

面向移动办公终端的可信计算与零信任架构融合方案

A Fusion Architecture of Trusted Computing and Zero Trust for Mobile Office Terminals

刘有泽,田嘉,齐霄,旷炜(中讯邮电咨询设计院有限公司,北京 100048)

Liu Youze, Tian Jia, Qi Xiao, Kuang Wei (China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘要:

移动办公对终端安全的要求不断提高,传统零信任准入架构“重身份、轻环境”的问题愈发明显。可信计算作为一种先进安全技术,利用TEE硬件信任根实现平台完整性度量和远程证明。提出面向通用安卓终端的可信计算与零信任架构融合方案,通过TEE信任根、Android Keystore与Key Attestation构建从硬件到应用层的信任链,以轻量级“挑战—响应”协议实现设备完整性度量和防篡改证明。零信任网关根据实时验证结果决定访问权限,为构建新型信任体系与动态安全边界提供了创新性技术路径。

关键词:

可信计算; TEE; Key Attestation; 零信任; 平台完整性; 动态安全边界

doi:10.12045/j.issn.1007-3043.2026.09.003

文章编号:1007-3043(2026)09-0013-06

中图分类号:TN918

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

Mobile office requires increasingly strict terminal security. The problem of the traditional zero-trust access architecture that is "over-reliant on identity verification while neglecting contextual environment attributes" has become increasingly prominent. Trusted computing, as an advanced security technology, utilizes the TEE hardware trust root to achieve platform integrity measurement and remote attestation. A fusion scheme of trusted computing and zero-trust architecture for general Android terminals is proposed, and a trust chain from the hardware layer to the application layer is built by using the TEE trust root, the Android Keystore and Key Attestation. The lightweight "challenge-response" protocol is used to achieve device integrity measurement and anti-tampering proof. The zero-trust gateway decides access permissions based on real-time verification results, providing an innovative technical path for building a new trust system and dynamic security boundaries.

Keywords:

Trusted computing; TEE; Key attestation; Zero trust; Platform integrity; Dynamic security boundaries

引用格式:刘有泽,田嘉,齐霄,等. 面向移动办公终端的可信计算与零信任架构融合方案[J]. 邮电设计技术,2026(9):13-18.

0 引言

移动办公场景下,终端承载着公文流转、审批等关键业务,但存在设备所有权、系统准入凭证安全维度低等问题,面临诸多挑战。零信任架构以持续验证取代一次性边界准入^[1],在身份认证、通道加密、动态权限维度已较为成熟,但在终端环境感知维度存在漏

洞:准入决策仅依据用户身份,无法感知终端运行环境是否可信。终端被Root或植入恶意框架后,攻击者可在合法会话下获取敏感数据。

基于上述问题,本文提出一种可信计算与零信任架构融合方案。该方案利用主流安卓移动终端广泛集成的ARM TrustZone TEE与Android Key Attestation机制^[2],在不替代现有身份认证的前提下,对准入流程增加基于硬件信任根的远程证明环节,根据验证结果执行三级动态准入控制。方案信任根可在企业侧自

收稿日期:2026-07-23

建,适用于对数据主权有严格要求的企业场景。

1 关键技术概述

可信计算(Trusted Computing)的定义为:通过硬件信任根实现平台完整性度量与远程证明,确保系统状态可预期且可验证^[3]。ARM TrustZone 作为其在移动端的重要实现,提供 CPU 级硬件隔离^[4]。本方案在此基础上采用 Android Keystore 密钥管理、Key Attestation 设备状态证明和 JWT 凭证传递 3 项核心机制。

1.1 ARM TrustZone 与 TEE 双世界模型

ARM TrustZone 是 ARM 架构从 ARMv6 起引入的硬件安全扩展^[5],在 CPU 层面将系统划分为普通世界与安全世界(见图 1),通过总线级硬件隔离强制执行。普通世界运行 Android/Linux 等通用操作系统,安全世界运行 TEE;普通世界的任何代码(包括被 Root 的内核)均无法访问安全世界内存^[6]。世界间的切换由 EL3 安全监视器通过 SMC 指令控制,由硬件强制实施上下文保护。

