一个面向智能电话的移动可信平台设计

杨 健[1,2] 汪海航[1] Fui Fui Wong[1] 于 皓[1]
(同济大学电子与信息工程学院 上海 201804)[1] (大理学院数学与计算机学院 大理 671003)[2]

摘 要 由于手机病毒或设备失窃,导致手机上的私密数据面临泄漏的危险。为了满足移动平台的安全需求,TCG的MPWG提出移动可信平台规范。然而MPWG并没有明确规定特定的技术方法来实现移动可信模块(MTM),现有研究中没有整体的可实际部署于智能手机环境的MTM平台框架性设计,对可信软件栈(TSS)也没有可以实施的详细的部署方案。设计了一个面向智能手机的移动可信平台服务模型,它将基于TrustZone的纯软件MTM实现与基于Java Card的智能卡MTM实现结合起来构建两个可信引擎。提出其中可信构建块的部署流程并对其安全性进行了分析。

关键词 移动可信平台模块,TrustZone,智能卡,Java Card,可信软件栈(TSS),软件部署
中图法分类号 TP393 **文献标识码** A

Mobile Trusted Platform Model for Smart Phone

YANG Jian[1,2] WANG Hai-hang[1] Fui Fui Wong[1] YU Hao[1]
(Department of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)[1]
(Department of Mathematics and Computer Science, Dali University, Dali 671003, China)[2]

Abstract As virus or equipment lost, secret data on mobile phone is facing the danger of leakage. To meet the security needs of mobile platforms, TCG's MPWG has proposed the Mobile Trusted Platform specification, which does not specify a particular technical approach to design a Mobile Trusted Module(MTM). Existing research does not provide an overall framework of the MTM, which can actually be used in the smart phone environment, and nor a detailed deployment process of the Trusted Software Stack(TSS) of the framework. A model design on mobile trusted platform for smart phone was proposed in this paper, which combines the pure software MTM based on TrustZone technology with smart card MTM based on Java Card to build two trusted engines. The deployment scheme of trusted computing bases and security analysis of this model were put forward as well.

Keywords MTM, TrustZone, Smart card, Java card, TCG software stack, Software deployment

1 引言

当今智能手机性能和功能迅速发展,并大量应用于人们的生活和工作中,在帮助人们实现通信和各种数据处理任务的同时,也带来了更多的安全和隐私保护问题。例如,手机在丢失或遭受恶意软件攻击后,其关键数据面临泄露的危险。另一方面,手机上的大量私密数据可以通过无线网络使用云存储服务的远程数据存取和验证功能。然而,这需要在终端对数据进行加密和数据签名等预处理,会消耗大量的计算资源,现有智能手机还无法承担这样繁杂的计算工作。借助多方计算和代理运算的思想,可以将这样的运算交由一个经过认证的可信的第三方代理来完成。然而,运算代理能够保证数据的安全和隐私的一个决定性条件是手机与运算代理之间经过相互认证,建立安全的数据传输信道。利用现有的移动可信计算研究成果,本文面向手机应用环境下的数据安全存储和远程验证功能,设计一个移动可信平台模型来提供数据的安全和隐私保护服务。在终端设备上,结合现有的两种MTM实现,以设备只读ROM和设备上的身份识别智能卡为安全核心建立可信构建块(TCB),提出在卡上及卡外的应用及可信软件栈(TSS)的详细部署流程。通过具体案例分析并验证模型的安全性和可应用性。

本文第2节介绍了相关工作的研究基础;第3节详细介绍了模型的组织结构和可信软件部署流程,分析和解决了一些具体应用中的相关问题;第4节分析了模型的安全性能;第5节通过具体应用场景分析和验证了模型的有效性和实用性;最后进行总结和展望。

2 相关工作

TCG的移动电话工作组(MPWG)为了解决移动平台安全需求,已经发布了一个可信移动电话参考体系结构规范[1],即从现有可信PC结构中移植TPM、隔离性和完整性度量以适应移动设备的资源受限特性。然而MPWG并没有明确规定特定的技术来实现移动可信平台。MTM更像是一种服务而不是一个固定的微芯片,可以以软件形式实现,因此,不同

到稿日期:2011-10-09 返修日期:2012-02-17 本文受上海市科委2010年专项基金项目(10490503700)资助。
杨 健(1976-),男,博士生,讲师,主要研究方向为移动云计算、可信计算,E-mail:sbjc1215@126.com;汪海航(1965-),男,教授,博士生导师,主要研究方向为信息安全、智能信息系统;Fui Fui Wong 博士生,主要研究方向为云计算;于 皓 博士生,主要研究方向为物联网。

