

# 可信计算研究

陈建勋,侯方勇,李磊

(国防科技大学 计算机学院,湖南 长沙 410073)

**摘要:**网络中存在的各种隐患已经严重威胁到信息安全,网络攻击越来越趋于隐蔽化,攻击手法趋于复杂化,并且新的攻击手段不断更新,传统网络防护技术尽管也在不断发展,但已显得力不从心。可信计算的思想是从内部入手,从根源上防止各种安全隐患问题的发生。为对可信计算研究现状有一个直观的认识,提出了对“可信计算”体系结构的看法,详细介绍了可信计算终端的概念、特点和原理机制,对可信终端关键部件的结构和特点进行了描述。综述了可信计算在国内外的研究进展情况及目前可信计算的研究内容,并结合已有研究成果,对可信计算未来的研究方向进行了展望。

**关键词:**可信计算;可信模块;可信软件协议栈;可信终端;信任链

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2010)09-0001-04

## A Review of Trusted Computing

CHEN Jian-xun, HOU Fang-yong, LI Lei

(School of Computer, National University of Defence Technology, Changsha 410073, China)

**Abstract:** A variety of hidden dangers that exist in the network has been a serious threat to information security, network attacks are increasingly covert, attack methods become more complicated, and the new means of attack constantly updated, traditional network protection technology, although also growing, but it has become inadequate. Trusted computing idea is to start from within, from the root causes of the problem to prevent the occurrence of a variety of security risks. To have a direct-viewing understanding to trusted computing research, present the “trusted computing” architecture views, introduced in detail the trusted computing terminal’s concept, characteristics and principles of mechanisms, have carried on the description to the trusted computing terminal key component’s structure and characteristics. Summarized the trusted computing in the domestic and foreign research development situation and the present trusted computing research content, and to integrate existing research results, future research on trusted computing direction was predicted.

**Key words:** trusted computing; trusted platform module; TCG software stack; trusted terminal; trusted chain

## 0 引言

在最初的信息安全建设中,人们首先想到的是防止外部攻击以及本地网络安全边界问题,因而重点采用访问控制、入侵检测、网络隔离和病毒防范等方法来解决信息安全问题。之后认识到,作为网络组成部分的终端是安全保障比较脆弱的地方,也是一般网络安全解决方案所容易忽视的地方,通过对网络安全事件的研究分析,网络上几乎所有的安全问题都来自终端<sup>[1]</sup>。当前网络安全措施存在的三个缺陷:一是主防外次防内;二是忽略了对终端的保护;三是合法用户在登陆网络时未进行严格的认证和授权控制,致使资源

滥用,存在弱点的系统被恶意程序利用进行非法破坏<sup>[2]</sup>。以被动防御为主导思想的传统安全技术已经无法抵御现今多种多样的攻击入侵,仅仅靠传统技术进行“防、堵、卡”解决不了问题,更不能有效解决由隐患终端内部引起的安全威胁,因此提出了可信计算的概念。

## 1 可信计算的体系结构

根据“可信计算”的定义及当前“可信计算”在实际生活中的应用,提出以下体系结构,如图1所示。

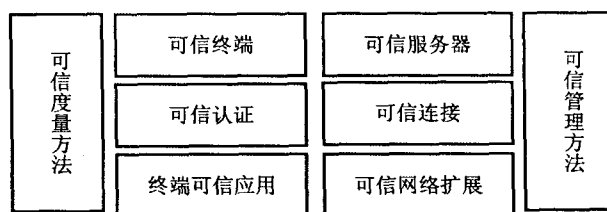


图1 可信计算体系结构

收稿日期:2009-12-30;修回日期:2010-03-09

基金项目:国家自然科学基金(60903040);国防科技大学预研项目(JC08-06-01)

