



Security of the Internet of Things

Technical White Paper

V1.0.0

DAHUA TECHNOLOGY CO., LTD.

Legal Statement

Copyright Statement

© 2017 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 can copy, transmit, distribute or store any content of this document in any form.

Products described in this document may contain software copyrighted by Dahua or some other third person. Unless approved by the related obligee, no one can copy, distribute, modify, extract, decompile, disassemble, decode, reverse engineer, lease, transfer or sub-license the above-mentioned software in any form which may lead to property infringement.

Trademark Statement

-  are trademarks or registered trademarks owned by Zhejiang Dahua Technology Co., Ltd.
- HDMI logo, HDMI and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC. This product has been authorized by HDMI Licensing LLC to use HDMI technology.
- VGA is the trademark of IBM.
- Windows logo and Windows are trademarks or registered trademarks of Microsoft.
- Other trademarks and company names mentioned are the properties of their respective owners.

Disclaimer

- Within the scope allowed by applicable laws, in any case, this company won't compensate any special, contingent, indirect and secondary damages resulting from relevant contents and products described in this document, nor compensate any losses in profits, data, reputation, document loss or expected savings.
- Products described in this document are provided "as is". Unless required by applicable laws, this company doesn't provide any express or implicit guarantees for all contents in the document, including but not limited to guarantees for marketability, quality satisfaction, application to specific purpose and non-infringement of third-party rights.
- The security technologies, capability and characteristics described in this document shall be subject to the specific product model, software version, software platform and the implementation of specific solution. It does not provide any expressed or implied guarantee that all the products or solutions of Dahua provide all the security technologies, capability and characteristics described in this document.

Export Control Compliance Statement

Dahua abides by applicable export control laws and regulations, and implements export, re-export and transfer requirements of hardware, software and technology. Regarding products described in this manual, please fully understand and strictly conform to applicable export control laws and regulations at home and abroad.

About This Document






- If the PDF document obtained cannot be opened, please upgrade the reading tool to the latest version or use other mainstream reading tools.
- The company reserves the right to modify any information in this document at any time. The modified contents will be added to the new version of this document without prior notice. There may be slight difference in part of the product functions before and after the update.
- This document may contain technical inaccuracies, discrepancies with the product function and operation or typographical errors. All subject to the final interpretation of the company.

Overview

From the security threats faced by the Internet of Things, this white paper mainly introduces the network security architecture, security technology and security strategy adopted by Dahua

Symbol Definition

The following symbols may appear in the document. Please refer to the table below for the respective definition.

Symbol	Definition
 Danger	It means highly potential danger. It will cause severe injury or casualties if it fails to avoid.
 Warning	It means moderate or low potential danger. It may cause slight or moderate injury if it fails to avoid.
 Caution	It means potential risk. It may cause device damage, data loss, weaker performance or other unpredictable consequences if it fails to avoid.
 Tip	It means that it can help you to solve some problems or save your time.
 Note	It means the additional information, which is the emphasis and supplement of the main body.

Revision Record

No.	Version No.	Revision Content	Release Date
1	V1.0.0	Initial Release	2017.11.10

Legal Statement	I
Preface	III
1 Overview of the Internet of Things	1
2 Security Threats	3
3 Dahua IoT Security System	5
3.1 Security Device	5
3.2 Security Communication	6
3.3 Security Cloud	6
3.4 Security Lifecycle Management	6
4 Introduction of Dahua IoT Security Defense	7
4.1 Data Security	7
4.1.1 End-to-End Data Encryption.....	7
4.1.2 Data Redundancy Backup	8
4.1.3 Data Access Strategy	8
4.1.4 Hardware Encryption Module	8
4.2 Identity Security.....	9
4.2.1 User Account Security	9
4.2.2 Account Authorities Security	10
4.2.3 Session Security.....	11
4.3 Network Security	12
4.3.1 Secure Transmission	12
4.3.2 Security Isolation.....	12
4.3.3 Flow Control.....	13
4.3.4 Attack Prevention	13
4.4 System Security	13
4.4.1 Cloud Upgrade Service	13
4.4.2 Firmware Upgrade Security.....	14
4.4.3 Secure Operating Environment.....	15
4.4.4 Network Service Strategy	16
4.4.5 Log Audit.....	16
4.5 Security Lifecycle Management.....	17
4.5.1 Secure Development Lifecycle Management	17
4.5.2 Supporting System.....	19
5 Policy and Compliance	20
5.1 Security System	20
5.2 Policy Compliance	20
5.3 Privacy Policy	21
6 Conclusions	22

1

Overview of the Internet of Things

The Internet of Things (IoT) connects huge amount of devices and takes us into a whole new world with all the things perceptive, connected and intelligent, thus greatly improves the social operation efficiency and makes people's life convenient. IoT has a wide range of applications, including smart home, intelligent building, smart health-care, logistics, transportation, police affairs, etc. As predicted by Gartner, the number of world IoT devices will increase to 20.8 billion by 2020, and the combined growth will up to 34%. IoT will infiltrate to all aspects of people's lives and reach a wide range of industries.

Security Issues

As an extension of Internet, IoT is also facing security issues and security threats as the traditional Internet does. For example, how to protect the data to be confidential, complete and available? How to prevent data from being intercepted, forged, faked and tampered with? Besides, IoT inevitably brings new security problems due to its own characteristics:

- A large amount of IoT applications are closely related to life, such as camera, which can directly or indirectly expose users' privacy information through the collection of information.
- Due to the self-limitation of resources, a lot of IoT devices lack security measures of encryption, authentication and access control management, making the data in IoT easy to be stolen or unauthorized accessed, and leading to data leakage.
- IoT devices are in large amount and scattered. It is difficulties to monitor the upgrade process and security state of the massive IoT devices.

Security Incidents

In real life, the security incidents caused by IoT devices are already shocking:

- According to the media report: On October 21, 2016, Eastern United States was attacked by the most serious DDoS attack in history with attack traffic of more than 1 Tbps. Nearly half of the U.S. network was attacked and paralyzed. The cause of the incident was the micro-smart devices which were common but easily to be ignored in our daily life, including camera, home router and digital video recorder (DVR). These devices were infected by Mirai malware, resulting in attacks which crippled hundreds of well-known websites such as Twitter and Amazon for several hours.
- In 2015, HackPWN security expert demonstrated how to open the door, start the car and open the trunk of BYD car by using the BYD cloud service vulnerabilities.
- On December 23, 2015, hacker took BlackEnergy and some other related malicious code as main attack tools, remotely controlled the power control system node to deliver power cut-off instruction, and blocked the system recovery by wiping off and covering data, shutdown and interfering service call. A large number of users have been affected by a few hours of power outage in more than half of the Ukrainian Ivano-Frankivsk region.