的厂商可以根据各自的应用环境设计不同的 MTM。

传统的移动可信计算思想是在移动设备上增加硬件芯片，提供安全的硬件隔离的可信服务，而这在移动设备的设计空间和电量限制下难以实现。在文献[2]中，提出了一种内核级别的域隔离措施，即扩展基于 SELinux 的内核来提供 MTM 所需的平台特性。然而，这种方法需要定制的操作系统内核，难以适应手机的多种操作系统环境。基于已有的平台特性的两种重要的 MTM 实现方法是：利用 ARM 的 Trust Zone 技术实现纯软件的 MTM 可信构建块[3]和利用基于 Java Card 技术的智能卡构建安全元来实现 MTM[4-6]。前者除了需要 ARM TrustZone 支持的处理器核心以外，并不需要额外的硬件设备，而可信构建块完全以软件方式实现，利用 TrustZone 特性，可以提供细粒度的内存和处理器隔离边界；而后者则在智能卡上驻留 Java Card Applet 组成的 MTM，其主要优势是所有特定智能卡的安全属性能被基于智能卡的 TPM 所继承，除了兼有智能卡本身的安全措施以及 MTM 所需的密码学算法，还提供了 MTM 要求的保护能力，并且通过 JVM 本身特性提供应用隔离措施[7]。基于 TrustZone 的纯软件 MTM 和基于 Java Card 的智能卡 MTM 实现也是本文模型的设计基础。

现在，移动可信平台的研究很多注重于特定协议算法的性能评估，以及 MTM 的功能和性能优化。例如直接匿名证明(DAA)在 Java 嵌入式系统[6]和近场通信环境[8]中的实施与性能验证，对手持设备上基于软件的 TPM(SW-TPM)实现的能量和执行时间负载进行评估[9]，基于软件的 MRTM 实现的优化方案[10,11]以及使用 TPM 实现远程验证功能以在可信的基于位置服务中增强移动通信安全[12]。对于移动可信平台软件的部署问题，文献[2]中分析了当前 J2ME 环境下可选的部署方式。然而，这些方式将 TSS、底层命令库和抽象层作为统一的单元来设计 Java 应用所采用的可信服务代码的共享方式，没有充分考虑可信服务面向不同的应用可能采用灵活的上层结构的特点。

国内关于移动可信计算的研究也已经开展起来，但大多偏向于身份认证[16,17]、访问控制[18]和移动节点接入[19,20]等移动可信平台应用。文献[16]中提出了口令、指纹识别与 USIM 卡结合的用户域认证方案，但其实现仍然是基于 PC 机的可信计算思想。还有研究涉及到移动可信计算在传统平台上的应用，如嵌入式系统、安全存储管理[21]等内容。也有研究涉及移动可信平台实现的可行方案，但都没有提出具体的实施方案。

可以看到，现有的研究成果中，并没有完整的可实际部署于移动电话环境的 MTM 框架性设计，没有根据设备本身的不可移除 ROM 的特性和 SIM 卡可移动特性提供一个综合的移动可信平台框架，对 TSS 也没有可以实施的详细的部署方案。据悉，我们的研究成果是首次将基于 TrustZone 的纯软件 MTM 实现与基于 Java Card 的智能卡 MTM 实现结合起来构建面向智能手机可信服务的移动可信平台模型。本文提出了模型设计以及可信构建块的部署流程并对其安全性进行了分析，在最后以具体的例子验证了该模型的可实用性。

3 模型设计

根据 TCG 的移动可信平台模块规范[13]，移动电话产业涉及 4 个不同平台利益相关者：设备制造商(DM)、通讯服务提供商(CSP)、应用服务提供商(ASP)和终端用户。规范中要求分离可信的和隔离的操作域，也就是所谓的可信引擎。根据规范的要求，本文设计了如下的移动电话可信平台模型。

3.1 模型结构

在本设计中，有两个 MTM 可信引擎，分别是基于 ARM 处理器核心的 TrsutZone 技术的纯软件 MTM 实现和基于 JavaCard 的利用智能卡的保护和隔离措施的 MTM 实现。图 1 是本设计的模型结构图，其中各组成部分分别为：

