage, from privacy policy, privacy friendly settings, data collection , data transmission, data storage, data deletion and other aspects for the overall specification and guidance of data processing. Dahua products strictly follow the basic requirements of data minimization and privacy friendly settings, and continuously integrate privacy protection technologies and applications such as data masking, data encryption, face occlusion, trusted computing, etc.

Through intelligent recognition technology, it dynamically locates and occludes (supporting faces and human bodies) to improve privacy protection capabilities.

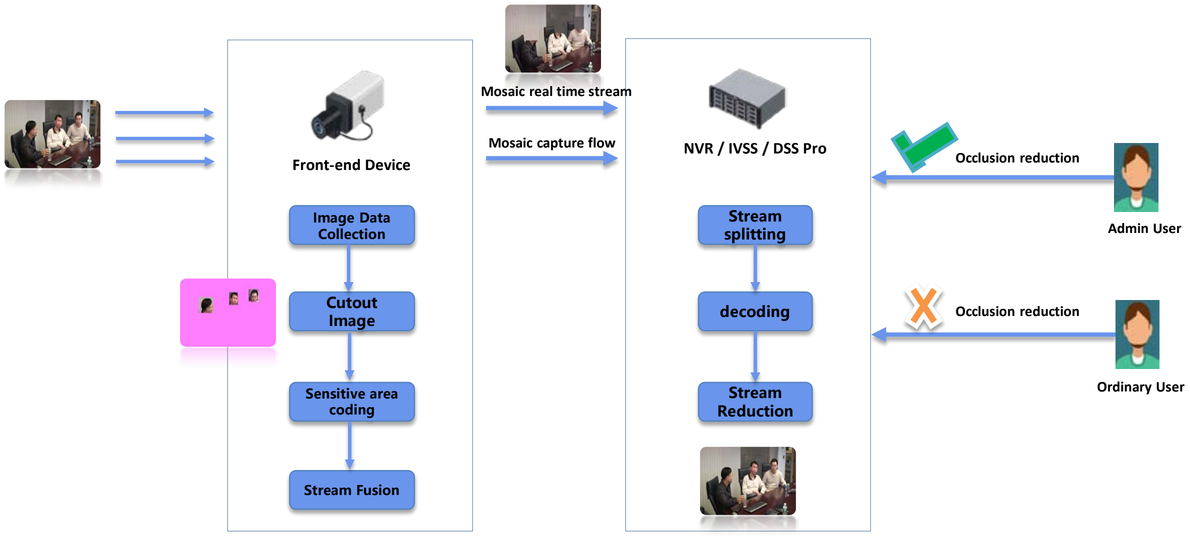


Figure 4-24 Face Occlusion Technology

Based on intelligent face recognition technology, the face parts in the collected image are identified during the image encoding stage, and intelligent matting is performed to hide the personal privacy data in the image. Only users with administrator rights can restore the original image, ordinary users cannot restore it.

5 Security Center

5.1 Overview

The core goal of the security center is to deeply integrate security protection and business scenarios, help users clearly understand the security status and capabilities of the device, and assist users to conveniently and easily set the best security configuration suitable for the scenario.

Based on the inspection and analysis of the current account status, functional configuration, security module and other features of the device, it comprehensively presents the device's weakness to the user. At the same time, the device provides centralized security feature management capabilities, which complement each other to better help users understand and strengthen the device.