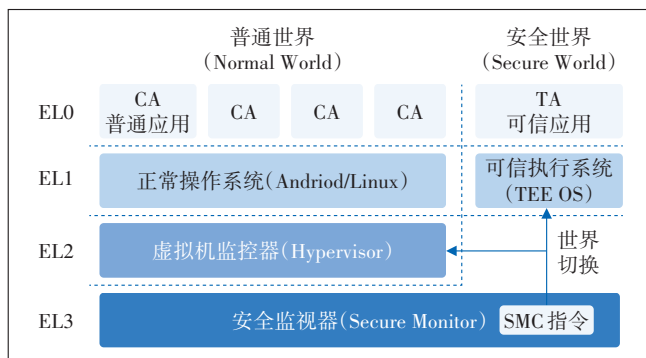


图1 TrustZone 双世界模型

即使 Rich OS 被 Root 攻击,TEE 内部的可信应用须经签名验证方可加载。设备安全属性的采集与签名均在安全世界完成,由此建立“即使操作系统被攻破,证明密钥仍不可导出”的安全保障。

1.2 Android Keystore 系统架构

Android Keystore 是 Android 的密钥管理框架,其密钥生成与初始化委派给 TEE 执行,私钥离开安全世界即不可用。系统自底向上分为 4 层,其架构如图 2 所示。

a) 应用层。企业应用通过 Android Keystore API 发起密钥生成和签名操作,但不持有任何密钥材料,所有密码运算委托下层执行。

b) 系统服务层。运行于普通执行环境,核心组件

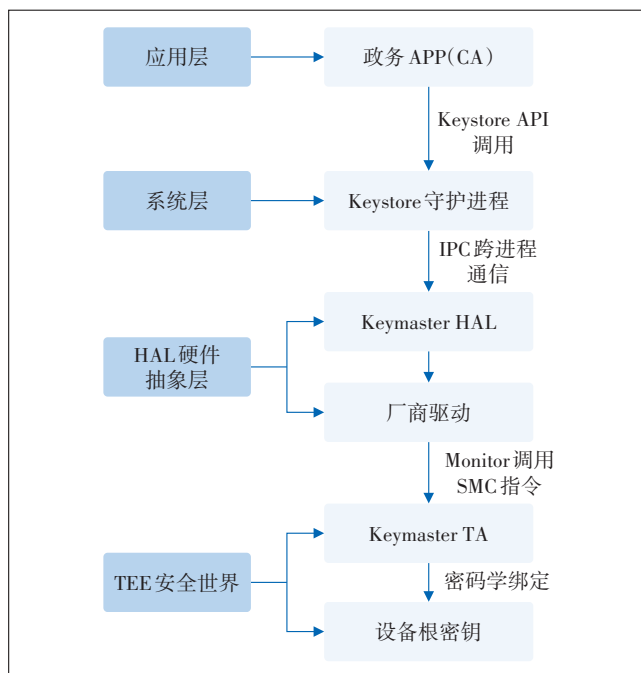


图2 Android Keystore 4层架构

为 Keystore 守护进程,充当应用与 Keystore 系统之间的接口,负责将应用层请求通过 IPC 路由至硬件抽象层。

c) 硬件抽象层(Keymaster HAL)。位于普通执行环境内核边界,承担 REE 与 TEE 之间的通信桥梁角色,通过专用驱动将密钥操作请求跨越 TrustZone 硬件边界转发至安全世界中的可信应用。

d) TEE 安全世界。Keymaster TA 以可信应用的形式驻留于硬件层,是密钥操作的实际执行实体。应用请求密钥时通过指定硬件绑定标志,确保密钥与当前设备密码学绑定。

