移动警务端边扩展类终端可信防护方案研究

赵荣辉[1]，王志宇[1]，苏　禹[2]

（1. 公安部第一研究所，北京　100048；2. 中国信息安全研究院有限公司，北京　102209）

摘　要：针对移动警务端边架构中扩展类智能终端可信防护难题，提出一种创新的可信防护策略和度量方法，基于可信计算、密码学等技术，以边缘网关物理可信根为基础构建扩展终端可信信任链，实现对扩展终端系统全生命周期的可信度量与防护。经实际案例验证，该方法有效解决了扩展终端可信防护技术瓶颈，显著提升了多形态终端安全管理效能，满足公安及相关行业对移动终端安全可信的严格要求。

关键词：移动警务；端边架构；可信防护；可信度量；信任链

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 08. 004

引用格式：赵荣辉，王志宇，苏禹. 移动警务端边扩展类终端可信防护方案研究［J］. 网络安全与数据治理，2025，44(8)：24 - 29.

Research on trusted protection solution of mobile police terminal and edge equipment

Zhao Ronghui[1]，Wang Zhiyu[1]，Su Yu[2]

（1. First Research Institute of the Ministry of Public Security，Beijing 100048，China；

2. China Information Security Research Academy Co.，Ltd.，Beijing 102209，China）

Abstract：Due to the difficulty of extended smart terminal protection，this article supposes a sort of innovative trusted protecting strategy and measurement methods that the gateway device（or the edge equipment）creates trusted chain from hardware root component by using trusted computing technology and business cryptography suits，and realizes the trusted measurement and protection of the entire life cycle of the extended terminal system. Through practical pilot test，the solution can efficiently solve the bottleneck of extended terminal trusted protection technology，drastically improve the performance and efficiency of versatile terminal security management and totally meet the specific requirements of higher security and reliability in public security.

Key words：mobile police；terminal and edge architecture；trusted protection；trusted measurement；trust chain

0　引言

在公共安全领域，移动终端操作系统生态呈现出特殊的技术发展趋势，如高安全性、高可靠性、强身份认证等。当前，Android 系统凭借其开放性与广泛适配性在公共安全相关行业移动终端领域占据主导地位。随着移动互联网的快速发展以及人工智能决策能力的提升，移动操作系统正加速向微内核架构转型，以实现面向全场景覆盖与万物互联业务的高效协同。在此背景下，以工业和信息化部指导、开放原子开源基金会社区孵化的 OpenHarmony 开源鸿蒙自主操作系统为代表的移动终端装备已逐步在公安、政务等关键行业展开示范应用，推动行业信息化建设的自主安全进程。

公安行业作为公共安全信息化建设的前沿阵地，已构建起基于网络安全等级保护制度与内生防御可信计算体系的新一代移动警务安全架构[1-2]，通过系统性防护策略有效抵御移动警务业务流程中的潜在安全威胁。在移动终端装备安全管理方面，《智能手机型移动警务终端 第 1 部分：技术要求》（GA/T 1466. 1—2018）[3]、《智能手机型移动警务终端 第 2 部分：安全监控组件技术规范》（GA/T 1466. 2—2018）等系列公安行业标准发挥了关键作用[4]。随着 5G 通信技术的成熟应用以及物联网技术的迅猛发展，移动警务逐渐向端边架构延伸拓展，大量诸如智能手表、执法记录仪、便携式数据采集终端等扩展类智能终端被接入移动警务网络，这在丰富警务功能的同时，也给移动警务安全带来了前所未有的新挑战。现有移动警务可信计算体系在应对端边架构扩展类终端时，暴露出诸多问题。例如，防护覆盖范围存在局限性，无法全面涵盖不同品牌、不同功能的扩展类终端；在策

