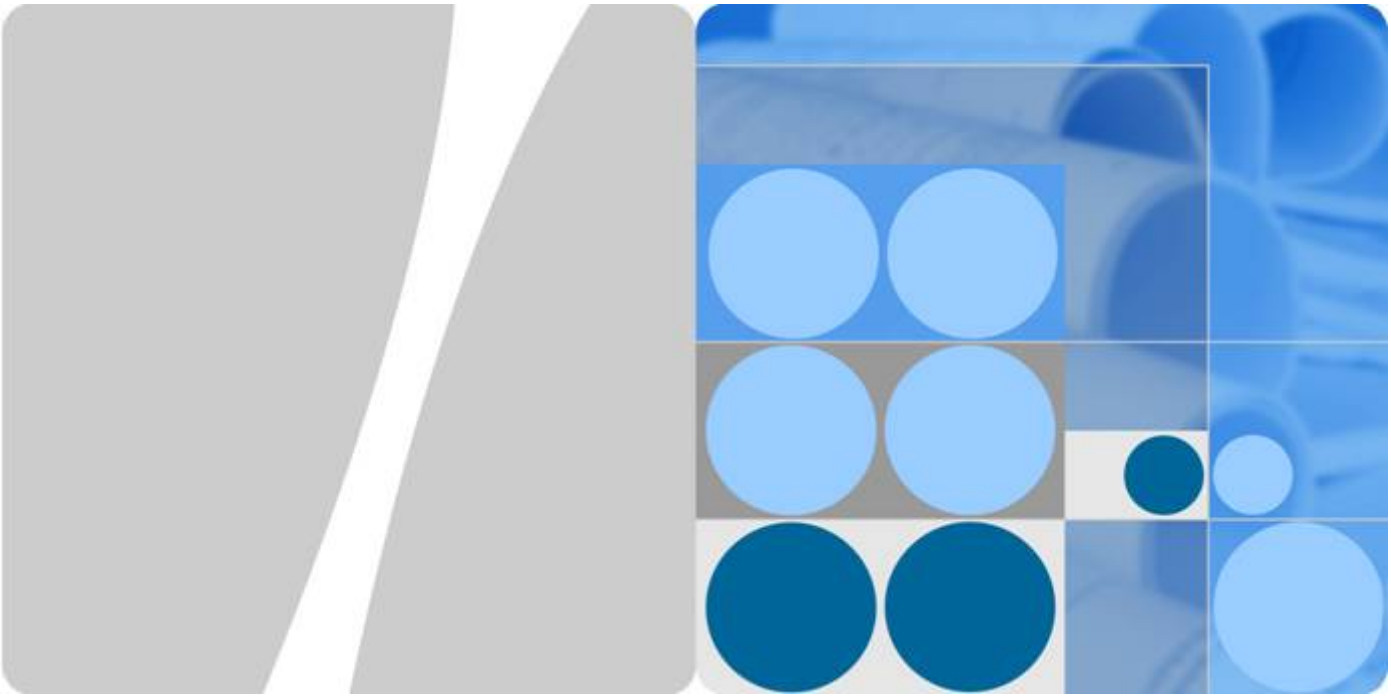


Ascend310

V100R001

安全技术白皮书

文档版本　01

发布日期　2019-03-12

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

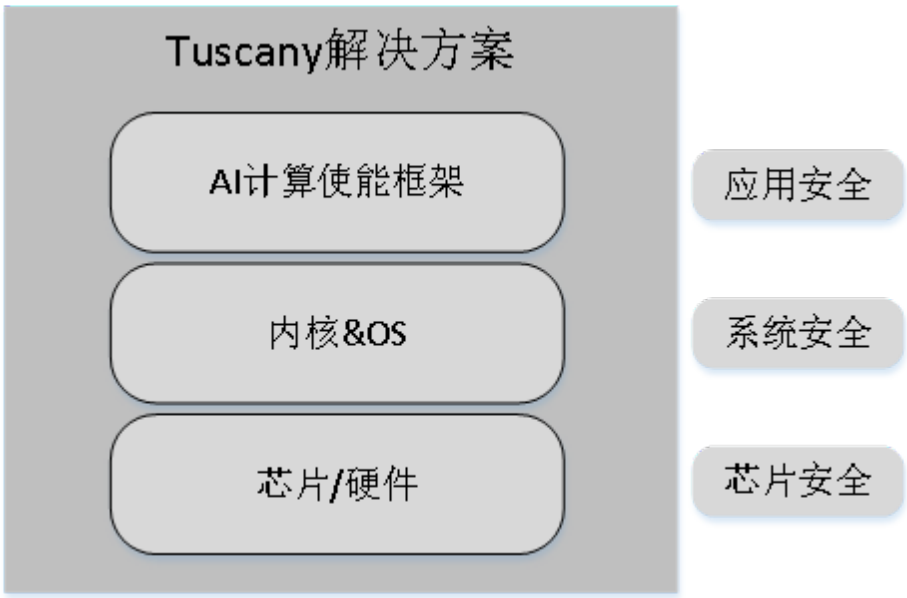
客户服务电话： 4008302118

目 录

1 概述

Tuscany解决方案是面向AI应用开发提供的AI计算平台，包含计算资源、运行框架以及相关配套工具等，让开发者可以便捷高效的编写在Acsend硬件设备上运行的人工智能应用程序。Tuscany解决方案是AI应用设备的重要支撑部分，将努力为各AI应用产品打造安全的和可靠的AI计算平台。我们面临的主要安全问题和威胁分类如下：

- **芯片安全**：针对芯片的软件破解，恶意攻击等；
- **系统安全**：SOC操作系统的漏洞、安全策略配置、开源软件漏洞等；
- **应用安全**：开发程序被篡改、AI模型泄露、AI应用程序被恶意攻击等；



2 芯片安全

2.1 调试接口保护

- JTAG端口保护：为了防止非法通过JTAG端口对芯片运行指令的跟踪和调试，芯片提供eFuse控制接口，提供熔断eFuse后对JTAG端口进行闭锁和鉴权认证的机制。
- UART端口保护：正式发布版本上，UART端口默认禁止使能。
- USB端口保护：正式发布版本上，USB端口默认禁止使能。

2.2 安全启动

提供一个片上ROM，固化码字作为整体安全方案的首个环节，为后续安全启动、安全升级提供支持。

所有芯片启动映像文件（如bootloader、kernel、system等映像）的生成，使用签名保护。

从Onchiprom中启动，烧录以及启动每一段镜像文件都需要通过安全认证，认证不通过的镜像不被加载和执行。

2.3 安全升级

