

可信计算的研究与发展

禹蒲阳, 康国胜

(湖南科技大学 知识处理与网络化制造湖南省普通高校重点实验室, 湖南 湘潭 411201)

摘要:传统信息安全系统以防外部入侵为主,与现今信息安全的主要威胁来自内部的实际不符合。可信计算由内部防护,从根源上防止各种安全隐患问题的发生,成为信息安全研究的一个新阶段。其主要思想是将安全芯片嵌入到计算机硬件设备平台中,利用平台的安全特性来保障安全。概述了可信计算的研究背景及其基本概念,分析了国内外发展现状和可信计算对产业界带来的影响,最后针对可信计算的发展现状进行了展望以及对可信计算的重点研究问题与研究方法进行了思考。

关键词:可信计算;可信计算平台;可信平台模块;可信支撑软件

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2011)08-0233-04

Research and Development of Trusted Computing

YU Pu-yang, KANG Guo-sheng

(Hunan Province Key Laboratory of Knowledge Processing and Networked Manufacture,
Hunan University of Science and Technology, Xiangtan 411201, China)

Abstract: Traditional system of information security focuses on external invasion, which can not solve the practical situation of that the main menace in current information security systems comes from the inside. Trusted computing is to start from the within, from the courses of the problem to prevent the occurrence of a variety of security risks, making it become the new stage of information security. Its main idea is that the whole system's security is greatly improved via bringing security chip architecture in the computing hardware platform. In this paper, the background and basic concepts of trusted computing are introduced in detail, and its development both at home and abroad, and effects on industrial circles are presented. At last, a prospect about the development of trusted computing is made and the key research issues and research methods are given.

Key words: trusted computing; trusted computing platform; trusted platform module; trust software stack

1 可信计算的研究背景

传统信息安全系统以防外部入侵为主,与现今信息安全的主要威胁来自内部的实际不符合。采用传统的信息安全措施的最终结果是防不胜防。这是由于只封堵外围,没有从根本上解决产生不安全的问题。

概括起来,信息安全事故产生的技术原因主要有几点:

(1)目前的PC机软硬件结构简化,可任意使用资源,特别是修改执行代码,植入恶意程序;

(2)PC操作系统对执行代码不检查一致性,病毒程序可利用这一弱点将病毒代码嵌入到执行代码中进

行扩散;

(3)黑客可利用被攻击系统的漏洞,从而窃取超级用户权限,并植入攻击程序,最后进行肆意破坏,攻击计算机系统;

(4)合法的用户未得到严格的控制,从而可越权访问,致使不安全事故的发生^[1,2]。

所有这些入侵攻击都是从个人计算机终端上发起的。因此,应采取防内为主、内外兼防的模式来保护计算机,提高终端节点的安全性,建立具备安全防护功能的电脑系统。

为从终端上解决计算机系统安全的问题,需要建立信息的可信传递。这就和SARS期间隔离患者以控制病源的传播一样。计算机终端的“可信”实现了,人与程序之间、人与机器之间的数据可信传递就能得到保证。鉴于此,“可信计算”被提上了议事日程,这就是它的研究背景。所以,可信计算的核心就是要建立一种信任机制,用户信任计算机,计算机信任用户,用户在操作计算机时需要证明自己的身份,计算机在为

收稿日期:2011-01-20;修回日期:2011-04-22

基金项目:湖南省软科学研究计划项目(2006JT2003);湘潭市科技计划项目(JZ200738)

作者简介:禹蒲阳(1973-),女,工程师,硕士,主要研究方向为多媒体技术、人机交互技术;康国胜,硕士研究生,主要研究方向为服务计算。

用户服务时也要验证用户的身份。这样一种理念来自于人们所处的社会生活。社会之所以能够和谐运转,就得益于人与人之间建立的信任关系。与社会所不同的是建立信任的途径不同。社会之中的信任是通过亲情、友情、爱情等组带来建立,但计算机是没有感情的实体,一切的信息都是二进制串,所以在计算机世界中就需要建立一种二进制串的信任机制,这就必须使用密码技术,从而密码技术成为了可信计算的核心技术之一。