略协同方面，难以实现边缘网关与扩展终端之间的有效配合，导致安全防护出现漏洞，难以保障扩展终端的安全可信运行。

因此，本文提出一种移动警务端边架构可信防护策略和度量方法，对于保障移动警务系统的安全性、稳定性以及提升警务工作效能具有至关重要的现实意义。

1 关键技术

1.1 可信计算

20 世纪 90 年代，可信计算组织（Trusted Computing Group，TCG）提出了 TPM 标准，旨在基于硬件锚点构建安全信息系统，改善个人计算机安全性[5]。美国 NIST 和商务部先后推出了 NIST SP800-111[6] 和 NIST SP800-164[7]，前者规定了移动终端操作系统启动度量和存储加密，后者是草案，规定了可信根的构建和可信度量过程。2017 年，网络工程师 Gilman 和软件工程师 Barth 阐述了零信任网络方案[8]，为企业机构在互联网上构建安全系统提出建议，其中在可信终端一章节描述了 TPM 在零信任架构中的关键作用。

2022 年，《移动警务 可信计算总体技术要求》（GA/T 2001—2022）[9] 发布。该标准规定应基于物理硬件可信根构建可信度量和信任链的技术体系，在宿主设备启动流程中，以可信平台控制模块（Trusted Platform Control Module，TPCM）作为信任锚点，依据既定的执行序列，对主板、固件、引导程序及操作系统等核心组件实施完整性验证，并将度量结果记录于平台状态寄存器（Platform Configuration Register，PCR）。终端操作系统可信度量流程如图 1 所示。

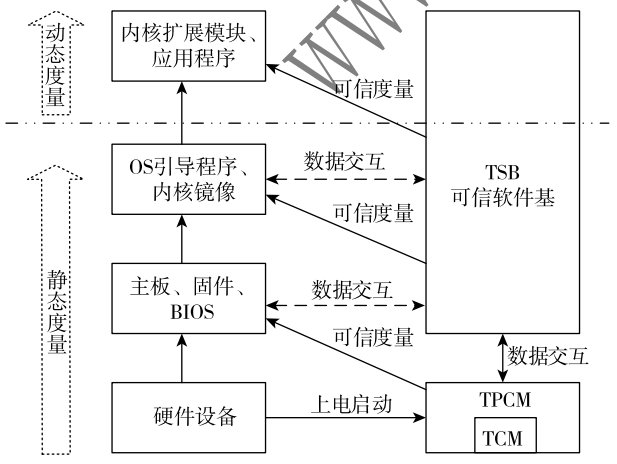


图 1 终端操作系统可信度量流程

1.2 警用无线局域网

警用无线局域网（Police Wireless LAN，PWL）是以多种无线局域网技术为基础，按照公安信息化实战需求和安全要求进行协议重新开发而形成的公安专用无线局域网技术。PWL 通过重构无线局域网协议实现了空口安全加密及关键信息零泄露。PWL 无线局域网组网设备中，PWL STA（Station，接入设备）是 PWL 通信终端为各类警用设备提供 PWL 通信能力、具备符合国密要求的硬件加密模块；PWL AP（Access Point，接入点）是供 PWL STA 接入的接入点，为多 PWL AP 设备提供集中管理和网络转发功能；PWL NAC（Network Access Controller，网络接入控制器）控制 PWL AP 和 PWL STA 建立安全连接并对 PWL 进行安全管控。

2 方案设计

传统的可信计算体系在单一设备的可信防护场景下展现出一定效能，但在应用于移动警务端边架构时，暴露出显著的技术局限性。从安全防护体系的灵活性维度分析，现有方案难以适配扩展类终端的异构化特性[10]。扩展类终端在硬件配置、操作系统架构及应用场景等方面呈现高度差异化特征，不同型号终端的处理器、内存管理机制及通信协议存在显著差异。传统可信防护方案采用的标准化监管框架，无法有效兼容终端的多样性，致使部分扩展终端因缺乏适配性验证机制而脱离安全防护范畴，形成安全防护的监管盲区。在硬件实现层面，成本控制与设备空间限制因素严重制约了可信体系的扩展能力。受移动警务终端轻量化设计要求及成本预算约束，扩展类智能终端难以额外部署硬件可信根模块，导致传统基于硬件可信根的可信度量与信任链构建机制无法在扩展终端上有效实施[11]，难以建立完整的信任传递路径，无法实现对扩展终端全生命周期的可信防护，进而削弱了移动警务端边可信方案的整体安全性。

