# 基于可信计算的多租户隐私数据保护①

裴华艳[1], 王焕民[2]

[1](甘肃广播电视大学 教务处, 兰州 730030)
[2](兰州交通大学 机电技术研究所, 兰州 730070 )

**摘 要**: 针对多租户应用的隐私数据保护问题, 在分析多租户应用的特点和隐私数据保护需求的基础上, 将可信计算技术引入多租户隐私数据保护, 基于虚拟可信平台模块 vTPM 提出了一种具有定制性的加密保护方案, 利用 vTPM 提供的加密密钥对租户的隐私数据进行加密, 同时利用 vTPM 的密钥保护和管理功能对加密密钥进行保护. 最后, 基于 Xen 实现的 vTPM 实现了本方案.

**关键词**: 多租户应用; 虚拟可信平台模块 vTPM; 隐私数据保护

## Privacy Data Preservation of Multi-tenancy Based on Trusted Computing

PEI Hua-Yan[1], WANG Huan-Min[2]

[1](Office of Academic Affairs, GanSu Radio and TV University, Lanzhou 730030, China)
[2](Mechatronic Technology Institute, Lanzhou Jiaotong University, Lanzhou 730070, China)

**Abstract**: To address the problem of privacy data preservation of multi-tenancy applications, on the basis of analyzing characteristics of multi-tenancy applications and the corresponding demands of privacy data preservation. The trusted computing technique was introduced into privacy data preservation of multi-tenancy, presented an encryption and preservation approach with customizability based on virtual trusted platform module(vTPM). Privacy data of multi-tenant was encrypted by making use of encryption key provided by vTPM , and the encryption key was protected by using encryption key preservation and management of vTPM. Finally, the approach was implemented based on the Xen implementation vTPM.

**Key words**: multi-tenancy applications; virtual trusted platform module(vTPM); privacy data preservation

多租户应用采用单实例多租赁模式, 不同租户对不同数据有不同的隐私保护需求[1], 隐私保护机制需要具有可定制性, 以满足这一需求. 多租户应用需要满足租户隔离和多租户共享等特性, 隐私保护机制需要与这些特性进行有效的结合, 以满足多租户应用处理的逻辑性能需求. 在多租户应用模式下, 租户的数据由软件服务提供商统一进行管理和维护, 隐私数据不能让任何非法人员访问和使用, 多租户隐私保护机制需要确保即使恶意用户非法获取隐私数据, 也能够确保数据本身的安全性.

## 1 多租户应用及其隐私数据保护

### 1.1 多租户应用

在 SaaS 服务模式下, 将具有共性需求的用户群体称为租户, 用户以租户为单位租用软件服务[2], 根据租用软件的数量和时间长短支付租金[3]. 从架构层面来看, SaaS 与传统软件应用模式的区别主要在于多租户模式.

多租户(Multi–tenancy Technology)是一种软件架构技术, 是指多个租户(Tenant)共享使用同一个软件应用实例. 多租户技术将硬件资源和运营管理维护资源以服务的形式提供给多个租户复用, 每个租户按需使用, 不影响其他租户的使用, 也感觉不到平台同时也在为其他租户服务. 实现多租户架构的关键是通过一定的技术策略确保不同租户的数据隔离性和安全性, 保证不同租户既能共享同一个软件应用实例, 又能为

①收稿时间:2015-03-12;收到修改稿时间:2015-04-29



© 中国科学院软件研究所 http://www.c-s-a.org.cn

每个租户提供独立的应用体验和数据空间[4].

### 1.2 多租户隐私数据保护要求

多租户应用采用单实例多租赁模式, 不同租户具有不同的功能需求和个性化定制需求, 对不同的数据有不同的隐私保护需求, 这要求多租户隐私数据保护机制具有租户定制性, 通过提供可定制的功能, 能够为不同的租户提供不同的隐私数据保护服务, 使同一软件应用实例的不同租户能够根据自身的隐私数据保护需求选择合适的保护服务.