1.3 Key Attestation 证书体系

Key Attestation 是 Android 安全特性,实现设备状态不可伪造的密码学证明^[10]。应用调用 Keystore API 生成密钥对时,Keymaster TA 同步生成 X.509 证明证书。证书链由三级组成:厂商根证书签发芯片平台中间证书,中间证书签发叶证书;叶证书在 TEE 内生成,其公钥与设备硬件绑定。Key Attestation 证书体系如图 3 所示。

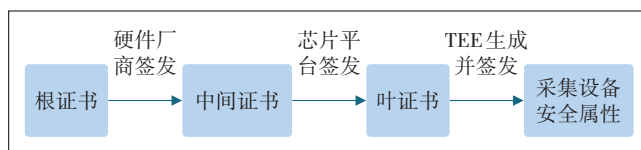


图3 Key Attestation 证书体系

叶证书中的证明扩展字段由 TEE 采集并签名,记录了系统镜像验证状态、引导加载程序锁定状态、操作系统版本等关键安全属性。采集与签名均在安全世界完成,利用设备根密钥进行密码学签名,通过 X.509 证书链验证确保叶证书确由 TEE 硬件签发且未被篡改。

1.4 JWT 凭证传递机制

JWT(JSON Web Token)是一种紧凑、自包含的令牌格式,由头部、载荷和签名3个部分构成^[7]。验证者将设备证明结论(风险等级、授权范围)作为载荷写入并使用自身私钥签名,网关使用验证者公钥即可独立验签。JWT 的技术优势在于:签名机制保证载荷不可篡改;内置过期时间字段实现凭证自动失效,为周期性重评估提供机制保障。

2 系统架构

2.1 三方证明架构

本方案参照 IETF RATS(RFC 9334) Background Check 模型划分证明方(Attester)、验证方(Verifier)和依赖方(Relying Party)3个逻辑角色^[8],整体架构如图4所示。

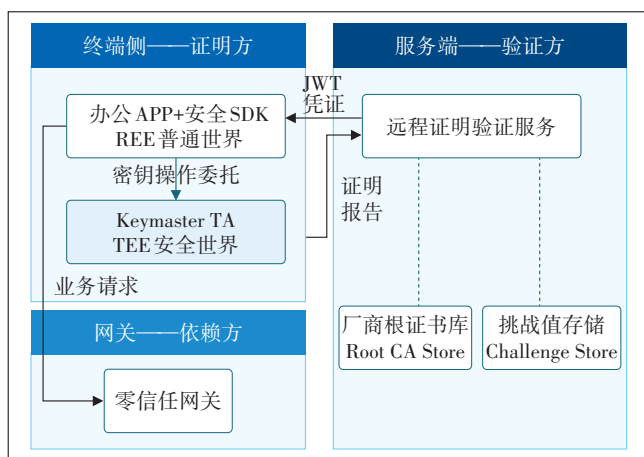


图4 三方远程证明架构

证明方位于移动终端侧,由安全 SDK 与 Keymaster TA 协同构成。安全 SDK 嵌入普通执行环境的企业应用,负责证明流程发起与 REE 侧安全指标采集;Keymaster TA 驻留在 TEE 侧,完成临时密钥生成、安全属性采集和证明证书签名,私钥材料始终驻留在安全世界内部。

验证方部署于企业服务端,承担远程证明验证与决策职能,维护设备厂商根证书库并执行递进式验证

(详见第3章),验证通过后签发 JWT 凭证。

依赖方为企业零信任网关,根据 JWT 风险等级执行差异化准入策略:网关无须感知终端 TEE,仅当凭证缺失或过期时触发重新证明;该流程遵循最小权限原则,仅依据风险等级决定放行范围。