The security problem of IoT needs us to pay high attention to. The country has implemented a series of laws and regulations to strengthen the construction of network security, such as Law

of the People's Republic of China on Network Security, and Some Views of China on Strengthening the Construction and Networked Application of Public Safety Video Monitoring. According to Gartner, the global expenditure on IoT security reached \$348 million in 2016, which rose 23.7% from \$281.5 million in 2015. In 2018, the IoT security spending is expected to reach \$547 million. IoT security will become an important topic we have to face.

From the terminal layer of perceptive devices such as camera and the network layer of data transmission, to the platform layer of operation and maintenance management and the cloud, the security threats faced by IoT are shown in Figure 2-1.

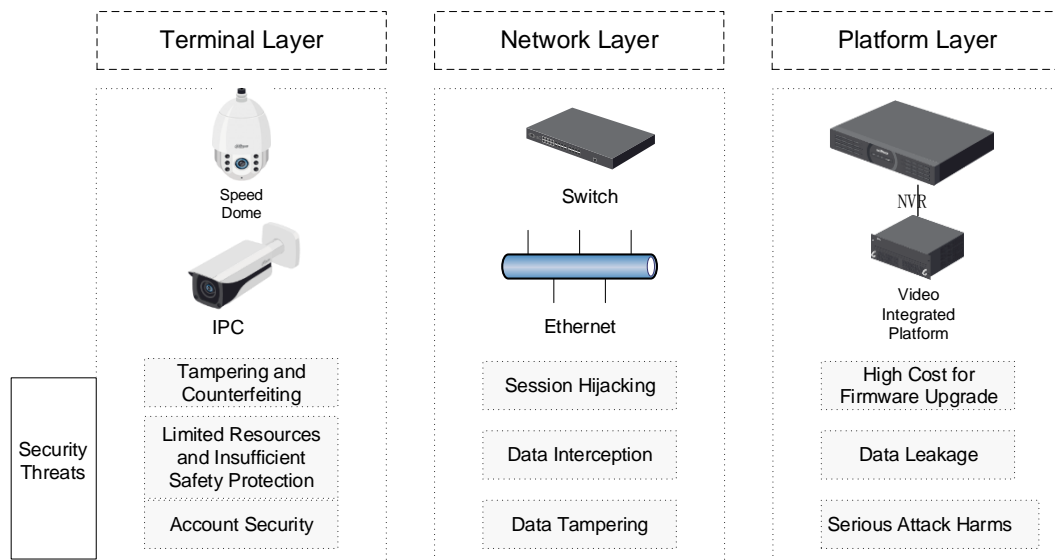


Figure 2-1

Terminal Layer

The form of terminal device varies widely and is widely distributed in all walks of life, from intelligent traffic, smart buildings to safe cities.

Considering the individual differences and service diversity, the security threats faced by the terminal devices are listed below:

- The terminal devices of IoT are usually installed outdoor. The devices are easily got in touched but not managed, resulting in physical attacks, being tampered with and counterfeited.
- Most of the IoT terminals are small built-in devices. Due to the cost and computing power reason, the security technology such as anti-virus and content detection cannot be applied in terminal devices, leading to weak safety ability of the terminals.
- IoT terminal devices are widely used. The device amount is huge and the cost of software vulnerabilities fixing is high.

Network Layer

Data collected by the device layer and the device configuration information need to be transmitted to the management layer through the network. In the process of network transmission, data is facing the ever-present threats from network attacks at any time:

- IoT data is transmitted through the Internet. Due to the defects of transport protocol or lack

of encryption during communication, the data is easy to be hijacked, reset, tampered with and intercepted by some intermediary, resulting in the stolen of users' data and personal privacy.

- Transition to IP. Face the security problems from IP system, such as attacks and invasion from the Internet.

Platform Layer

IoT platform layer provides enterprises and users with visual platform to manage the massive device terminals. It provides different applications and services, and let the devices and protocols from different regions and different types to interact. Security threats as shown below.

- The devices managed by the platform are scattered and diverse, and may come from different manufacturers. It's difficult for the platform to connect the models from different manufacturers and devices with different interacted protocols. Meanwhile, it's difficult to manage the upgrading process and safe state of massive devices.
- The platform supports different user operations. Overpower access due to the improper permission setting or verification makes the risk of leakage of important data such as personal privacy and security credentials.
- The platform provides abundant applications and data center outlets, and the interaction agreement with the peer end is also varied, thus the network attack methods are endless. For example, the risk of DDoS network attack is high.
- Currently, many platforms have open API interfaces, which may cause new security threats, such as injection attacks.

3

Dahua IoT Security System

Due to the distribution nature of IoT, the devices may be distributed across different regions, and the terminal devices transmit information to the IoT platform through Internet connection. Terminal devices which differ in thousands ways, ubiquitous security risks in the transmission network, and privacy data on the IoT platform, make the different components of IoT cross different security trust regions. Therefore, IoT needs a multiple peer-to-peer security defense system.

Dahua integrates the whole management process of Software Security Development Lifecycle into the development process of company collaborative products. Based on a perfect safety management system, Dahua realizes a multiple end-to-end security defense system including terminal layer (end), network layer (tube) and platform layer (cloud), providing user with safe and reliable IoT security products and solutions. Dahua IoT security defense hierarchy is shown in Figure 3-1.