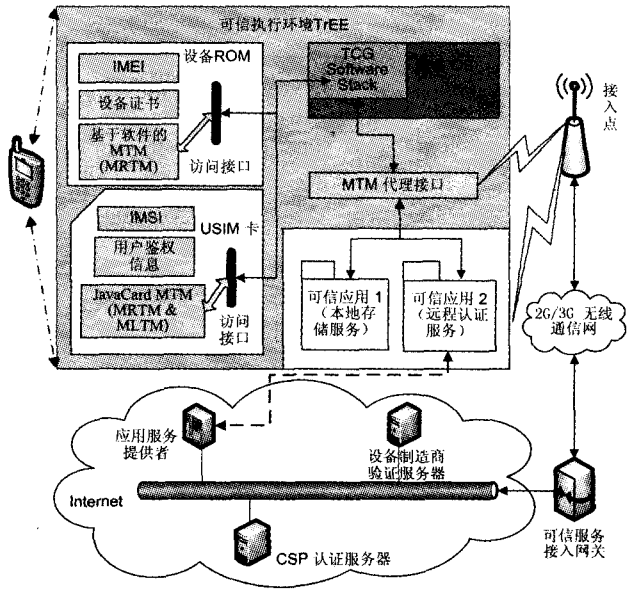

图 1 设计模型结构图

设备 ROM：移动电话中的不可擦除 ROM 由 DM 设定内容，其中除了包含唯一的标志设备的 IMEI 编码[14](International Mobile Equipment Identity)以外，还有 MTM 的软件实现，以及 MTM 命令解析接口等。除此之外，ROM 中还包含设备公钥证书。设备 ROM 上的 MTM 引擎的利益相关者是 DM，它也是这个 MTM 的拥有者。

USIM(Universal Subscriber Identity Module)卡：本文采用 USIM 卡来标识用户在移动通信网络中的身份，原因在后面详述。除了包含标识卡的 IMSI(International Mobile Subscriber Identity)编码和用户鉴权信息以外，还包含有 MTM 的引擎实现以及相应的受保护的安全存储空间(密钥存储空间以及 PCR)。USIM 的利益相关者是 CSP 和手机用户，因此卡上的一个上层可信引擎包含两个附属引擎：一个 MRTM(所有者是 CSP)和一个 MLTM(所有者是用户)。由于不影响功能的实现，两个附属可信引擎在本文中并不分开讨论，统一以一个 MTM 来表示实现。

TSS(TCG Software Stack)：包含两个层次，MTM 驱动抽象层和应用层 MTM 命令解析接口。TSS 驻留在操作系统内核，是可信执行环境的一部分。它可以通过与 CSP 等建立安全信道后远程安装，或直接作为 OS 的部分来由 DM 完成部署，可以在不同系统上部署并为上层应用软件提供统一的可信服务接口。

MTM Agent：是可信应用与 MTM 可信执行环境进行交互的接口。作为可信执行环境的一部分，它经由 CSP 等可信服务提供商来远程部署。

可信应用程序：这是设备上使用 MTM 功能的应用软件，它通过调用 MTM 代理接口来利用 MTM 的服务，如本地安

全数据存储应用或远程的云服务可信验证和可信服务。

可以看到，模型中并不提供应用直接访问 MTM 的能力，因为移动设备 OS 对应用软件的隔离保护措施不同[14]，开放直接访问底层 MTM 功能会对 OS 设计及 TSS 部署增加很大的困难。然而，统一由设备 OS 提供符合 TCG 规范的命令接口，可以很好地适应现在基于操作系统的各种应用的开发模式。

3.2 MTM 及 TSS 设置和部署

整个模型的部署过程包含如下几个阶段(见图 2)。

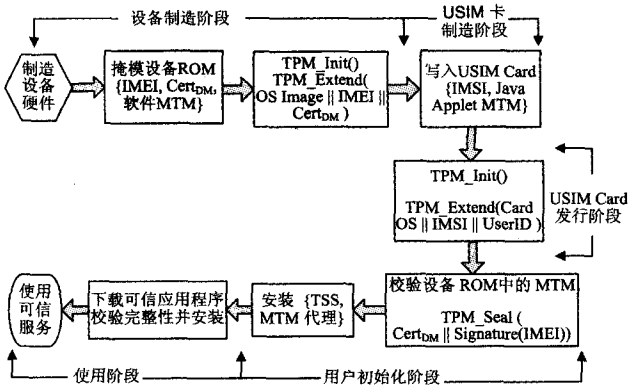

图 2 MTM 与 TSS 设置和部署流程

(1)在设备制造过程中，设备制造商在设备 ROM 上设置 IMEI 号，实现公钥证书及 MTM 的纯软件，并安装 OS。这个 ROM 是要求满足 ETSI 标准的防篡改的只读存储器。在出厂之前，设备初始化 MTM 并度量 OS 内核映像、IMEI 号及设备公钥证书的完整性，保存度量值并扩展 PCR，这些值作为平台的初始状态值：

$$PCR_{dev} \leftarrow TPM\_Extend(SHA\text{-}1(SHA\text{-}1(Kernel_{OS}) \| IMEI \| Cert_{DM})))$$

其中，$Kernel_{OS}$ 代表手机 OS 的内核映像；$Cert_{DM}$ 是设备公钥证书。

(2)USIM 卡制造过程中，安装以 Java Applet 形式存在的 MTM 以及相关的命令和解析接口。在发行时，卡片除了记录鉴权加密信息以外，还将 USIM 卡片上操作系统，以及 IMSI 和用户 ID 组合起来扩展到卡上 MTM 的 PCR 中：

$$PCR_{card} \leftarrow TPM\_Extend(SHA\text{-}1(SHA\text{-}1(Kernel_{OR}) \| IMSI \| UserID)))$$