2.2 3层信任链

3层信任链的架构如图5所示。

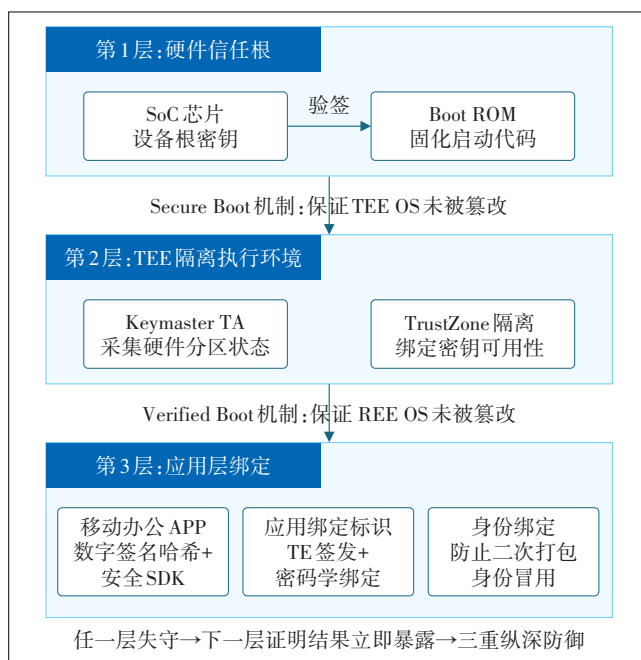


图5 3层信任链

a) 第1层:硬件信任根。信任根源于 SoC 芯片出厂时记录于 eFuse 中的设备根密钥,材料不可读取、不可修改^[9]。芯片上电后固化 Boot ROM 逐级验证启动加载程序签名,校验通过后移交执行权,确保设备从第一行代码起即处于已知可信状态。缺失这一层,上层安全机制均缺乏信任锚点。

b) 第2层:TEE 隔离执行环境。第2层依赖 TEE 硬件隔离保护操作系统的环境安全。Keymaster 可信应用从引导加载程序、Boot 分区到 System 分区,任一分区签名校验失败即导致 TEE 密钥不可用,通过证明属性直接暴露系统篡改状态。

c) 第3层:应用层身份绑定。通过证明证书中的应用绑定标识实现应用级防冒。该标识为企业应用的数字签名哈希,在 TEE 证明证书生成时自动写入,与密钥密码学绑定。应用二次打包必然导致签名改变,验证者比对标识即可识别。

2.3 设备状态采集与风险评估模型

设备状态采集与风险评估模型将双路采集的异构安全指标转化为统一准入等级,使网关无需理解TEE内部细节即可执行决策。

2.3.1 双路采集

硬件路由TEE内部的Keymaster TA执行环境级采集,内容为设备硬件安全状态,封装于证明证书扩展字段^[10],经设备根密钥签名后不可伪造。

软件路由安全SDK在普通执行环境中进行采集,采集Root权限状态、注入框架痕迹、关键安全配置及网络环境。采集结果使用TEE临时私钥附加签名,与硬件路数据建立密码学绑定,确保双路数据归属于同一证明会话。软件路定位为辅助参考——攻击者可篡改采集结果但无法通过TEE签名验证,其价值在于提供硬件路无法覆盖的补充信息。

2.3.2 双路非对称融合评估

双路数据汇聚至验证者后进行非对称交叉验证,遵循“硬件优先”原则,即TEE采集的硬件指标具有最高可信权重;软件路指标异常时直接判定为最高风险等级。验证者采用加权评分机制将多维度安全指标量化为风险分数,按安全敏感程度分配权重,加权总分映射至三级准入等级。

a) 拒绝访问。任一硬件路指标异常,或证书链验证未通过,引导加载程序处于解锁状态,证明证书过期或挑战值验证失败,即判定为最高风险等级,触发企业安全告警。

b) 受限访问。TEE硬件路指标全部通过,但软件路检测到越权痕迹、注入框架或安全配置不合规,或设备指纹不在可信库中,终端被授予只读权限,禁止写入与下载。

c) 全权限访问。即双路指标均通过且验证一致。

针对国产终端因采用厂商自有签名密钥而无法通过Google认证体系校验的问题,评估模型采用设备指纹库作为补充验证机制:已知可信设备指纹直接获得全权限,未知指纹按受限访问处理。指纹库在企业侧进行维护,不向外部泄露终端硬件特征。