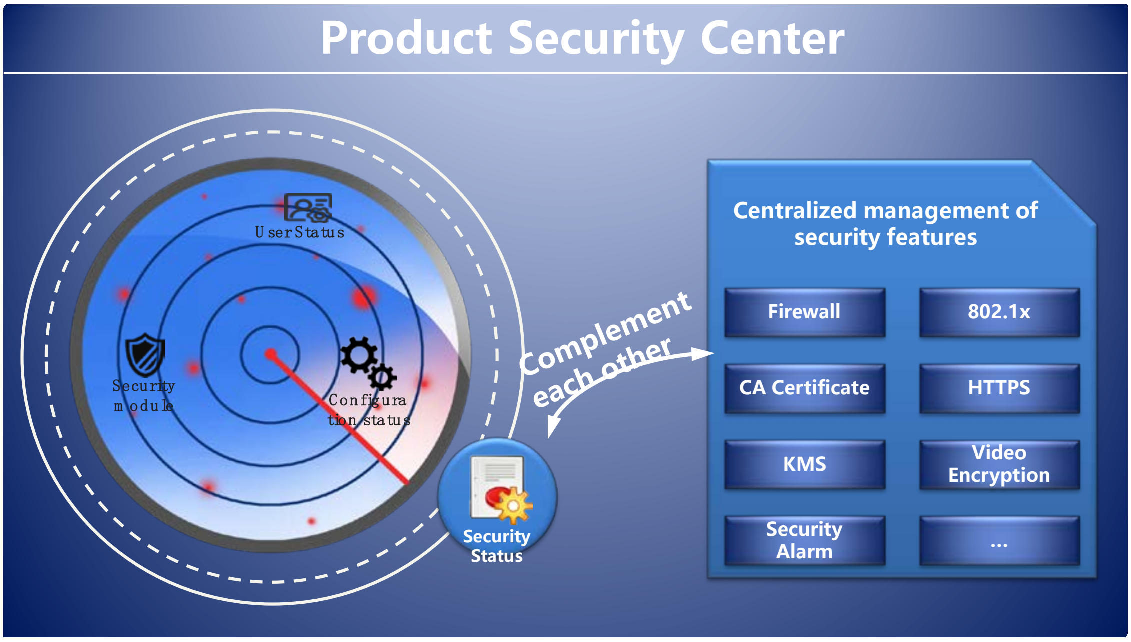


Figure 5-1 Security Center

5.2 Security Scan

The security scan module which is integrated in the device can comprehensively scan the account status, function configuration status, logging status and security module capability of the device based on the current operation state of the device, so as to help users understand the security status of the device configuration and the security capability supported by the device. Users can optimize and improve device security based on scan results and business scenario requirements.

5.3 Security Configuration Centralized Management

All configurable security functions in the device have been loaded into the security center configuration page to form a centralized device security management center. At the same time, effective linkage is formed between security modules, helping users to better apply device security features.

6 Security Compliance

6.1 UL CAP Certification（UL 2900）

UL CAP certification is the world's first and only standards-based security evaluation program for IoT devices and systems, with primary focus on software vulnerabilities, software weaknesses, and adequate implementation of security controls. The technical criteria in UL 2900 are based on existing industry best practices and guidance documents as well as IEC, ISO, and other international standards work. The CAP assessment includes Documentation Review, Source Code Analysis, Known Vulnerability Testing, Malware and Virus Analysis, Fuzzing Testing and Penetration Testing, etc., to comprehensively review the product's security performance.

Dahua passed UL CAP security certification in October 2019, and the certificate number is ULCAP_133.

All products of Dahua must pass unified and strict Code Analysis, Vulnerability Testing, Malware and Virus Analysis, Fuzzing Testing, Penetration Testing and other security assessments before release.

Certificate inquiry address：https://iq.ulprospector.com/en

6.2 TÜV Rheinland Protected Privacy IoT Product Certification

The promulgation of the GDPR, the "most stringent" data protection regulation in history, has set strict, high-level, wide-ranging protection standards for the data security and privacy protection.

Based on the EU GDPR, Technical Guideline TR-02102 Cryptographic Mechanisms of BSI and Internal 2PfG Standard, TÜV Rheinland provides Document Audit, Personal Data Protection, Privacy Data Processing, Penetration Testing, Factory Inspection and other comprehensive testing and evaluation services for Dahua's IPC, NVR, DSS Platform, IVS and other products.