其中，$Kernel_{OR}$ 代表卡片操作系统的内核映像；$UserID$ 代表手机用户的识别信息。

(3)卡片发给用户后，用户将 USIM 卡插入手机中并第一次开机时，USIM 卡加电，完成自检以及 MTM 的初始化任务后，调用卡上 MTM 命令代理，请求验证设备的公钥证书。若通过设备认证，则将设备公钥证书以及签名的 IMEI 用当前 USIM 上的 PCR 值封装。然后 USIM 卡与 CSP 建立可信信道，下载并在对应的操作系统下安装移动可信模块的 TSS，设置相应的接口。TSS 作为可信执行环境的一部分，也可以在设备制造过程中以 OS 内核的形式安装。

(4)MTM 代理安装。在通过 USIM 的验证后，设备从移动运营商或其他可信服务提供商处下载并安装安全的经过签名的 MTM 代理接口。因为 MTM 代理也属于可信执行环境的组成部分，除了在安装时需要验证证书以外，运行中也需要对其进行细粒度的完整性和安全性保护，这些运行时的保护措施由特定 OS 来提供。

(5)MTM 应用软件部署。通过 MTM 移动环境下的软件完整性校验，可以实现软件基于签名的校验和安装。应用软件面向特定的可信服务功能可提供本地数据的安全存储或远程云存储服务的验证和数据校验等。

3.3 关于安全启动和可信链路

移动可信计算定义了安全启动(secure boot)的服务。相比于一个可靠启动(authenticated boot)，如果当前加载的软件的完整性校验失败，则安全启动将终止软件执行，甚至是终止设备的启动。这意味着一个远端参与者可以假设一个特定的软件配置在设备上运行[1,4]。

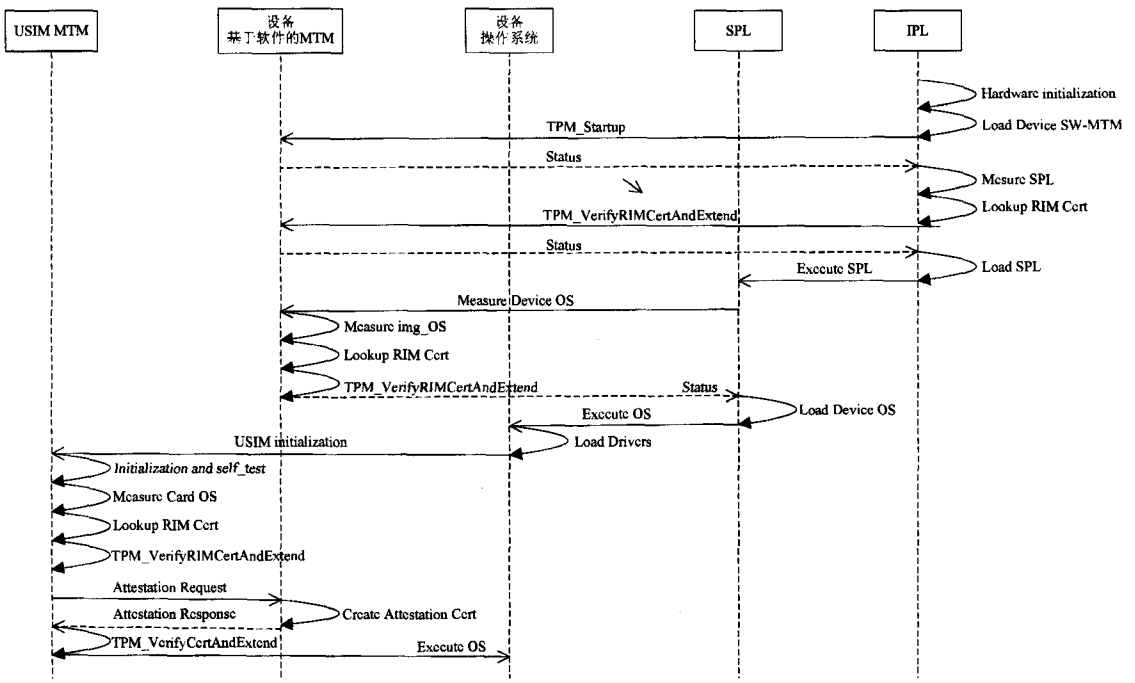

图 3 启动校验过程

智能手机软件启动始于 IPL(InitialProgramLoader)和 SPL(SecondProgramLoader)的载入。前者负责主板、硬件、

电源初始化和 SPL 载入，后者则负责 OS 的载入。模型中安全启动的实现基础是 CPU 的 TrustZone 特性[3]，而设备 ROM 中软件 MTM 的度量和载入则由 IPL 完成，因此可信度量核心根(CRTM)也包含在 IPL 模块中。可信链路的建立流程如下：

