



基于用户卡的可信执行环境初始化方案

王磊¹, 鲁萌²

(1. 中国电信股份有限公司广州研究院, 广东 广州 510630; 2. 中国信息通信研究院, 北京 100191)

摘 要: 智能终端具备的可信执行环境在加载环节存在加载证书权威性问题的。在分析可信执行环境(TEE)初始化架构和初始化方案的基础上, 利用信任链技术, 设计提出了将运营商用户卡作为可信根, 进行智能终端可信执行环境初始化的方案, 为电信运营商利用用户卡资源参与可信执行环境的产业链建设提供思路。

关键词: 用户卡; 卡初始化; 可信执行环境

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017034

Initialization scheme of the trusted execution environment based on the user card

WANG Lei¹, LU Meng²

1. Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

2. China Academy of Information and Communication Technology, Beijing 100191, China

Abstract: Smartphones with a trusted execution environment (TEE) has an authority issue of the certificate with the loading stage. Based on the analysis of the initialization architecture and initializing scheme of the trusted execution environment, by using trust chain technology, a scheme was proposed to initialize the trusted terminal of the operator's card as the trusted root, and ideas were provided for the telecom operators to use the user card resources to participate in the construction of the industrial chain of the trusted execution environment.

Key words: user card, card initialization, trusted execution environment

1 引言

随着集成电路、移动智能操作系统和移动应用的快速发展, 移动智能终端的计算、存储和通信能力不断提升, 但同时也面临更多的安全威胁和风险。智能终端在安全支付、企业服务和基于 Web 的服务中扮演着越来越重要的角色, 终端安全正成为保护消费者和企业利益的强制性要求。

移动嵌入式处理器主流供应商 ARM 提出了一套基于 TrustZone 技术的系统级安全解决方案, 该技术是在尽量不影响系统功耗和性能的前提下, 通过硬件来实现安全环境

与普通环境的隔离, 并通过软件提供基本的安全服务和接口, 构建由软硬件结合的系统级安全。方案通过将保护措施集成到 ARM 处理器、总线架构和系统外设 IP 地址等措施, 保证安全内存、加密块、键盘和显示器等外设免遭软件攻击, 并建立一个隔离的可信执行环境 (trusted execution environment, TEE) 为安全敏感应用提供安全服务^[1]。

在基于 TrustZone 架构的 TEE 初始化过程中, 一个可靠的可信根是整个系统安全的基石, 但目前该可信根一般由片上系统固化的设备密钥来提供, 这种方式会存在系统密钥更新困难、无法针对每个用户进行个性化的 TEE 初



始化等问题^[2]。从而使攻击者有机会采用如离线攻击等方式干扰终端 TEE 初始化过程,或通过可信根进行旁路攻击,增加系统运行恶意代码的风险。

2 基于 TrustZone 技术的 TEE 架构

2.1 TrustZone 软硬件架构

TrustZone 将单颗 CPU 内核隔离成安全和普通两个逻辑区域:安全内核和普通内核,CPU 以时分方式执行普通和安全内核的代码,该架构通过处理器硬件扩展的方式来保证安全内存和安全外设可以拒绝非安全事务的访问而无需使用专用安全处理器,从而达到节省芯片面积和功耗的目的。为了隔离所有的 SoC 资源,该架构首先对内存进行了隔离,CPU 在安全环境(即 TEE)和普通环境(即 rich execution environment,REE)下的进程有独立的物理地址空间,TEE 有权访问两个环境的地址空间,但 REE 只能访问普通环境的地址空间。TEE 和 REE 通过监控模式在两个环境间进行通信和切换,REE 可通过安全监控调用指令(secure monitor call,SMC)或者硬件中断方式进入监视模式;TEE 进入监视模式的方式相对灵活,可通过直接写程序状态寄存器(current program status register,CPSR)或硬件中断进入监视模式。为防止恶意软件采用中断向量方式对系统造成破坏,架构还对中断向量进行了扩展,在普通环境和安全环境分别采用 IRQ 和 FIQ 作为中断源。TrustZone 的硬件架构如图 1 所示。