2.1 总体设计

本文聚焦移动警务端边场景中扩展类智能终端的可信防护技术难题，对边缘终端层设备[12]进一步细分，创新性地实现扩展类终端接入认证与可信度量等核心环节的深度耦合。该架构以边缘网关作为主节点，将物理可信根（TPCM/TCM）作为可信信任链的锚点，通过可信传递机制构建扩展类终端（从节点）的可信信任链，实现对扩展终端系统从初始化、启动到运行全生命周期的动态可信度量[13]。移动警务端边架构可信防护组网如图 2 所示。

本文方案总体架构依赖三个条件：（1）边缘网关设备需兼容 PWL，采用国密算法及专用通信协议构建安全传输通道，通过双向认证机制和动态密钥协商技术，保障通信过程的机密性、完整性和抗抵赖性；（2）基于物理可信根构建的可信信任链，需遵循可信计算规范，

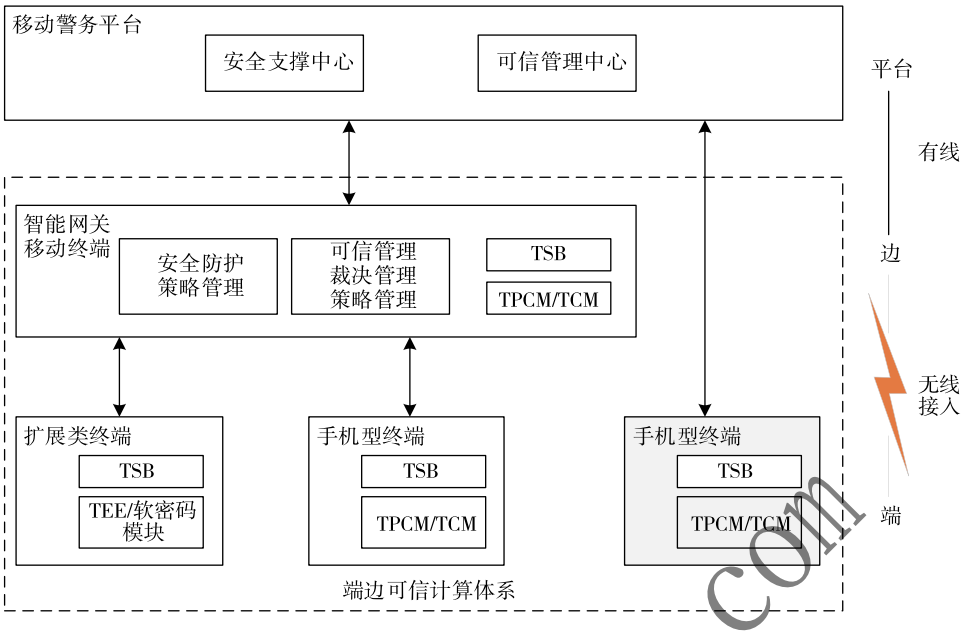


图 2　移动警务端边架构可信防护组网

通过可信度量根（Root of Trust for Measure，RTM）、可信存储根（Root of Trust for Storage，RTS）和可信报告根（Root of Trust for Report，RTR）的协同工作，实现信任的逐级传递与验证；（3）扩展类智能终端需具备可信执行环境（Trusted Executive Environment，TEE），通过安全芯片或可信软件基（Trusted Software Base，TSB）实现硬件级防护，同时预置可信度量模块（Trusted Computing Module，TCM）和可信存储模块（Trusted Storage Measurement，TSM），结合可信基准库的动态更新机制，确保可信度量的时效性和准确性。

2.2　可信方案

移动警务端边可信计算方案由边缘网关与扩展类终端的相关逻辑实体构成。端边架构可信防护方案的业务逻辑如图 3 所示。

边缘网关在开机上电启动后，首要任务是发起数字证书申请流程。此过程通过与公安认证中心进行基于安全协议的交互，遵循严格的身份验证与密钥交换机制，获取合法有效的数字证书。该数字证书依据公钥基础设施（Public Key Infrastructure，PKI）体系颁发，用于边缘网关在后续通信中的身份标识与验证，确保其在公安网络环境中的合法性。边缘网关构建可信信任链的过程基于物理可信根，即可信平台控制模块（TPCM）。TPCM 作为可信计算的核心硬件组件，具备安全存储与密码运算功能。从 TPCM 出发，运用哈希算法等度量手段，依次对主板 BIOS（Basic Input Output System）、固件等关键组件进行完整性度量。通过将各组件的度量值与预存的基准值进行比对，确保组件未被篡改，从而构建起完整且可信赖的信任基础。