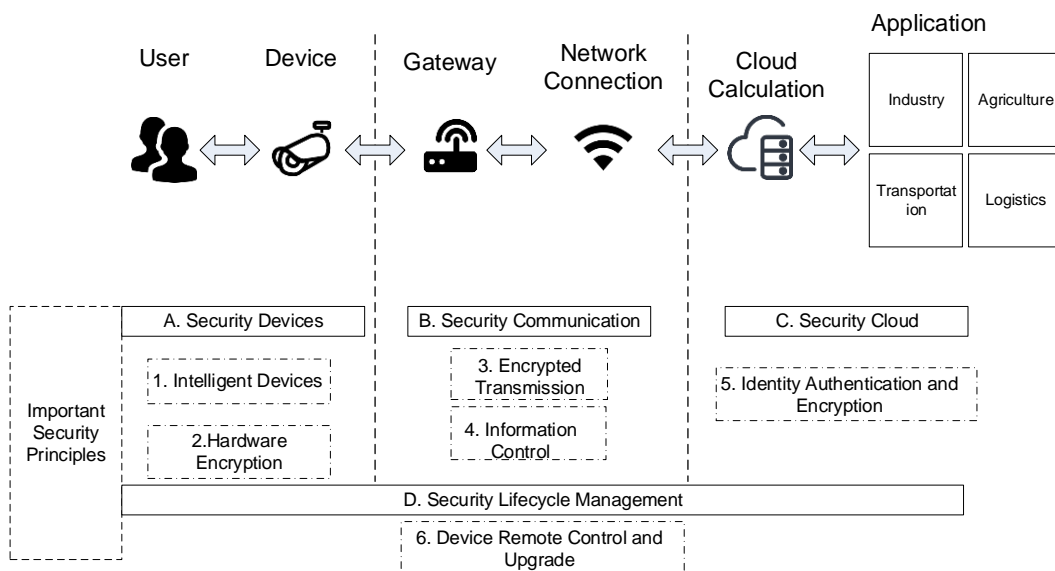


Figure 3-1

3.1 Security Device

Terminal layer involves the hardware when deploying the IoT solutions. IoT devices are widely distributed in large number. They are exposed, sensitive and vulnerable. Dahua is committed to integrating more security functions on the terminals when designing and producing devices (including OEM device). For example, Dahua uses identity authentication function of device to prevent abnormal terminals from connecting to the network, provides hardware encryption module to protect local data security effectively, and uses safety test and integrity checking of firmware to ensure the upgraded firmware package safe and effective.

3.2 Security Communication

Network layer is the medium used to transmit data safely. The data on IoT devices can be viewed and used by users only when it's transmitted to a server or the cloud through the network. The data contains a lot of sensitive information, so only the safe transmit channel can ensure that the data is not stolen or tampered with.

3.3 Security Cloud

Platform layer is responsible to analyze storage and process massive data on the terminal. It is open to users, supports multi-user concurrent operation, and provides a wide range of application ports, therefore is more vulnerable to the network attack. Meanwhile, the analysis and processing of massive data raises higher performance requirements of the platform.

Dahua provides its cloud upgrading solutions depending on cloud service and cloud storage. The devices can connect to the cloud service directly and the device firmware can be upgraded fast and effectively, providing a safe and convenient way to patch security vulnerabilities. Dahua operation and maintenance management platform provides visual operation and maintenance measures like real-time monitoring, video analysis, household register management of monitory area, and visual reports, which improves the operation and maintenance efficiency.

3.4 Security Lifecycle Management

In addition to the three levels according to architectural hierarchy, Dahua realizes the operation, maintenance and control of IoT device and security with a view to the overall IoT security structure and solution. From the factory to installment and deployment, then to practical application, Dahua monitors the IoT security dynamically, realizes the full lifecycle management, reinforces the security features of each part, so as to promote IoT security continuously.

Dahua introduces Security Development Lifecycle (SDLC) management flow to the development process, and combines the enterprise security requirements with Dahua collaborative project development process. It identifies the security risks in products and solutions systematically, and carries out end-to-end project SDLC management.

From the perspective of data security, identity security, network security and system security, this chapter describes the application status of the above-mentioned security technologies on the device layer, network layer and platform layer of IoT security. Also the Dahua Security Development Lifecycle Management System based on the product development process is stated.

4.1 Data Security

Dahua has a profound understanding of the importance of data security for customer business and customer privacy. From the perspective of data security lifecycle, Dahua formulates corresponding data security management policies according to each lifecycle phase, including data generation, storage, transmission and extinction, to ensure the end-to-end data security.

4.1.1 End-to-End Data Encryption

Dahua provides end-to-end data security protection for IoT.

Sensitive Information Protection

The leakage of sensitive information like username, password, personal name, telephone number, E-mail and address will allow the attacker to steal user information at its own will for a long time without the user's perception.

To avoid leakage of sensitive data, the device can store sensitive data safely. The device stores sensitive data with encryption, to prevent attackers from obtaining sensitive information by getting documents through firmware static analysis and device login.

Business Data Protection

Data encryption through the whole process including data generation, transmission, storage and application, it ensures data security to the maximum extent.

After high strength encryption, the business data is transmitted from the terminal to back-end storage or platform system, and stored directly in the form of encrypted data on the platform.

When there is a business query request, the data is still sent to the client in an encrypted manner, and displayed after local decryption on the client. Data is in encrypted status through the whole course, which can prevent data leakage effectively. Business data protection flow is shown in Figure 4-1.

