

基于加密 SD 卡的内网移动终端可信接入方案

李济洋^{1,2}, 赵鹏远^{1,2,3}, 刘喆^{1,2}

(1. 武汉大学国家网络安全学院, 湖北 武汉 430072;

2. 武汉大学空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430072;

3. 河北大学网络空间安全与计算机学院, 河北 保定 071002)

摘要: 为了解决因不可信移动终端非法接入内网导致的信息安全问题, 设计了一种基于加密 SD 卡的内网移动终端可信接入方案。通过可信计算技术, 以加密 SD 卡作为可信硬件设备实现了移动终端设备的可信启动、完整性验证与内网可信接入, 并对接入后移动终端与内网的数据交互过程提供了一种加密通信安全存储机制。实验结果表明, 该方案在不改变移动终端基本架构的前提下, 较为高效地对移动终端进行安全性认证, 并在一定程度上保护内网环境的安全。

关键词: 移动终端; 可信计算; 加密 SD 卡; 完整性度量

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019042

Trusted access scheme for intranet mobile terminal based on encrypted SD card

LI Jiyang^{1,2}, ZHAO Pengyuan^{1,2,3}, LIU Zhe^{1,2}

1. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

2. Key Laboratory of Aerospace Information Security & Trusted Computing, Ministry of Education, Wuhan University, Wuhan 430072, China

3. School of Cyber Science and Engineering, Hebei University, Baoding 071002, China

Abstract: In order to solve the problem of information security caused by illegal access of untrusted mobile terminals to intranet, a trusted access scheme for intranet mobile terminals based on encrypted SD card is designed. By using encrypted SD card as trusted hardware equipment, trusted start-up, integrity verification and Intranet trusted access of mobile terminal devices are realized. A secure storage and encrypted communication mechanism for data interaction between mobile terminal and Intranet is also created. The experimental results show that the scheme can effectively authenticate the security of mobile terminals without changing the basic architecture of mobile terminals, and to some extent protect the security of the Intranet environment.

Key words: mobile terminal, trusted computing, encrypted SD card, integrity measurement

收稿日期: 2019-04-02; 修回日期: 2019-06-06

通信作者: 李济洋, ninjalee@whu.edu.cn

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA016002)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016002)

论文引用格式: 李济洋, 赵鹏远, 刘喆. 基于加密 SD 卡的内网移动终端可信接入方案[J]. 网络与信息安全学报, 2019, 5(4): 108-118.

LI J Y, ZHAO P Y, LIU Z. Trusted access scheme for intranet mobile terminal based on encrypted SD card [J]. Chinese Journal of Network and Information Security, 2019, 5(4): 108-118.

1 引言

随着信息技术的不断进步,智能终端产品不断更新换代,整个信息产业领域早已迈入移动互联网时代。近十年来,移动终端硬件性能配置与操作系统效率不断提升,智能移动终端的计算能力相较于传统终端已毫不逊色,应该领域也变得更加广泛,经济、文化、教育、能源甚至政治、军事等领域智能移动终端的普及率已不亚于 PC 终端。但在智能移动终端带给人们便携和高效的同时,许多安全问题随之而来。移动终端硬件架构与操作系统的日趋统一,在为移动终端应用开发提供优质环境的同时,为不法分子攻击提供了方便之门,这使移动终端中存在的安全问题越来越尖锐。

2017 年,中国互联网协会、国家互联网应急中心在京联合发布《中国移动互联网发展状况及其安全报告(2017)》^[1],该报告基于 CNCERT 抽样监测以及统计,2016 年仅智能手机一项中国大陆活跃设备数已达到 23.3 亿部,这一数据相较于 2015 年接近翻一番。而智能手机作为智能移动终端只是其中具有代表性的一部分,随着移动互联网产业的不断升级,智能移动终端早已不局限于智能手机,各种智能穿戴设备、智能家居设备、智能车载设备等层出不穷。在个人移动终端的应用之外,移动终端在政务、教育、交通、电力等国家重要组织机构中也得到了广泛使用。因其便携性与日益强大的数据处理能力,大量的业务数据通过移动终端进行采集和处理,与此同时,移动终端管理上的难度与数据泄露的风险也逐渐攀升。

从内部网络的整体系统来看,移动终端的可信只能保证内部网络中一个组成部分的可信,虽然引入可信计算平台对移动终端可以起到一定的防护作用^[2],然而要想不改变移动终端主板的原

生架构,并完成基于可信计算平台实现从用户到终端再到网络的整体安全可信,必须引入新的外置安全模块。在充分考虑用户不安因素的基础上,不仅要分别考虑用户、终端和网络的安全,还要将三者联动考虑,将用户、移动终端的安全状态延伸到整个网络,让整个网络变得安全可信,从而从根源上解决内部网络终端存在的安全威胁。基于上述安全问题,本文提出了一种内网移动终端可信接入方案,以解决内网环境中用于办公的移动终端接入认证方面的安全问题。