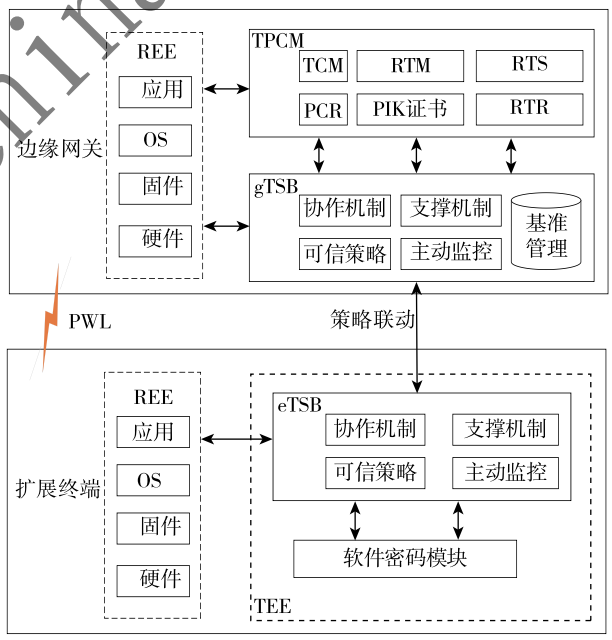


图 3　移动警务端边架构可信防护方案业务逻辑

3　测试验证

3.1　环境配置

以一种警用扩展类智能手表终端（HUAWEI WATCH 4，Harmony OS 4.0）接入移动警务边缘智能无线网关（OpenHarmony OS）场景为例，验证端边可信计算防护策略和可信度量过程。实验环境相关配置信息如表 1 所示。

表 1　实验环境配置

名称		型号	操作系统	用途
移动警务终端	智能手机型	HUAWEI Mate60	Harmony OS	远程终端可信报告验证
	扩展类	HUAWEI WATCH4	Harmony OS	可信报告生成封装
	智能网关型	ZD-PWSIG-M2100	OpenHarmony3. 2	可信验证
可信管理中心	可信管理服务网关	ZD-TCMS V1. 0	UOS	基准管理、证书管理、裁决及可信策略管理
PWL	PWL 设备	ZD-PWLE-A100/A150	——	端边架构下的 PWL 组网

智能手机型（手机）和扩展类移动警务终端（智能手表）符合《联接智能网关型设备的移动警务终端 第 1 部分 技术要求》（报批稿）及《联接智能网关型设备的移动警务终端 第 2 部分 接入技术要求》（报批稿），边缘智能网关符合《智能网关型移动警务终端 第 1 部分 技术要求》（报批稿）、GA/T 1466—2018、GA/T 1720—2020 以及 GA/T 2001—2022 等公共安全行业标准规范。

3.2　测试过程

端边扩展类终端可信度量过程如图 4 所示，扩展类终端可信度量的前置条件为：警用边缘网关 G 的启动和运行阶段可信度量、终端 TCM/TPCM/硬件密码模块（内置安全芯片形态）初始化、操作系统证书申请流程及系统管控组件启动等全部完成。其中，扩展类终端和网关终端都符合 GM/T 0024—2023[14] 和 GM/T 0058—2018[15] 规定的双证书体系，签名密钥对由本地终端密码模块生成，加密密钥对由后端密钥管理中心（Key Management Center，KMC）生成，对于端边扩展类终端来说，加密密钥对由边侧网关生成。