作者简介:陈建勋(1980-),男,陕西西安人,硕士研究生,研究方向为可信计算;侯方勇,博士,副教授,研究方向为计算机体系结构、射频技术等。

(1)可信终端:可信终端是可信计算的一个重要组成部分,在整个可信计算体系结构中,处于基础性地位,包括可信硬件(TPM)、可信操作系统、可信应用软件。

(2)可信服务器:是指网络中提供服务的服务器是可信的,与可信终端相对应,与可信终端之间进行身份认证、数据传输等。

(3)可信认证:认证机制是有关安全性信息的规则(包括信任链、身份识别等机制)。

(4)可信连接:是指网络连接的可信,包括可信传输和可信接入。

(5)终端可信应用:包括基于可信网络上信息传递和可信交易。

(6)可信网络扩展:是指可信网络中的可信终端经过可信认证后网络范围逐渐扩大。

(7)可信度量和可信管理方法:可信度量方法是对可信计算的评估方法,包括可信等级、度量策略等。可信管理方法是指对网络应用体系中各个方面的可信技术和产品进行统一的管理和协调,从整体上提高整个计算机网络的可信等级的能力。

## 2 可信计算终端

各厂商对“可信计算”的理解不同,但主要设计思想是在终端的物理主板上设置一个安全芯片,作为平台的安全底层信任模块,配合系统软件保护终端的安全<sup>[3]</sup>。结构如图 2 所示。

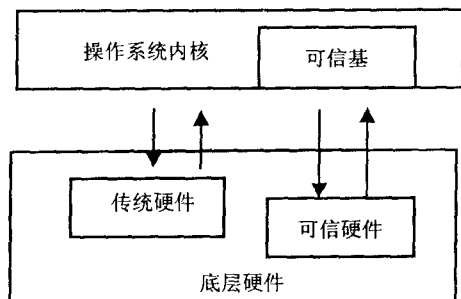


图 2 可信终端结构

图 2 中,可信终端包括可信的底层硬件和含可信内核的操作系统。可信硬件的主要作用是提供密码保护和存储;含可信内核的操作系统的主要作用是提供双重执行环境。

## 3 可信终端的特点和原理机制

### 3.1 可信终端的特点

●可信终端有以下特点:

(1)终端上的各种行为都是可预知和可控制的,终端存储、处理、传输信息具有完整性和机密性的特点,

其硬件环境配置、操作系统内核、应用程序具有完整性的特点<sup>[4]</sup>。

(2)终端具有机密性、完整性、可控性、可用性和抗抵赖性。

(3)可信终端上的任何操作都是经过授权和认证的。

(4)以 TPM 为基础,可信终端对系统一致性进行验证,其内部元素之间也存在严密的相互认证<sup>[5]</sup>。

●通过三个方面体现终端可信机制:

(1)完整性度量:可信终端的一个重要特征是完整性的度量,其功能是按照信任链的顺序提取、存储软硬件特征信息,信任根是完整性度量的起点。通过度量对需要保护和控制的软硬件提取特征信息,将信息的散列值保存在 TPM 自身拥有的安全存储器中,并与之前存储在终端中的正确特征信息散列值进行比对,确定其可信性,信任通过则进行下一步操作,从而实现信任传递。

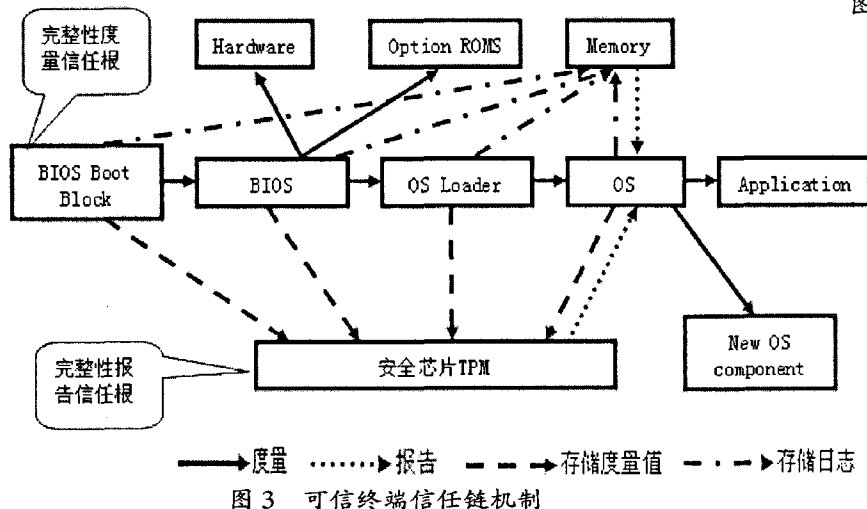
(2)安全存储机制:密钥和关键信息的安全存储是可信终端的一个重要的功能,它解决了传统安全解决方案的致命缺陷带来的问题,即硬盘存储的密钥和关键信息易于被盗取或篡改。