2 相关研究工作

目前,移动终端普及各个行业与领域,网络技术也发展迅速,内联网的安全性受到越来越多的关注,并出现了许多内网移动终端安全解决方案。可信计算基于硬件安全模块构建可信计算平台,使用可信平台模块(TPM)芯片,通过完整性度量、完整性验证、隔离修复等技术从系统底层开始通过层层度量认证设备安全性状态,并构建一条完整的信任链,从而构成一个安全可信的终端系统^[3-4]。可信计算组织曾成立了移动电话事业部(MPWG, mobile phone working group),试图在移动电话领域拓展可信计算业务,发布移动可信模块(MTM, mobile trusted module)相关使用规范,在移动电话中部署类似可信平台模块芯片解决移动电话的安全问题^[5]。由于早期移动电话智能化程度不高,从硬件配置到操作系统和 PC 平台均有较大区别,在移动终端上实现可信计算技术的具体方案最终未能落地。近年来,随着移动互联网的发展,移动终端的硬件架构、操作系统与业务能力逐步逼近 PC 终端,其安全需求也越来越高。学术界与工业界对移动终端设备安全问题不断重视,移动终端可信状态的研究与开发重新成为热点内容^[6]。郑宇等^[7]基于可信移动平台技术(TMP, trusted mobile platform)对终端内部

的相关认证信息安全传递问题进行了深入研究,该研究成果以 OMAP730 处理器搭建硬件平台基础,设计了 3 种可信终端方案,分别是内置软件形式 TPM、内置硬件形态 TPM 和外置的独立 TPM。陈书义等^[8]通过对终端安全边界组件的可信设计,实现了一种基于移动可信模块的可信平台体系。王晋等^[9]基于智能电网中移动终端应用场景,提出了一种基于内置可信硬件的智能移动终端远程证明方案。赵波等^[10]也提出了一种基于可信计算技术、面向嵌入式系统的安全启动机制,在嵌入式平台现有的硬件架构下,通过设计外置 TPM 模块,信任链从嵌入式终端 Bootloader 阶段开始,一直传递至上层应用程序,对嵌入式设备安全起到了一定保护作用。

上述工作多以 TPM 为终端设备的信任根,对于移动终端的使用环境及便携性要求没有进行进一步的研究与分析,无法直接应用于内网环境中使用的移动终端的可信性验证;而且对于接入服务器端的移动终端设备仅提供基础的完整性认证服务,针对终端与服务器的数据交互过程未能提供一套完整的解决方案。

3 基于可信计算的內网移动接入方案设计

3.1 內网移动终端可信接入架构

移动终端的可信接入过程主要分为 2 个阶段:第一阶段是移动终端内部完整性证明,通过引入可信硬件构建信任根,在移动终端内部实现 TPM 的相应功能,以构建信任链的方式将信任的状态一层一层传递到整个移动终端,完成移动终端内部可信环境的建立;第二阶段是移动终端可信接入,通过移动终端设备向内网服务端证明自身硬件以及软件配置信息等完整性状态符合相应的安全策略,从而允许移动终端设备的接入访问,实现移动终端设备的远程证明。在远程证明的完整性度量模型中,可信计算平台依靠 TPM 部件和平台完整性度量存储报告机制,向认证服务端报告平台或平台关键部件的完整性度量值^[10]。

在通过完整性校验、实现网络接入后,为了进一步保护移动终端设备接入过程中由内网服务端下载的业务数据,需要进行基于密码算法的加解密处理,使重要数据以密文的形式存储在终端设备上,且仅能通过安全应用访问读取,从而保

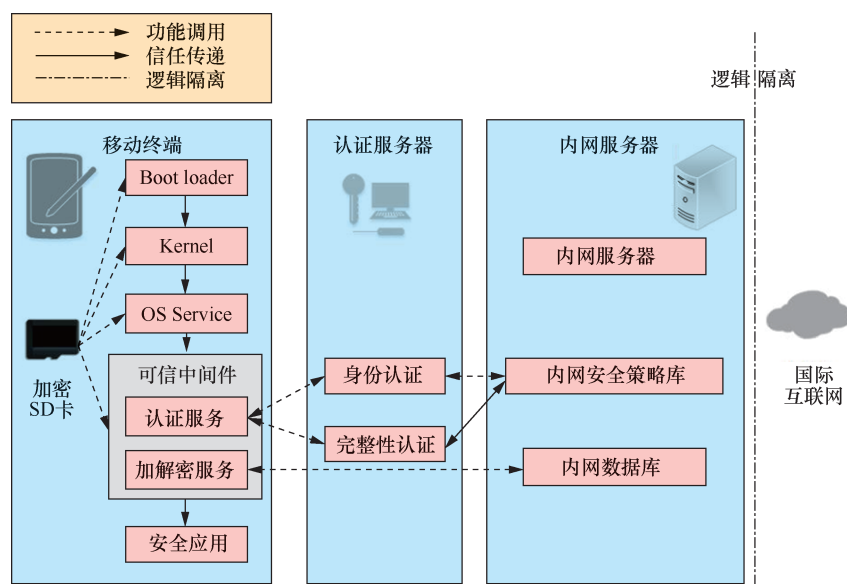


图 1 整体结构

证整个接入流程不会存在恶意入侵以及隐私泄露等安全问题^[11]。

本文所提接入方案采用加密 SD 卡作为移动终端可信接入的硬件基础，加密 SD 卡适用于标准 SD 卡槽（也可以通过读卡器接入 OTG 接口或者 Type-C 接口），在不改变移动终端硬件架构的前提下，适用于目前市面上大多数移动终端设备。加密 SD 卡提供读写、随机数生成、摘要算法、密钥生成、数据加解密、电子证书管理、安全存储空间等功能^[12]。本文方案利用加密 SD 卡的合规真随机数发生器生成密钥对 AIK (Pub, Prvt)，并将其存入安全存储空间中。在加密 SD 卡完成注册后，除非进行格式化，否则无法修改或者覆盖安全存储空间内的数据，从而确保密钥对 AIK (Pub, Prvt) 的唯一性和不可替代性^[13]，并以其为信任根，通过层层度量的信任传递方式构建信任链。对加密 SD 卡提供的各类密码算法进行统一整合封装为可信中间件，为远程证明、数据加密等安全功能提供技术支持。