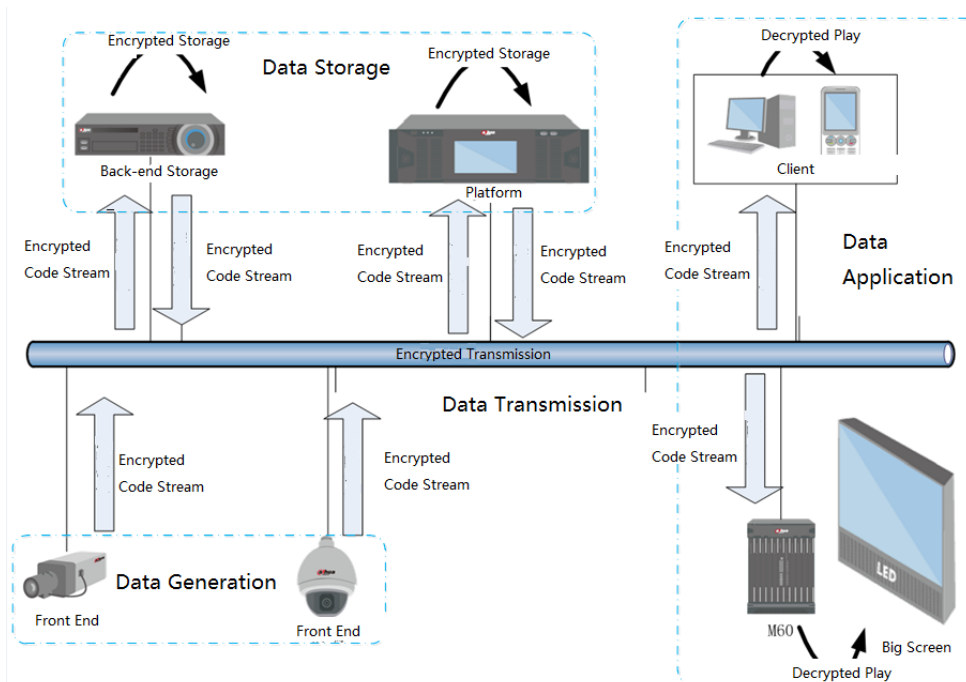


Figure 4-1

4.1.2 Data Redundancy Backup

To reduce the data loss or service interruptions due to hardware failure, natural disasters or other disasters, Dahua solutions provide disaster tolerance backup ability for the stored data, to ensure the security of users' data.

4.1.3 Data Access Strategy

Dahua provides security guarantee for enterprise and user data access. There is strict access rights management when accessing the data of Dahua products. Any third-party application shall be authorized by the enterprise or user before their access to the data. Meanwhile, the operation will be recorded in the corresponding operation logs, so that it's available for subsequent trace and audit.

4.1.4 Hardware Encryption Module

The hardware encryption module is used to provide hardware encryption function in the system, and the key is protected inside this module. Dahua promotes the data security protection level of the system through the hardware encryption module.

- The hardware encryption module transfers the key of the encryption algorithm of internal application software to the chip's hardware safely for protection.
- When it is needed, the application software can call the encryption algorithm in the hardware by running engine instructions through functions and return results to help complete the whole software functions.
- As there's no copy of the keys of the encryption algorithm available on the device end, the attacker cannot guess or steal the encryption keys, and ensure the security of local sensitive data effectively.

4.2 Identity Security

4.2.1 User Account Security

Non-reserved account, password strength requirement, password policy and son on can guarantee device user account security. .

- Non-Reserved Account

When device is shipped out of the factory, there is no reserved account. When a user runs the device for the first time, he or she will be required to create an original account belonged to himself / herself to avoid any user unknown retention account existed and may be used by the attackers.

- Password Protection Polity

The device makes minimum security requirements for the password used by the user and guides users to use a stronger password.

- ◇ 8 characters at least.
- ◇ Combine 2 types of characters at least.

Security tips for login prompt, password strength and session authentication:

- ◇ On adding an account interface and modifying password interface or some account display interfaces, the device clearly displays the security level of current password to remind the user of the password security situation.
- ◇ When the user is logging in, whether the user name is wrong or the password is wrong, the device only returns the “Invalid user name or password”, ensuring the unguessability of the device account.
- ◇ The device has no default password. It is compulsive for the user to set the user password during the initialization process.

After the user’s password is modified, the device is forced to log out current user’s online sessions and requires a re-authenticated login. It is to prevent any illegal user from keeping the connection and going on operating.

- Password Blast-Proof

To prevent the account password from being cracked violently, Dahua devices use password blast-proof technology, which is a kind of password protection security technology based on the idea of improving the attack time cost.

The principle of password blast-proof is that when a host starts password blasting behavior to the device, the device will enter account lock period. During the lockup period, login will be failed no matter the host password is correct or not. The attacker can try very limited times of password during the specified period, so that password blast behavior can be stopped effectively. Password blast-proof technology is shown in Figure 4-2.

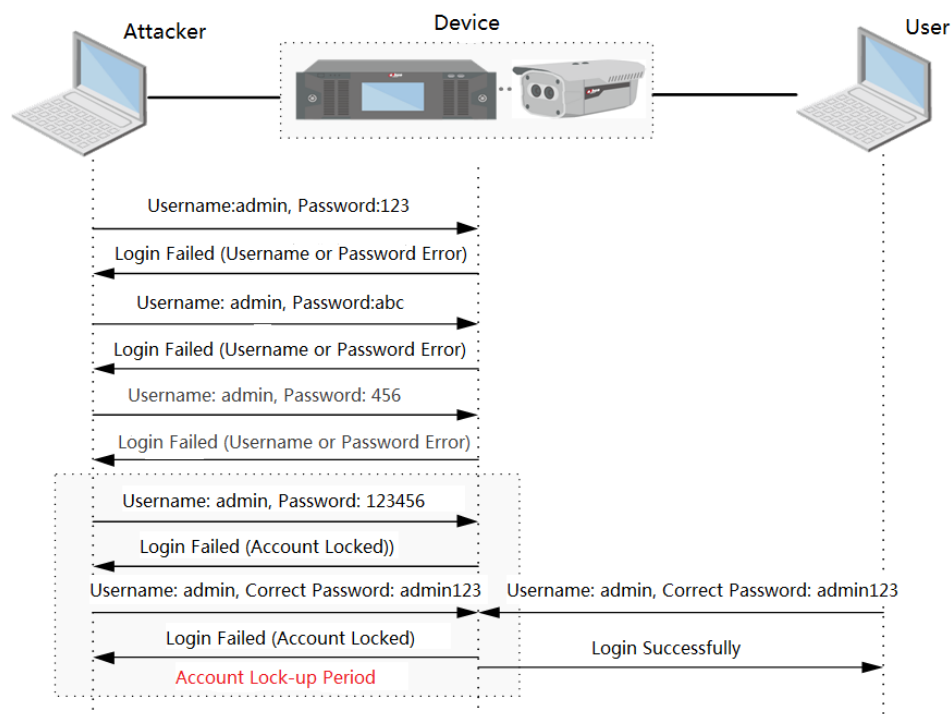


Figure 4-2

In order to prevent the malicious attackers from making use of the account lockup mechanism and launching malicious login requests continuously, causing the normal users unable to use the device, the password explosion-proof technology has built-in host identification ability. The account lockup period is only valid for the host which launches password blasting attacks only, and the normal users can still properly use the device.

4.2.2 Account Authorities Security

The device has a set of flexible and safe authority management system. Users can be divided into two grades called administrators and ordinary users. Each user grade has corresponding authority settings. In the range of the current user grade authority setting, users can be flexibly allocated the minimum authority settings they need.