(3)可信报告:通过可信报告机制实现终端软硬件是否可信的验证和判定。该机制可以获取 TPM 中的特征信息,完成可信性的查询、对比,如果通过验证表明该特征信息满足某种特定要求,则认为该平台此时处于可信状态。

### 3.2 可信终端信任链机制

终端的可信建立在以 TPM 为信任根和从信任根开始的信任链上。TCG 认为如果从一个初始的“信任根”出发,在终端环境的每一次转换时,这种信任可以通过传递的方式保持下去,那么终端上的计算环境就是可信的。一个可信终端中有两个信任根:完整性度量信任根和完整性报告信任根。BIOS Boot Block 作为终端完整性度量信任根,TPM 作为终端完整性报告信任根。当终端启动时,完成 TPM 初始化,激活 SMBus 总线,为 TPM 分配 I/O 地址,配置 TPM,建立并验证 TPM 设备同驱动之间的通信流,对 PCR 执行 TPM—SHA1Start 和 TPM—SHA1Update 以及 TPM—SHA1CompleteExtend 操作,完成 HASH 操作,将缓冲区的数据传输到 TPM 并读取 TPM 的响应值。通过 bPhyPresenceTPMCmdId 参数的设定,与 TPM 通信。BIOS Boot Block 会度量 BIOS 的完整性值并将该值与存储在 TPM 配置寄存器 PCR 中的值对比,如果数值匹配,则将控制权交给 BIOS;然后 BIOS 度量 Hardware 和 ROMS,将度量到的完整性值继续与存储在 TPM 配置

寄存器 PCR 中的值对比,如果数值匹配,则将控制权移交下一信任级。之后终端装载操作系统并进行完整性检查,检查内核文件其他操作系统关键文件的完整性,加载执行操作系统内核文件。用户在使用操作系统前,检查信任根与终端、信任根与当前用户的对应关系,以确定用户身份可信。如果检验通过,用户输入用户名和口令进入操作系统,之后检查应用程序完整性。以上过程中如果一个组件被改动过,那么系统将拒绝执行下一步,如图 3 所示。



### 3.3 可信终端的身份标识机制

可信计算中,身份识别机制占有十分重要的位置,它包括终端的身份、终端拥有者的身份,终端用户身份,身份不同则权限不同,不同的密钥表示不同的身份,通过密码学对各种密钥的识别来保证各种身份的可靠性和不可抵赖性。

#### 4 可信模块和可信软件协议栈

#### 4.1 可信模块(TPM)

可信模块 TPM 是一个芯片,是可信计算平台的信任根,它从硬件底层提供对计算机软硬件环境的保护<sup>[6]</sup>。TPM 是一个带有密码运算功能和存储功能的小型芯片,内部集成了 CPU、RAM、ROM、密码运算处理器,随机数生成器、I/O 部件等模块<sup>[7]</sup>,通过 LPC (Low Pin Count)总线与 PC 芯片组合结合在一起,被固定连接在主板上,具有身份认证、密码运算、数字签名、可靠性认证、可信度量的存储和报告等功能。

根据 TCG 规范, TPM 的密码运算包含 SHA-1 散列算法、随机数产生器、对称密钥和非对称密钥生成机制、非对称加密和解密、对称密钥加密和解密。TPM 特有的安全存储器用于存储各软硬件的完整性信息<sup>[8]</sup>。TPM 的体系结构如图 4 所示。

在 TPM 中,配置寄存器(PCR)是一个非常关键的

部件,具有防篡改功能,主要用于存放可信任链建立过程中的实体的度量值。每一次度量值是以如下扩展方式加入 PCR 的:  $[PCR(new)] = SHA-1([PCR(old)] +$

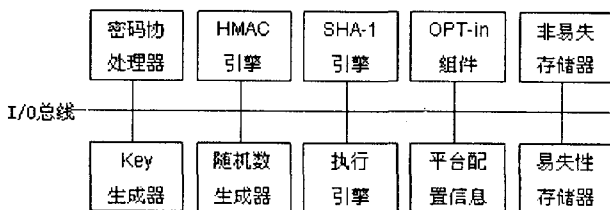
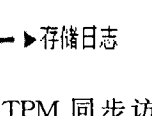