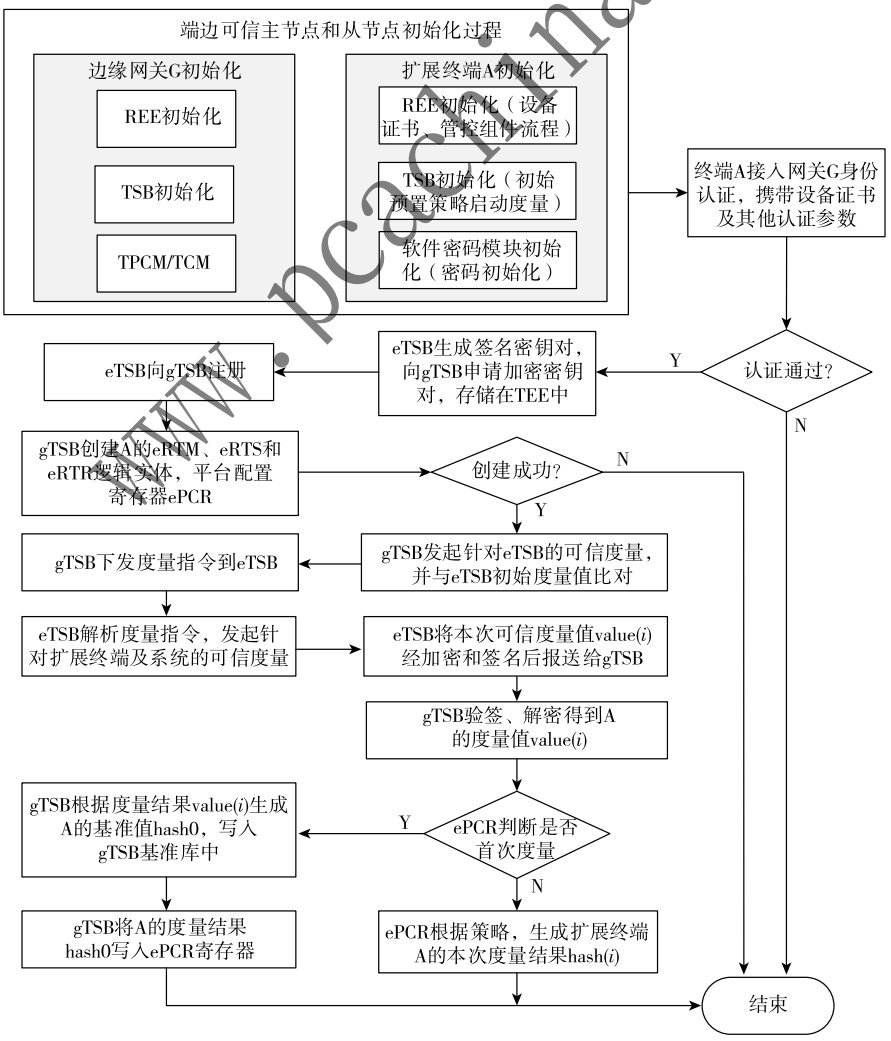


图 4　端边扩展类终端可信度量过程

实验过程中，扩展终端 A 接入边缘网关 G 的端边可信计算防护策略和度量过程包括以下步骤：

（1）边缘网关 G 开机上电启动，完成移动警务设备数字证书申请、主节点 TPCM/TCM 起始信任链构建、可信度量以及系统管控组件服务（以下简称“系统管控服务”）启动等流程之后，结束边缘网关的初始化流程。

（2）扩展终端 A 开机上电启动，完成设备证书（软证）申请、软密码模块和系统管控模块初始化之后，终端 A 的可信软件基 eTSB（Embedded Trusted Software Base）调用软密码模块，且按照出厂预置通用可信策略执行初始可信度量，将初始度量值 $value_0 = [v_1, v_2, \cdots, v_n]$ 存储于 TEE，扩展终端 A 完成初始化流程。

（3）扩展终端 A 发起接入边缘网关 G 的身份认证流程，基于 PWL 接入边缘网关 G，携带 A 终端设备证书及其他认证参数。

（4）完成步骤（3）北向接入边缘网关身份认证之后，扩展终端 A 的 eTSB 调用本地软密码模块生成可信防护业务使用的 SM2 签名密钥对，向边缘网关 G 的可信密码模块（TPCM/TCM）申请 SM2 加密密钥对；申请请求中携带扩展终端 A 的可信签名公钥 TC_Pubk_Sig。

