

# 一种基于 TPM 的数据链系统密钥管理方案

路士兵,朱 麟,夏 鑫  
(公安海警学院,浙江 宁波 315801)

**摘 要:**深入研究密钥管理机制的安全性、合理性和实用性,设计和实现适应于 TPM 芯片的密钥管理机制和证书管理机制,提高可信计算平台的安全性、可维护性和易用性,是可信计算平台有效应用的基础,关系到电子政务、电子商务等网络虚拟业务的普及和发展。密钥安全是密码系统安全运行的关键,密钥管理方案是信息安全管理的重要内容,支撑着密码保障的全过程。然而,密钥管理方案的设计却容易被人们忽视。鉴于可信计算的信任链传递机制有效保护了计算机中存储数据的机密性和安全性,并能够防止恶意软件对计算机的攻击。提出了数据链系统的安全管理模型,设计并实现了一种基于 TPM(可信平台模块)的数据链系统密钥管理方案。通过认证,表明该方案能够很好地保证数据链系统密钥管理的真实性、完整性和机密性。

**关键词:**可信计算;可信平台模块;密钥管理;信息安全;数据链系统

**中图分类号:**TP302

**文献标识码:**A

**文章编号:**1673-629X(2019)04-0087-04

**doi:**10.3969/j.issn.1673-629X.2019.04.018

## A Key Management Scheme of Data Chain System Based on TPM

LU Shi-bing, ZHU Lin, XIA Xin  
(China Maritime Police Academy, Ningbo 315801, China)

**Abstract:** Further study of safety, rationality and practicability of the key management mechanism, design and implementation of key management mechanism and certificate management mechanism adapted to the TPM chip, improvement of the security the trusted computing platform and its maintainability and ease of use, is the foundation of effective application of trusted computing platform, which is related to e-government, e-commerce and other network popularization and development of virtual business. The key safety is the key to the operation of the cryptographic system. The key management scheme is an important content of information security management, which supports the whole process of the cryptographic protection. However, the design of the key management scheme is easily ignored. The trust chain transmission mechanism of trusted computing can effectively protect the confidentiality and security of the data, and prevent the computer being attacked by the malicious software. So we propose a model of safety management of data chain system, and design and implement a scheme of data chain system key management based on TPM (trusted platform module). The authentication shows that this scheme can effectively ensure the authenticity, integrity and confidentiality of the key management of data chain system.

**Key words:** trusted computing; trusted platform module; key management; information security; data chain system

## 0 引言

数据链系统密钥管理的稳定关乎各个部门的安全,如何保证这套系统的平稳运行,是需要好好规划的重点内容。安全防御的技术尤为重要,随着时间的推移,慢慢的由被动式防御向主动式防御发展。

密钥的保密是密码系统安全运行的重要环节,设计一种密钥管理方案或者一种合适的密码算法在系统安全运行中同样重要<sup>[1]</sup>。

文献[2]表明可信计算被认为是最有可能从根本

上解决信息系统安全问题的一种方法。目前国内外的学术机构和业界针对可信计算的研究内容相当广泛,正处于发展的上升期。基于可信平台模块(trusted platform module, TPM)的密钥管理机制的研究也在不断深入,学术界和产业界正在合作探索有关这方面的标准和规范。文献[3]在实现可信启动的过程中,不是基于一个可信的硬盘而是一个 CD,这和其他模型中实现可信启动的观点不同。文献[4]在 FreeBSD 系统的基础上,启动可信的过程分为五个等级,按照流程

收稿日期:2018-04-27

修回日期:2018-08-28

网络出版时间:2018-12-20

基金项目:公安部技术研究计划项目(2016JSYJC60)

作者简介:路士兵(1978-),男,副教授,从事嵌入式系统、可信计算和信息安全方面的研究。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20181220.1035.024.html>

进行启动时,对下一级进行验证,只有通过验证之后才能向下传递,这种传递方法,正是可信计算的根本所在。文献[5]介绍了安全加载和可信加载的区别和联系。文献[6]设计了一个可信启动过程,结合 TPM 提供的可信计算功能和保护存储,以及 TCG 规范中涉及到的可信度量和信任链的思想,实现了一种基于可信的模型。文献[7]提出一种基于可信引导的方案,使用可信服务器,需要验证下一层服务器,验证它的完整性,只有通过验证,才能进行转移控制权。文献[8]中提到 TPM 只是可信计算平台的基础,要让其应用中发挥作用,需要理解 TPM 的功能特点和关键机制,然后才能运用 TPM 的功能为应用服务。文献[9]中说明应用之间并没有非常清晰的分隔,虽然在进程中有隔离机制,但是各个应用之间的关系错综复杂,仍然可以进行你来我往的通信,这就存在潜在的风险。