Device authority management system is based on the Discretionary Access Control (DAC) access control system. The device has integrated the capability sets owned by each account created by the user:

- Each subject (user) owns a username and the username belongs to a group or has a role identity.
- Each object owns an access control list (ACL) which qualifies the access rights of the subjects to it.
- Each time a visit occurs, ACL will check the user's identity to control the user's access to the device. As shown in Figure 4-3.

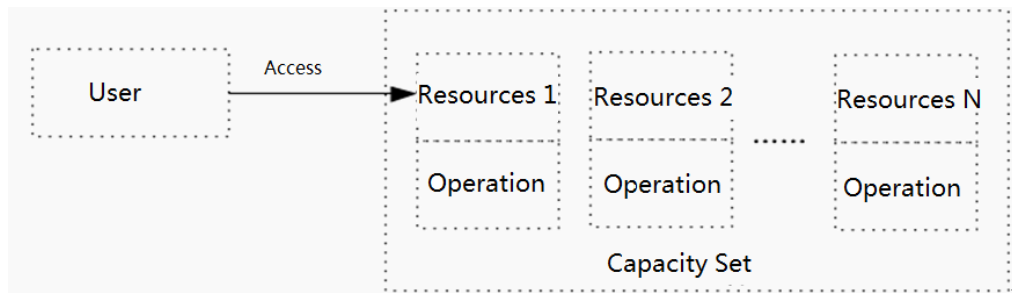


Figure 4-3

4.2.3 Session Security

In the session authentication process, the main security issues come from the expressly transmission of user information. In digest authentication, the digest information of the password is transmitted instead of sending the password directly, and the digest information is irreversible, so as to improve the security of authentication interaction. The digest authentication technology has the following advantages:

- Not transmit password expressly on the network.
- Prevent malicious users from capturing and resending the authentication handshake process.

Digest authentication technology is shown in Figure 4-4.

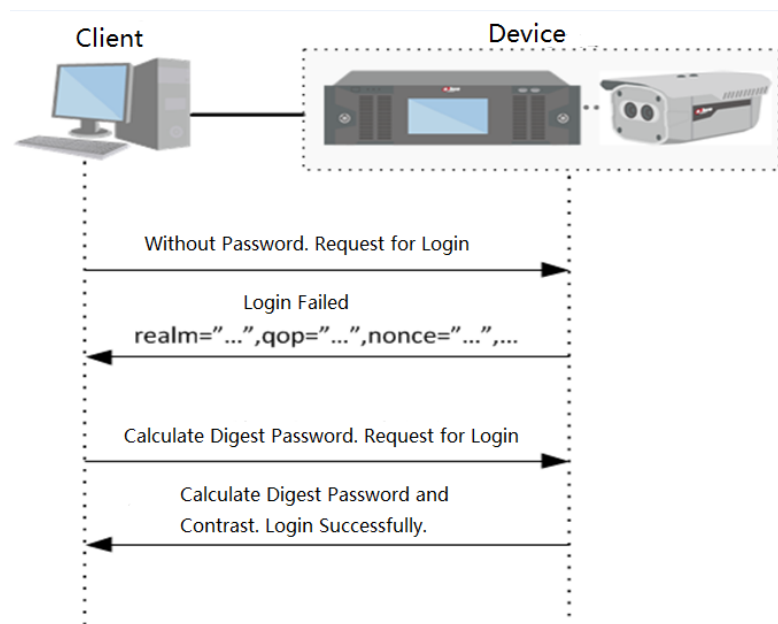


Figure 4-4

The device ensures user session security through multiple authentication and protection processes of the user session.

- Session credentials are random to ensure that external guessing cannot solve it;
- Session credentials are bound to login IP address to avoid being abused by other attackers;
- Enhance the anti-violent cracking mechanism, once detecting violent cracking of user sessions, device can log off threatened sessions to avoid being used by attackers;
- Use user authorities to check session credential to avoid the user of low authorities operating actions of high-level.

4.3 Network Security

4.3.1 Secure Transmission

In the process of network transmission, in order to ensure the data transmitted between IoT device and platform is integrity and confidential, Dahua adopts the standard protocol of secure transmission for network transmission (like TLS).

Security transmission standard protocol needs to use certificates to verify identity, and the device certificate is provided by the manufacturer when it is shipped out of the factory. To solve the user's certificate trust problem, Dahua devices provide certificate import function which supports the users to use their trusted certificates. Meanwhile, it supports the users to upgrade the certificates regularly to apply the certificates more safely.

4.3.2 Security Isolation

Security Device Isolation

IoT data is transmitted via the Internet. Install border security isolation devices at the network exits, and apply isolation policies on the security isolation devices according to the flow source IP address, destination IP address, source port, destination port and application protocol, to achieve the strict control of the flow. Besides, the security isolation devices can realize the hidden purpose of the IP address of the user network.

In addition to the Internet border security, in the different security zones of the IoT local area, the deploying of security devices can realize the isolation of zones with different security grades, to ensure that data is transmitted in strict accordance with the access control strategy.

Data Package Filter

Dahua devices support the data package filter technology. It is to achieve the purpose of controlling package passing or discarding directly on the device. Package filter technology means to check each data package received according to the package filter policy, and make a decision whether to pass or discard the data package.

Data package filter technology is achieved by checking the IP header and TCP header or UDP header. Main information as below:

- IP source address ,IP target address
- Protocol (TCP package, UDP package, ICMP package)
- Source port of TCP or UDP package
- Target port of TCP or UDP package
- ICMP message type
- ACK position of the TCP package header
- Package arrival port
- Package outgoing port

Technical advantages of the package filter technology are as below:

- Filter illegal client objects and allow only legal client objects. It is to reduce the threats to the host.
- Realize specific defensive action when the device is faced with attacks. It is to improve the device ability to cope with risks.

Dahua devices support configuration protocol ports and forwarding ports.

- Change the default HTTP and TCP ports. These two ports can be set to any number between 1025~65535. After changing the default port, it reduces the risk that the attacker will guess which port you are using.
- Enabled IP filter function. Only devices with specified IP addresses can visit the system.
- Only forward the network ports that need to use and avoid forwarding a long port area. Do not set the IP address of the device to demilitarized zone (DMZ).
- Close client (such as SmartPSS) automatic login function and add a defense line to prevent the unauthorized ones from accessing the system.
- If you have manually opened the HTTP and TCP port mapping on the router, we strongly recommend you to close the UPnP function. After the UPnP protocol is enabled, the router will automatically map the internal network port. Although it is convenient for users to use, it will cause the system to automatically forward the data of the corresponding port. In the actual application environments, we strongly recommend you to close this function.
- If you are not using SNMP function, we recommend that you close this function.
- We recommend that you use PoE to connect to IP cameras to NVR, to make it isolated from other networks.