3 远程证明协议

远程证明协议基于Key Attestation机制和IETF RATS(RFC 9334)Background Check模型^[11],分为设备注册、挑战值获取与TEE证明执行、证明材料封装与验证、JWT签发与网关准入执行4个阶段。

3.1 设备注册与用户绑定

用户首次登录时,认证后触发设备注册流程,设备注册流程如图6所示。SDK调用Keystore API生成设备持久密钥对(EC P-256),应用绑定标识(应用签名哈希)由TEE写入证书扩展字段,随证明证书链上传至验证方。验证方验证后创建设备绑定记录,关联用户标识、设备标识与密钥指纹。

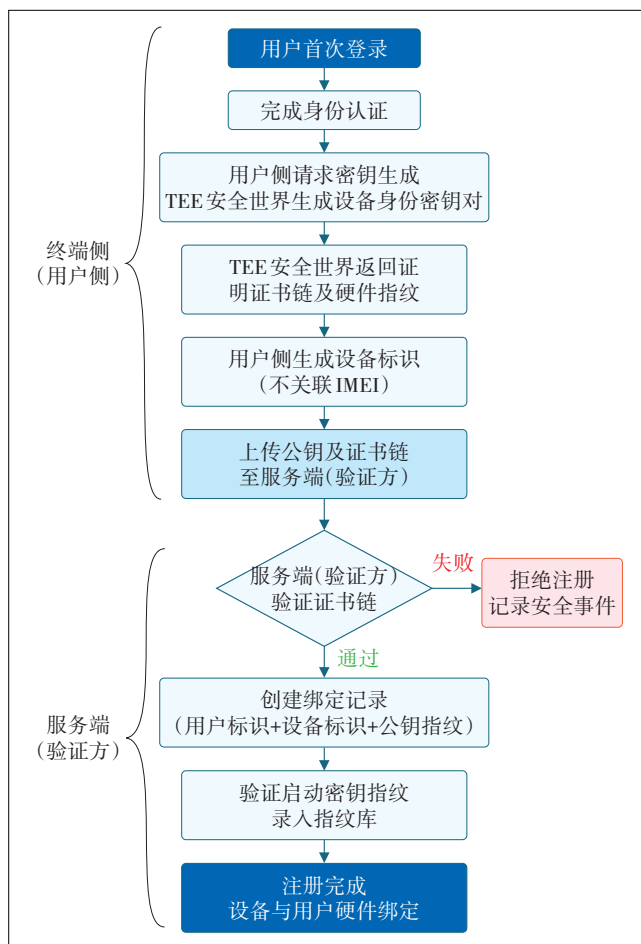


图6 设备注册流程

本机制的安全价值在于:攻击者窃取凭证后在另一设备登录时,其TEE生成的密钥对与原始设备完全不同,密钥指纹与绑定记录不匹配,系统将其识别为新设备首次接入并触发安全审核,而非自动注册通过。

3.2 挑战值获取与TEE证明执行

证明方向验证方发起准入请求,验证方返回一次性挑战值(TTL=60 s)。安全世界内的可信应用生成临时密钥对(私钥始终驻留在安全世界内部),将挑战值嵌入证明证书扩展字段,采集设备安全属性,使用设备根密钥签发X.509 Attestation证书。挑战值获取流