3.2 内网移动终端可信接入模型

3.2.1 移动终端内部完整性证明模型

基于安全 SD 卡，将其作为外置可信平台模块，结合用户手动输入的 PIN 码实现信任基的构

建，并设计一种适用于移动终端的信任链模型，从 Bootloader 到上层应用程序启动过程中，各个组件的度量标准值由安全 TF 卡中的密钥签名存放，并进行度量对比，保证整个系统启动过程的可信，如图 2 所示。

整个移动终端可信启动流程如下。

步骤 1 引入第三方可信硬件设备安全 SD 卡，将具备度量功能的相关执行代码存放于安全 SD 卡的安全存储区域中，该区域受到硬件安全技术保护，设定其在任何情况下均不会受到非法入侵及篡改。则具备度量功能的 Boot loader 代码可以成为整个移动终端启动过程中的信任起点，提供最初始的信任状态。

步骤 2 移动终端设备通过电源加电启动后，首先从处理器片内 ROM 镜像的启动引导代码，引导移动终端系统开始执行 Boot loader 代码，并将其加载到设备内存中。Boot ROM 通过硬件方式固化在对应移动终端硬件设备中，用户不具备 Boot ROM 相关更改权限。

步骤 3 系统在 Boot loader 启动后，先完成硬件的初始化，然后对内核 Kernel 进行寻址，通过其中的度量功能，对内核 Kernel 进行可信度量，将度量值与预先存储在加密 SD 卡中的标准值进

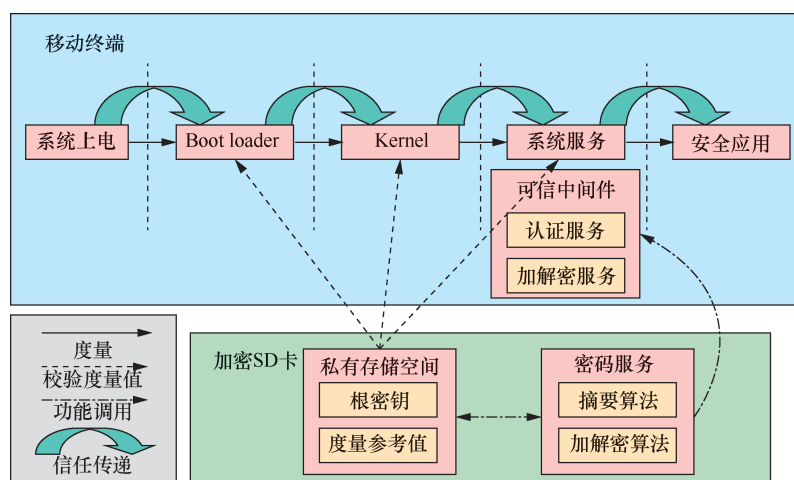


图2 信任链构建

行比对,如果比对结果一致,证明内核 Kernel 运行状态安全可信,则将控制权限赋予 Kernel。

步骤 4 移动终端内核 Kernel 装载完成,进一步完成各种软硬件环境的初始化,加载移动终端设备功能相关的各类驱动程序,挂载根文件系统,同时执行 Init 进程,完成软硬件环境初始化,启动移动终端设备操作系统。

步骤 5 移动终端操作系统启动完毕,准备执行各项身份认证、业务数据读写等工作。

3.2.2 移动终端可信接入模型

移动终端接入网络进行身份验证的流程中,有移动终端、内网服务端和认证服务器 3 个实体参与。加密 SD 卡在初始化过程中,生成了公私密钥对 AIK (Pub, Pvt) 且存入安全存储空间中。在加密 SD 卡完成注册后,除非进行格式化,否则无法修改或者覆盖安全存储空间内的数据,从而确保密钥对 AIK (Pub, Pvt) 的唯一性和不可替代性。将装载加密 SD 卡的移动终端视为一个

整体,通过随机数结合密钥对 AIK (Pub, Prvt) 的方式完成其身份认证,在利用移动终端可信中间件中认证服务模块模拟 TPM 对移动终端进行完整性度量^[14],将度量值存储在加密 SD 卡的私有存储区。

