Huawei Atlas 500

Security Technical White Paper

Issue	02
Date	2019-07-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

About This Document

Purpose

This document describes the security technologies supported by the Huawei Atlas 500 AI edge station (Atlas 500 for short).

Intended Audience

This document is intended for:

- Huawei presales engineers
- Channel partner presales engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
📖 NOTE	Calls attention to important information, best practices, and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
02	2019-07-27	This issue is the second official release.
01	2019-06-10	This issue is the first official release.

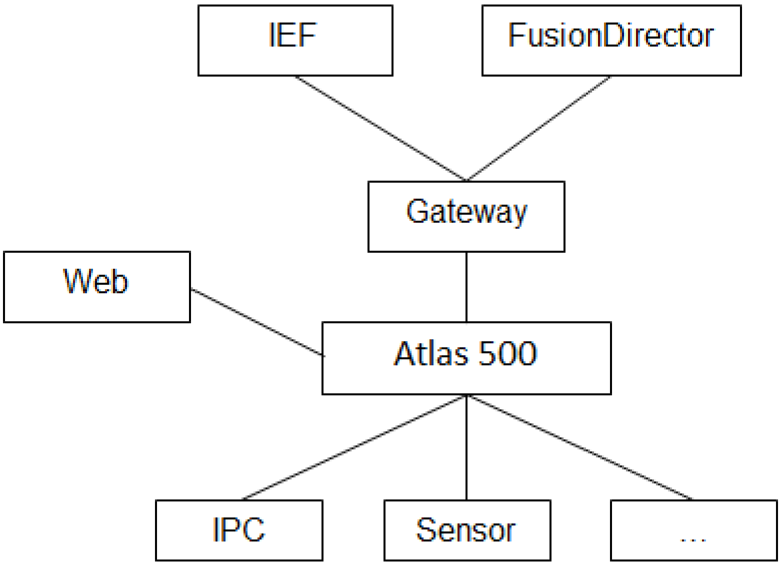
Contents

1 Introduction

The Atlas 500 is intended for intelligent video and image analysis in edge scenarios. It also provides general computing capabilities, storage capabilities, and flexible network access capabilities. The application domain covers various industries, such as transportation, electric power, security protection, and industrial manufacturing. It can be deployed in complex environments such as street cabinets, shopping malls, supermarkets, and police stations.

The Atlas 500 can be connected to cloud servers to implement cloud-edge collaboration. For example, an image is downloaded from the cloud for automatic deployment, and the processed result is uploaded to the cloud for storage.

Figure 1-1 Atlas 500 network topology



The Atlas 500 faces two types of security threats in edge application scenarios:

- Security threats to the service software system. The service software system includes software installed by users. The security of the service software system depends on the software provided by users, such as host processes and container services. The security threats affect the service software and the entire system.
- Security threats to the management software system. The management software system supports hardware management and system management. The security of the

management software system depends on the firmware of the Atlas 500. The security threats affect the normal running of the system and the system reliability.

This document describes the security of the management software system, that is, the security of the operation and management interfaces provided by the Atlas 500 system and the firmware security. The security of third-party service software is not involved.

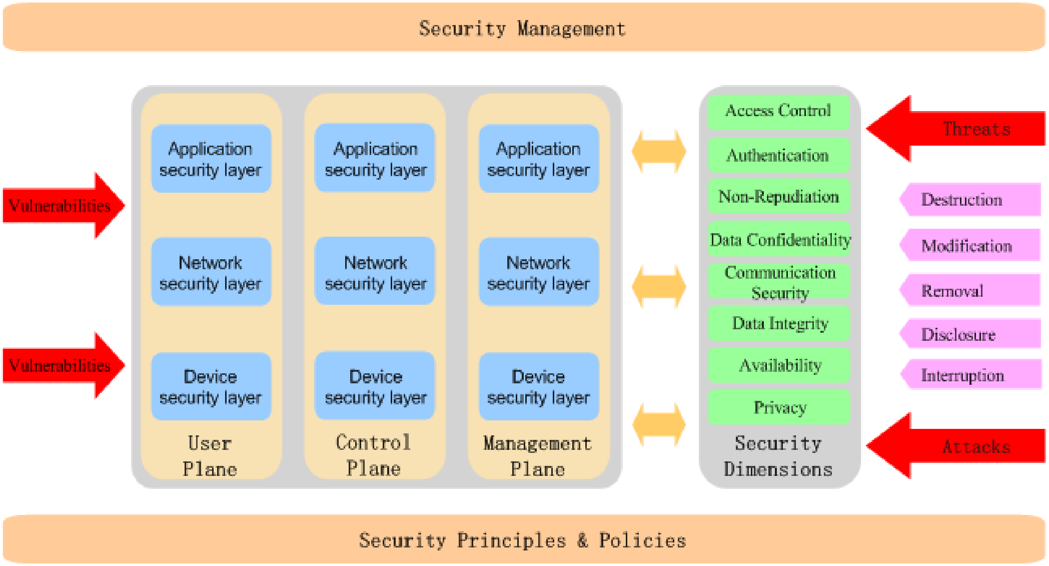
The Atlas 500 management software system faces the following security risks:

- External attackers exploit system vulnerabilities or bugs to obtain administrative and control rights and perform unauthorized operations.
- External attackers steal administrator accounts and access the system to steal private data such as videos and images stored by users.
- Internal unauthorized users exploit system vulnerabilities to obtain higher control rights, and perform unauthorized operations.
- Third-party software installed by users performs unauthorized operations to obtain key resources that are unnecessary for running services.