程如图7所示。

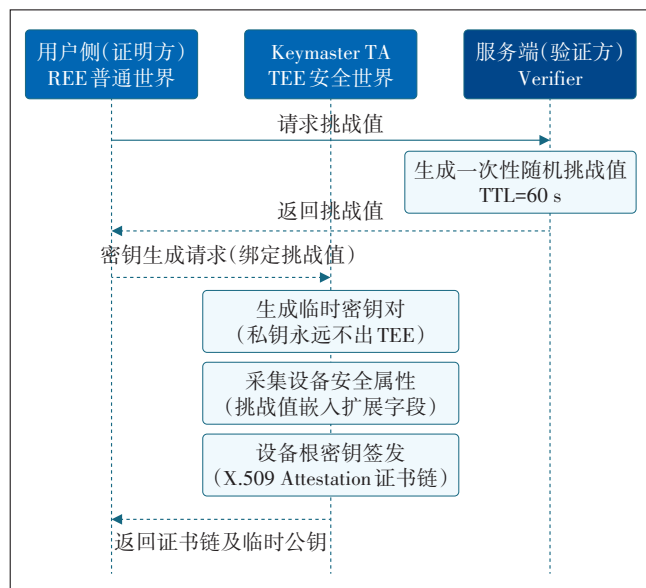


图7 挑战值获取流程

3.3 证明报告组装与验证

安全SDK在普通执行环境同步采集软件安全指标,使用安全世界内生成的临时私钥对采集结果执行附加签名,与硬件路数据建立密码学绑定后封装发送验证方。证明材料的封装与验证流程如图8所示。

验证方执行递进式验证,任一步失败即终止并返

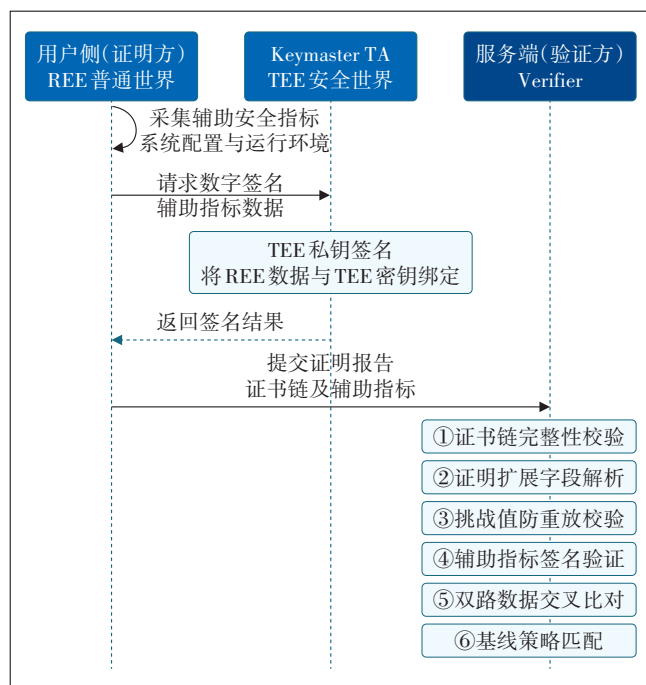


图8 证明报告组装与验证流程

回拒绝。具体验证流程为:X.509证书链逐级验证;证书扩展字段解析,提取硬件安全属性;挑战值时效与唯一性校验;多指标签名验证;双路数据非对称比对,以硬件路结果为基准核对软件路数据一致性,硬件指标异常时跳过软件路直接判定;基线策略匹配与风险评分。

3.4 JWT签发与零信任准入决策

验证通过后,验证方签发JWT凭证,载荷包含风险等级、授权范围和有效期,由验证方进行私钥签名。终端携带JWT访问企业资源,网关验证签名后提取风险等级执行准入:全权限则放行全部API,受限则仅放行读取操作,拒绝则返回HTTP 403并记录安全事件。JWT签发与网关准入执行流程如图9所示。