在多租户应用中, 所有数据由软件服务提供商统一进行管理, 租户通过租用的方式共享使用软件, 在这种应用模式下, 软件服务提供商需要对租户数据进行有效的隔离, 确保不同租户的数据完全独立. 多租户隐私数据保护机制要能够确保有效的租户隔离性, 限制租户对数据的访问范围和使用权限, 确保每个租户只能访问和使用自己的隐私数据, 且无法获取其他租户的隐私数据.

在多租户应用模式下, 租户的财务数据、信用卡 PCI 数据和关键客户的联系方式等隐私数据不能让非法人员访问、统计和使用, 隐私保护机制需要确保能够做到这一点. 如果这些数据由于黑客攻击、病毒或管理疏忽等原因导致泄露, 为了避免给租户造成重大损失, 隐私保护机制要能够确保数据本身的安全性.

## 2 可信计算技术

### 2.1 可信平台模块

可信计算是一项由可信计算小组[5](Trusted Computing Group)推动和开发的技术, 其核心思想是通过在现有计算机系统的硬件平台中引入安全芯片, 构造“信任链”和“信任度量”来提高整个系统的安全性, 这种安全芯片被称为可信平台模块(Trusted Platform Module).

可信平台模块是可信计算平台(Trusted Computing Platform)的核心, 是一个由密码协处理器、密码引擎和存储器等部件组成的小型片上系统. TPM 使用符合标准规定的密码算法, 对外提供非对称密钥生成算法、非对称密码算法、加解密运算、数字签名运算和随机数产生运算等[6]. TCG 规范定义的 TPM 体系结构如图 1 所示.

其中, I/O 是 TPM 的输入输出接口, 主要负责内外部总线之间通信协议的转换和总线上信息流的管理. 密码协处理器内含一个 RSA 引擎, 主要负责 RSA 算法(TPM 使用的主要密码算法)的实现, 提供对内/外的内部存储数据和传输数据的加/解密功能[7]. 密钥生成器负责生成对称密钥和 RSA 密钥, 可信计算技术没有限制这两类密钥的生成次数. HMAC 引擎通过 HMAC 运算生成消息摘要值来确认报文数据是否正确, 以防止数据和命令发生错误或被篡改. 随机数发生器除了用于 RSA 密钥对的生成, 还负责产生各种运算所需的随机数. SHA–l 引擎负责完成基本的 hash 运算, 提供可被外部调用的 hash 接口. 非易失性存储器用于保存永久身份和与 TPM 相关联的状态. 易失性存储器用于保存 TPM 运行时产生的临时数据.

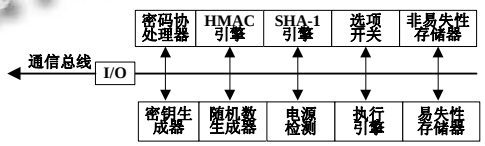


图 1 TPM 的体系结构

### 2.2 信任根

在可信计算平台中, 要建立可信机制首先要拥有信任根[8][9][10][11][12](Roots of Trust), 信任根由可信度量根、可信存储根和可信报告根组成.

可信度量根(Root of Trust for Measurement)是一个计算引擎, 能够在平台内部进行可靠的完整性度量. 完整性度量(Integrity Measurement)是使用密码杂凑算法计算对被度量对象的杂凑值的过程. 可信计算平台从 RTM 开始运行, 它是可信平台中信任链建立的起点和传递的根.

可信存储根(Root of Trust for Storage)是一个记录并维护完整性度量的摘要值和摘要序列的引擎[13]. RTS 将完整性度量保存在日志中, 将其散列值保存在配置寄存器 PCR 中. RTS 还负责存储和保护委托给 TPM 的密钥(用于完成解密和签名操作)和数据, 同时管理少量的内存.

