Research on Trusted Application Environment based on PTM

Tianhua Liu, Dawei Zhang, and Yichen Jiang

School of Computer and Information Technology, Beijing Jiaotong University, Beijing

dwzhang@bjtu.edu.cn

***Abstract*—Trusted Computing leverages Trusted Platform Module (TPM) as the root of trust to build secure computing environment so as to improve the security of terminals. But there are some security problems of user roaming and migration of sealed data because of binding between platforms and TPMs. Users oriented trusted computing model is built based on Portable Trusted Module (PTM). Trust chains in computing system is delivered effectively to end users based binding between user identities and PTMs. Trust measurement, trust storage and trust reporting based on PTM are also given in this paper.**

***Keywords*—trusted computing, trusted platform module, portable trusted module**

基于 PTM 的可信应用环境研究

刘天华　张大伟　蒋逸尘

北京交通大学计算机与信息技术学院，北京，中国

摘　要　为了提高计算终端的安全性，可信计算技术引入可信平台模块 TPM 作为系统的可信根来构建安全计算环境。由于 TPM 与平台间的一一绑定关系，使得基于 TPM 的用户漫游和封装数据迁移存在一定问题。基于便携式可信模块 PTM 构建的以用户为中心的可信应用模型，通过信任根与身份的一一绑定，将计算系统的可信有效地传递到终端用户，通过对基于 PTM 的信任模型、可信度量、可信存储和可信报告机制的研究，构建出一个以用户为中心的可信计算环境。

关键词　可信计算，可信平台模块，便携式可信模块

1．引言

随着信息和网络技术的不断发展，大量重要的应用程序和科研数据会存储在多种类型的计算终端上，信息安全问题也逐渐受到重视。为了解决来自于计算终端的安全隐患，可信计算组织(Trusted Computing Group, TCG)提出了可信计算概念并制定了相关标准解决安全问题[1]。TCG 将“信任”描述为“如果一个实体的行为总是按照预期的方式和目标进行，它就是可信的”[2]。可信计算的基本思想是:建立一条从信任根开始到应用的可信链，通过逐级地信任建立，把这种信任扩展到整个计算机系统[1]。网络中交互实体之间通过远程证明(Remote Attestation)技术来实现平台完整性证明。可信计算与传统安全体制的最大不同是可信计算是以硬件安全芯片即可信平台模块(Trusted Platform Module, TPM)[2]或可信密码模块(Trusted Cryptography Module, TCM)[3]为可信根，保证整个计算平台的安全和可信。

近年来，可信计算技术在国内外得到了迅速的发展。2003 年国际 IT 巨头厂商 Intel、Microsoft 等成立了可信计算组织，同年 10 月发布了 TPM 主规范(v1.2)[4]。此后，全球上百家大型 IT 企业都进入了可信计算领域，Microsoft 基于 TPM 提出了下一代安全计算基(NGSCB)的概念[5]。Intel 则通过其硬件优势在其部分商用平台上实现了支持 Intel® Trusted Execution Technology(TXT)技术的终端可信产品[6]。欧洲于 2006 年启动了名为“开放式可信计算(Open Trusted Computing)”的可信计算研究计划，有 23 个科研机构和工业组织参加研究[7]。2009 年 TPM v1.2 被接受为 ISO/IEC 标准 11889。可信计算已然成为一种全球性行为。

作为关系国家安全的核心技术，我国的可信计算研究在国家相关重要政策的引导下也迅速发展。2006 年 11 月中国可信计算工作组成立，如今工作组已经包括了 19 家成员，他们涉及芯片、PC 系统、网络接入、系统/应用软件、CA 证书等多个领域，可信产业链发展初具规模。2007 年

中央高校基本科研业务费支持（资助号：2011JBM228）

国家密码管理局出台《可信计算密码支撑平台功能与接口规范》[3]，以指导我国相关可信计算产品的开发和应用。国内产业界也推出了多款可信计算产品。2000 年 6 月武汉瑞达公司和武汉大学合作，开始研制安全计算机，2004 年 10 月通过了国家密码管理局技术鉴定，鉴定指出：“这是我国第一款自主研制的可信计算平台”。2005 年联想集团的“恒智”芯片和可信计算机相继研制成功。同年，北京兆日公司的 TPM 芯片也研制成功。2008 年，国民技术有限公司（原中兴集成电路）推出了符合 TCM 规范的“SSX44 可信密码模块安全芯片”[1]。