Dahua series of products have passed TÜV Rheinland Protected Privacy IoT Product IoT product privacy protection certification in 2018, the certificate numbers are:

- IPC(IP Camera) Q 50437998
- NVR(Network Video Record) Q 50437996
- DSS Platform(Digital Surveillance System Platform) Q 50459589
- IVS(Intelligent Video Server) Q 50433648

Dahua passed the assessment and obtained the privacy protection certification of IoT products, which means that the products of Dahua better comply with GDPR requirements and set a benchmark for the industry in terms of cyber security and privacy protection.

In combination with the internal security design principles, personal information security specification, GDPR Act and TÜV Rheinland standards, Dahua formulated the "Dahua Personal Data and Privacy Protection Standards ", introduced privacy baseline in the product requirements and design stage, and strictly implemented in the whole series of products.

Certificate inquiry address：https://www.certipedia.com/quality_marks

6.3 TÜV Rheinland Protected Privacy IoT Service Certification

Based on the EU GDPR, C5 and Technical Guideline TR-02102 Cryptographic Mechanisms of BSI and Internal 2PfG Standard, TÜV Rheinland provides comprehensive assessment services such as Physical Security, Data Security, Application Security, Cyber Security, and APP Security, Security Development Process, and Security Emergency Process for the Iaas / PaaS / SaaS layer of Dahua Imou Cloud, and conducts Penetration Testing.

Dahua passed the TÜV Rheinland Protected Privacy IoT Service Certification in December 2019 with certificate number 50458168.

Dahua passed the assessment and obtained the privacy protection certification of IoT services, which means that Imou Cloud's cyber security and privacy protection capabilities have reached industry-leading levels.

Certificate inquiry address：https://www.certipedia.com/quality_marks

7 Security Suggestion

7.1 Mandatory actions to be taken for basic equipment network security

1. **Use Strong 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; character types include 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 overlapping characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

7.2 " Nice to have" recommendations to improve your equipment network security

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign them a set of minimum permissions.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