(1)整个模型的 CRTM 包含在 IPL 中，位于移动设备中防篡改的 ROM 中，它与 IMEI、公钥证书和出厂配置放置在一起，并且在出厂后不可更改(掩模 ROM)。在出厂前测试阶段，MTM 在写入后，对手机 ROM 中其他关键部分(包括 SPL 和存储器中初始操作系统内核映像)进行可信度量，记录度量值并将其扩展到 PCR 中。

(2)USIM 在发行后，在第一次插入加电时，验证操作系统映像，并校验设备 ROM 上的完整性证书。也即验证设备可信性，如果设备可信，则将设备可信度量值迁移并封装到 USIM 上。

(3)如果 USIM 中已经记录了设备验证状态，则在每次手机启动、卡片加电时，校验设备、手机操作系统以及卡片的可信状态。在此验证过程中，若发生不一致现象，则停止操作系统的继续运行，实现安全启动。整个模型正常启动的验证过程如图 3 所示，这也是模型的信任链传递过程。

3.4 几个问题及其解决

3.4.1 密码学运算的效率问题

现有大量研究表明，可信计算服务消耗的时间主要集中在大量的密码运算上。文献[6]中认为，DAA 在 Java 移动平台上应用时，纯 Java 实现只有当系统支持 Java 执行加速时才可实际应用。尽管智能卡运算功能不断提高，卡内的密码学运算机制已经可以用于承载 MTM 所需的运算，但对于复杂的安全协议来说，可以考虑计算量大的一些操作，如大数模幂(密码学在纯 Java 应用中的计算瓶颈)以及一些大数字对象的 hash 等功能应考虑在设备操作系统的受保护单元完成。

另外，根据具体应用，可以对 MTM 的功能进行细分和裁剪，以满足特定的应用需求并符合 USIM 对空间的限制条件，如文献[10]中采用的：根据应用需求对 MTM 功能函数进行划分，在需要的时候才载入安全 RAM 执行；设置满足移动计算需求的密钥结构以减少密钥存储空间；对于 MRTM 来说，去除不必要的数据等技术，例如关于变更所有者或是管理 locality。

3.4.2 换卡对整个设计模型的影响

因为某些原因，用户需要将 USIM 卡换到其他手机上使用，或是在相同的手机上使用不同的卡，对于本地安全存储和远程身份认证两个可信应用，有如下的解决方案：

当可信服务用于本地的文件安全存取功能时，有两种情况：1)若是设备使用新的 USIM 卡，则需要在换卡之前，使用可迁移密钥对数据文件重新加密，并将密钥迁移至移动设备的 MTM 上。然后更换新的 USIM 卡，并将设备 ROM 的 MTM 上的可迁移密钥迁移回新卡上的 MTM，就可以在需要的时候进行解密。2)若是直接将 USIM 卡移动到其他手机上，则在设备完整性度量验证通过后，更新 USIM 卡上 MTM 的度量状态，然后可以直接将加密后的文件拷贝到新设备上完成解密，因为我们的设计中 USIM 是独立的可信模块，而最终的数据安全存储所需的密钥保护服务是由 USIM 上的 MLTM 来提供的。

当可信服务用于远程身份验证时，因为要由 USIM 卡上的 MTM 来具体实施验证协议，所以，验证之前除了完成新卡与设备之间的相互验证，还必须要更新新卡上的 MTM 的度量信息、设备 IMEI 证书和公钥证书。实际上，这可以通过对卡上 MTM 进行重置并重新初始化(见 3.2 节的(2)和(3)步)来实现。

3.4.3 为什么是 USIM 不是 SIM

相对于 SIM 卡的单向鉴权(网络鉴权用户)，USIM 卡鉴权机制采用双向鉴权(除了网络鉴权用户外，用户也鉴权网络)，有很高的安全性。

相对 SIM 卡机卡接口速率，USIM 卡机卡接口速率大大提高，从而提供卡片与主机之间的大数据通讯能力。

相对 SIM 卡对逻辑应用的支持，USIM 可以同时支持 4 个并发逻辑应用，可以有效提高卡片的运算性能以及与外部主机程序的交互能力。

3.4.4 卡的主动式验证

SIM 的验证命令可以通过 SIM 卡上的主动式命令来实现[7]。其中，2G 的 STK(SIM Application Toolkit)技术和 3G 的 USAT(USIM Application Toolkit)技术是在原来 SIM 卡被动式的操作模式基础上，增加了新的主动式操作的能力，即允许 SIM 卡中的应用和服务主动与手机终端进行交互操作。USIM 卡引入了全新的 BIP(Bearer Independent Protocol)协议接口，通过 BIP 协议结合 USAT 应用，手机终端允许 USIM 卡和远程服务器之间进行高速的、透明的数据传输，实现透明的远程验证协议。