构建一个安全的环境,以实现数据链系统的整体安全,是可信计算研究的方向。对此,文中提出一种基于 TPM 的数据链系统密钥管理应用方案,以期实现更多的安全功能。

## 1 数据链系统安全管理模型

根据数据链系统的安全要求和任务特点,数据链可分为通用数据链和专用数据链两种,系统按功能划分为四个区域,由外至里分别是:外网、内网、密码服务中心和安全监控中心。其安全管理模型如图 1 所示。

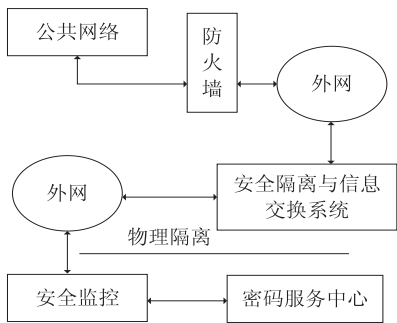


图 1 数据链系统安全管理模型

外网,即以互联网为依托的政府公共信息网,用于展示政府单位的风采和形象,宣传政府有关海洋、边境、口岸管理政策,实现政府与公众的双向信息交流,提供网上信息咨询服务。外网不涉及敏感或机密信息,所有对外公开发布的信息都必须进行敏感性界定,因此,外网可按照一般公共信息系统进行安全管理,保证其完整性和真实性。依托互联网络通信设施与其他友邻单位、上级或下级单位互联互通,必须使用 VPN 等相关密码加密设备,对链路传输的所有信息进行加密处理。

内网,即政府单位内部的指挥和办公自动化网,承载了本单位指挥自动化和网络化办公的各种指挥命

令、情况数据、业务信息等的传输和存储。在内网中,密码技术支持着各种业务应用和资源管理,所有用户按照权限划分,登录时进行身份认证和访问控制,实施严格的安全监控和跟踪审计。

密码服务中心,即系统安全管理的核心区域,承担着数据链系统的所有密码服务功能,如证书发放、密钥管理、权限管理等。

安全监控中心,即跟踪、监控、管理平台,承担系统内网和密码服务中心的安全监控任务,对发生的各种安全事故,实施应急响应和处理。

## 2 数据链密钥管理方案

该方案假定数据链系统中所有的服务器、终端和 UKey 都嵌有 TPM 模块,并由密码服务中心提供统一的密码服务<sup>[10]</sup>。密码服务中心包括密钥管理中心和数字证书认证中心,能够为政府单位数据链系统中的所有应用服务器以及使用单位和个人配发数字证书,并对系统中的所有用户和密码安全设备实施统一的管理<sup>[11]</sup>。

该方案的数据链系统采用基于 UKey 的挑战/响应双因子身份认证模式,并结合一次性动态口令技术和 USB 技术。由于 UKey 中嵌入了 TPM 模块,在 TPM 模块中可以存储相关数据,还可以自动生成随机的密钥,降低了泄密的可能性。

### 2.1 方案执行过程

该方案的具体执行过程可分为注册、登录认证两个阶段。在注册阶段,密码服务中心接受用户的注册请求,然后生成一个保存了用户认证信息的 UKey,并通过某种途径发放给用户;在登录认证阶段,用户利用 UKey 向终端发起认证请求,认证通过后,UKey 与终端绑定在一起,向服务器发起认证请求,所有认证请求都需要经过数次数据包交换来验证双方的身份。

#### 2.1.1 用户注册过程

初始运行前,每台机器和 UKey 都通过密码服务中心产生可以证明自己身份的身份密钥 AIK,并获得 AIK 证书。身份私钥由 TPM 内部产生,从不向外面泄露,并且只用来执行签名,不用来加密。身份公钥存储在 TPM 内部。每个 TPM 还产生存储密钥,存储密钥只用来加密,不用来签名。UKey 中存储有双证书(签名证书和加密证书)和用于终端密码重构的关键参数,由密码服务中心统一产生和配发,用于用户与通信终端之间的登录认证和密码装置的重构。UKey 与对应的终端绑定在一起,绑定过程由密码服务中心完成,不同的 UKey 与不同的终端不能互用。