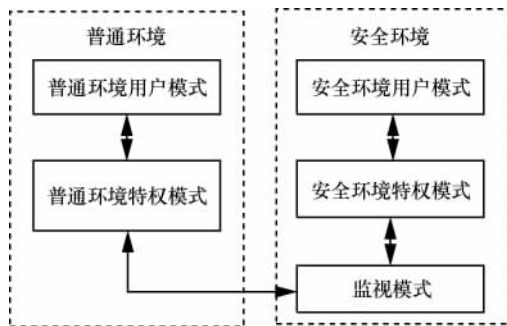


图 1 TrustZone 硬件架构

在上述硬件架构的基础上,TrustZone 将安全性从普通操作系统(即 rich OS,ROS)中分离出来,并实现新的安全操作系统(即 trust OS,TOS),并具备独立的中断处理、调度、进程和内容管理表,TOS 和 ROS 间的交互被限制在消息传递和共享内存传递数据。TrustZone 定义了一套 API 标准,其中 REE 下的 API 提供运行于 REE 的可信应用访问

TEE 中的应用及与应用进行数据交换的底层通信接口;TEE 下的 API 向 TEE 中的可信应用提供访问操作系统核心服务(如可信存储)的接口^[3]。TrustZone 的软件架构如图 2 所示。

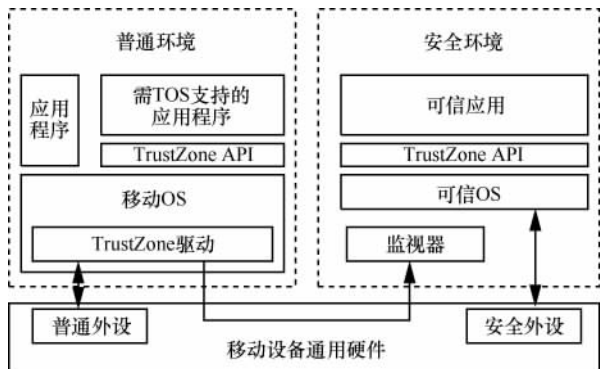


图 2 TrustZone 软件架构

2.2 基于 TrustZone 的 TEE 架构设计

智能卡及终端安全的标准组织 GP(Global Platform)基于 TrustZone 技术制定了 TEE 标准,TEE 可作为一个独立的执行环境,驻留在其所连接的支持 TrustZone 主处理器上的安全区域,从而确保在 TEE 中实现敏感数据的存储、处理和保护,其 TEE 系统架构如图 3 所示^[4]。

2.3 常规 TEE 初始化过程

基于 TrustZone 的 TEE 设备在开启时,其初始化过程分为两个阶段:通过安全初始化的方式启动 TEE;然后基于 TEE 的安全服务,通过可信初始化的方式启动 REE,一级认证一级,一级信任一级^[5]。初始化过程如图 4 所示。

当移动设备启动时,安全初始化过程首先执行固定区域 ROM 里的代码,启动 TEE BootLoader,然后加载 TOS 并开启各种安全服务。在安全初始化过程中,每个执行的模块须对下一个模块的代码执行完整性校验,完整性校验依赖于存储在 SoC 上的代码完整性证书,如果校验失败,则引导过程终止。TEE 启动后会开启可信验证服务,可利用其提供的可信功能接口进行后续代码的完整性度量,因此 REE 的初始化引导过程将只进行完整性度量和记录,不做校验,度量结果由可信验证服务提供完整性保护。由此可见,安全初始化的信任根为 SoCROM,可信初始化的信任根为 TEE 及其中的安全服务,从而形成一条完整的信任链。