《可信计算密码支撑平台功能与接口规范》中对于可信计算平台功能架构的定义如图 1 所示[3]：

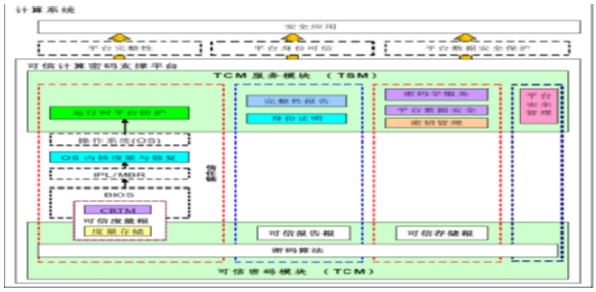

图 1 可信计算平台功能架构

作为系统可信根的 TCM/TPM 是计算机主板上的一部分，与计算平台一一对应。它具有三个重要的基本功能：

①. **可信度量**

从可信度量根开始，计算系统平台完整性度量值，记录该事件到事件日志，并把度量值记入可信密码模块内相应的平台配置寄存器(Platform Configuration Register，PCR)中，建立计算机系统平台信任链，确保系统平台可信。

②. **可信报告**

可信报告根标识平台身份的可信性，具有唯一性，以可信报告根为基础，实现平台身份证明和完整性报告。平台可向外部实体报告完整性度量值时，用平台身份密钥(Platform Identity Key，PIK)对度量值签名，接收方通过验证签名有效性以及校验完整性度量值来判断平台可信性。

③. **可信存储**

基于可信存储根，实现密钥管理、平台数据安全保护功能，提供相应的密码服务。TCM/TPM 通过使用存储根密钥(Storage Master Key，SMK)来分层保护平台数据。在数据保护方面，TCM/TPM 提供了数据加解密、数据封装(Seal、Unseal)和数字信封等方式。

一个计算平台上的多个用户可同时使用一个 TPM/TCM，体现出 TPM/TCM 与用户身份一对多的关系。这一可信应用模型存在如下几点问题[8]：

①. 系统的信任基础为计算平台而非用户本身。而在实际应用中用户是主体，用户希望把系统的信任基础由计算平台扩展到用户本身(如网银应用中用户可操控的 USB Key)，而固定于主板的可信模块是不能适用于这样的需求的。2007 年，Jonathan M.等人以“Turtles All the Way Down”形象地说明了这一问题[9]。例如，在远程证明的过程中，用户无法建立远程证明方(Remote Verifier)到用户间的可信路径(Trusted Path)，用户主机上的恶意软件可以将随意篡改的证明结果传递给用户及应用程序。攻击场景如图 2 所示：

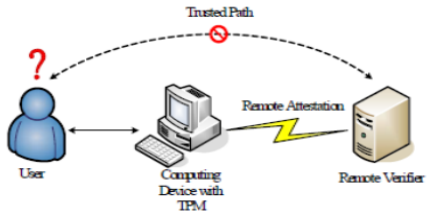

图 2 用户与远程证明方的可信路径问题

②. 个人计算平台和设备不断的多样化和小型化，个人用户会同时通过多个设备(用户漫游)来使用网络所提供的各种服务。在 TPM/TCM 与平台一对一绑定的模型下，用户受 TPM/TCM 保护的数据和程序不可避免地会在多个平台间不断地迁移(Migration)，由此带来的安全问题和管理开销不容忽视。图 3 为带有 TPM/TCM 主机间的数据迁移场景：

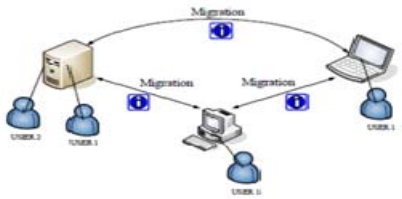

图 3 用户、TPM 与计算平台的关系

③. 如果不能够提供有效的备份机制，可信平台存在“单点失败”问题。如果某一主机唯一的 TPM/TCM 失效，系统的可信启动、可信报告和可信存储都将失效，依赖于远程证明和封装存储的服务和数据无法使用。这会极大降低系统的可用性。

为了解决上述问题，我们借鉴可信计算引入 TPM/TCM 作为平台信任根的思想，引入硬件密码模块作为用户信任根，提出了基于 USB Key 的便携式可信模块(Portable trusted Module, PTM)的概念。PTM 是一个带有密码芯片、LCD 屏和按键的 USB Key，它通过软件实现提供了可信度量、可信存储和可信报告的安全原语(Security Primitives)，是一个与用户身份一对一绑定的个人安全设备。基于 PTM

提供的安全原语，通过交互协议的设计，本研究工作旨在提出可信路径、用户漫游和安全备份的一种新的解决方法，从而为用户构建一个更加安全、可靠的可信计算系统。

本文通过对 PTM 的硬件结构、安全原语和安全协议的研究，构建出一个基于 PTM 以用户为中心的可信计算环境，从而解决“*将计算系统的可信有效传递到现实世界的终端用户*”的问题。