近年来,体现整体安全的可信计算技术越来越受到人们的关注,这正是因为它有别于传统的安全技术,从根本上来解决安全问题。

2 相关概念

1999 年,可信计算联盟(TCPA, Trusted Computing Platform Alliance)由英特尔牵头,联合 IBM、惠普、微软等国际厂商发起成立了,同时提出了可信计算这一概念。2001 年 1 月, TCPA 发布了基于硬件系统的“可信计算平台规范(V1.0)”^[3]。通过在计算机系统中嵌入独立计算引擎,抵制信息篡改,保证数据加密和身份认证的可行,防止非法用户对内部的数据进行修改。

TCPA 于 2003 年改名为 TCG (Trusted Computing Group),同年 10 月发布了 TPM 主规范(V1.2)。TCPA 和 TCG 共同对可信计算平台、可信网络连接和可信存储等系列技术规范进行了制定。目前,可信计算机已经进入实际应用的新阶段。

2.1 可信计算的概念

TCPA 最早提出“可信计算”的概念。然而,一直以来尚未形成统一定义,且各成员之间对“可信计算”的定义各不相同。

TCG 对“可信”做出的定义是:“如果某个实体对给定的目标,在执行时其行为总是和预测的一致,那么该实体被认为是可信的”^[4]。

ISO/IEC15408 标准的对“可信”也做出了自己的定义:某个组件、过程或者操作的行为在任何操作条件下,其结果都可预测,同时病毒、应用软件以及一定的物理干扰带来的破坏可以进行抵抗,那么被认为是可信的^[5]。

比尔·盖茨则提出可信计算是一种可随时获得,并且可靠安全的计算,使人类对计算机的信任程度,就比如使用电力系统、电话系统那样的安全和自由^[6]。

由上述的定义可得出,这些定义基本上均集中于考虑结果的可预测性,而且要求满足可用性和高可靠性等方面的需要。

同传统的基于病毒防护、防火墙或者入侵检测等为基础的终端安全模式比较,可信计算有其特别的优

势,其主要思想是在计算机硬件平台上嵌入安全芯片,利用其安全特性来提高终端的安全。所以 TCG 有一个理念就是单单利用软件来实现信息安全是绝对不够的,硬件安全应该比软件安全更好一点,但是光靠硬件也是不行的,硬件必须要有软件的支撑才能运作。

因此,可从以下几方面来理解可信计算的概念:

(1)为保证对使用者的信任,需要对用户的身份进行认证;

(2)为保证使用者对平台运行环境的信任,需要保证平台软硬件配置的正确性;

(3)为保证应用程序运行的可信,需要保证应用程序的完整性和合法性;

(4)为保证网络环境下平台之间的相互信任,平台之间必须可以相互验证^[1-3]。

2.2 可信计算平台

可信计算平台是一个计算机软硬件实体,它能够提供可信的计算服务,并且能够保证可信系统的可靠性、可用性以及行为的安全性这三方面的性能。可信计算的思想起初受社会生活的启发,它的主要思路是为计算机系统建立一个信任根,然后建立一条信任链,信任由信任根开始传到硬件平台,然后到操作系统,再到应用程序,达到一级测量认证一级,从而一级信任一级,最后将信任扩大到整个计算机系统,从而保证计算机系统的安全和可信,如图 1 所示。

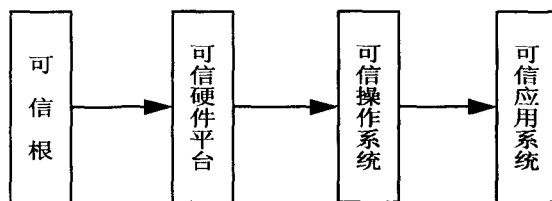


图 1 可信计算机系统

目前已实现的可信计算平台主要是可信 PC。其主要特征是在主板中嵌入可信构建模块 TBB。可信 PC 平台以 TBB 作为信任根。TBB 由可信测量根核 CRTM (Core Root of Trust for Measurement) 和可信平台模块 TPM (Trusted Platform Module), 以及它们同主板之间的联接构成^[7,9]。