图 4 TPM 的体系结构

(new - measured - value)],即首先把事件数据和当前 PCR 中的值进行连接,而后计算连接值的摘要值,最后把该值存储在 PCR 中。在系统启动过程中,序列中的每一个执行程序在执行之前的度量摘要值都存储在 PCR 中。

## 4.2 可信软件协议栈(TSS)



支持 TPM 平台的支撑软件,它规定了 TPM 与操作系统结合的方式,为 TPM 应用提供入口点,实现

对 TPM 同步访问、管理,它的结构分为三个层次<sup>[9]</sup>,分别是设备驱动程序库 (TDDL)、核心服务 (TCS)、服务提供者 (TSP)。TDDL 具有三个功能:一是提供标准接口。二是打开和关闭设备驱动,发送和接收数据,查询驱动程序属性。三是在用户模式和内核模式之间提供一个通信通道<sup>[10]</sup>。TCS (TSS Core Service) 是一个系统服务进程,在用户模式下通过 TDDL 与安全芯片进行操作,管理 TPM 资源,提供一个 TPM 命令数据块产生器,把 TCS API 请求转换为 TPM 能够识别的字节流。上层应用通过 TCS 接口能够方便使用安全芯片所提供的功能。TSP (TSS Service Provider) 是一个普通进程,属于 TSS 的最上层,在用户模式下为应用程序提供丰富的面向对象接口,应用程序可根据安全芯片提供的功能通过它来构建所需的应用。

## 5 可信计算在国内外的的发展状况

### 5.1 国外发展状况

20 世纪 70 年代初期,Anderson J P 首次提出可信系统的概念<sup>[11]</sup>,人们开始了对可信系统的研究。1983 年美国国防部推出了“可信计算机系统评价标准”,其中定义了可信计算机系统。1999 年 10 月,由 Intel、HP、Compaq、IBM 和 Microsoft 发起成立了可信计算联盟

TCPA(Trusted Computing Platform Alliance),该组织致力于构建新一代具有安全、信任能力的硬件运算平台。TCPA 的成立标志着可信计算由学术研究转向了应用开发。2003 年 4 月 8 日,TCPA 重组为“可信计算组”TCG(Trusted Computing Group),它的改组标志着可信计算技术进一步的发展,应用领域得到了进一步的扩大。2001 年 9 月,TCPA 针对可信计算提出技术规范 V1.1<sup>[12]</sup>,事隔两年,TCG 提出新规范 V1.2。TCG 继续以构建安全硬件平台为宗旨的同时,加强了对软件安全性的要求,从硬件和软件接口两方面,制订与厂商独立的可信计算平台工作标准。Microsoft 公司根据可信计算发展趋势,于 2002 年 5 月提出“高可信计算”概念,从目标、手段、实施三个方面对“高可信计算”进行了解释。从最终用户实际需要出发,其目标包括三个方面:安全性、可靠性、完整性,而实现这些目标的手段必须从商务和工程方面进行考虑,遵循的策略包括:安全策略、可用性策略、隐私保护策略、可管理性策略、准确性策略、易用性策略。

## 5.2 国内发展状况

我国较早进入了可信计算领域的研究,并取得了令人满意的结果。2000 年 6 月,武汉瑞达公司与武汉大学合作研制可信计算机平台。2004 年 6 月,中国首届可信计算平台讨论论坛在武汉召开。10 月,第一届中国可信计算学术会议在武汉召开。2005 年,联想集团先后研制成功 TPM 芯片和可信计算机。同一年,兆日公司也成功研制出 TPM 芯片。随着网络安全形势日益严峻,问题隐患的不断增多,同方、方正、浪潮、天融信等公司也开始进行了可信计算的研究。

2008 年 12 月 16 日,中国可信计算工作组召开了成果展示暨产业化发展战略新闻发布会,从此次盛会了解到可信计算在中国的发展情况,可信芯片的产量、产品数量、可信规模都有了长足的发展与进步。