具体步骤如下。

步骤 1 移动终端通过安全应用向内网服务端发起网络接入请求,请求接入内网服务器: Req_Access (Client)。

步骤 2 内网服务端接受请求后,向认证服务器发送移动终端身份挑战请求,请求认证服务器发起移动终端的身份认证挑战: Rsp_Challenge(Server)。

步骤 3 认证服务器接受内网服务端的挑战请求后,向申请接入内网的移动终端发起身份认证挑战 Rsp_Challenge(Server)。

步骤 4 移动终端接收到认证服务器发送的挑战信息后,通过安全应用调用可信中间件(认

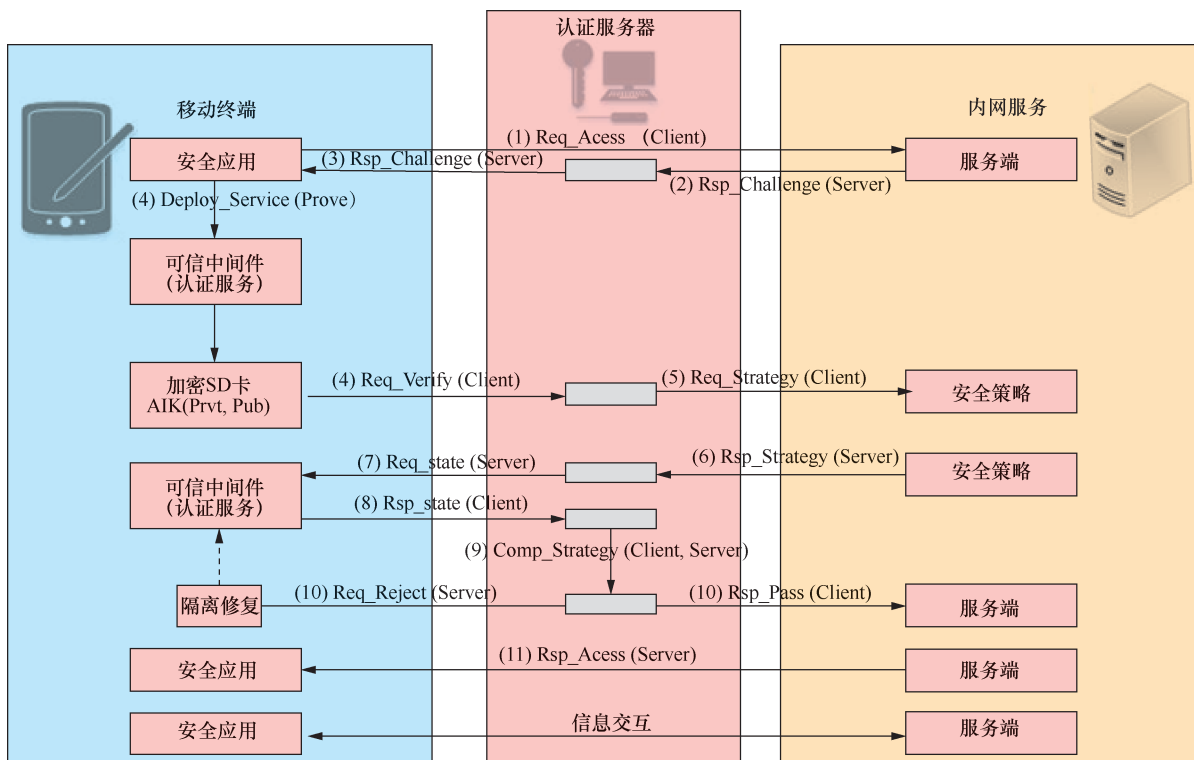


图3 接入认证模型

证服务),调用存储在SD卡安全空间中的公私密钥对 AIK (Pub, Prvt),通过公私密钥对配合随机数生成功能,完成可防制重放攻击的身份认证,将认证信息返回给认证服务器。

步骤 5 身份认证通过后,认证服务器向内网服务端反馈请求接入内网服务端的移动终端的身份信息,并且请求完整性策略: Req_Strategy(Client)。

步骤 6 内网服务端向认证服务器发送对移动终端要求的完整性策略: Rsp_Strategy (Server)。

步骤 7 认证服务器向移动终端发起完整性校验请求: Req_state (Server)。

步骤 8 移动终端度量完整性状态,并返回度量值至认证服务器,提供度量数据与完整性策略进行对比: Rsp_state (Client)。

步骤 9 认证服务器将完整性度量值与安全策略对比: Comp_Strategy (Client, Server)。

步骤 10 对比通过接入内网服务端,不通过则返回隔离修复,再次度量对比: Rsp_Pass (Client), Rsp_Reject (Server)。

步骤 11 通过接入,移动终端与内网服务器实现信息交互。

3.2.3 内网移动终端业务数据加密模型

移动终端接入内网服务器后,必然会与服务器之间进行各种数据的交互工作,如图4所示,本文方案提出了一套数据安全交互加密方法,从移动终端收发消息,均通过安全应用调用可信中间件基于加密SD卡提供的加解密服务接口,存储在移动终端的数据均以密文形式放置在加密SD卡的安全存储空间中,有效防护了由于移动终端的使用不当导致内网重要数据泄露风险。