（5）边缘网关 G 的可信软件基 gTSB 解析请求，调用 TPCM/TCM 生成扩展终端 A 的可信加密密钥对 Tc_Keys_Enc，使用 Tc_Pubk_Sig 加密 Tc_Keys_Enc，返回至扩展终端 A；gTSB 存储对应扩展终端 A 的签名公钥 Tc_Pubk_Sig 和 Tc_Keys_Enc。

（6）扩展终端 eTSB 解析响应消息并通过本地签名私钥 Tc_Prik_Sig 解密获取加密密钥对 Tc_Keys_Enc，安全存储在 TEE 软密码模块。

（7）eTSB 携带扩展终端 A 的终端系统特征参数向边缘网关 gTSB 申请可信策略，使用签名私钥对请求数据生成签名信息。

（8）边缘网关 G 获取扩展终端 eTSB 的注册数据，经 gTSB 验签后调用网关内置的 TPCM 创建对应 A 的可信根（eRTM、eRTS 及 eRTR，其中，e 代表 embedded）容器、平台可信配置寄存器 ePCR；初始化对应的 TCM 可信密钥和寄存区数据，返回注册响应并携带 A 的可信策略及可信根标识信息 Tc_ID。

（9）边缘网关 gTSB 以 TPCM/TCM 中扩展终端 A 的度量可信根 eRTM 为起始，构建扩展终端 A 的可信信任链。

（10）边缘网关 gTSB 向扩展终端 A 预置的 eTSB 可信软件基实体发起可信度量，生成度量值并与边缘网关 G 可信基准库中本类型扩展终端 eTSB 可信软件基的可信基准值比对。

（11）步骤（10）比对通过说明 eTSB 软件基未被篡改，eTSB 状态可信。

（12）eTSB 解析 gTSB 下发的度量指令，根据步骤（7）返回的可信策略，调用扩展终端 A 的系统管控服务发起 A 终端引导程序、系统内核、系统镜像及系统应用文件的可信度量，生成可信度量值 $value_1 = [v_1, v_2, \cdots, v_n]$ 并与步骤（2）存放在 TEE 中的初始度量值 $value_0$ 比较。

（13）步骤（12）比对通过，说明步骤（1）~（11）时序过程扩展终端 A 状态可信；eTSB 将 $value_1$ 经 Tc_Keys_Enc 公钥加密、Tc_Prik_Sig 签名后上报至 gTSB，同时携带主节点可信根标识 Tc_ID。

（14）gTSB 获取步骤（13）中的 $value_1$ 密文、签名信息后，调用步骤（4）中 TPCM/TCM 对应 A 的签名公钥 Tc_Pubk_Sig 验签、调用 Tc_Keys_Enc 私钥解密 $value_1$ 密文，得到 $value_1$。

（15）gTSB 调用 TPCM/TCM 将 $value_1$ 按照 PCR 寄存器度量结果算法：

$$hash_i = ePCR_{i+1} = SM3.\ Hash\ [ePCR_i \| value_1]$$

生成本次度量结果 $hash_i$，写入 ePCR 平台配置寄存器中。若判定本次结果写入为 ePCR 寄存器首次写操作，则 gTSB 将本次 $hash_i$ 作为扩展终端 A 的可信基准存入 gTSB 中的可信基准库中。