4 安全分析

4.1 可信引擎

在移动计算环境中，安全的利益相关者有设备制造商、通信网络服务、移动计算服务商以及终端用户。在本文设计中根据各方需求设置了两个可信引擎，并通过在两个引擎上的可信状态的转移实现移动终端上的可信服务。

设备在制造过程中在固化的 ROM 中存储有设备的 IMEI 和公钥证书，在假设设备制造商是可信的前提下，OS 映像的完整性度量值保存在软件实现的 MTM 中。可信链建立从 IPL 运行开始，在 OS 载入之前就在 RAM 中载入软件实现的移动设备的 MTM，并利用 TrustZone 技术提供的运算隔离性实现安全虚拟域(MTM 所在的可信构建块)和非安全虚拟域的隔离；然后载入 SPL，并对 OS 进行完整性度量，与初始化时的度量值进行比较，从而保证操作系统的完整性。在 OS 载入过程中，在无线通信模块初始化时，首先检测 USIM 卡，完成设备与 USIM 卡之间 MTM 的验证，然后度量并验证 USIM 卡上 TCB 的完整性，在通过验证后，将设备的可信状态继承到 USIM 卡上。通过利用 USIM 卡上固有的安全和隔离特性，实现可信域和不可信域隔离。

本设计中在一个可信平台模型上设置两个可信引擎，将设备可信状态以及证书安全转移到 USIM 卡上，并在可信服务中使用 USIM 卡作为用户的可信构建块，提供本地数据存

储封装和密钥保护，以及远程服务的验证和安全保证。USIM卡具有良好的防篡改特性，在卡上安装Java Card Applet实现的MTM可以充分利用JVM的安全隔离特性，并且卡上的安全算法也满足了MTM功能需求。

4.2 多因子认证与双可信引擎的可信平台模型的结合

基于TrustZone的软件MTM实现与Java Card MTM实现结合，可满足智能手机的实际应用环境和需求。USIM卡代表用户身份，除了使用PIN码作为验证用户身份的方法以外，还可以结合生物识别等认证方案[16]，将用户生物识别码作为安全状态记录到USIM的PCR中，能够给设备上的隐私数据提供最大限度的安全保证。这种结合还可以有效防止手机因为丢失而带来的数据泄露(参考3.4.2节所述)。

5 仿真及案例分析

模型中包含两个可信引擎，其中基于软件的MTM仿真功能由MTM emulator[22]来提供，另外一个智能卡上可信引擎则利用JCCDK v2.2.2[23]开发Java Card Applet实现所需MTM功能，卡外的可信应用程序、MTM Agent接口及远程验证服务均在Java环境下开发，而TSS则利用了TrouSerS软件包和相关工具来实现。所有软件和工具包部署在Ubuntu 10.04 Server中并验证运行通过。

5.1 本地安全数据存储

模型能用于移动设备的安全数据存储。通过安全存储软件，可以将手机上的机密数据加密后保存，密钥在USIM上的MTM中生成并保存在MTM密钥结构中，本地数据加密时还可以与特定PCR状态相关联，也即对数据进行封装，进一步保证数据的私密性。但要注意的是，为了防止设备失窃造成隐私数据泄漏，在使用可信服务之前，仍需要结合PIN码验证或是指纹识别等多因子认证方案。当设备丢失或失窃时，设备和卡会同时落入非法拥有者手中。因为手机上的私密数据的解密密钥由卡的MTM保护其安全，只有当验证输入PIN值或经过生物识别后才能对私密数据解封。非法拥有者不能通过这个验证，因此不能得到私密数据的解密密钥，从而防止了私密数据泄漏给非法用户。由于MTM提供的安全性，利用操作系统漏洞对加密数据的破解将非常困难，从而进一步降低了手机病毒带来的数据泄漏风险。

5.2 远程自动匿名证明(基于PCA或DAA)

在客户端使用远程服务时，需要双方的互相验证，这种互相验证需要以USIM卡上MTM作为认证代理：

客户端向远程服务器证明自己。在这个过程中，客户端接受到远程服务器的证明挑战后，向USIM卡发出申请，并附带远程服务器地址和相关挑战信息。USIM卡接受到请求后，基于私有CA或是DAA协议，生成相应的证明信息，并经由BIP协议接口发送给远程服务器。远程服务器验证后，返回验证结果给USIM卡。USIM卡将证明结果发送给客户端应用软件。