3 常规初始化方案的不足

一个安全可靠的可信根是整个移动系统安全的基础,

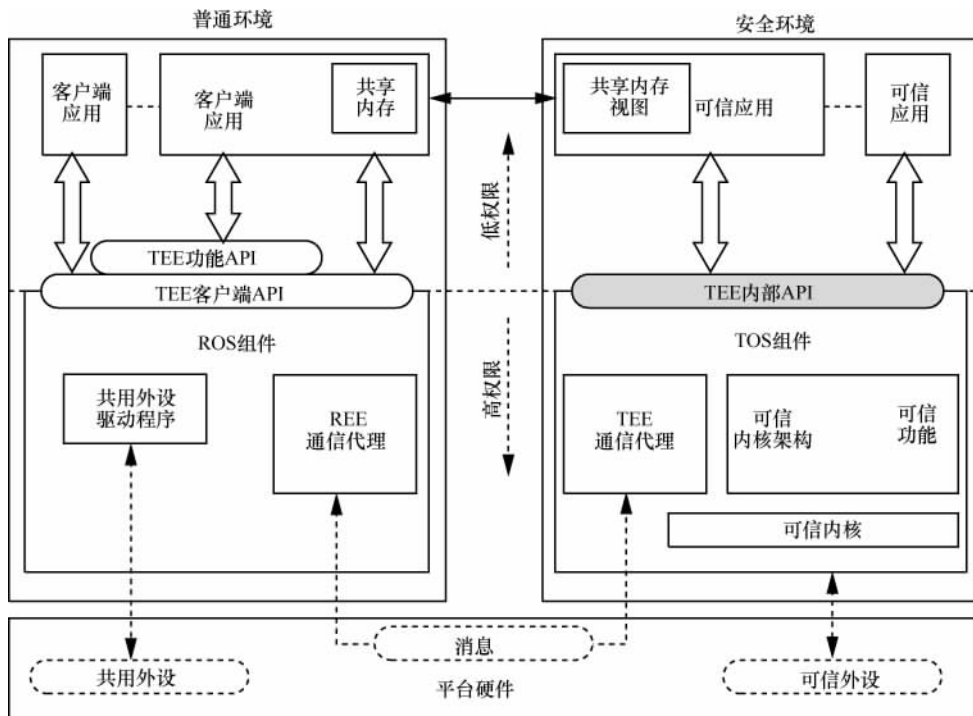


图3 GP TEE 系统架构

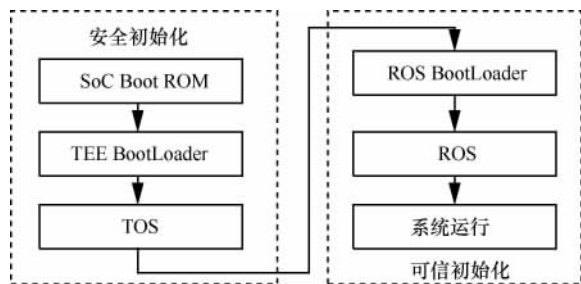


图4 常规 TEE 初始化过程

而目前基于 TrustZone 架构的可信根是由 SoC 上固化的设备密钥充当的,这种方式会使系统密钥更新存在困难,而且设备密钥固化存储在设备上,入侵者可能通过旁路或逆向工程等手段获得密钥,从而导致整个平台的安全性风险。此外,该方式也存在无法针对每个用户进行个性化的 TEE 初始化的问题。因此,如何在不变更 TrustZone 架构的前提下,向系统提供一个可灵活更改并防御软件攻击的信任根,是一个需重点考虑的问题。此外,TEE 虽然向应用程序提供了一个隔离的执行环境,但却未向用户或远程者证明这个环境是可信的,上述不足可以通过基于用户卡的 TEE 初始化方案加以弥补。

4 基于用户卡的 TEE 初始化方案

TEE 初始化是终端准备和设置 TEE 的过程,是 TEE

启动后到正常使用过程中的关键环节,经过这个环节,TEE 才可以向用户提供服务。TEE 初始化过程中,需要对 TEE 进行一系列的设置,并写入一系列的初始化参数,其中关键操作是写入 TEE 的信任根(包括各类基础密钥),只有完成了这个步骤 TEE 才可能成为一个可信实体,并具备向外部提供安全服务的能力。而用户卡存储了移动用户信息、加解密密钥等内容,可以实现身份认证、完整性度量以及用户数据加密/解密等功能,因其具有运算功能,能够通过自身安全机制确保自身内部静态数据和智能终端传输过程中数据的安全。TEEMP (trusted execution environment management platform,可信环境管理平台)实现对终端 TEE 环境中 TA(trusted application,可信应用)、SD (secure domain,安全域)的管理,执行安装、卸载、更新、锁定和解锁等操作;并同时为 TEE 进行管理,执行密钥更新、锁定、解锁和恢复出厂等操作。

本方案利用用户卡的安全存储能力,并通过智能终端与 TEEMP 之间的双向安全认证过程,实现 TEEMP 向智能终端 TEE 中安全地写入 TEE 配置参数,完成移动智能终端的 TEE 初始化。基于用户卡的 TEE 初始化方案架构如图 5 所示。