（16）流程结束。

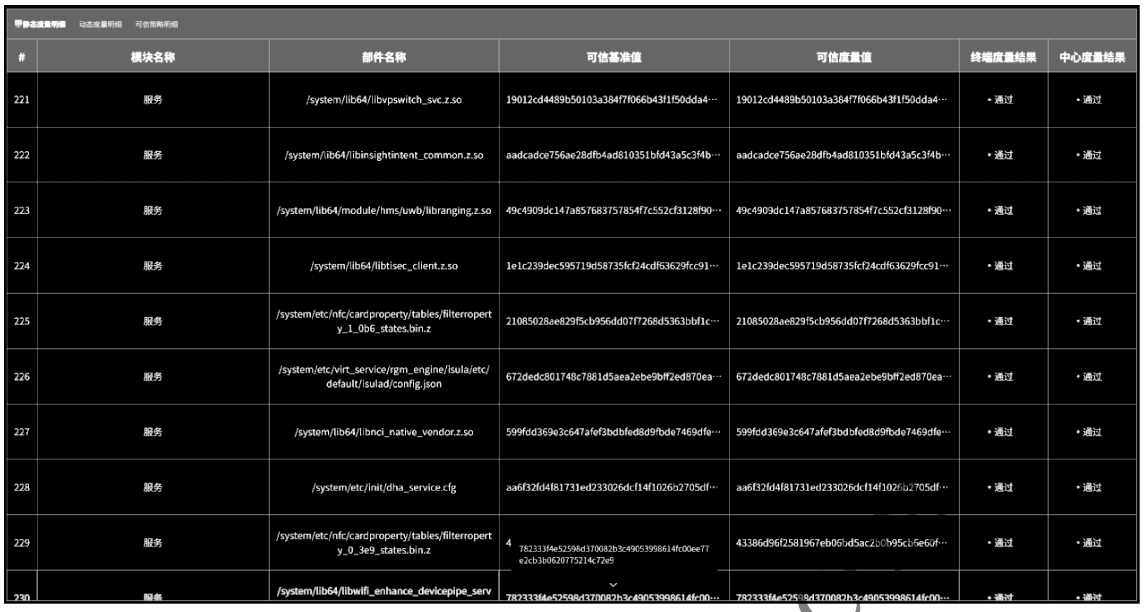
3.3 验证分析

验证过程以端边体系中的边缘网关物理可信根构建扩展类终端的可信信任链起始，可信信任链逐级度量获取扩展类终端的可信度量值，通过 TPCM/TCM 内置国密算法生成扩展类终端的可信状态结果值，将以上数值存入边缘网关的物理可信根 PCR 寄存器。智能手表度量结果如图 5 所示。

本文提出的可信防护方案围绕端边体系可信计算防护难点以及安全体系异构的现状问题，基于可信计算、国产商用密码及身份认证等技术实现端边体系扩展类终端的可信度量，符合公安移动警务领域相关规范性文件和技术标准要求。

4 结论

本文提出一种适用于移动警务场景的端边架构可信防护策略与度量方法，该方法严格遵循现有移动警务可信计算体系架构，深度契合端边协同新架构特性及扩展类终端安全需求。基于可信计算理论，综合运用设备身份认证、国密数字证书体系，结合 SM2/SM3 密码算法与随机选择算法，实现对边缘智能无线网关终端及扩展类



#	模块名称	部件名称	可信基准值	可信度量值	终端度量结果	中心度量结果
221	服务	/system/lib64/libvpswitch_svc.z.so	19012cd4489b50103a384f7f066b43f1f50dda4…	19012cd4489b50103a384f7f066b43f1f50dda4…	• 通过	• 通过
222	服务	/system/lib64/libinsightintent_common.z.so	aadcadce756ae28dfb4ad810351bfd43a5c3f4b…	aadcadce756ae28dfb4ad810351bfd43a5c3f4b…	• 通过	• 通过
223	服务	/system/lib64/module/hms/uwb/libranging.z.so	49c4909dc147a857683757854f7c552cf3128f90…	49c4909dc147a857683757854f7c552cf3128f90…	• 通过	• 通过
224	服务	/system/lib64/libtisec_client.z.so	1e1c239dec595719d58735fcf24cdf63629fcc91…	1e1c239dec595719d58735fcf24cdf63629fcc91…	• 通过	• 通过
225	服务	/system/etc/nfc/cardproperty/tables/filterroperty_1_0b6_states.bin.z	21085028ae829f5cb956dd07f7268d5363bbf1c…	21085028ae829f5cb956dd07f7268d5363bbf1c…	• 通过	• 通过
226	服务	/system/etc/virt_service/rgm_engine/isula/etc/default/isulad/config.json	672dedc801748c7881d5aea2ebe9bff2ed870ea…	672dedc801748c7881d5aea2ebe9bff2ed870ea…	• 通过	• 通过
227	服务	/system/lib64/libnci_native_vendor.z.so	599fdd369e3c647afef3bdbfed8d9fbde7469dfe…	599fdd369e3c647afef3bdbfed8d9fbde7469dfe…	• 通过	• 通过
228	服务	/system/etc/init/dha_service.cfg	aa6f32fd4f81731ed233026dcf14f1026b2705df…	aa6f32fd4f81731ed233026dcf14f1026b2705df…	• 通过	• 通过
229	服务	/system/etc/nfc/cardproperty/tables/filterroperty_0_3e9_states.bin.z	4 782333f4e52598d370082b3c49053998614fc00ee77e2cb3b0620775214c72e8	43386d96f2581967eb06bd5ac2b0b95cb5e6bf…	• 通过	• 通过
230	服务	/system/lib64/libwifi_enhance_devicepipe_serv	782333f4e52598d370082b3c49053998614fc00…	782333f4e52598d370082b3c49053998614fc00…	• 通过	• 通过