4.3.3 Flow Control

Deploy security device to control flow at the key nodes in the network. Adopting different flow control strategies according to different sources and services; it is to guarantee flows of high priority can be properly transmitted in the environment of poor network quality and smaller bandwidth.

4.3.4 Attack Prevention

There are endless network attacks. Just relying on traffic control and security strategy cannot guarantee the defense against attack. Dahua solution can provide the integrated deployment of professional security device to defense against attacks based on network protocol and system and application security vulnerabilities, such as DDoS attack, abnormal message attack, etc.

4.4 System Security

4.4.1 Cloud Upgrade Service

Dahua cloud upgrade service allows Dahua device to connect to the cloud upgrade system regularly or user manually triggering to check the upgrade version status. Under the condition of user confirming authorization, device can download program package initiatively from the upgrade server through secure connection to complete the upgrade process. It is to complete

device firmware OTA upgrade through the cloud upgrade service.

Dahua cloud upgrade service is on the public cloud, including cloud service interface and cloud data storage. According to their own needs, enterprises can choose the upgrade way of connecting to the public cloud on the network, or customizing Dahua cloud upgrade service on their enterprise intranet to build the local upgrade service.

Through the cloud upgrade service:

- Unified terminal device upgrade solutions, improve the efficiency of Dahua product program upgrade.
- Timely push solutions to repair security threats, to provide quick and timely solving channels for the possible security risks.

Cloud Upgrade Procedure is shown in Figure 4-5.

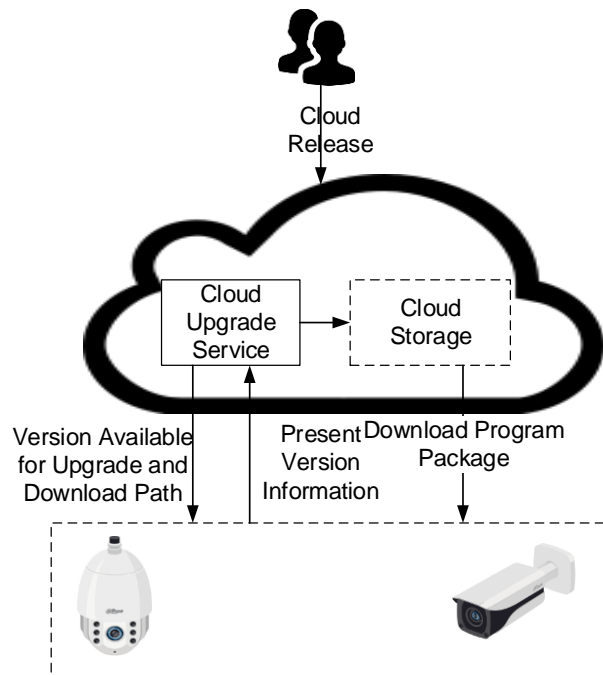


Figure 4-5

4.4.2 Firmware Upgrade Security

The terminal device has the firmware security upgrade capability, which is used to verify the firmware for upgrade, and identify the firmware packages not from Dahua or been illegally tampered with. During the upgrade process of Dahua terminal device, there will be security check for the loaded firmware packages (legality and integrity check). Only the security firmware packages officially released by Dahua are allowed to be used for upgrade. It is to ensure that the firmware package for upgrade is safe and effective.

Trust upgrade technology is to prevent the firmware from being maliciously tampered with and the user's device being upgraded. Using the signature ability of asymmetric algorithm, factory device has integrated a public key file provided by the manufacturer. The corresponding private key is only owned and kept by Dahua, and the signature technology of private key is applied on the release of the firmware package. The packing procedure of trusted firmware is shown in Figure 4-6.

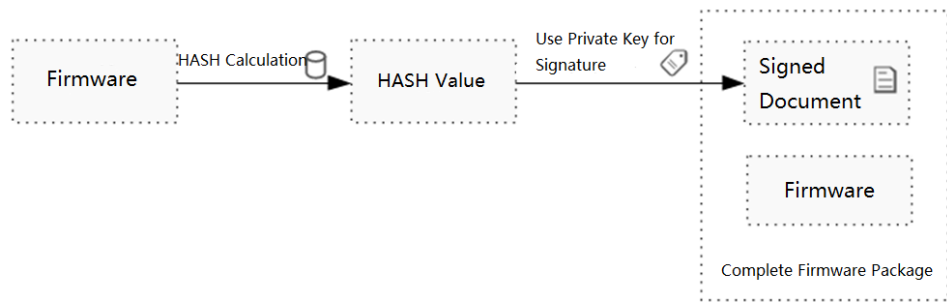


Figure 4-6

Dahua uses this private key to sign the firmware package completely, and then releases the private key together with the firmware package. When the device upgrades the firmware package, it will use the public key file in the integrate device for signature and verification. Only the firmware packages passed testing can be written really to the device flash. Firmware credibility verification procedure is shown in the Figure 4-7

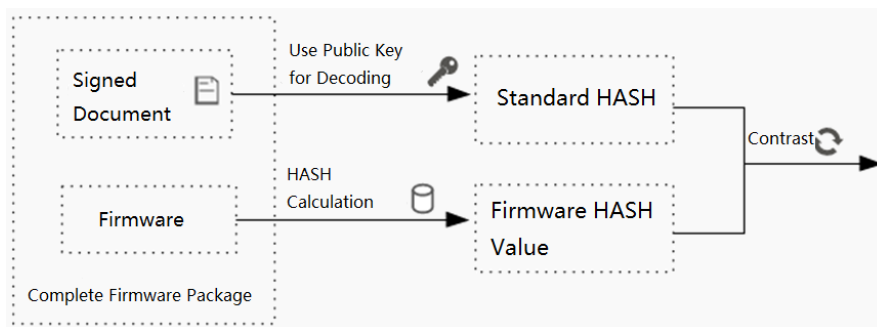


Figure 4-7

4.4.3 Secure Operating Environment

Terminal device realizes the end-to-end trusted system. By building “trust chain”, it guarantees the security of the device operating environment. From the bottom to the up, authentication is applied for each layer, which guarantees the call of each layer is safe and reliable, thus to ensure the whole operating environment is safe and reliable. It further strengthens the system layer safety, guarantees the device does not run illegal procedure, and reduces the risk of being attacked. The safe operating environment diagram is shown in Figure 4-8.