可信报告根(Root of Trust for Reporting)是一个计算引擎, 主要用于实现平台的完整性报告和身份证明, 能够可靠的报告 RTS 持有的数据. 可信平台通过可信报告根对完整性度量值进行报告, 并通过身份证明密钥对报告的完整性度量值进行数字签名[6], 接收方通过校验完整性度量值并验证签名的有效性来判断平台的可信性.



© 中国科学院软件研究所 http://www.c-s-a.org.cn

### 2.3 密钥

TCG 规范定义了多种密钥, 严格规定了每种密钥的使用范围.

签名密钥(Signing Key)主要用于对应用数据和消息进行签名, 是一种非对称密钥, 可迁移的签名密钥可以在可信平台模块之间进行传递.

存储根密钥(Storage Root Key)在可信平台创建时由其属主生成, 主要用于封装其它密钥或加密数据量较小的数据[6]. SRK 是系统中权限最高的存储密钥, 是 TPM 密钥存储保护体系的根密钥, 是加密保护所有其他密钥的基础. 为了保护存储根密钥 SRK, 将其存储在 TPM 的非易失性存储区, 其他密钥经 SRK 加密后存储于 TPM 外部.

身份证明密钥(Attestation Identity Key)是一个不可迁移的非对称签名密钥, 主要用于对 TPM 生成的性能参数、PCR 值等进行签名[13], 用来证明平台的身份和环境配置. TPM 通过使用 AIK 向实体证明自己的身份, 在一个安全平台上可以根据不同的目的创建多个 AIK.

背书密钥(Endorsement Key)是一个不可迁移的非对称密钥, 是一个 RSA 密钥对, 不能直接用于数据加密或签名, 其主要功能是生成身份证明密钥 AIK. EK 生成于平台的生产过程中, 唯一标识一个 TPM 的真实身份[13], 可用于在建立平台所有者时解密用户的授权数据, 以及解密生成 AIK 时与之相关的数据.

## 3 基于可信计算的多租户隐私数据保护方案

由于可信平台模块只能在非虚拟化环境下工作, 在多租户环境下使用可信计算技术, 首先需要对其进行虚拟化, 本文基于文献[14]的虚拟化可信平台模块 vTPM, 利用 vTPM 提供的密钥生成、密钥保护和密钥管理功能设计了一种多租户隐私数据加密保护方案.

### 3.1 数据加密密钥的保护

数据加密保护的关键是保护加密密钥. 可信平台模块能够为存储在平台之外的数据提供保护, 包括存储保护和传输保护. 在 TPM 中, 当数据量小于 2048 位时, 可直接利用平台提供的 RSA 算法实现加解密. 当数据量大于 2048 位时[15], 平台可以生成一次一密的对称加密密钥(小于 2048 位)用于外部数据的加密, 再利用 TPM 加密保护这个密钥.

可信平台模块的密钥管理和保护采用分层保护的思想, 密钥存储保护体系如图 2 所示, 首先用密钥 K 加密外部数据, 然后用上层密钥 K–1 加密 K, 最后, 由权限最高的存储根密钥 SRK 加密保护 K–1. 加密后的数据构成数据 Blob 文件存储在外部存储器中, 而密钥 Blob 文件和由 SRK 分级保护的层次密钥由密钥缓存管理器 KCM(Key Cache Manager)进行管理[11]. 在整个密钥存储保护体系中, 最重要的是确保 SRK 的安全.

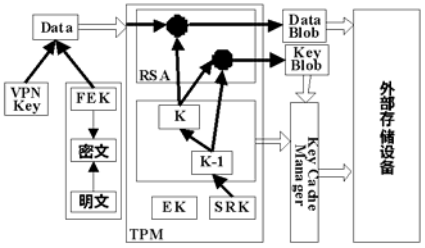


图 2　TPM 的密钥存储保护体系

根据 TCG 规范, TPM 能够建立以存储根密钥 SRK 作为根密钥的密钥体系, 由父密钥对其新生成子密钥的私钥进行加密, 从而产生一条到 SRK 的秘钥链. 文献[14]提供的虚拟 TPM 能够为每个 vTPM 实例创建一个独立的密钥体系, 使之不再依赖硬件 TPM 的密钥体系, 这样既有利于密钥的快速产生, 又能够简化 vTPM 实例的迁移. 虚拟 TPM 还能够为每个 vTPM 实例创建背书密钥 EK, 使虚拟 TPM 被迁移后, 依赖 EK 私钥解密信息的 TPM 指令集依然能够工作.