芯片的安全升级也是基于安全启动，只是升级过程中首先对升级包进行签名校验，只有签名校验通过的升级包才可进行升级，保证了升级的合法性、完整性和有效性。安全升级功能保证设备不被刷入未经授权的非法软件版本。

2.4 安全存储

针对一些无须修改的关键参数，提供efuse介质支持，一旦烧写，不可修改。

3 系统安全

3.1 系统安全

通过镜像签名认证机制保证设备系统的完整性，确保系统不会被非法篡改。

3.2 系统安全策略

解决方案的开发中对于使用的系统端口以及服务进行审视，对于生产运行的业务场景中，不会使用的服务或端口进行关闭。同时确保设备的安全功能不会被关闭。

3.3 系统配置和权限

系统重要配置参数和权限，纳入统一管理，合理配置系统参数和权限，控制人为不合理配置导致的安全漏洞。

3.4 系统日志管理

提供日志管理系统，并且对于设备的日志可以进行灵活的控制，可以设置日志的级别，可以监控到设备的管理活动。同时对于日志的记录，并可以方便进行定期的安全审视。

3.5 开源及第三方代码安全

系统中涉及到的开源和第三方代码，从安全角度出发进行选型和评估，定期进行安全检查和漏洞处理。

3.6 代码扫描

代码每天进行Fortify-C、Fortify-JAVA、Coverity、Cppcheck、warncheck、Pclint、Codemars和csecchеck扫描检查，发现的疑似问题都要求澄清。代码正式发布前，使用业界主流防病毒软件（如Symantec、trend OfficeScan、McAfee、Avira AntiVir、卡巴斯基等）对其扫描，保证软件包中未感染或嵌入病毒/木马。

4 应用安全

4.1 安全算法

采用国际标准或业界通用的安全算法(如AES、RSA、ECC、DSA)，对于不安全的算法及时升级或者替换，对于密钥、证书、授权认证的管理也有严格的流程。根据产品需要，芯片支持嵌入加密引擎的方式来提高加解密的性能和安全性。

