Huawei Atlas 200

Security Technical White Paper

Issue	01
Date	2019-07-27

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 Atlas 200 AI accelerator module (Atlas 200 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
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
	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
01	2019-07-27	The issue is the first official release.

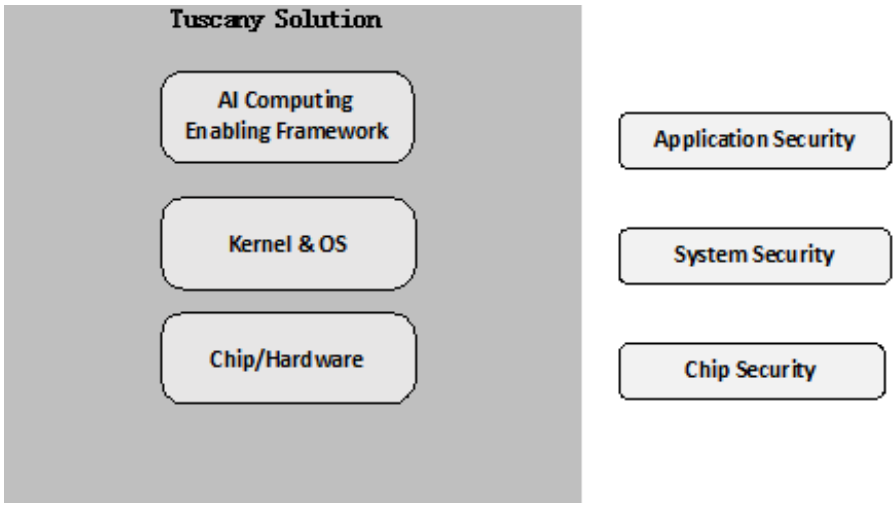
Contents

1 Introduction

Huawei Atlas 200 AI accelerator module is a high-performance AI computing module. It has a built-in Ascend 310 chip and builds powerful neural network computing capabilities based on the Tuscany solution.

The Tuscany solution is an AI computing platform designed for AI application development, including computing resources, running frameworks, and related tools. This platform enables developers to easily and efficiently write AI applications that run on the Ascend 310. The Tuscany solution is an important support for AI application devices and is dedicated to building a secure and reliable AI computing platform for AI application products. The major security problems and threats are as follows:

- Chip security: chip software cracking and malicious attacks.
- System security: SOC OS vulnerabilities, security policy configuration, and open-source software vulnerabilities.
- Application security: development program being tampered with, AI model disclosure, and malicious attacks on AI application programs



2 Chip Security

The Tuscany solution provides the following mechanisms for chip-level security protection.

2.1 Commissioning Port Protection

- JTAG port protection: To prevent unauthorized users from using the JTAG port to trace and debug chip instructions, the chip provides the eFuse control port, which allows locking the JTAG port and enabling the authentication mechanism after eFuse is blown.
- UART port protection: The UART port is disabled by default.
- USB port protection: The USB port is disabled by default.

2.2 Security Update

During the security upgrade of the chip, the upgrade package signature is verified first. Only upgrade packages that pass the signature verification can be used for the upgrade. This mechanism ensures the integrity, and validity of the upgrade. The secure upgrade function ensures that no unauthorized software is installed on the device.

2.3 Secure Storage

The eFuse medium supports parameters that do not need to be changed. Once the parameters are burnt, the parameters cannot be modified.

3 System Security

The Tuscany chip OS is developed by Huawei based on the open-source Linux OS. The security issues include the OS security and security policy. In the Tuscany solution, all vulnerability warnings of the open-source OS are intimately followed so that the vulnerabilities are repaired in a timely manner. The OS security policy ensures that the system rights are allocated in a reasonable manner, unnecessary services and protocol ports are disabled, and system accounts are under proper control.

3.1 System Security

The mirror signature verification mechanism protects the integrity of the device system and prevents the system against unauthorized modification.

3.2 System Security Policy

The system ports and services are reviewed during the solution development process to ensure that services or ports not required for production are disabled. The device security function is not disabled.