#### 2.1.2 用户身份认证过程

用户身份认证有两个阶段,一个是用户启动终端

时,终端与用户(即 UKey)之间的相互认证,另一个是用户终端与用户终端通信时相互之间的认证。

(1)终端与 UKey 之间的认证过程。

终端与 UKey 的认证使用一次性动态口令技术,相互之间的认证过程如图 2 所示。

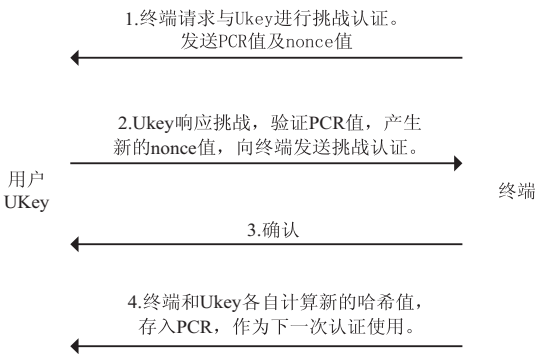


图 2 用户与终端的认证过程

(2)两通信终端之间的认证过程。

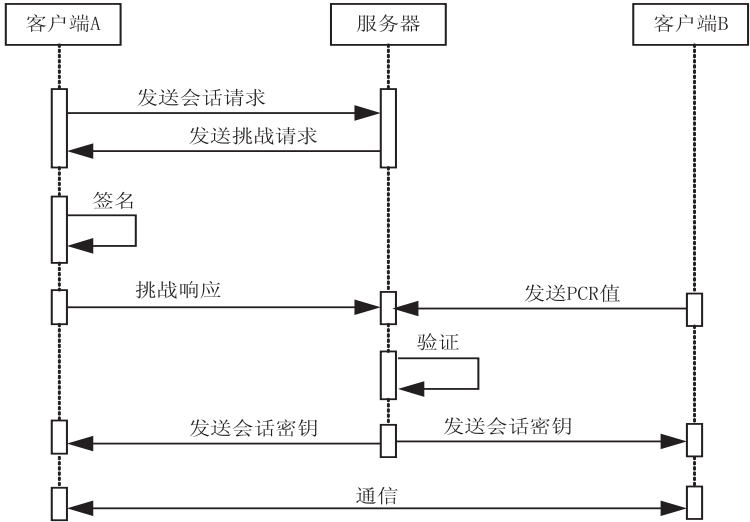


图 3 客户端之间的可信认证

认证完成后,客户端 A 和客户端 B 共享会话密钥 SessionKey,因此,可以确定两个相互通信的客户端是可信的。

第二种情况,客户端与服务器之间的认证使用 SSL 协议来完成,可以保证通信的机密性和交换数据的完整性,如图 4 所示。

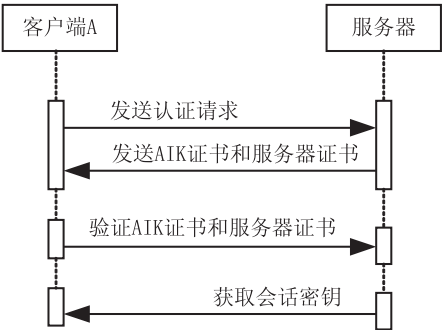


图 4 客户端与服务器之间的可信认证

一个可信平台要达到可信的目标,最基本的原则就是必须真实报告系统的状态,同时绝不暴露密钥和尽量不表露自己的身份。TCG 规范中,证明可以在不同层次进行:基于 TPM 的证明是一个提供 TPM 数据的校验操作,这是通过使用 AIK 对 TPM 内部某个 PCR 值的数字签名来完成的,AIK 是通过唯一秘密私钥 EK 获得的,可以唯一地确认身份;针对平台(to the platform)的证明则是通过使用平台相关的证书或这些证书的子集来提供证据,证明平台可以被信任以做出完整性度量报告;基于平台(of the platform)的证明通过在 TPM 中使用 AIK 对涉及平台环境状态的 PCR 值进行数字签名提供了平台完整性度量的证据<sup>[12-13]</sup>。

通常基于可信第三方 PCA 的可信计算平台身份证明主要有两种情况:

第一种情况,需要进行通信的两个客户端借助可信第三方进行相互认证,其认证过程如图 3 所示。

2.2 方案的安全性分析

该方案的业务流程是以服务器端和客户端的不同身份进入系统后,在确保用户登录为安全的情况下进行系统的维护和管理。

根据信息安全评估指南和 TCG 规范,可以看出文中提出的基于可信计算平台的数据链系统密钥管理方案很好地满足了信息的安全传输。

(1)只有得到授权的账号才能安全登录,按照权限的分类进行访问和执行修改;

(2)如何判断传输来的数据是否被篡改,针对平台(to the Platform)的证明则是通过使用平台相关的证书或这些证书的子集来提供证据,证明平台可以被信任以做出完整性度量报告,根据完整性度量报告确认数据的安全性;

(3)需要进行通信的两个客户端借助可信第三方进行相互认证,共享会话密钥,确保通信双方的可信;

(4) 客户端的认证方式, 通过使用 AIK 对 TPM 内部某个 PCR 值的数字签名来完成, AIK 是通过唯一秘密私钥 EK 获得的, 可以唯一地确认身份;