为了能够独立、灵活的管理每个虚拟 TPM 的密钥体系, 可以将虚拟 TPM 的 SRK、EK 和其他关键数据写入非易失性存储区, 并使用根植于硬件 TPM 中的对称密钥对其进行加密, 例如, 在系统启动过程中, 将该对称密钥密封在硬件 TPM 的配置寄存器 PCR 的状态中, 或者通过受密码保护的密钥对其进行加密.

### 3.2 虚拟可信平台模块

由于可信平台模块 TPM 只能工作在非虚拟化环境下, 在多租户应用中使用可信平台模块, 首先需要将其进行虚拟化, 文献[14]实现了可信平台模块的软件实现方式, 并提供了虚拟可信平台模块 vTPM.

虚拟可信平台模块能够为与其对应的虚拟机提供 TPM 服务, 并满足以下要求: 能够为运行在虚拟机上的操作系统提供应用模型和 TPM 指令集, 就像直接运行在硬件 TPM 平台上的可信平台模块为其操作系统提供的一样; 能够在虚拟机的整个生命周期内保持虚



© 中国科学院软件研究所 http://www.c-s-a.org.cn

拟机与其虚拟 TPM 的关联关系, 甚至当虚拟机和对应的虚拟 TPM 从一个物理机迁移到另一个物理机时.

虚拟可信平台模块的体系结构如图 3 所示, 整个 vTPM 由一个 vTPM 管理器和多个 vTPM 实例构成. 每个 vTPM 实例都能够实现 TCG TPM1.2 规范[16]. vTPM 管理器用于为每一个需要 TPM 功能的虚拟机分配并创建属于它自己的 vTPM 实例, 并将虚拟机的请求传递给相应的 vTPM 实例. 为了实现虚拟 TPM, 文献[14]对 TPM1.2 指令集进行了扩展, 新增了支持虚拟 TPM 管理、迁移和应用的指令. 在整个密钥和数据的存储保护过程中, 最重要的是确保存储根密钥 SRK 的安全, 为了保护它, SRK 和背书密钥 EK 永久存储在 vTPM 实例内部, 由 vTPM 实例进行保护.

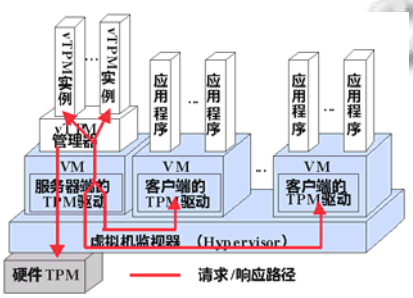


图 3 vTPM 的体系结构

### 3.3 方案的实现原理

在本方案中, 每个租户运行在虚拟服务器上, 对应并拥有独立的、唯一的虚拟机. 系统创建租户时, 根据租户是否有隐私数据加密保护需求, 决定是否为其虚拟机分配并创建 vTPM 实例. vTPM 实例将为其对应的租户提供硬件 TPM 拥有的密钥生成、保护和管理功能, 租户利用 vTPM 实例产生的密钥对自己的隐私数据进行加密, 然后基于 vTPM 实例提供的密钥管理和保护功能对密钥进行加密保护.

与硬件 TPM 一样, 每个 vTPM 实例对应一个唯一的存储根密钥 SRK, SRK 作为密钥存储保护体系的根密钥, 与 vTPM 实例进行绑定. 系统为租户创建 vTPM 实例时, 租户取得实例的所有权后, 系统会创建一个与该实例对应的唯一的存储根密钥 SRK.