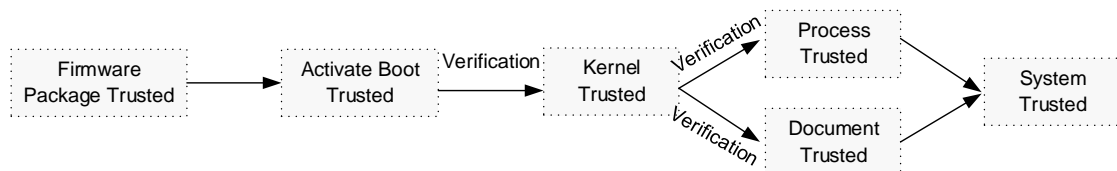


Figure 4-8

Dahua device has the ability to control the running of virus and malicious programs. Even if the device is implanted into a virus or malicious program, the virus or malicious program will be identified and blocked when they are trying to running, thus to deny the operation of such programs, and prevent virus and malware effectively.

The control technology of non-authorized program is achieved through the signature technology.

- Add program signing to legal and executable programs.
- During the program startup period, the operating system kernel will check and approve the program and its signature.

If the kernel finds that the program is not trusted, it terminates the program and thus achieves the capability of anti-virus / malicious program.

4.4.4 Network Service Strategy

The device closes some default service to reduce the device threat risk:

- Close Telnet debugging service by default.
- Close SSH debugging service by default.
- Close SNMP service by default.

The device supports more secure services. We strongly recommend that you set up HTTPS/SFTP as the default service and replace some insecure web services:

- HTTPS access function, replaces HTTP service.
- SFTP service, replaces FTP service.

The device provides port configuration capability to the already supported services, and users can configure ports freely to achieve the purpose of hiding ports.

4.4.5 Log Audit

The terminal device has a perfect log management system to record every important or critical operation.

The log management system classifies log according to its importance. The importance level of security logs is especially high, and any other grades of log will not be able to cover the security level logs, to ensure the memory of device security events.

The following operations (including but not limited to) have the log files.

- User login and logout.
- Add, delete and modify user account and password.
- Import and export system configuration.
- Modify critical configuration of the system (including alarming, video configuration, etc.)
- Upload files.
- Restart and upgrade the device.
- Modify system time.
- Abnormal handling (abnormal events including network offline, no hard disk, hard disk error, hard disk capacity low or video loss, etc.)
- Illegal security operation (like account locking, session explosion, etc.)

Each log includes below key contents:

- Operating source, including user and source IP.
- Operating contents.
- Operating time.

The device is equipped with network log backup capability, which can enable the network logging function, and save important logs synchronously to the log server.

4.5 Security Lifecycle Management

Based on the product collaborative development procedure, and taking the safety and reliability of the product and solution on the client side as the core target, Dahua security development lifecycle (SDLC) management system is established. It takes the security problem of Dahua products as a normal state to manage. Lead Dahua R&D process system with a combination of historical practice and current situation of ability, and accumulate safety technical ability, to form Dahua's own safety standards and regulations, safety technology capacity library and collection of safety tools. It is to support SDLC process better and respond to security incidents actively. Dahua security management system is shown in Figure 4-9.

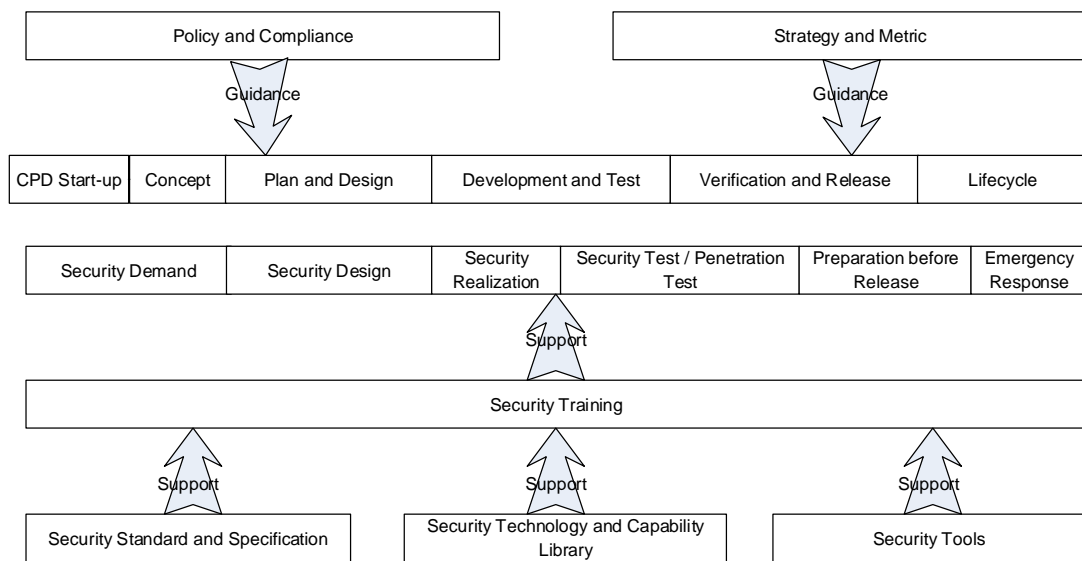


Figure 4-9

4.5.1 Secure Development Lifecycle Management

4.5.1.1 Security Training

At each stage of the product development process, Dahua security engineers will carry out training for the developers on secure development specification and security awareness, and so on. It is to improve the security awareness of the developers and build the secure development ability for the whole staff.

4.5.1.2 Security Needs

On the basis of the current existing security baseline, Dahua constantly improves the ability baseline of security and privacy protection. At the front end of product design and development, Dahua begins to analyze security needs and privacy protection according to business functions, business procedure and system structure, assess the product security risks and form analysis files of security needs.

4.5.1.3 Security Design

Under the premise that the security demand analysis is completed, security designers make security design and improve the analysis of product attack surface, to realize security threat modeling and form security demand design files, which are used to guide the implementation and tests of detailed security demands.