2009 年,中国可信计算工作组健全了可信计算相关标准规范;扩展与丰富芯片产品;进一步丰富行业应用与解决方案。工作组在《可信计算密码实施平台接口规范》的基础上,制定了测评以及接口等方面一系列的标准,为可信计算制定出了一个明确的可信计算的标准体系。目前可信计算领域的学术机构和商业界对可信计算的研究涉及多个方面,包括:

1)可信程序开发方法和可信程序开发工具的研究<sup>[13]</sup>。为了在开发系统过程中提高系统安全性,减少系统被恶意攻击的可能,拥有科学、先进理念的开发方法和高效、安全、功能完备的开发工具则必不可少。

2)软件构件可信性的建模、评估和预测。随着软件开发技术的不断完善,未来应用程序将由各种功能

不同的构件组装而成,不必按照传统思路从零开始进行开发,而具有可信性的构件是实现可信应用程序的前提,也只有确定了构件可信性的描述方法,才能对其进行评估和预测。

3)对容错和容侵技术的研究。计算机系统性能好坏的一项重要指标是容错性能,由于计算机初期的设计问题,使目前的计算机系统不可避免地存在各种安全隐患,要消除这些隐患是不大可能的,因此研究容侵技术保证系统受到攻击时仍能按预期设定执行关键操作则显得至关重要。

4)在分布式计算环境下对认证、授权等安全技术的研究。分布式计算已经成为主流模式,网格计算、公用计算、对等计算等概念已被人们熟知,在现有大规模、高复杂网络环境下,传统的网络安全技术已无法满足分布式计算的发展需求,因此分布式计算环境下的认证、授权等技术的研究则显得十分重要。

5)信任管理的研究。可信计算环境中,网络系统之间相互独立,系统之间进行信息交互是建立在相互信任的基础之上<sup>[14]</sup>,如何确定系统间的信任关系已经成为可信计算研究的基础性问题,通过信任管理实现正确判断系统信任关系,因此对信任管理的研究是实现网络环境可信的关键环节。

## 6 结束语

随着电子技术的不断发展,计算机网络已经融入到普通民众的生活之中,网上签名、电子商务在现实生活中具有同等的法律效力,但未来长期一段时间内,网络中运行的可信程序和传统网络技术仍然无法解决日益增多的网络安全问题,致使商业犯罪数量居高不下,给国家、企业带来巨大损失,因此,信息科学技术领域最重要的研究课题之一仍然是构建高可信性计算环境。可信计算的研究从三个方面考虑:一方面是学术领域对硬件平台、操作系统、应用程序、程序开发环境、网络系统及拓扑结构上进行理论研究,提供理论支持及可行性方案,确定可信计算未来发展方向。二是商业界研究制定可信计算平台工业标准,兼容不同厂商软硬件产品,避免资源浪费和重复研究,集中力量共同营造网络可信环境。三是可信计算应充分考虑网络技术现有手段和网络技术发展趋势,将可信计算的研究与未来信息应用、现有技术手段结合起来,才能更有市场价值。

## 参考文献:

- [1] IEEE Computer Society. 50 years of computing[J]. Computer

余数据报文的发送,达到提高网络工作效率的目的,加强了此方案的可行性。

通过文中提出的非 DHCP 客户机地址重用机制,实验中,当非 DHCP 客户机退出网络后,原来它占用的地址 10.10.104.66 得到重用,分配给 DHCP 客户机 C 使用,解决了原来非 DHCP 客户机退出网络后,地址浪费的弊端,一定程度上增加了网络内可用的 IP 地址数量,是对 DHCP 协议的扩展。

#### 4 结束语

DHCP 协议是应用非常广泛的一个应用层协议,文中提出了改进的 DHCP 服务器端地址分配方案和非 DHCP 客户机地址重用机制,并在 Linux 平台下进行了开发实现。通过实验表明,改进的 DHCP 服务器端地址分配方案,避免了原来协议中二次或者多次 DHCP 过程的发生,有效控制了 DHCP 过程中大量无效广播报文的产生,提高了网络性能;非 DHCP 客户机地址重用机制,对退出网络的非 DHCP 客户机的地址,可以进行回收分配,提高了网络内地址的利用效率。从协议的角度来说,是对主机动态配置协议功能的完善和性能的优化。