2．基于 PTM 的信任模型

PTM 可信应用模型应充分吸取 TPM/TCM 系列规范的设计理念和 USB Key 应用的成功模式，从涵盖 TPM 核心概念的角度出发，与 TPM/TCM 技术规范衔接，然后设计出以用户为中心的便携式可信模块方案。在涵盖 TPM 核心概念的同时，充分发挥将可信延伸到终端用户的特点，为以用户为中心的可信应用场景提供合理的补充。传统 TPM 要求与主机平台绑定，而在便携式 TPM 模型中，TPM 与主机是分离的，这要求对传统可信计算模型中，用户身份与主机平台、TPM 的对应关系、密钥存储层次结构等重新进行建模。我们提出了 PTM 与用户身份 1:1 绑定、与平台 1:n 绑定的应用模型。将信任扩展到了平台用户。其基本结构如图 4 所示：

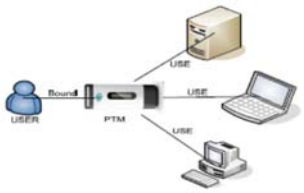

图 4 PTM 的可信应用模型

在用户平台和身份绑定关系方面，涉及到两方面的内容：

- **用户管理**

  对于 PTM 单一用户的授权和认证协议的设计。

- **平台管理**

  多平台信息在 PTM 中的注册方法；多平台状态信息验证和评估；多平台状态信息更新；平台与 PTM 间的相互认证方法等。

在 PTM 的部署方案中，我们考虑了两种不同的情况以适应于不同的应用需求：方案一为 PTM 与 TPM 共同存在于宿主机上，二者通过交互配合共同完成可信度量、可信存储和可信报告过程，PTM 作为将信任链延伸到终端用户的有效工具；方案二为 PTM 单独存在于宿主机上，一般发生于宿主机 TPM/TCM 失效(PTM 作为备份 TPM/TCM)或瘦客户端机器(如 sun 公司的 SunRay 系统)，PTM 需单独完成可信度量、可信存储和可信报告过程。两种不同方案在信任链的建立过程中会有所差异。

同时，在可信应用模型的构建上还要考虑 PTM 与主机间的信任建立问题。在这一过程中，我们采用 PTM 固件自身进行完整性度量并通过远程证明机制向主机证明自身平台可信。这一方案的实现必须与 PTM 固件安全原语和程序的设计相结合。

3．用户可感知的远程证明方法

PTM 可向外部实体提供完整性度量值来实现远程证明，所报告的度量值作为判断可信计算平台可信性的依据。TPM/TCM 规范中规定的完整性报告应满足如下要求：

1) 平台能够向验证者提供指定 PCR 值，无需任何授权。
2) 平台能够向验证者提供指定 PCR 值以及使用平台身份密钥对 PCR 值的签名。
3) 平台可向验证者提供指定 PCR 的相关事件日志信息。
4) 验证者可通过分析完整性度量事件日志信息判断该 PCR 值是否来自正确的度量过程。
5) 验证者应使用平台身份密钥验证 PCR 值签名，获得平台完整性报告结果。
6) 验证者将验证结果提供给平台。

在现实应用中，远程证明方是否可信需要用户做出最终的判断。平台上的恶意软件往往会干扰这一过程，而如何通过 PTM 构建一条由远程方到用户的可信路径是一个关键问题。我们通过在 PTM 上加入可信输入输出模块，即液晶屏和按键使用户可直接观察和控制证明过程。通过固件程序保证液晶屏上的显示和按键操作无法被 PTM 外的任何程序所控制，并通过相关的密码协议和安全原语的设计来构建一条用户到远程主机的可信路径。在证明协议的基础结构上，我们拟采用目前得到广泛应用的 SSL/TLS 协议，以利于 PTM 在现有网络交易系统中的部署。

4． 支持用户漫游的可信存储方案

可信存储机制中主要涉及到密钥管理和数据保护两方面的内容。可信计算中的密钥安全性直接关系到整个可信计算平台的安全程度，在整个可信计算体系中占有举足轻重的地位。与传统的 TPM 密钥管理相比较，便携式可信模块密钥管理不同之处主要体现在以下几个方面：

1） 密钥管理

传统的 TPM 模块与计算机平台进行绑定，而便携式可信模块与用户身份进行绑定。PTM 密钥管理与平台的关系如图 5 所示。在整个密钥体系中，每个密钥在开始创建的时候都指定了固定的密钥属性。密钥按照属性不同分为：可迁移密钥(Migratable Key)、不可迁移密钥(Non-Migratable Key)。不同于传统的 TPM 模块是与计算机平台进行绑定的，PTM 与身份进行绑定。在密钥的分层管