具体工作流程如下。

步骤 1 移动终端通过安全应用请求从服务端下载数据: Req_Data(Download)。

步骤 2 外网服务端接收数据下载请求,进行传输数据: Rsp_Data(Server)。

步骤 3 通过可信中间件(加解密服务)在接入数据流写入存储空间前进行加密处理,写入存储空间的数据流,即密文: Encrypt (Storage)。

步骤 4 通过可信中间件(加解密服务)实现对数据的读写等操作: Decrypt (Read), Encrypt (Write)。

步骤 5 移动终端通过安全应用向服务端请求上传数据 Req_Data(Upload)。

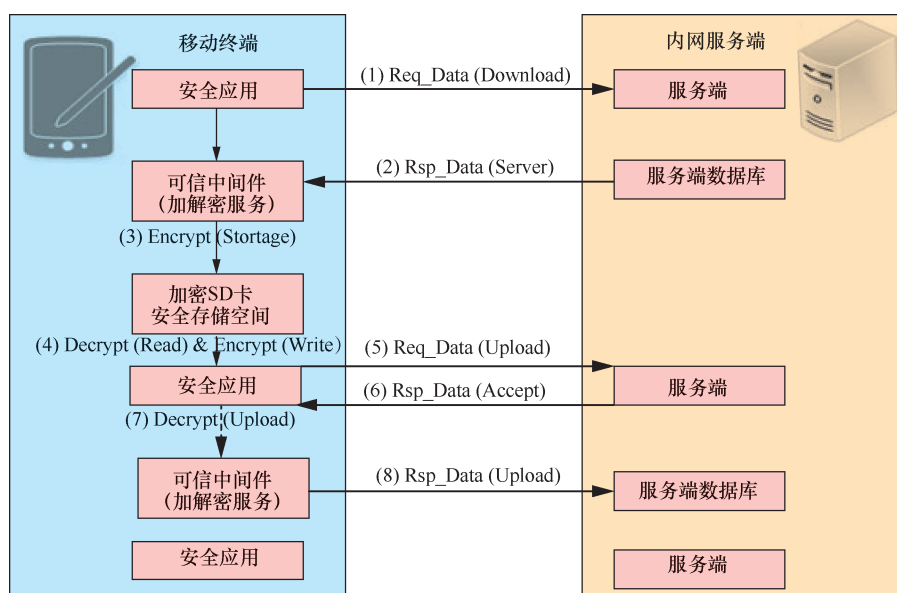


图4 数据加密

步骤 6 内网服务端接受上传请求：
Rsp_Data(Accept)。

步骤 7 安全应用通过可信中间件（加解密服务）对上传数据流进行解密操作：Decrypt (Upload)。

步骤 8 移动终端通过安全应用上传数据至服务端：Rsp_Data(Upload)。

4 实验方案

4.1 实验环境搭建

为了验证本文提出的基于加密 SD 卡的内网移动终端可信接入方案，搭建了对应的演示系统，并对其安全性功能与运行性能进行了测试，具体的硬件配置环境如下。

加密 SD 卡：三未信安公司生产的安全 microSD 卡，该安全 SD 卡采用国产安全芯片，内置自主版权的 SOC 操作系统；内置合规电子硬件随机数发生器（合规真随机数发生器满足国家随机数检验标准及 FIPS-140-2 安全标准）；提供安全存储空间，为数据与密钥提供硬件层面的安全保护，支持多密钥多证书安全加密存储；基于硬件的密码算法实现，支持国密算法及通用算法（公钥私钥加解密处理、数据摘要、签名验签等密码功能）。

移动终端环境：迅为 iTOP-4412 核心板，四核核心板，处理器方面搭载一块三星 Exynos4412 四核处理器、主频为 1.4 GHz；存储设备方面配置 1 GB DDR3 主存，8 GB eMMC 只读存储空间；电源方面配置三星电源管理芯片，同时适用 5 V 电源；扩展接口方面支持 SD/MMC/SDIO 接口存储卡扩展，最高支持 32 GB 存储扩展；同时支持 JPEG 硬件编解码；操作系统方面移植 Android 4.2.2 操作系统，对应内核版本为 Linux 3.0。符合本文方案对于移动终端平台的所有需求。

内网服务器模拟环境：Intel NUC, Core i5 5250U 处理器，1.6 GHz 主频，8.00 GB 内存，SUSE Linux

Enterprise 11 操作系统。

4.2 实验系统方案设计

4.2.1 移动终端内部完整性证明

使用模拟类似 TPM 可信根的部分功能，本文对功能接口进行封装，设计实现类似 TSS 的模拟可信根中间件。在安卓下对安全 SD 卡的访问接口进行封装，得到可供上层直接调用的接口包，实现了模拟可信根设备管理、国密算法调用、通用算法调用、远程证明等功能，包括实例创建、销毁，用户验证，密钥生成，密钥管理，安全散列，安全存储，随机数生成等。1) 连接、断开设备：连接加密 SD 卡后，创建设备实例，获取句柄，才能进行其他操作。断开与设备的连接后不能调用设备的任何功能。2) 访问控制：每个加密 SD 卡只设置一个用户，以 PIN 码认证。

未进行认证之前，可以使用安全 SD 卡的以下功能：生成随机数、对称密码算法、摘要算法、读写公有区文件等。用户认证通过后，除了上述功能，还可以进行以下操作：在安全 SD 卡内部生成非对称密钥并存储，非对称密钥的签名验签、加解密，证书的导入导出，私有区文件读写等。

由于安全 SD 卡的硬件特性，为了防御可能的攻击，在系统启动后，针对可信中间件的实时特性，设计了针对 Boot loader、Kernel 和安全 App 的完整性校验，终端用户可以实时对上述内容进行完整性校验，系统会给出相应反馈。该设计实现了应用场景交互过程中的按需度量，增加了攻击者对移动终端进行攻击的复杂度，有效增强了移动终端的安全性。在移动终端初次使用系统加电后，Boot loader 的程序对 Kernel 进行度量，调用 SHA1Input(&sha,(const unsigned char *) buf_kernel, 0x50000)，采用 SHA-1 算法得到 Hash 值作为各组件的摘要，初始生成的需要验证的模块度量值作为校验的标准值，调用 write_refvalue_emmc(CFG_KERNEL_OFFSET, Message_Digest)，