图 5　智能手表可信度量结果

移动终端（涵盖智能手表、智能手环、智能车载终端等可穿戴设备）的可信防护。文中提出的方案解决了扩展类智能终端在移动警务端边架构中的可信防护难题，实时验证终端操作系统与应用程序的完整性，将扩展类终端运行时的可信状态监测无缝接入公安统一移动警务可信管理平台。在信任链构建方面，创新采用接力递进式传递策略，以物理可信根作为信任链起点，通过细粒度策略决策机制，推动传统可信计算标准架构的演进升级，填补了规格较低、数量较大的物联网设备的可信计算防护缺口，为公安及其他行业在移动终端安全可信保障与风险监测领域提供了可靠的技术解决方案，在实际应用中具有重要的参考意义。

参考文献

[1] 沈昌祥. 可信计算平台与安全操作系统 [J]. 网络安全技术与应用，2005（4）：8－9.

[2] 沈昌祥. 用主动免疫可信计算 3.0 筑牢网络安全防线营造清朗的网络空间 [J]. 信息安全研究，2018，4（4）：282－302.

[3] 中华人民共和国公安部. 智能手机型移动警务终端 第 1 部分：技术要求（GA/T 1466.1－2018）[S]. 2018.

[4] 中华人民共和国公安部. 智能手机型移动警务终端 第 2 部分：安全监控组件技术规范（GA/T 1466.2－2018）[S]. 2018.

[5] ARTHUR W, CHALLENER D, GOLDMAN K. A Pratical Guide to TPM2.0 [S]. 2015.

[6] National Institute of Standards and Technology, U.S. Department of Commerce. Special publication 800－111 guide to storage encryption technologies for end user devices [S]. 2007.

[7] National Institute of Standards and Technology, U.S. Department of Commerce. Special publication 800－164 guidelines on hardware-rooted security in mobile devices (Draft) [Z]. 2012.

[8] GILMAN E, BARTH D. Zero trust networks, building secure systems in untrusted networks [Z]. O'Reilly, 2017.

[9] 中华人民共和国公安部. 移动警务可信计算总体技术要求（GA/T 2001－2022）[S]. 2022.

[10] 张焕国，罗捷，金刚，等. 可信计算研究进展 [J]. 武汉大学学报（理学版），2006（5）：513－518.

[11] 郭晨雪，王超，姬胜凯. 可信计算信任链技术研究[J]. 网络安全技术与应用，2023（6）：19－20.

[12] 苑洁，李小勇. 云边端可信协同关键技术研究 [M]. 北京：北京邮电大学出版社，2024.

[13] 周棟淞，彭泓力，杨洁. 基于可变长信任链的实时操作系统软件可信度量技术[J]. 通信技术，2024，57（10）：1088－1094.

[14] 中华人民共和国国家密码管理局. SSL VPN 技术规范（GM/T 0024－2023）[S]. 2023.

[15] 中华人民共和国国家密码管理局. 可信计算 TCM 服务模块接口规范（GM/T 0058－2018）[S]. 2018.

（收稿日期：2025－06－04）

作者简介：

赵荣辉（1985－），通信作者，男，硕士，副研究员，主要研究方向：移动通信、信息安全。E-mail：rhzhao@sonicom.com.cn。

王志宇（1977－），男，硕士，副研究员，主要研究方向：移动通信、信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部