4.1 初始化方案框架设计

该方案要求支持 UICC 架构的用户卡已经预置或动态

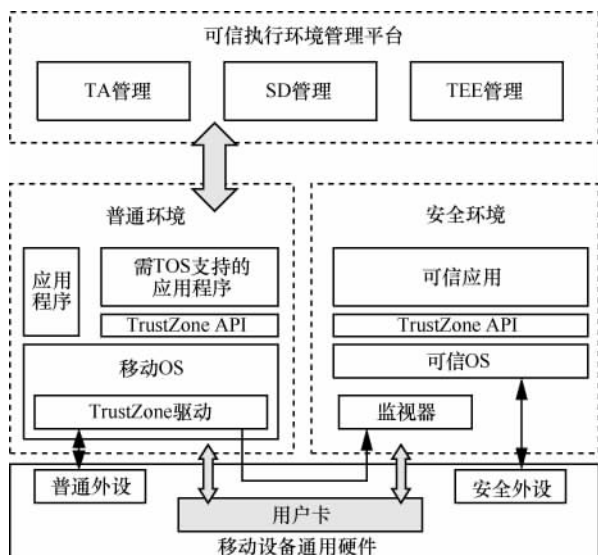


图5 基于用户卡的可信执行环境初始化方案架构

下载了TEEMP的证书,并且智能终端的TEE中已预置终端证书及私钥,支持OMA接口,具备访问用户卡的能力。终端TEE能够通过安全通道访问终端REE,并能够通过REE接口API访问用户卡。TEEMP已经预置了REE中认证应用CA的根证书,用于验证终端证书,并已经配置了终端TEE的个人化参数,用于TEE初始化。针对智能终端基于用户卡的TEE初始化,涉及如图6所示的方案框架。

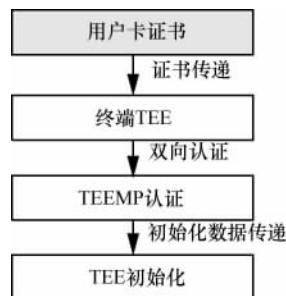


图6 基于用户卡的TEE初始化框架

TEE会首先获取用户卡中的TEEMP证书,并通过TEE与TEEMP间的安全通道(HTTPS)与TEEMP进行双向认证,认证通过后,TEEMP传递初始化数据对TEE进行初始化。

4.2 初始化流程

终端在启动时会自动检测TEE的初始化状态,如发现TEE尚未初始化,则会触发自动初始化过程。当用户更换UIM卡后,系统在启动时可检测到TEE服务提供方已更换,用户可以选择重新对TEE进行初始化,否则无法继续使用终端原TEE配置。TEE初始化的总体业务流程如图7所示。