#### 参考文献:

- [1] Droms R. Dynamic Host Configuration Protocol[S]. IETF, RFC2131,1997.
- [2] Droms R, Alexander S. DHCP Options and BOOTP Vendor Extensions[S]. IETF, RFC2132,1997.
- [3] Mizoguchi S, Hori Y, Sakurai K. Monitoring Unused IP Addresses on Segments Managed by DHCP[C]//Fourth International Networked Computing and Advanced Information Management. Gyeongju, Korea: IEEE Computer Society Press, 2008:510-515.
- [4] Grochla K, Buga W, Dzierzega J. Demonstration of automatic address and radio parameters assignment in MANET using DHCP protocol extensions[C]//IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops. Kos: IEEE Press, 2009:1-3.
- [5] Joens Y T, Hublet C, De Schrijver P. DHCP reconfigure extension[S]. IETF, RFC3203, 2001.
- [6] Mohandas B K, Liscano R. IP address configuration in VANET using centralized DHCP[C]//33rd IEEE Conference on Local Computer Networks. Montreal, Que: IEEE Press, 2008:608-613.
- [7] Floris A, Tosetti L, Veltri L. Solutions for mobility support in DHCP-based environments[C]//IEEE International Conference on Communications. Anchorage, Alaska: IEEE Press, 2003:1043-1047.
- [8] Wang Jenq-Haur, Tsai Chun-Yi, Lee Tzao-Lin. DHCP support for secure automatic detection of host status[C]//13th Asia-Pacific Computer Systems Architecture Conference. Hsinchu: IEEE Press, 2008:1-4.
- [9] Komori T, Saito T. The secure DHCP system with user authentication[C]//27th Annual IEEE Conference on Local Computer Networks. The University of South Florida: IEEE Press, 2002:123-131.
- [10] Dai Jiang-Whai, Chiang Ling-Feng. A new method to detect abnormal IP address on DHCP[C]//IEEE Region 10 Conference TENCON. Taipei: IEEE Press, 2007:1-5.
- [11] 贾小东,孙向辉,彭四伟. DHCP 协议缺点及其解决方案[J]. 计算机工程, 2007, 33(23):138-139.
- [12] 任凤姣,王洪,贾卓生. DHCP 安全系统[J]. 计算机工程, 2004, 30(17):127-129.
- [13] 余堃,童永清. 基于智能卡和 PKI 的可信计算平台的研究与实现[D]. 成都:电子科技大学, 2008.
- [14] 王震宇,刘鑫杰,任杰,等. 嵌入式终端可信计算环境的关键技术[J]. 计算机工程, 2008(11):239-241.
- [15] DoD 5200.28-STD. Department of defense trusted computer system evaluation criteria[S]. 1985.
- [16] TCG. The dependable computing[EB/OL]. 2004. <http://www.dependability.org/>.
- [17] TCG. TCG Specification Architecture Overview[EB/OL]. 2008-01-12. [http://www.trustedcomputinggroup.org/groups/TCG\\_1.1\\_Architecture\\_Overview.pdf](http://www.trustedcomputinggroup.org/groups/TCG_1.1_Architecture_Overview.pdf).
- [18] 秦中元,胡爱群. 可信计算系统及其研究现状[J]. 计算机工程, 2006(4):38-45.
- [19] 林闯,彭雪梅. 可信网络研究[J]. 计算机学报, 2005, 28(5):751-758.

(上接第4页)

- [1] Innovation Technology Professional, 1996, 29(10):24-28.
- [2] Denning P J, McCalfe R M. Beyond calculation: the next fifty years of computing[M]. New York: Springer-Verlag New York inc, 1997:26-27.
- [3] 周明天,谭良. 可信计算及其进展[J]. 电子科技大学学报, 2006, 35(4):690-691.
- [4] Pearson S. Trusted Computing Platform, the Next Security solution[R]. Bristol, UK: HP Laboratories, 2002.
- [5] 邵时,袁亚. 基于可信计算技术嵌入式安全终端的研究与实现[D]. 上海:华东师范大学信息学院, 2007.
- [6] 谭兴烈. 可信计算平台中的关键部件 TPM[J]. 信息安全与通信保密, 2005(2):58-62.
- [7] Marshall D A, Michael V J. Trusted computing update[J]. Computer & Security, 1995(14):57-58.