客户端请求远程服务器发送其证明服务可信的消息。客户端将证明请求信息发送给USIM卡，USIM卡据此生成挑战信息并经由BIP协议接口发送给远程服务器。远程服务器根据挑战生成响应，并发送给USIM卡。USIM卡验证响应信息，并将验证结果发给客户端软件。

可以看到，客户端与远程服务器之间的验证是以USIM卡作为中间代理的，经由USIM卡上的MTM提供可信服务，使得USIM卡可以度量和验证客户端软件的完整性，而USIM卡与远程服务器之间的验证信息经由BIP协议接口来传输并提供相应保护。经由USIM卡提供的可信服务，可实现客户端应用与远程服务器的相互验证。

结束语 为了满足智能手机在本地数据安全存储和远程匿名验证的需求，本文将基于TrustZone的纯软件MTM实现与基于Java Card的智能卡MTM实现结合起来构建面向智能手机可信服务的移动可信平台模型，在模型中建立两个可信引擎，并将设备与系统的可信度量传递到用户使用环境，由智能卡MTM来提供面向用户的可信服务。模型中将TSS部署在操作系统核心层，由设备制造商将其作为系统服务嵌入到操作系统中，并提供标准访问接口；而面向不同可信服务的解决方式是提供一个由网络服务商发布的MTM代理，作为可信服务的上层接口，建立起底层MTM驱动、命令与上层可信应用软件之间的联系。通过安全分析和案例分析表明，我们的系统借助USIM卡的主动式命令能够建立起面向本地数据安全存储和远程匿名证明的可信服务平台。

未来的工作主要包括：

面向本地数据存储安全和远程匿名证明的需求，探讨USIM卡上MTM可信引擎和其附属的面向移动运营商和设备拥有者的不同子可信引擎的功能子集划分，并利用Java Card Applet实现原型系统，测试系统性能，尤其是涉及到DAA的密码学运算性能。

根据模型实现原型系统，以具体的本地数据安全服务为需求，建立原型系统以验证模型的有效性、安全性和性能。

BIP协议是3G技术中USIM卡发起主动式命令的重要内容，探讨在原型系统中结合USAT指令与BIP功能，以进一步增强USIM卡上基于Java Card的MTM可信服务能力。

针对DAA的效能问题和基于PCA匿名认证的瓶颈问题，基于本文提出的模型特点，设计符合安全条件的直接匿名认证协议，并在实际系统中进行验证。

参 考 文 献

[1] TCG. TCG Mobile Trusted Module Specification[S]. TCG, 2010

[2] Zhang Xin-wen, Acliçmez O, Seifert J-P. A trusted mobile phone reference architecture via secure kernel[C]// Proceedings of the 2007 ACM workshop on Scalable trusted computing. ACM: Alexandria, Virginia, USA, 2007: 7-14

[3] Winter J. Trusted computing building blocks for embedded linux-based ARM trustzone platforms[C]// Proceedings of the 3rd ACM workshop on Scalable trusted computing. ACM: Alexandria, Virginia, USA, 2008: 21-30

[4] Dietrich K, Winter J. Implementation Aspects of Mobile and Embedded Trusted Computing[C]// Proceedings of the 2nd International Conference on Trusted Computing. Oxford, UK: Springer-Verlag, 2009: 29-44

[5] Dietrich K. An integrated architecture for trusted computing for java enabled embedded devices[C]// Proceedings of the 2007

ACM workshop on Scalable trusted computing. ACM: Alexandria, Virginia, USA, 2007: 2-6

[6] Dietrich K. Anonymous Credentials for Java Enabled Platforms: A Performance Evaluation [C] // Proceedings of INTRUST 2009, 2010. Oxford, UK: Springer-Verlag, 2010: 88-103

[7] Microsystems S. Java Card(TM) Specification 2. 2. 2[S]. Final Release. March 2006

[8] Dietrich K. Anonymous RFID authentication using trusted computing technologies[C] // Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues. Istanbul, Turkey: Springer-Verlag, 2010: 91-102

[9] Aaraj N, Raghunathan A, Jha N K. Analysis and design of a hardware/software trusted platform module for embedded systems[J]. ACM Transactions on Embedded Computing Systems, 2009, 8(1): 1-31

[10] Ekberg J-E, Bugiel S. Trust in a small package: minimized MRTM software implementation for mobile secure environments[C] // Proceedings of the 2009 ACM workshop on Scalable trusted computing. ACM: Chicago, Illinois, USA, 2009: 9-18

[11] Dietrich K, Winter J. Towards customizable, application specific mobile trusted modules [C] // Proceedings of the fifth ACM workshop on Scalable trusted computing. ACM: Chicago, Illinois, USA, 2010: 31-40

[12] Othman H, Hashim H, Razmi Y M A, et al. Forming Virtualized Secure Framework for Location Based Services(LBS) using Direct Anonymous Attestation(DAA) protocol[C] // 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE: Washington DC, USA, 2010: 622-629