具体流程如下:终端启动时,会首先检查用户卡状态并判断TEE是否已经完成初始化。当检测到TEE未初始

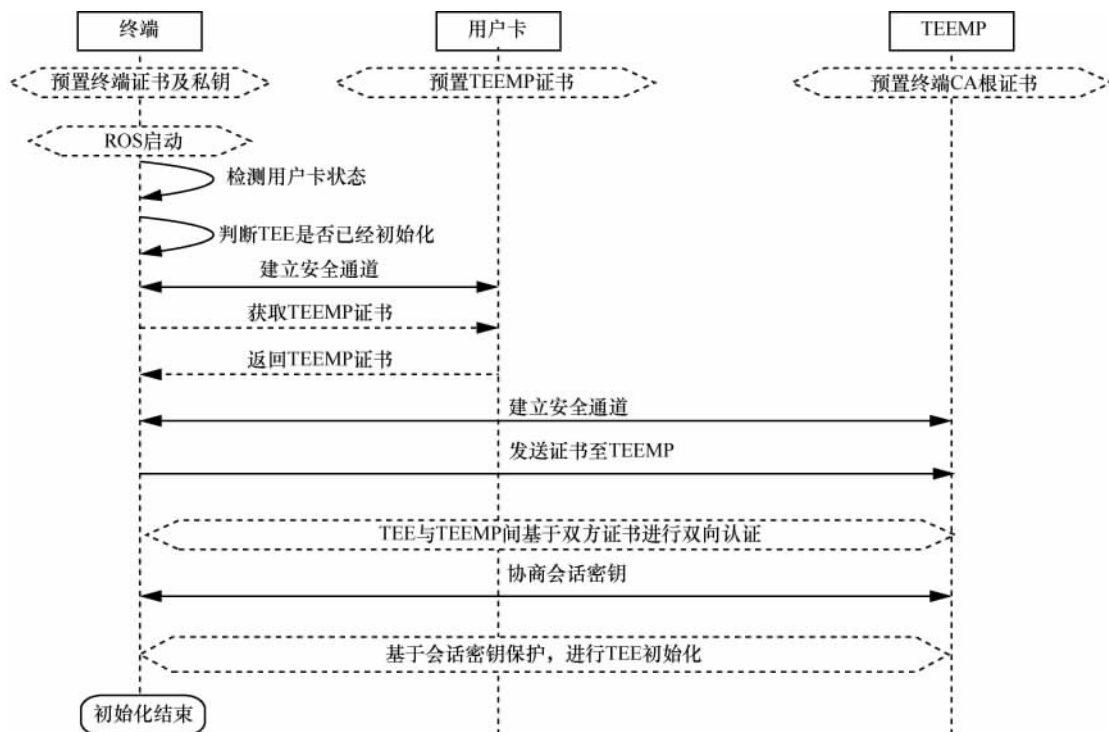


图7 TEE初始化的总体业务流程

化时,会通过机卡安全通道向用户卡获取 TEEMP 证书,如果用户卡无法给出 TEEMP 证书,则说明该用户卡并非运营商发行的用于初始化 TEE 的常规用户卡,TEE 只需执行无需用户卡参与的常规初始化过程,建立 TEE,而无需对运营商的 SD、TA 等 TEE 进行初始化。一旦 TEE 从用户卡中获取到 TEEMP 证书后,会通过 ROS 建立与 TEEMP 间的安全通道,将 TEEMP 证书传递给 TEEMP,进行卡有效性校验和 TEEMP 的有效性校验。TEE 与 TEEMP 间的双向校验完成后即协商会话密钥,并使用该密钥对两者之间传递 TEE 初始化相关数据的会话进行加密保护。

在这一过程中,终端 TEE 与 TEEMP 间的基于证书的双向认证流程如图 8 所示。

终端 TEE 首先通过验证 TEEMP 证书的方式对 TEEMP 的合法性进行验证,然后 TEEMP 采用相同方式验

证终端合法性。当双方完成验证后,开始会话密钥协商过程并确定加密方案和会话密钥,会话密钥确定后即开始 TEE 初始化数据的加密传输过程。

4.3 初始化方案评估

TrustZone 系统的软硬件组合向用户提供了定制 TEE 初始化方案的可能。采用用户卡进行 TEE 初始化的方案借助了一个可信实体——用户卡,能够保证终端启动后信任链仍然有效,可以有效防止以 CA 等软件形式对 TEE 进行初始化时,终端操作系统可能面临的风险。

用户卡是电信运营商联系用户的重要纽带,采用用户卡对用户 TEE 初始化后,运营商能够借助 TEEMP 对用户 TEE 进行有效管理:一方面能够有效避免第三方平台可能存在的客户隐私泄露和权限滥用问题;另一方面能够保证在用户换卡后,通过号码关联用户原有配置并自动完成用户 TEE 的初始化,并可以对用户 TEE 进行动态地可信更