2 Security Architecture

The Atlas 500 uses a three-layer and three-plane end-to-end security architecture model. This architecture analyzes security threats and attacks on each layer and each plane and provides technical protection measures. Subsequent chapters in this document further analyze the technical protection measures. The following figure shows the security architecture of the Atlas 500.

Figure 2-1 Atlas 500 security architecture



3 Security Design

3.1 Account Security

The Atlas 500 supports management interfaces such as Web, Redfish, and WebSocket interfaces, and provides unified user management. The Atlas 500 supports only one external login user and the user cannot be deleted. Adding users is not allowed.

The account security measures include password complexity check, password validity period, and anti-brute force cracking.

- **Password complexity check**: The system verifies the password complexity to prevent simple passwords. The password must meet the following requirements:
  - Contains at least eight characters.
  - Contains at least three types of the following characters: lowercase letters (a to z), uppercase letters (A to Z), digits (0 to 9), and special characters.
  - Cannot be the same as the username or the username in reverse order.

  - Must be different from five recently used passwords.
  - Cannot contain character strings in the weak password dictionary.
- **Password validity period**: The system checks the password validity period (the default validity period is 30 days). The user will be prompted to change the password 10 days before the password expires. If the password has expired, the user needs to change the password before logging in to the system.
- **Anti-brute force cracking**: The account will be locked after consecutive login failures.
  - When the number of login failures caused by incorrect passwords reaches the specified limit (5 times by default), the account will be locked. After an account is locked, the account cannot log in to the system until the system automatically unlocks the account (the default lockout duration is 300 seconds).

3.2 Authentication Management

The user needs to be authenticated before logging in to the system through the Web or CLI interfaces. The authentication method is username+password. The user can configure devices and query information only after being authenticated.

3.3 Certificate Management

SSL certificates are used to establish Web HTTPS connections and verify the identity of websites.

Certificate management refers to various management operations on SSL certificates, including viewing the current certificate information (such as the user, issuer, validity period, and serial number), generating certificate signing request (CSR) files, importing signed certificates generated by the CSR files, and importing custom certificates. The certificate format can only be X.509.

The Atlas 500 uses self-signed SSL certificates by default. The certificate signature algorithm is SHA256 RSA (2048 bits). For security purpose, customers can import their own certificates to replace the default user-defined certificates in the system. The Atlas 500 supports two methods for replacing self-signed certificates:

- **Using a Certificate Generated by the Atlas 500**

  a. Log in to the WebUI of the Atlas 500 and modify the certificate user information.

  b. Generate a CSR file.

  c. Export the CSR file.

  d. Submit the CSR file to the certificate authority (CA).

  e. The CA generates a signed certificate in CER, CRT, or PEM format.

  f. Import the signed certificate.

  NOTE

  The signed certificate must match the CSR. Otherwise, certificate import will fail.

  g. Restart the system for the new certificate to take effect.

- **Using a Certificate Provided by the User**

  a. Customize a certificate or purchase a certificate from a CA.

  b. Log in to the Atlas 500 WebUI and import the certificate to the Atlas 500.

c. Restart the system for the new certificate to take effect.

3.4 Session Management

- **Generating a Session**

  Session IDs are generated by using secure random numbers. One user can create only one session at the same time.

- **Destroying a Session**

  A session can be terminated in either of the following ways:

  - Termination upon timeout: If a persistent connection session, such as a Web or SSH session, is inactive for a specified timeout period, the session is automatically disconnected.
  - Manual termination: A user initiates a request to terminate a session. The administrator can terminate other sessions.

3.5 Security Protocols

By default, SSH and HTTPS are used to access the EMM. The transmission channels are encrypted by using security protocols. HTTP is insecure and is disabled by default.

The secure transmission protocols provide the following features:

- SSH
  - Supports user password authentication.
  - Supports SSHv2.
- HTTPS
  - TLS 1.2 is enabled by default.
  - Supports the AES_128_CBC_SHA256 and AES_256_CBC_SHA256 secure encryption algorithms.

3.6 Data Protection

All sensitive data related to the Atlas 500, such as the passwords and keys, is encrypted to prevent disclosure.

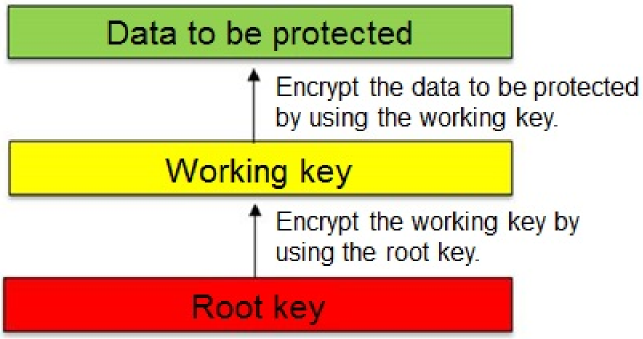
The Atlas 500 supports encryption and signature protection for upgrade packages to prevent the content of upgrade packages from being cracked or tampered with and ensure the confidentiality and integrity of the upgrade packages.