由于不同租户对不同的隐私数据有不同的加密保护需求, 在存储根密钥 SRK 产生之后, 租户将通过其 vTPM 实例产生一个租户主密钥 TMK(Tenant Main Key), 如果租户对隐私数据的保护要求较高, 就通过 vTPM 实例产生的其他密钥对 TMK 进行加密; 如果租户对隐私数据的保护要求较低, 就直接用 SRK 加密 TMK.

每个租户的 TMK 由两对非对称密钥组成: 用来加密的称为租户加密密钥 TEK(Tenant Encryption Key)[17], 用来签名和验证的称为租户签名密钥 TSK(Tenant Signature Key). TEK 的公钥用于加密租户隐私数据的主密钥 PMK(Privacy Main Key), 确保只有合法的租户才能够获取 PMK; TSK 用于保护加密后的 PMK 的完整性. 每个 PMK 由三类对称密钥组成: 第一类用于加密隐私数据本身, 称为隐私加密密钥 PEK(Privacy Encryption Key); 第二类用于计算隐私数据的校验值, 只有具有写权限的租户拥有, 称为隐私数据写密钥 PWK(Privacy Written Key); 第三类用于校验隐私数据的校验值. 对租户隐私数据实施保护的步骤如下:

(1)在创建隐私数据文件之前, 租户通过 vTPM 实例随机产生两个密钥 PEK、PWK. PEK 直接加密隐私数据本身; 当需要对隐私数据进行写操作时, PWK 用于计算隐私数据的校验值.

(2)租户从 vTPM 实例获取 TEK 和 TSK, 用 TEK 对 PEK 和 PWK 进行加密保护, 加密结果称为该租户的加密密钥块 EKB(Encryption Key Block).

(3)对 EKB 进行 HASH 运算, 并通过 TSK 对 HASH 进行数字签名, 以保证数据的完整性.

(4)EKB 及其 HASH 签名构成访问该隐私数据的密码元数据, 即该隐私数据对应密钥的集合, 并存储在 md-file 中.

### 3.4 方案的实现

Xen 是一个由剑桥大学开发的开源虚拟机监视器, 能够支持在单个计算机上同时运行 100 个虚拟机. IBM 公司基于 Xen 实现了 vTPM, 其体系架构如图 4 所示, 本文基于此实现了本方案.

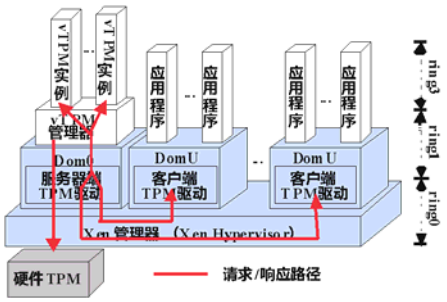


图 4 Xen 实现的 vTPM 体系架构



© 中国科学院软件研究所 http://www.c-s-a.org.cn

在系统引导阶段, Xen 的内核代码被装载到 ring0 的内存, Xen 在 ring1 上启动名为 Dom0 的 Linux 内核, 作为唯一运行在 Xen 管理器上的虚拟机. 根据租户的数量, Dom0 管理器可以创建多个运行在 ring1 虚拟机内核中的 DomU, 作为租户的虚拟机, 与租户一一对应. vTPM 管理器作为进程运行在 Dom0 下, 根据不同租户是否有隐私数据加密保护需求, vTPM 管理器决定是否为其创建 vTPM 实例, vTPM 实例完全依照 TCG TPM1.2 规范设计. 服务器端的 TPM 驱动程序能够给每个租户的 TPM 驱动命令包增加 4bit 的 vTPM 实例标识, 使租户的虚拟机与其 vTPM 实例一一对应. 在方案实现中, 部分秘钥产生代码如下:

```
Tspi_Context_Create(&hContext);
Tspi_Context_Connect(hContext, NULL);
Tspi_Context_GetTpmObject( hContext, &hTPM);
Tspi_Context_LoadKeyByUUID (hContext,
TSS_PS_TYPE_SYSTEM,SRK_UUID, &hSRK );
initFlags = TSS_KEY_TYPE_STORAGE |
TSS_KEY_SIZE_2048 |
TSS_KEY_NO_AUTHORIZATION |
TSS_KEY_NOT_MIGRATABLE;
Tspi_Context_CreateObject (hContext,
TSS_OBJECT_TYPE_RSAKEY,initFlags, &hKey );
Tspi_Key_CreateKey (hKey, hSRK, 0 );
```