[13] TCG, TCG Mobile Reference Architecture[S]. TCG. 2007

[14] Kostiainen K, Reshetova E, Ekberg J E, et al. Old, new, borrowed, blue —: a perspective on the evolution of mobile platform security architectures[C] // Proceedings of the first ACM conference on Data and application security and privacy. ACM: San Antonio, TX, USA, 2011: 13-24

[15] Khan S, Khan S, Nauman M, et al. Realizing dynamic behavior attestation for mobile platforms[C] // Proceedings of the 7th International Conference on Frontiers of Information Technology. ACM: Abbottabad, Pakistan, 2009: 1-6

[16] 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

[17] 李建，何永忠，沈昌祥，等. 基于可信移动平台的跨身份标志域访问模型[J]. 计算机应用研究，2009，26(1)：321-324

[18] 李涛，胡爱群. 可信模块与强制访问控制结合的安全防护方案[J]. 东南大学学报：自然科学版，2011，41(3)：513-517

[19] 孙丽娜，常桂然，王兴伟. 无线网络下可信移动节点接入认证方案[J]. 计算机应用，2011，31(11)：2950-2953

[20] 吴振强，周彦伟，乔子芮. 移动互联网下可信移动平台接入机制[J]. 通信学报，2010，31(10)：158-169

[21] 余鹏飞，吴俊军，王同洋，等. 基于智能卡技术的移动存储安全管理研究[J]. 计算机工程与科学，2010，32(4)：29-32

[22] Ekberg J E, Kylänpää M. MTM emulator[OL]. http://mtm.nrsec.com/ index.html

[23] Oracle. Java Card Development Kit 2. 2. 2[OL]. http://www.oracle.com/ technetwork/ ava/javacard/overview/index.html

---

(上接第 13 页)

[65] Cui D, Gao Z Y, Zhao X M. Cascades in Small-World modular networks with CML's method[J]. Modern Phys. Lett., 2007, 21: 2055

[66] Cui D, Gao Z Y, Zhao X M. Cascades with coupled map lattices in preferential attachment community networks [J]. Chin. Phys., 2008, 17(5): 1703-1708

[67] Cui D, Gao Z Y, Zheng J F. Tolerance of edge cascades with coupled map lattices methods[J]. Chin. Phys., 2009, 18(3): 992-996

[68] Bao Z J, Cao Y J, Ding L J, et al. Synergetic behavior in the cascading failure propagation of scale-free coupled map lattices[J]. Physica A, 2008, 387: 5922-5929

[69] Fan W, Yeung K H. Protection against Cascading Failures in Scale-free Networks[C] // Proceedings of the 7th Asian Control Conference. 2009: 27-29

[70] Watts D J. A simple model of global cascades on random networks[J]. Proc. Natl. Acad. Sci. U. S. A, 2002, 99: 5766-5771

[71] Buzna L, Peters K, Helbing D. Modelling the dynamics of disaster spreading in networks[J]. Physica A, 2006, 328: 132-140

[72] Weng W G, Ni S J, Yuan, H Y, et al. Modeling the dynamics of disaster spreading from key nodes in complex networks [J]. Int J Mod Phys C, 2007, 18(5): 889-901

[73] Guo Q, Li L X, Chen Y H, et al. Modeling dynamics of disaster spreading in community networks[J]. Nonlinear Dyn, 2011, 64: 157-165

[74] Buzna L, Peters K, Ammoser H, et al. Efficient response to cascading disaster spreading[J]. Phys. Rev. E, 2007, 75: 056107

[75] Buldyrev S V, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464: 1025

[76] Parshani R, Buldyrev S V, Havlin S. Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition[J]. Phys. Rev. Lett., 2010, 105: 048701

[77] Huang X Q, Gao J X, Buldyrev S V, et al. Robustness of interdependent networks under targeted attack[J]. Phys. Rev. E, 2011, 83: 065101

[78] Smart A G, Amaral L A N, Ottino J M. Cascading failure and robustness in metabolic networks [J]. PNAS, 2008, 105(36): 13223- 13228

[79] Yan Y, Liu X, Zhuang X T. Analyzing and identifying of Cascading failure in supply chain networks[C] // ICLSIM. 2010: 1292-1295

[80] Jin C, Huang Y Y, Gao P. Analysis on Cascading Failure Propagation in Logistics System under Emergency [C] // ICEEE. 2010: 5660604

[81] Sahasrabudhe S, Motter A E. Rescuing ecosystems from extinction cascades through compensatory perturbations [J]. Nature Communication, 2011(1)

[82] Wang W X, Yang R, Lai Y C. Cascade of elimination and emergence of pure cooperation in coevolutionary games on networks [J]. Phys. Rev. E, 2010, 81: 035102