理结构中，我们划分出跨平台密钥和单平台密钥的不同层次结构。从而形成不同的密钥树分枝，以利于多平台情况下的密钥管理。基于这样的密钥管理结构，可设计出多种数据保护方案，以利于用户实现基于 PTM 的可信域扩展。

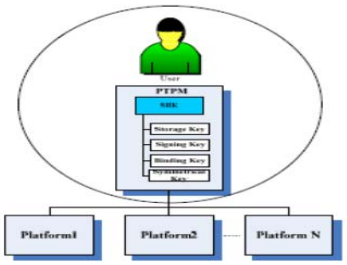

图 5 PTM 密钥与平台的关系

2） 数据保护

数据安全保护是 PTM 的核心功能之一，其数据安全保护基于 PTM 采用片内的加密算法对被保护数据进行加密，数据安全保护方式包括：数据加解密、数据封装等方式。将数据与特定的平台状态(PCR 值)及 PTM 绑定在一起，这种操作称为数据封装。受保护的数据只能在特定的绑定了 PTM 的系统平台以及平台特定的完整性状态下才能被解封。数据加密使一个数据只能绑定于一个可信密码模块。

在 TCM 规范中，使用对称密码算法的封装表示为：

sealedData = SMS4_Encrypt (key, (data || PCR_{Value} || TCM_Proof))

其中 TCM_Proof 为 TCM 唯一性标识。

数据的解封表示为：

a) 可信密码模块解密数据：

data || PCR_{Value} || TCM_Proof = SMS4_Decrypt (key, sealedData)

b) 可信密码模块比对当前 PCR 的值是否与解密出的 PCRValue 相同

c) 可信密码模块比对解密出的 TCM_Proof 是否与内部存储的数值相同

d) 若比对相同，输出 data。

使用椭圆曲线密码算法的封装表示为：

sealedData=SM2_Encrypt($SM2_{PUBKEY}$,(data||PCR_{Value}||TCM_Proof))

数据的解封表示为：

a) 可信密码模块解密数据：

data||PCR_{Value}||TCM_Proof=SM2_Decrypt($SM2_{PRIKEY}$,sealedData)

b) 可信密码模块比对当前 PCR 的值是否与解密出的 PCR_{Value} 相同

c) 可信密码模块比对解密出的 TCM_Proof 是否与内部存储的数值相同

d) 若比对相同，输出 data。

在用户漫游的情况下，存在多平台间的数据封装和解封的需要，使用平台的二进制配置信息 PCR 值无法适应于多平台多配置的应用环境。因此我们针对不同的应用场景拟采取两种方案来解决这一问题。方案一为在用户较为固定的应用场景中，如面向企业的客户应用，拟采取通过第三方发放授权平台配置列表的方法来实现多配置数据封装和解封。方案二为用户随意的应用场景，我们拟采取基于组签名的方法来解决这一问题。系统通过将合法的不同配置绑定到一组签名私钥上，当客户端配置满足这一配置时，即使用相应的私钥签名挑战数据，验证方通过验证签名结果来判断平台状态，如果验证通过则解封数据。

5．结论

本文通过对 PTM 的硬件结构、安全原语和安全协议的研究，构建出一个基于 PTM 以用户为中心的可信计算环境，从而解决“***将计算系统的可信有效传递到现实世界的终端用户***”的问题。本工作在理论上对目前基于平台绑定的 TPM/TCM 构建的可信计算技术的有益扩充；在实践上可将研究结果直接应用到目前广泛使用的电子商务、电子政务系统中，在不改变现有用户体验(沿用了传统的 USB Key 设备)的情况下，有效地解决网络交易的安全可信问题。因此，本研究工作在理论和实践上都具有非常重要的意义。

参考文献(References)

[1] C. Shen, H. Zhang, D. Feng, Z. Cao, J Huang, A survey of information security. Science in China, 2007, 37(2): 129-150.

[2] Trusted Computing Group: TCG Specification Architecture Overview. TCG, 2007. http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14/

[3] SCA. Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing. OSCCA, 2007. http://www.oscca.gov.cn/Doc/17/News_1133.htm

[4] TCG: TPM Main. TCG, 2005. http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[5] Microsoft: Next-generation secure computing base. Microsoft. http://www.microsoft.com/resources/ngscb/default.mspx

[6] Intel: Intel® Trusted Execution Technology (Intel® TXT). Intel, 2007.http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf

[7] OTC: Open Trusted Computing. OTC. http://www.opentc.net

[8] D. Zhang, Z. Han, G. Yan. A portable TPM based on USB key. Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010: 750-752.

[9] J. McCune, A. Perrig, A. Seshadri, et al. Turtles All The Way Down: Research Challenges in User-Based Attestation. Proceedings of the 2nd USENIX workshop on Hot Topics in Security. Boston, USA, 2007.15-19