4.2 数据安全存储及访问

芯片支持安全存储区，用于存储重要数据，安全存储使用加密，签名等保护措施，对机密数据项进行安全保护，只有特定的硬件或模块才能进行访问，同时安全存储不可更改，从而实现对存储数据的防破解，防伪造，防盗用；

4.3 模型保护

对于AI应用的网络模型文件，Tuscany提供签名和加密机制，仅在运行时，在内存中完成解密和校验，从而实现在存储和传输过程中对网络模型的保护。

4.4 认证与会话控制

对于AI应用的开发态环境，提供认证和会话管理机制，保障开发安全：

- 系统提供认证（即登录）和注销功能。
- 系统使用用户名/口令的方式认证客户端。
- 用户最终认证处理过程在服务端进行，而不是依靠客户端进行认证。
- 认证处理模块需对提交的参数进行合法性检查。
- 如果用户未通过认证，则禁止其进行其它任何操作。
- 所有的业务逻辑不能绕过认证。
- 认证失败后，只给出一般性的提示，不能提示给用户详细以及明确的错误原因。
- 基于会话对用户登录与鉴权进行管理。
- 用户登录时连续多次登录失败锁定用户账号。
- 用户帐号被锁定后，系统能够在一段时间后自动解锁。

- 系统支持会话超时机制，在超时后清除会话信息。

4.5 安全通信

对于AI应用的开发态环境，提供跨主机组件间的加密通道：

- 用户登录开发环境使用HTTPS协议。
- 跨主机组件间采用TLS加密协议。

4.6 最小授权

除非需要使用系统资源，解决方案中涉及的运行程序都运行在操作系统的普通用户上。系统文件只能被授权用户访问。

5 安全面

5.1 管理安全面

Tuscany只提供部分管理API接口和日志文件给产品管理程序，并不提供对外网络管理接口。

5.2 控制安全面

Tuscany只提供对外网络控制面接口监听服务，用于开发环境下与MindStudio的连接，默认是打开。在生产环境下，产品需要关闭该接口服务，保障生产环境安全性。

提供SSH服务，只允许非root用户通过SSH登录，支持证书和口令认证。

5.3 用户安全面

Tuscany只提供API接口给产品AI应用程序调用，并不提供对外网络业务数据处理接口。

6 总结

华为致力于提供业界最好的产品和服务以满足客户的需求。我们非常重视网络安全，已经投入了很多资源去提升和改善我们公司、业界同行以及其他各方的能力，为产品提供安全保障。

华为在内部还建立了独立的网络安全实验室及安全测试团队，对产品进行网络安全专项测试；同时华为积极、持续地参与ITU-T、3GPP、IETF等国际电信标准组织中的安全标准制定，加入FIRST（应急事件及安全团队论坛）等安全组织，并通过和主流安全厂商紧密合作，为行业的健康发展作出自己的贡献，努力保障全球客户的网络安全。

华为成立了监控、受理产品安全漏洞的专门组织PSIRT（产品安全事件应急响应团队），华为希望安全研究人员、行业组织、政府组织和供应商主动与华为PSIRT联系，报告潜在的华为产品的安全漏洞或安全问题。

华为PSIRT E-mail邮箱：**mailto:PSIRT@huawei.com**

注：

1. 华为面向全球发布了网络安全白皮书——《网络安全透视： 21世纪的技术与安全——一场艰难的联姻》。该白皮书由华为全球网络安全官约翰.萨福克（John Suffolk） 撰写，详细参见如下链接：

   中文：**http://www.huawei.com/ilink/cn/download/HW_187369**

   Eng：**http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_187368.pdf**

   a. 关于华为PSIRT的详细说明请查看如下链接：

      中文：**http://www.huawei.com/ilink/cn/special-release/HW_093772**

      Eng：**http://www.huawei.com/ilink/en/special-release/HW_093771**

7 缩略语

表 7-1 缩略语清单

英文缩写	英文全称	中文全称
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用软件编程接口
CA	Conditional Access	条件接收
DSA	Digital Signature Algorithm	数字签名算法
OS	Operating System	操作系统
RSA	RSA Algorithm	公开密钥密码体制