3.3 System Configuration and Rights

Important system parameters and rights are managed in a unified manner and are properly configured to prevent security vulnerabilities caused by improper configuration.

3.4 System Log Management

The solution provides a log management system. You can flexibly control device logs, set log levels, and monitor device management activities. In addition, logs can be periodically reviewed.

3.5 Open-Source and Third-Party Code Security

Open-source and third-party code involved in the system are selected and evaluated from the security perspective, and security check and vulnerability fixing are performed periodically.

3.6 Code Scanning

Fortify-C, Fortify-JAVA, Coverity, Cppcheck, Warncheck, Pclint, Codemars, and CSECCheck are used to check the code and fix detected problems everyday. Before the code is officially released, mainstream antivirus software such as Symantec, Trend OfficeScan, McAfee, Avira AntiVir, and Kaspersky are used to scan the code to ensure that the software package is not infected or embedded with viruses or Trojan horses.

4 Service Application Security

The Tuscany solution supports multiple security mechanisms including security algorithms, security communication, and security authentication to prevent data breach, unauthorized access, and data damage and ensure application security.

4.1 Security Algorithm

International standards and common security algorithms such as AES, RSA, ECC, and DSA are used. Insecure algorithms are upgraded or replaced in a timely manner. Management for keys, certificates, and authorization must follow strict processes. Based on product requirements, the chip supports the embedded encryption engine to improve the performance and security of encryption and decryption.

4.2 Secure Data Storage and Access

The chip supports secure storage areas for storing important data. The encryption and signature mechanisms ensure that confidential data items can be accessed only by specific hardware or modules. In addition, secure storage areas cannot be changed, preventing storage data cracking, forgery, and embezzlement.

4.3 Model Protection

The Tuscany solution provides the signature and encryption mechanisms for network model files of AI applications. Decryption and verification are performed in the memory when the system is running to protect the network models during storage and transmission.

4.4 Authentication and Session Control

The AI application development environment supports authentication and session control to ensure development security.

- The system provides the authentication (login) and logout functions.
- The system uses usernames and passwords to authenticate clients.
- The final user authentication process is performed on the server rather than on the client.
- The authentication module checks the validity of the submitted parameters.
- Unauthenticated users are forbidden to perform any operations.
- No service logic can bypass authentication.
- If authentication fails, only a general message is displayed. The detailed failure cause is not provided.
- The system manages user login and authentication based on sessions.
- Consecutive login failures will cause the account to be locked.
- After a user account is locked, the system automatically unlocks the account after a period of time.
- The session timeout mechanism clears the session information after a session times out.

4.5 Secure Communication

The AI application development environment supports cross-host inter-component encryption channels.

- HTTPS is used for logging in to the development environment.
- TLS is used for cross-host inter-component communication.

4.6 Minimum Authorization

Unless system resources are required, all programs involved in the solution are run by common users of the OS. Only authorized users can access the system files.

5 Security Planes

The Tuscany solution provides only an AI computing platform. The production environment does not provide external network interfaces. Therefore, the separation of the management plane, control plane, and user plane is not involved.

5.1 Management Security Plane

The Tuscany solution provides only a part of the management APIs and log files for the product management program, and does not provide external network management interfaces.

5.2 Control Security Plane

Tuscany supports network interconnection with the MindSpore Studio development environment. Generally, the development environment is a closed network environment and the entire system belongs to the same trust domain.

The production environment does not need to connect to MindSpore Studio. All external network service interfaces (IDE-daemon-host monitoring ports) of Tuscany can be disabled. For details about how to disable the interfaces, see the *Communication Matrix*.

5.3 User Security Plane

Tuscany provides only APIs for product AI applications and does not provide external interfaces for processing service data.

A Appendix

A.1 Conclusions

Huawei is devoted to providing best products and services in the industry to meet customer requirements. We attach great importance to cyber security and provide security assurance for products.

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

A

AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
C	
CA	Conditional Access
D	
DSA	Digital Signature Algorithm
O	
OS	Operating System
R	
RSA	RSA Algorithm