(5) 服务器和客户端有签名及生成随机数功能, 可以进行加密和解密。任何一个密钥都是有寿命的, 由可信终端进行分发和管理;

(6) 安全芯片存储在 TPM 模块, 任何一级使用终端都有自我检测和物理保护功能, 保证数据传输链路的安全和数据的完整性。

### 3 结束语

分析了数据链系统的组成和安全要求, 数据链系统中存储和传输的数据或信息主要有指控命令、监控信息、业务数据、日常值班值勤及请示报告、会议事务等各种机关内部的公文流转审批等, 并根据数据链系统的安全要求和任务特点, 提出了一种数据链系统的密钥管理方案。该方案除了满足包括政府在内的各级部门的指挥控制、政务信息化需要的同时, 还兼公开信息发布的职能。按照该密钥管理方案, 数据链系统信息安全保障是各部门信息化的关键环节, 是提高各级政府部门信息化水平和工作效率的基础, 也是决定基于 TPM 的数据链广泛应用的前提。最后通过安全性分析, 表明该方案能够很好地保证数据链系统密钥管理的真实性、完整性和机密性。

#### 参考文献:

[1] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 1999.

(上接第 86 页)

2016;1517-1525.

[14] MARTÍNEZ M, EDUARDO C. Análisis geoestadístico espacio tiempo basado en distancias y splines con aplicaciones[J]. Lancet, 2012, 365(9464): 1099-1104.

[15] 周同雪, 朱明. 视频图像中的运动目标检测[J]. 液晶与显示, 2017, 32(1): 40-47.

[16] METTES P, GEMERT J C V, CAPPALLO S, et al. Bag-of-fragments: selecting and encoding video fragments for event detection and recounting[C]//International conference on multimedia retrieval. Shanghai: ACM, 2015: 427-434.

[17] ONEATA D, VERBEEK J, SCHMID C. Action and event recognition with fisher vectors on a compact feature set[C]//IEEE international conference on computer vision. Sydney, NSW, Australia: IEEE, 2013: 1817-1824.

[2] 石勇. 面向云计算的可信虚拟环境关键技术研究[D]. 北京: 北京交通大学, 2017.

[3] NAKAMURA M, MUNETO S. Designing a trust chain for a thin client on a live Linux CD[C]//Proceedings of the 2007 ACM symposium on applied computing. Seoul, Korea: ACM, 2007: 1605-1606.

[4] ARBAUGH W A, FARBER D J, SMITH J M. A secure and reliable bootstrap architecture[C]//Proceedings of the 1997 IEEE symposium on security and privacy. [s. l.]: IEEE, 1997: 65.

[5] CHALLENGER D, YODER K, CATHERMAN R, et al. A practical guide to trusted computing[M]. [s. l.]: IBM Press, 2007: 13-28.

[6] 方艳湘, 黄涛. Linux 可信启动的设计与实现[J]. 计算机工程, 2006, 32(9): 51-53.

[7] 黄涛, 沈昌祥. 一种基于可信服务器的可信引导方案[J]. 武汉大学学报: 理学版, 2004, 50(S1): 12-14.

[8] 刘孜文, 冯登国. 基于可信计算的动态完整性度量架构[J]. 电子与信息学报, 2010, 32(4): 875-879.

[9] 赵勇, 韩臻, 刘吉强, 等. 适合于可信度量的可信应用环境体系结构[J]. 通信学报, 2007, 28(11A): 125-129.

[10] 侯方勇, 周进, 王志英, 等. 可信计算研究[J]. 计算机应用研究, 2004, 21(12): 1-4.

[11] 司丽敏. 可信计算平台信任链理论与技术研究[D]. 北京: 北京工业大学, 2011.

[12] CHEN Xiaofeng, FENG Dengguo. Direct anonymous attestation for next generation TPM[J]. Journal of Computers, 2008, 3(12): 43-50.

[13] AVIZIENIS A, LAPRIE J C, RANDELL B, et al. Basic concepts of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11-33.

[18] 刘翔, 吴谨, 祝愿博, 等. 基于视频序列的目标检测与跟踪技术研究[J]. 计算机技术与发展, 2009, 19(11): 179-182.

[19] WANG L, XIONG Y, WANG Z, et al. Temporal segment networks: towards good practices for deep action recognition[C]//European conference on computer vision. [s. l.]: [s. n.], 2016: 20-36.

[20] 孙艳丰, 张坤, 胡永利. 基于深度视频的人体行为特征表示与识别[J]. 北京工业大学学报, 2016, 42(7): 1001-1008.

[21] BRIELMANN A A, SPERING M. Effects of reward on the accuracy and dynamics of smooth pursuit eye movements[J]. Journal of Experimental Psychology Human Perception & Performance, 2015, 41(4): 917-918.