4 安全性分析与效果评估

本章从攻击防御能力与准入安全能力2个维度,对方案引入远程证明前后的安全性提升进行综合评估。安全防护能力对比如表1所示。

与 Google SafetyNet、Play Integrity API 等方案相比,本方案不依赖 Google Play Services 且不受设备型号限制,验证服务部署于企业侧,信任根自主可控;提供全权限、受限、拒绝的三级准入等级。终端仅需集成SDK即可灰度部署,JWT无状态验证降低了大规模终端场景下验证服务的横向扩展复杂度,对国内运营商网络环境具有天然适配性。

5 结束语

本文提出一种可信计算与零信任架构融合的远程证明方案,利用商用安卓终端广泛集成的 ARM TrustZone TEE 与 Android Keystore 机制,通过 Key Attestation 证书链验证实现硬件级远程证明,将准入决策依据从“用户是谁”延伸至“设备是否可信”。本方案信任根可在企业侧自建,适用于金融、能源等对数据主权有严格要求的行业。未来,可引入AI驱动的设备行为分析与边缘计算分布式验证,并将应用拓展至物联网终端准入与跨域联合身份认证等场景,提升终端准入智能化水平。

参考文献:

- [1] NIST SP 800-207 Zero trust architecture[S].
- [2] 中国信息通信研究院云计算与大数据研究所. 零信任安全发展研究报告(2022年)[R]. 北京:中国信息通信研究院,2023.