密封保存在安全 SD 卡的安全非易失存储空间中作为标准值。在移动终端后续工作过程中，每次启动过程均会调用完整性度量函数与完整性标准值，通过 `read_refvalue_emmc(CFG_KERNEL_OFFSET, PCR)` 读取度量值，调用 `cmp_pcr(Message_Digest, PCR)` 进行度量值验证：如果完整性验证通过，则继续启动内核；如果验证不通过，则认为其完整性被破坏，可能代码被篡改，需要提示用户并中断 Kernel 的启动过程。Kernel 启动后，系统调用安全 SD 卡中的 `sansec.SWSDDemo.sym`，并加载 Android 根文件系统。调用 `SWJAPI()` 和 `ShowMeasure()` 对 android 根文件系统中的关键应用程序进行安全度量。如果有不安全程序，则提示给用户；如果所有组件都通过安全度量，则 Android 系统完成安全启动全部过程。实现流程如图 5 所示。

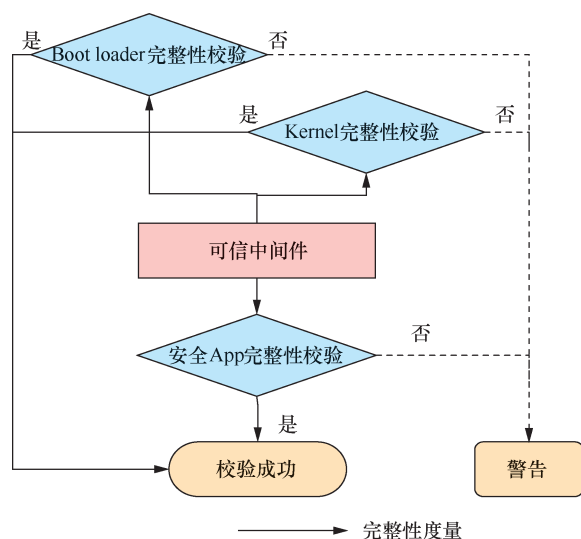


图5 可信中间件的完整性度量流程

4.2.2 移动终端可信接入内网

移动终端安全接入原型系统网络架构的实现如图 6 所示，其中，移动终端作为网络访问者，通过建立数据传输通道，向内部网络发起访问，通信服务器作为策略执行点，将访问请求发送给作为策略决策点的认证服务器，由认

证服务器的访问控制策略决定移动终端能否访问内网服务端。

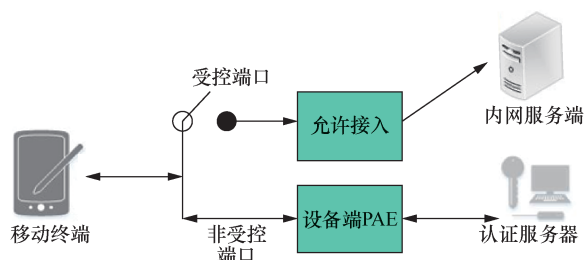


图6 访问控制实验模型

移动终端接收内网认证端的质询消息后，向对方报告身份信息和自身平台完整性信息，该过程分为 2 个阶段，即身份认证阶段和平台完整性认证阶段。移动终端身份认证在身份证明协议的规范下，调用 `SDKey` 实例生成随机数、执行密码运算等，向内网认证端发送相关证明信息，方法如下。

```

public Nar() {
    //移动终端作为访问请求者
    .....
    this.sdkey = sdkey;
    StartConnect();           //启动连接
    tncClient=new TNCClient(sdkey,this);
    SendAttestationMessage(); //发送证明信息
    .....
}
  
```

平台完整性认证中，移动终端接收到来自内网认证端的质询信息后，根据完整性证明协议，调用 `SDKey`，获取移动终端的平台完整性度量值，然后将相应度量值信息发送给内网认证端，接受认证，方法如下。

```

public class Attestation {
    public static final int TNC_PLATFORM_
    ATTESTATION=1; //平台身份证明标识

    public static final int TNC_INTEGRITY_
    ATTESTATION=2; //平台完整性证明标识

    int type=Utility.ByteArrayToInt ( Arrays.
  
```

```
copyOfRange(message,0,4);
    if (type == TNC_PLATFORM_ATTES-
TATION)                //平台身份证明
    {
        SendAttestationMessage();
//发送身份证明信息
    }
    else
if(type==TNC_INTEGRITY_ATTESTATION)
//完整性证明
    {
        SendIntegrityMessage();
//发送平台完整性信息
    }
}
```

本文利用可信网络的开源架构 TNC@FHH 对内部网络的结构进行了改造, TNC@FHH 是遵循 TNC 的相关规范和架构设计。移动终端安全接入网络架构主要基于 IEEE 的 802.1X 协议实现, 基于端口的接入控制 (port-based access control) 策略。在移动终端安全接入网络架构中, 移动终端以端口认证实体 (PAE, port authentication entity) 的形式向内部网络设备发起访问请求, 对建立通信线路的通信端口而言, 如果认证成功, 则为客户端 (或应用程序) “打开” 这个端口, 允许所有的通信报文通过; 否则将该端口保持 “关闭” 状态, 此时只允许符合 802.1X 协议要求的认证报文 EAPoL (extensible authentication protocol over LAN) 通过。

移动终端接入内部网络的认证过程如下。

步骤 1 移动终端按照协议向客户端 PAE 发送 EAPoL 报文, 这时, 受控端口对客户端是断开状态, 客户端 PAE 只能通过非受控端口与设备端 PAE 通信。