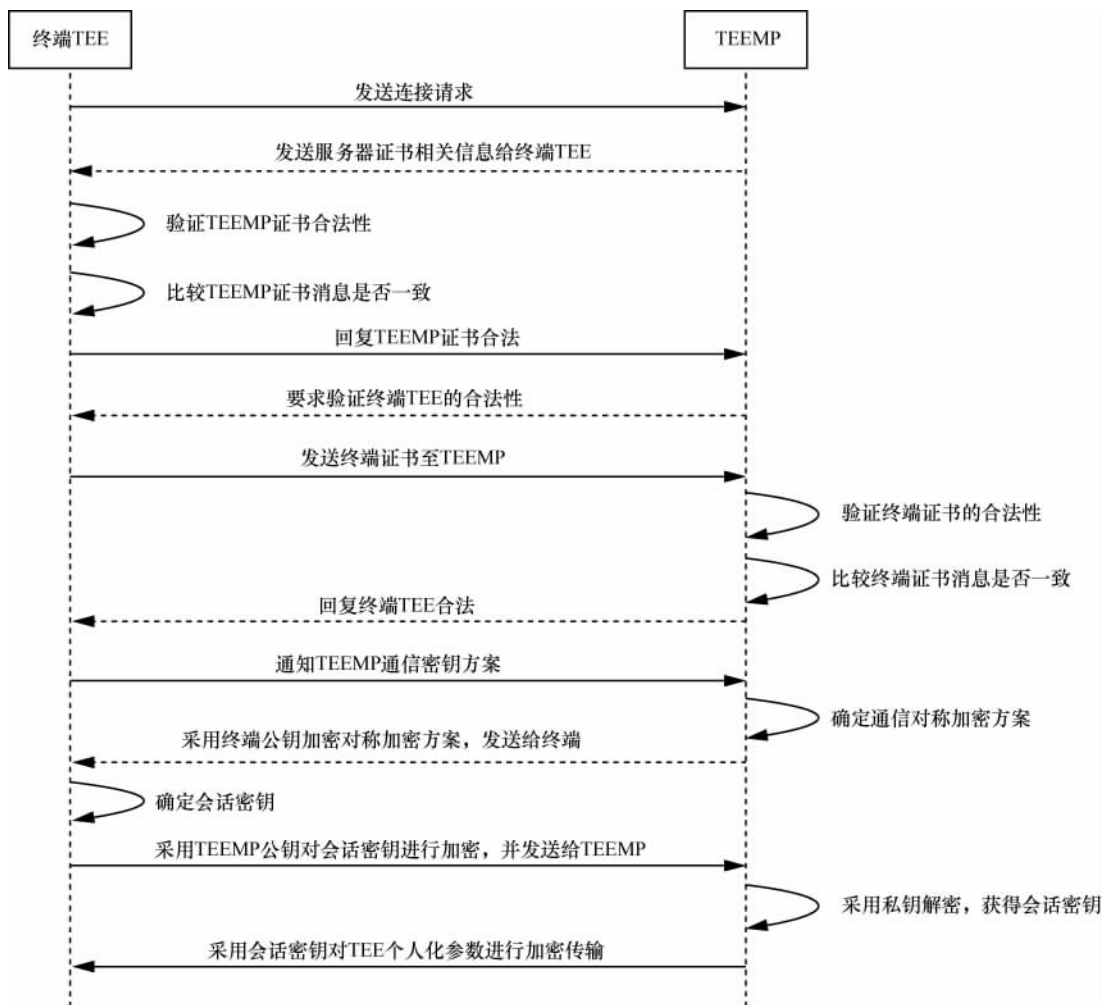


图 8 终端 TEE 与 TEEMP 间的基于证书的双向认证流程



新,保证用户可信环境的有效性。

而针对 TrustZone 架构下,TEE 虽保证了 TA 的运行安全,但无法通过自身功能向用户或远程应用提供证明凭证的问题,本方案可以结合运营在 TEE 中的 TA 提供远程证明功能加以实现。TEE 可以保证 TA 运行 TEE 中,而 TA 可以远程证明 TOS 是可信的。

5 结束语

由本文的分析可知,TEE 作为一种基于硬件隔离的安全解决方案,在有效地提升移动终端安全性的同时也面临一些不足。采用用户卡对 TEE 进行初始化的方案能够满足终端开机后对 TEE 进行动态可信初始化的需求,此外,该方法还可实现 TEE 的动态可信更新,对于对数据安全性要求较高的行业类终端,可以充分利用卡+终端的能力保证客户终端安全。

参考文献:

- [1] ANWAR W, LINDSKOG D, ZAVARSKY P, et al. Redesigning secure element access control for NFC enabled Android smartphones using mobile trusted computing[C]//The 2013 IEEE International Conference on Information Society, June 24-26, 2013, Toronto, Canada. New Jersey: IEEE Press, 2013: 27-34.
- [2] ZHENG X Y. Analysis and research of TrustZone technology[J]. Chinese Journal of Computers, 2016(9): 1912-1928.
- [3] Global Platform device technology. TEE system architecture version 1.0. technical report GPD_SPE_009, global platform.org [R/OL]. (2011-12-01)[2016-12-02]. <http://www.globalplatform.org/specificationsdevice.asp>.
- [4] GlobalPlatform Inc. GlobalPlatform device technology TEE system architecture version 1.0[EB/OL]. (2011-12-01)[2016-12-02]. <http://www.globalplatform.org/specificationsdevice.asp>.
- [5] Unified extensible firmware interface specification, version 2.4 [EB/OL]. (2014-12-01)[2016-12-02]. https://www.baidu.com/link?url=V5ABpKe6y6sK0qCg18NU4Ia42HpUazbjaKTbRzA3h8uS0_cIzXjXjHoYVM78gY_G&wd=&eqid=a20d780700003c540000000358845f61.
- [6] 焦四辈, 杨正军, 国炜, 等. 智能终端可信执行环境安全性分析[J]. 互联网天地, 2016(8): 8-13.
- JIAO S B, YANG Z J, GUO W, et al. Analysis of security on intelligent terminal trusted execution environment[J]. China Internet, 2016(8): 8-13.

[作者简介]



王磊(1982-),男,现就职于中国电信股份有限公司广州研究院,主要研究方向为智能终端安全、物联网技术和安全方案。

鲁萌(1984-),女,现就职于中国信息通信研究院,主要研究方向为大数据安全。