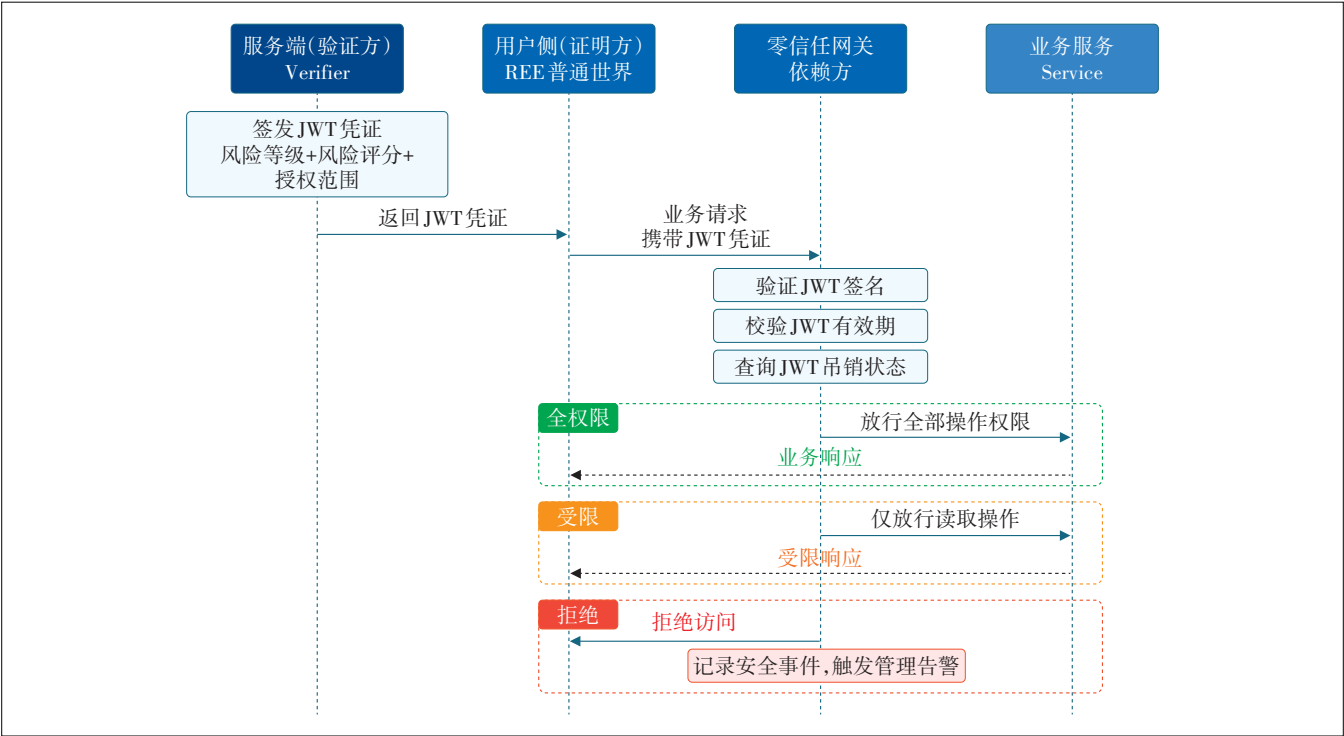


图9 JWT签发与零信任准入决策流程

表1 安全防御能力对比

安全维度	攻击/风险场景	传统零信任准入	本方案增强后
系统完整性防护	Root工具(Magisk等)修改或回滚系统分区	依赖MDM/MAM软件检测,可被Root工具绕过	Verified Boot状态由TEE采集签名,普通世界无法伪造或隐藏
注入框架防御	Xposed/Frida注入劫持	不支持检测	安全SDK在REE侧对进程内存映射与注入框架特征进行双重扫描,结果交叉验证
引导加载程序安全	解锁Bootloader后刷入恶意系统	不支持	Bootloader锁定状态被记录于证书相关字段
安全补丁合规	未及时修补已知漏洞的设备	不支持	OS补丁级别在TEE证书中可审计
重放攻击防御	截获合法证明报告重放	依赖HTTPS传输层安全	挑战值一次一密,独立于传输层
中间人攻击防御	篡改或伪造传输中的证明数据	依赖TLS证书体系	证书链验证+TEE签名
设备身份冒用防御	凭证迁移至其他设备冒用	无硬件绑定	设备公钥指纹+Verified Boot Key指纹+应用签名哈希三重硬件绑定
模拟器或虚拟机伪造	在非真实设备上运行并伪造环境	无检测能力	无法生成设备根密钥签名的证明证书
应用篡改检测	应用二次打包或注入恶意代码	不支持	应用绑定标识绑定签名哈希,重打包失效

注:方案防护范围覆盖设备启动链完整性、操作系统运行时可信性及凭证防篡改与防重放。TEE固件自身漏洞利用与硬件侧信道攻击不在本方案防护范围内。

- [3] Trusted Computing Group. TCG specification architecture overview [R]. Beaverton:Trusted Computing Group,2004.
- [4] 张锋巍,周雷,张一鸣,等.可信执行环境:现状与展望[J].计算机研究与发展,2024,61(1):243-260.
- [5] Pinto S, Santos N. Demystifying Arm TrustZone: A Comprehensive Survey[J]. ACM Computing Surveys,2019,51(6):1-36.
- [6] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: what it is, and what it is not [C]//2015 IEEE Trustcom/BigDataSE/ISPA. Helsinki;IEEE,2015:57-64.
- [7] IETE RFC 7519 JSON Web token (JWT)[S].
- [8] IETE RFC 9334 Remote attestation procedures (RATS) architecture[S].
- [9] Ekberg J E, Kostianen K, Asokan N. The Untapped Potential of Trusted Execution Environments on Mobile Devices[J]. IEEE Security & Privacy,2014,12(4):29-37.
- [10] 张涵,于航,周继威,等.面向隐私计算的可信执行环境综述[J].计算机应用,2025,45(2):467-481.
- [11] 王晋,喻瀚,刘畅,等.智能电网环境下一种基于SDKey的智能移动终端远程证明方案[J].信息安全,2018(7):1-6.

作者简介:

刘有泽,毕业于北京邮电大学,助理工程师,硕士,主要从事终端安全技术的相关研究工作;田嘉,毕业于中国人民大学,工程师,硕士,主要从事移动信息安全的相关研究工作;齐霄,毕业于北京交通大学,高级工程师,硕士,主要从事移动安全的相关研究工作;旷炜,毕业于清华大学,高级工程师,硕士,主要从事安全平台相关的工作。