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

11. Audio and Video Encrypted Transmission

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

Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. Network Log

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

14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

8 Security Incident Response

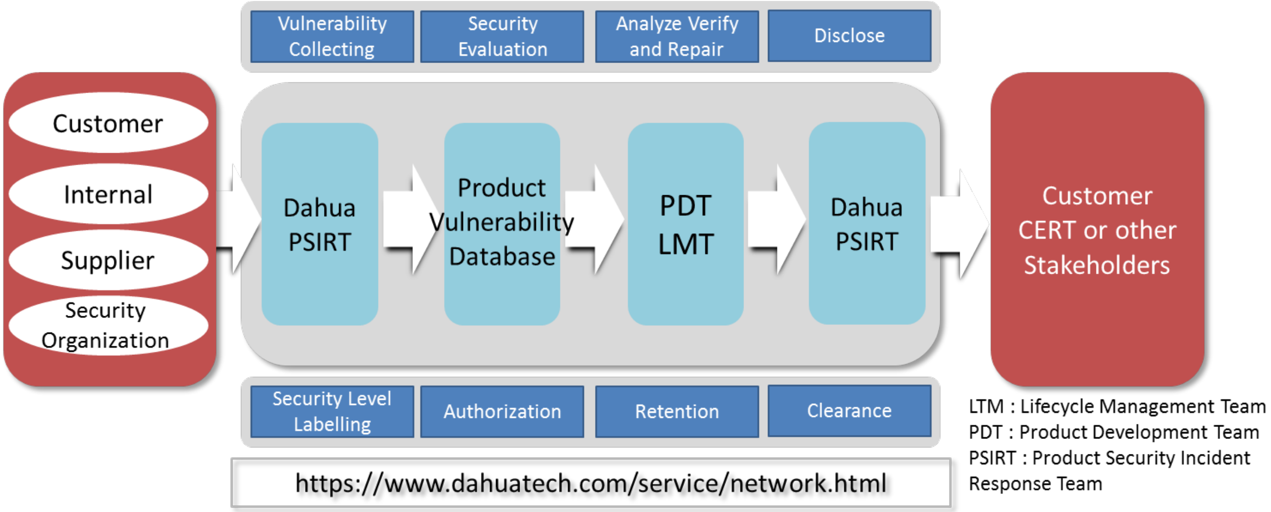

Vulnerability Collecting
Security Evaluation
Analyze Verify and Repair
Disclose
Customer
Internal
Supplier
Security Organization
Dahua PSIRT
Product Vulnerability Database
PDT LMT
Dahua PSIRT
Customer CERT or other Stakeholders
Security Level Labelling
Authorization
Retention
Clearance
https://www.dahuatech.com/service/network.html
LTM : Lifecycle Management Team
PDT : Product Development Team
PSIRT : Product Security Incident Response Team

Figure 8-1 Product Security Incident Response System

Dahua PSIRT (Product Security Incident Response Team) is responsible for the management of security ecology and product vulnerabilities in accordance with industry practices. The 24/7 response to global security issues provides customers with security alarms and reinforcement services in a timely manner. It ensures that security issues reported to Dahua through formal channels can be responded to within 24 hours and no later than 48 hours.

For the management of security issues, Dahua PSIRT team adopts two forms – SN (Security Notice) and SA (Security Advisory) – to communicate with customers, ensuring that we inform customers with security issues in an appropriate manner during the different stages of issue discovery.

Dahua PSIRT team follows the ISO/IEC 30111:2013 vulnerability handling process and ISO/IEC 29147:2018 vulnerability disclosure standards, establishing the disclosure processes of product security vulnerability, security advisory, and security alarm. Dahua also encourages end users, partners, suppliers, government agencies, industry organizations and independent researchers who find potential risks or vulnerabilities related to Dahua products to actively report such security issues to us.

Dahua PSIRT team actively participates in industry and public activities, and open-mindedly maintains communication with government CERT, customer CERT/PSIRT, other suppliers, researchers and third-party coordinating agencies. By joining FIRST (Forum of Incident Response and Security Team), CNAs (an international CVE number issuing agency), CNNVD (China National Vulnerability Database of Information Security), CNVD (China National Vulnerability

Database), CCTGA (China Cyber Threat Governance Alliance) and other information security organizations, we are able utilize the member’s benefits in order to realize the working mechanism of cyber security threat intelligence sharing and mutual cooperation.

9 Security Commitment

Dahua has always regarded cyber security and privacy protection as one of the company's highest programs and has continuously invested special funds to comprehensively improve security awareness and capabilities aims at providing sufficient security protection for its products. Dahua has established a professional security team, which provides whole life cycle security management and control for product design, development, testing, production, sales and aftersales While insisting on data minimization, service minimization, strictly prohibiting backdoor, removing unnecessary and unsecure services (such as Telnet, etc.), Dahua constantly introduce innovative security technologies, strive to promote and improve the product security capability, and better meet the security requirements of users in different scenarios.

Dahua established DHCC (Dahua Cybersecurity Center) to solve cyber security issues and provide reliable and secure solutions for global customers, including Security Advisories, Security Alarms, Vulnerability Report and Response Processes, and sharing Security Suggestions and Research Results, etc. For the latest and detailed security information, please visit：
https://www.dahuatech.com/service/network.html.

Dahua also established PSIRT (Product Security Incident Response Team), which is responsible for accepting, processing and publicly disclosing security vulnerabilities related to Dahua products and solutions, responding to global security issues 24/7, and providing customers with security advisories and reinforcement services in a timely manner. Dahua hope and encourage end-user, partner, supplier, government agency, industry organization, and independent researcher who discover potential risks or vulnerabilities to actively contact Dahua PSIRT (CyberSecurity@dahuatech.com). If it involves sensitive information such as vulnerabilities, we recommended that you use Dahua PGP public key for encryption.

【Enabling a Safer Society and Smarter Living】