4.5.1.4 Security Implementation

In the product software development processes, the security implementation process meets the safety standards and specifications, including but not limited to the disabling of safety hazard functions, opening source libraries and the management, code scanning and code inspection of third-party software.

4.5.1.5 Security Test / Penetration Test

After the software development is completed, it must be tested by the Dahua professional testing team on the security (including but not limited to the Fuzzing test, attack surface re-inspection and dynamic analysis) and penetration. The vulnerabilities and device problems found in testing shall be repaired before product release.

4.5.1.6 Preparation before Release

Dahua products (including software and hardware) must go through security review before release, develop security response plan, and release operation guidance document and secure operation manual.

4.5.1.7 Security Emergency Response

During the usage, IoT devices may encounter different security threats and vulnerability risks. The security emergency response system built by Dahua monitors the network security situation at real time, gives first-time response to security vulnerabilities and risks, carries out emergency response plan and implements vulnerability repair and management.

Dahua is an important member of CNAs (CVE Numbering Authorities) which is a member organization of MITRE. This organization will promptly notify the related members actively when it finds security vulnerabilities, so Dahua can immediately get the security vulnerabilities found by external organizations and do the repair. On the other hand, after finding the security vulnerability, Dahua will maintain the corresponding CVE (Common Vulnerability & Exposures) number and disclose it promptly to customers and the public. The ways for Dahua to find vulnerabilities includes but not limited to being found by company security researchers, submitted by external moral hackers and reported by external security organizations (like CNVD, ZDI, etc.).

Dahua specially sets up an emergency response center. Professional security observers obtain security warnings from security organizations, vulnerability sharing platforms and personal

white hats and reports the security events to network security implementation team. The security test personnel will analyze and classify the events, issue comprehensive solutions, and publish the handling results and solutions to the public. Collect vulnerability and compile corresponding test case to ensure that this vulnerability will not appear in the later versions of the program.



Note

Customers who have encountered security-related issues or need consulting during the use of Dahua devices can send email to cycersecurity@dahuatech.com for help.

4.5.2 Supporting System

In the practice of SDLC process, Dahua establishes and constantly improves the security standards and specifications, builds security technology and capability library, and introduces or develops security tools to support the ever-changing security threats.

- Security standard and specification: form complete security standards and specifications to guide the safety demand analysis, design, implementation and test.
- Security technology and capability library: provide public support for the security capabilities of Dahua products.
- Security tools: Dahua provides security capability test tools through self-research and introduction, which greatly improves the efficiency of security capability detection.

Dahua specially sets up a network security product line, which is committed to building security standards and specifications, developing security capability public library and test tools, providing vulnerability detection and security test for program release, monitoring security vulnerability publishing, giving network security emergency response, and providing customers with safety solutions in a timely manner.

5.1 Security System

Dahua establishes security management system based on ISO27001:2013 to ensure that the safety management of products / solutions is policy compliance. The company has passed ISO27001 information security management system whose safety standards are widely used in the world. It adopts the method focused on risk management to guarantee the confidentiality, integrity and availability of the company and customer information, and ensures the continuous running of the system through regular evaluation of risks and control measures.

5.2 Policy Compliance

Dahua improves its own management and mechanism according to national laws, industry standards and industry best practices. It passed a series of standard authentication, third-party audit and internal security assessment, striving to meet the compliance requirements multi-dimensionally.

According to the different compliance requirements of different perspectives, different industries and different regions, the compliance at Dahua can be divided into:

- Management System Compliance
 - ◇ The company's mature security management mechanism and compliance to industry best practices;
 - ◇ ISO27001: Information Security Management System;
 - ◇ BSIMM: Building Security in Maturity Model.
- Legal Compliance
 - ◇ Conform to the Law of the People's Republic of China on Network Safety, Some Views of China on Strengthening the Construction and Networked Application of Public Safety Video Monitoring, Guidelines of China on the Construction of Public Security Video Transmission Network (Draft), and other laws and regulations.
 - ◇ To operate in different areas, it is necessary to meet the local laws and regulations. Dahua has a professional legal team to evaluate the laws and industrial regulations of the corresponding areas to ensure the legal compliance of the products and solutions.
- Industry Standards

Conform to the relevant national standards in the industry, actively participate in the formulation of industry standards, and track the progress of standard updates. Comply with the China Basic Requirements of Network Information Security Level Protection 2.0, China Information Security Requirements of Public Security Video Monitoring Network, and Guiding Opinions of China on the Construction of Public Security Video Transmission Network.

5.3 Privacy Policy

Dahua has formulated a strict privacy protection policy. It uses user authorization principle and minimum authority principle to collect and transmit individual and private data. This operation must provide clear personal data and privacy statement and get authorization in advance. The data owner has the right to revoke the authorization at any time.

The privacy policy defines the scope, purpose, storage and confidential policies of products and platforms for personal data collection. Data collected is used only to provide services to users and will not be provided, sold, rent, shared or traded with any third party. At the same time, Dahua uses various technical means to ensure that the customer's personal information exists only in Dahua's business scope.



Note:

The privacy policy of Dahua is completely transparent to the public, which can be referred to at Dahua's official website. Dahua privacy policy's official website: <http://www.dahuasecurity.com>.

6

Conclusions

Billions of device terminals connected to the Internet of Things have brought a huge challenge to the IoT security. Different industries have different security demands. The network security threats are increasingly updating and continuously changing. Any static security solution cannot solve network security threats perfectly. The nodes of the IoT are linked to each other closely. Adhering to the attitude and way of development cooperation, Dahua cooperates with the security enterprises, state organs and units in and across the industry, devotes itself to the development of security technologies, and actively introduces newer and stronger security solutions, so as to strengthen the end-to-end security of IoT.

- Each solution goes through a systematic analysis of the security requirements and design review.
- Each type of product goes through strict security test and penetration test.
- Each line of code goes through the review of professional tools and security experts.

We are open to every security issue and working with industry security experts to establish systematic emergency response systems.

Dahua makes the world a safer place.

【 SOCIAL SECURITY IS OUR RESPONSIBILITY 】

 **DAHUA TECHNOLOGY CO., LTD.**

Add: No. 1199 Bin'an Road, Binjiang District, Hangzhou, China.

Post Code: 310053

Website: www.dahuasecurity.com