## 4 结语

多租户技术是实现 SaaS 服务模式的核心, 本文针对多租户应用的特点和多租户隐私数据保护的需求, 将可信计算技术引入隐私数据保护, 提出了一种可定制的多租户隐私数据加密保护方案. 该方案利用虚拟可信平台模块 vTPM 提供的密钥产生、保护和管理等功能为不同租户提供了不同级别的隐私数据保护服务, 满足了多租户隐私数据保护的可定制性、隔离性和安全性等要求. 最后, 基于 Xen 实现的 vTPM 实现了本方案, 从而为云计算环境下多租户隐私数据的保护提供了一种新的思路.

## 参考文献


1 张坤.面向多租户应用的云数据隐私保护机制研究[博士学位论文].济南:山东大学,2012.

2 林海略,韩燕波.多租户应用的性能管理关键问题研究.计算机学报,2010,33(10):1881.

3 彭荣.SaaS 模式下多租户系统架构及关键技术研究[硕士学位论文].大连:大连海事大学,2010.

4 叶伟等.互联网时代的软件革命–SaaS 架构设计.第一版.北京:电子工业出版社,2008:67.

5 TCG. https://www.trustedcomputinggroup.org.

6 陈仁海.嵌入式可信计算平台中加解密算法的研究[硕士学位论文].济南:山东大学,2012.

7 孟璟,徐宁.可信平台模块 TPM 安全芯片的性能测试.电子测试,2007,(1):32.

8 Trusted Computing Group. TPM Main Part 1: Design Principles Specification Version 1.2. TCG Published, 29 March 2006. https://www.trustedcomputinggroup.org.

9 Trusted Computing Group.TPM Main Part 2: TPM Structures Specification version 1.2. TCG Published, 29 March 2006. https://www.trustedcomputinggroup.org.

10 Trusted Computing Group.TPM Main Part 3: Commands Specification Version 1.2. TCG Published, 29 March 2006. https://www.trustedcomputinggroup.org/resources

11 Trusted Computing Group.TCG Specification Architecture Overview. Specification Revision1.2.TCG Published , 28 April 2004. https://www.trustedcomputinggroup.org

12 TCG Infrastructure Working Group.TCG Infrastructure Working Group. Use Cases Summary. Draft Version 0. 1. 7 March 2004. https://www.trustedcomputinggroup.org/resources.

13 陆建新.可信存储及其在安全数据管理中的应用研究[硕士学位论文].上海:上海交通大学,2008.

14 Berger S, Caceres R,Goldman KA, et al. vTPM: virtualizing the trusted platform module. Proc. of the 15th USENIX Security Symposium (USENIX Security 2006). Canada, 2006. 307–308, 310.

15 Bajikar. Trusted Platform Module (TPM) based Security on Notebook PCs-White Paper. Mobile Platforms Group, Intel Corporation, Jun. 20, 2002. 1–20.

16 Trusted Computing Group. TCG TPM Specification Version 1.2-Part 3 Commands.TCG Published, 9 July 2007. http://www.trustedcomputinggroup.org/resources/tpm_main_specification/.

17 章勤,刘树明.基于可信计算平台的加密文件系统.微处理机,2008,(1):41.




© 中国科学院软件研究所 http://www.c-s-a.org.cn