步骤 2 设备端 PAE 通过非受控端口接收来

自移动终端的认证请求后, 将该请求转发至认证服务器。

步骤 3 认证服务器根据相关协议和访问控制策略对移动终端的身份状态和完整性状态进行审核, 认证通过后开放受控端口, 否则拒绝移动终端的连接请求。

步骤 4 移动终端通过安全认证后, 可以安全接入内部网络。

4.2.3 移动终端业务数据加密存储

系统设计采用 SM4 加密算法。SM4 是一种分组加密算法, 通过将原始数据划分为固定长度的多个数据块依次进行加密, 最终得到整个文件的加密结果。SM4 算法的分组长度为 128 bit, 密钥长度为 128 bit。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同, 只是轮密钥的使用顺序相反, 解密轮密钥是加密轮密钥的逆序。当密钥长度为 128 bit 时, 足以应对各方面的安全性需求, 同时算法的加密过程是基于置换和替代的, 适用于软件实现, 具有安全高效的特点。因此, 系统采用密钥长度为 128 bit 的 SM4 算法作为数据加密的算法。通过加密 SD 卡的加密功能, 在移动终端收发数据时经可信中间件对数据进行加解密处理, 用于加解密的密钥存储在安全 SD 卡内部受硬件保护, 从而确保存储在加密 SD 卡中的业务数据安全。

4.3 实验系统测试

(1) 篡改移动终端安全运行环境攻击测试

攻击者通过篡改移动终端运行环境中有关完整性状态的重要组件, 使移动终端运行时完整性度量值与标准值不一致, 从而导致移动终端完整性认证失败, 无法正常运行移动终端中的安全应用实现业务流程。恢复组件完整性状态后, 即可再次通过完整性状态认证, 正常运行安全应用。

(2) 数据盗用非法复制攻击测试

攻击者不经过安全应用直接读取或复制经安

全处理过的密文数据，仅能获取数据经对称加密处理后的无效乱码，无法获取有效数据。

(3) 性能测试

为了测试原型系统的性能，本文综合统计装载加密 SD 卡后移动终端设备完成整个可信接入过程耗时，并引入取消可信认证完整性度量相关功能后的正常接入过程做对比实验。全过程为移动终端可信启动、可信网络接入服务器成功的总耗时；对照组实验则注释掉完整性度量、可信认证等功能，如图 7 和表 1 所示。

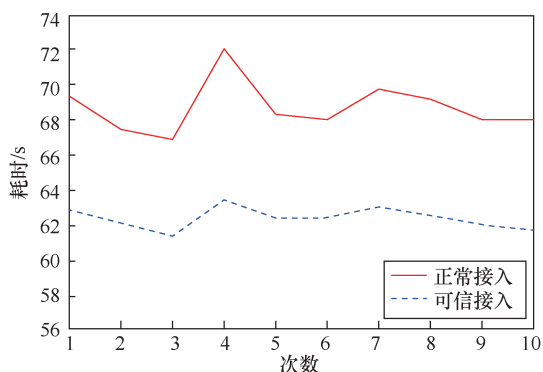


图 7 可信接入开销

表 1 可信接入时间延迟

次数	正常接入耗时/s	可信接入耗时/s	额外开销/s
1	69.3	62.8	6.5
2	67.6	62.1	5.5
3	66.9	61.6	5.3
4	72.1	63.3	7.9
5	68.4	62.3	6.1
6	68.2	62.2	6
7	69.8	63	6.8
8	69.2	62.7	6.5
9	67.9	62.2	5.7
10	68.2	61.7	6.5

测试中，移动终端系统运行均未出现异常状况，因可信环境建立造成的额外时间开销在 5.3~7.9 s 之间，平均开销对系统启动的影响在 8% 左右，对系统启动过程造成的影响在可接受的范围内。

5 方案分析

在企业机构信息化建设过程中，内网覆盖的工作人员完成业务工作时大量使用移动终端。一种适用于移动终端的安全接入方案，需要具备如下 2 个条件：1) 移动终端身份以及平台完整性验证；2) 移动终端使用过程中产生的业务数据安全存储。

本文方案通过引入加密 SD 卡的形式，构建整个移动终端接入流程的可信。目前投入使用的绝大多数移动终端具备标准 SD 卡槽，相较于 USBKey 等外接安全模块，加密 SD 卡因其小巧便携更适用于移动终端，且不需要改变移动终端的硬件架构。目前一体化较高的为提供加密 SD 卡的智能手机，也可以通过读卡器等工具接入 OTG 接口或者 Type-C 接口作为外置可信硬件提供各类可信服务。针对第一个要求，本文方案以加密 SD 卡为可信硬件，在移动终端中创建一个可信根，并以之为起点通过层层度量的方式构建一条信任链，将信任状态传递到整个移动终端。本文方案同时为移动终端的身份证明设计了身份认证与完整性度量工作，通过引入可信网络连接的思想，保证移动终端接入内网服务器时的状态可信，有效地防制重放攻击等常见的安全接入问题。针对第二个要求，本文方案采用的加密 SD 卡具备数据加密存储功能，通过调用内置加密算法，提供基于安全存储设备的数据加密存储，实现重要数据的安全存储。