The Atlas 500 also encapsulates the Linux shell. Users cannot directly access files in the file system after logging in over SSH. This mechanism prevents file damage and information leakage.

The Atlas 500 supports backup of key data files and calculation and storage of file checksums. It also provides a backup and restoration mechanism for file verification failures to prevent data file damage caused by abnormal system power-off and ensure the availability and integrity of data files.

3.7 Key Management

The Atlas 500 key management involves root keys and working keys. The root key is used to encrypt the working key, and the working key is used to encrypt the data to be protected. The following figure shows the key mechanism.


Data to be protected
Encrypt the data to be protected by using the working key.
Working key
Encrypt the working key by using the root key.
Root key

- Key generation: The root key is generated by using a secure random number. The working key is generated by using a secure random number.
- Key usage: Each key is used for only one purpose.
- Key storage: The root key is divided into multiple components for permission control. The working key is encrypted by using the root key.
- Key update: The keys can be manually updated. After the command for updating the key is run, the system generates a new key randomly and the old key is destroyed.

3.8 System Hardening

The Atlas 500 adopts minimum installation, which allows only the minimum required components to be installed on the embedded Linux system. All components and commands that are not used are deleted.

For security purposes, the Linux shell command line is encapsulated so that only the whitelist commands can be run.

Security hardening has been performed on the SSH and RESTful servers in the system. Only secure algorithms are used. Insecure protocols and ports are disabled by default.

3.9 Secure Boot

Principles of Secure Boot

Secure Boot uses the digital signature technology check the system code integrity during system startup process. The upper level program uses both hash verification and digital signature to check the code integrity of the lower level program. If the code of the lower level program fails to pass the digital signature integrity verification, the system cannot be started. This mechanism ensures that the lower level code has not been tampered with.

Atlas 500 Secure Boot Solution

Digital signatures are generated for released firmware. The trusted root is burnt in the CPU One Time Programmable (OTP) memory. Signature verification is performed on the firmware during the system startup process. Only firmware that passes the verification is loaded and started. This mechanism ensures that the code used in the startup process has not been tampered with.

3.10 Log Audit

The Atlas 500 supports log audit. The log information includes the username, user IP address, time when the operation was performed, and the specific operation performed.

The Atlas 500 logs are stored in the flash file system. When the size of a log file reaches a specified limit, the system automatically backs up the log file.

3.11 Resource Isolation

The Atlas 500 allows users to set resource limits for each deployed container service, such as CPU resource limit and memory resource limit.

The Atlas 500 allows users to import data to a container by mounting a volume. The container exclusively uses the content of the volume.

3.12 Permission Control

Common accounts that are not used for login are created in the Atlas 500 system. These accounts are used to run containers. The container software installed by users has only the permissions of common users. This mechanism prevents abnormal activities of container software from damaging the system security.

4 Security Technology Development Trends

With the development of edge computing applications, Huawei is improving its edge security technologies to meet customers' rising demand on security. The improvement directions are as follows:

- Perform security hardening for third-party software package installation activities. For example, check whether the installation package contains malicious code.
- Enhance the isolation between containers to ensure service independence and data security.
- Check the entire software startup process to ensure trusted booting.

A Appendix

A.1 Conclusions

Huawei is devoted to providing best products and services in the industry to meet customer requirements. To achieve this goal, Huawei inputs many resources to help itself, other companies in the industry, and other parties to improve their capability and to ensure the network security.

Huawei has established an independent cyber security lab and security test team to perform cyber security tests on products. In addition, Huawei actively participates in the formulation of security standards in international telecommunication standards organizations such as ITU-T, 3GPP, and IETF, joins security organizations such as Forum of Incident Response and Security Teams (FIRST), and cooperates closely with mainstream security service vendors. Huawei works to build a healthy industry and ensure the cyber security of global customers.

Huawei has established the Product Security Incident Response Team (PSIRT) to monitor and handle product security vulnerabilities. Huawei looks forward to working with security researchers, industry organizations, government institutions, and suppliers to discover potential security vulnerabilities or security issues of Huawei products.

Huawei PSIRT email: **mailto:PSIRT@huawei.com**

Note:

1. Huawei has released a global cyber security white paper, *Cyber Security Perspectives: 21st century technology and security － a difficult marriage*. This white paper is released by Huawei Global Cyber Security Officer John Suffolk. For details about the document, see the following link: **https://www.huawei.com/ucmf/groups/public/documents/attachments/hw_187368.pdf**.
2. For details about Huawei PSIRT, visit the following website: **https://www.huawei.com/en/psirt/about-huawei-psirt**

A.2 Acronyms and Abbreviations

C

CA	Certificate Authority
CSR	Certificate Signing Request
I	
IoT	Internet of Things
O	
OTP	One Time Programmable
S	
SSH	Secure Shell