本文方案实现了内网移动终端可信接入的相关需求，有效地增强了移动终端平台的安全性能。

6 结束语

本文基于可信计算的思想，通过引入加密 SD 卡的方式，设计并实现了一种移动终端远程可信接入方案。该方案从移动终端内部完整性证明、移动终端可信接入和重要数据存储安全加密 3 个方面实

现了内网环境下移动终端安全校验及可信接入。并且通过加密 SD 卡的方式充分利用大多数移动终端具备的标准 SD 卡槽接口, 无须改变移动终端硬件结构, 具备较高的实用性与可行性。但本文方案仅在部分 Android 系统版本的移动终端进行实验验证, 在模拟客户端中测试了原型系统工作效率, 并未在具体业务环境中进行试点, 有关 OTG 接口或者 Type-C 接口接入方式仅验证了可行性, 未进一步验证其数据传输效率。后续工作将会引入具体工作流程中进行测试更为复杂的安全需求。

参考文献

- [1] 中国互联网协会. 中国移动互联网发展状况及其安全报告 (2017) [R]. 北京: 中国互联网协会. 2017.5.
Internet Society of China. China mobile Internet development and security report (2017) [R]. Beijing: Internet Society of China. 2017.5.
- [2] 赵波, 张焕国, 李晶, 等. 可信 PDA 计算平台系统结构与安全机制[J]. 计算机学报, 2010, 33(1): 82-92.
ZHAO B, ZHANG H G, LI J, et al. The system architecture and security structure of trusted PDA[J]. Chinese Journal of Computers, 2010, 33(1): 82-92.
- [3] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学: 技术科学, 2007, 37(2): 129-150.
SHEN C X, ZHANG H G, FENG D G, et al. Summary of information security[J]. Scientia Sinica Informations, 2007, 37(2): 129-150.
- [4] 张立强, 张焕国, 张帆. 可信计算中的可信度量机制[J]. 北京工业大学学报, 2010, 36(5): 586-591.
ZHANG L Q, ZHANG H G, ZHANG F. The trust measurement scheme in trusted computing[J]. Journal of Beijing University of Technology, 2010, 36(5): 586-591.
- [5] 段新东, 马建峰. 可证明安全的可信网络存储协议[J]. 通信学报, 2011, 32(5): 169-174.
DUAN X D, MA J F. Provable secure trusted protocol for network storage[J]. Journal of Communications, 2011, 32(5): 169-174.
- [6] ZHANG H G, WANG F. A behavior based remote trust attestation model[J]. Wuhan University Journal of Nature Sciences, 2006, 11(6): 1819-1822.
- [7] 郑宇, 何大可, 何明星. 基于可信计算的移动终端用户认证方案[J]. 计算机学报, 2006, 29(8): 1255-1264.
ZHENG Y, HE D K, HE M X. Trusted computing based user authentication for mobile equipment[J]. Chinese Journal of Computers, 2006, 29(8): 1255-1264.
- [8] 陈书义, 闻英友, 赵宏. 基于可信计算的移动平台设计方案[J]. 东北大学学报(自然科学版), 2008, 29(8): 1096-1099.
CHEN S Y, WEN Y Y, ZHAO H, et al. Conceptual design of trusted mobile platform[J]. Journal of Northeastern University (Natural Science), 2008, 29(8): 1096-1099.
- [9] 王晋, 喻潇, 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]. 信息安全学报, 2018, 7(1): 1-6.
WANG J, YU X, LIU C, et al. A remote attestation scheme for intelligent mobile terminal based on SD key in smart grid environment [J]. Netinfo Security, 2018, 7(1): 1-6.
- [10] 赵波, 费永康, 向骥, 等. 嵌入式系统的安全启动机制研究与实现[J]. 计算机工程与应用, 2014, 50(10): 72-77.
ZHAO B, FEI Y K, XIANG S, et al. Research and implementation of secure boot mechanism for embedded systems[J]. Computer Engineering and Applications, 2014, 50(10): 72-77.
- [11] 赵世军, 冯登国. 基于属性证明的可信网络接入方案[J]. 武汉大学学报(理学版), 2012, 58(6): 519-525.
ZHAO S J, FENG D G. A TNC Trusted network connection schema based on property attestation[J]. Journal of Wuhan University (Natural Science Edition), 2012, 58(6): 519-525.
- [12] 彭国军, 邵玉如, 郑伟. 移动智能终端安全威胁分析与防护研究[J]. 信息安全学报, 2012, 12(1): 58-63.
PENG G J, SHAO Y R, ZHENG Y. Mobile intelligent terminal security threat analysis and protection research[J]. Netinfo Security, 2012, 12(1): 58-63.
- [13] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[C]//The 11th ACM Symposium on Access Control Models and Technologies. 2006: 19-28.
- [14] 李春雅. 基于 802.1X 的可信网络连接认证模型研究和实现[D]. 西安: 西安电子科技大学, 2010, 10(7): 85-92.
LI C Y. Research and implementation of the trusted network connection authentication model based on 802.1X[D]. Xi'an: Xidian University, 2010, 10(7): 85-92.

作者简介



李济洋 (1994-), 男, 湖北武汉人, 武汉大学硕士生, 主要研究方向为信息系统安全、网络安全。



赵鹏远 (1979-), 男, 河北保定人, 武汉大学博士生, 主要研究方向为信息系统安全、网络安全、可信计算。



刘喆 (1989-), 男, 山东青岛人, 武汉大学博士生, 主要研究方向为信息安全。