2.3 可信计算平台模块 TPM

在可信计算技术体系中,最核心的就是可信平台模块 TPM 芯片。TPM 是一种 SOC 芯片,它是可信计算平台的信任根,其中信任根的可信性由物理安全和管理安全确保^[1-6]。

TPM 功能结构如图 2 所示,其主要组成部件有: CPU、I/O、存储器、随机数产生器、嵌入式操作系统和密码协处理器等。它的功能主要有:可信度量的报告、可信度量的存储、签名、密钥产生、数据安全存储、加密等^[9,10]。

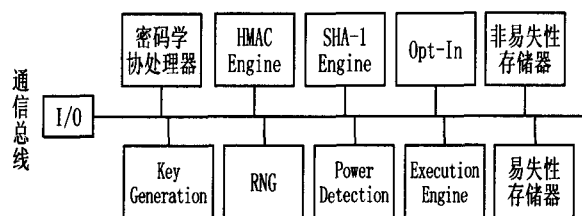


图2 TPM的体系结构

可信计算平台(TCP)技术将 BIOS 引导块作为完整性测量的信任根,TPM 作为完整性报告的信任根,对 BIOS 等进行完整性测量,保证计算环境的可信性。可信平台的信任链度量机制如图3所示。完整性测量由代理技术实现。TMP 拒绝下载和执行一切病毒等未经注册的软件,从而保证计算环境的可信。也就是说计算机在使用中无法涉及到不安全的操作与修改,而即便电脑被感染,因为病毒无法获得最大权限,因此电脑核心不会受损。

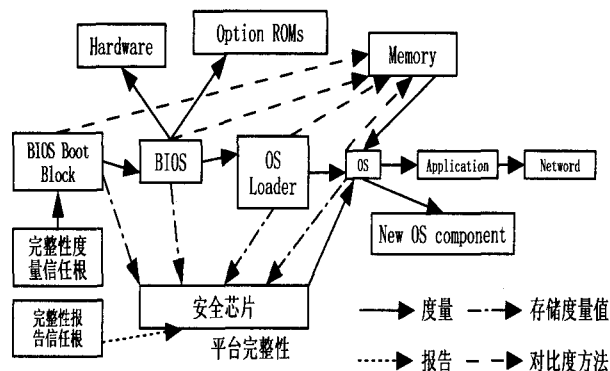


图3 可信平台的信任链度量机制

2.4 可信支撑软件 TSS

TSS(TCG Software Stack)^[7,8,11,12]是支持可信计算平台的软件,它的主要作用是为应用软件提供兼容异构可信平台模块的开发环境。它的设计目标是为TPM功能的应用程序的使用提供一个唯一的接口,即对TPM的同步访问、TPM资源的管理、TPM资源的适当释放等。TSS这一平台软件根据其结构可以分成三层,由下至上分别为TDDL、TCS和TSP,它们均运行于用户模式。TSS总体结构如图4所示。各部分的功能分别如下:

1)TDDL(TPM 驱动程序库)。它主要有两个功能:对各种不同安全芯片的差异进行屏蔽;提供用户模式和内核模式之间通信的通道。

2)TCS(TSS 核心服务)。它属于用户模式的系统进程,一般情况下以系统服务的形式存在,利用TDDL与安全芯片取得通信,并可以通过接口使用其提供的服务。TCS包含安全芯片所具有的原始功能、密钥管理等。

3)TSP(TSS 服务提供者)。它属于用户模式的用户进程,在TSS的最上层,TSP利用TCS来使用TPM

的功能,提供面向对象的接口,方便应用程序使用安全芯片提供的服务。

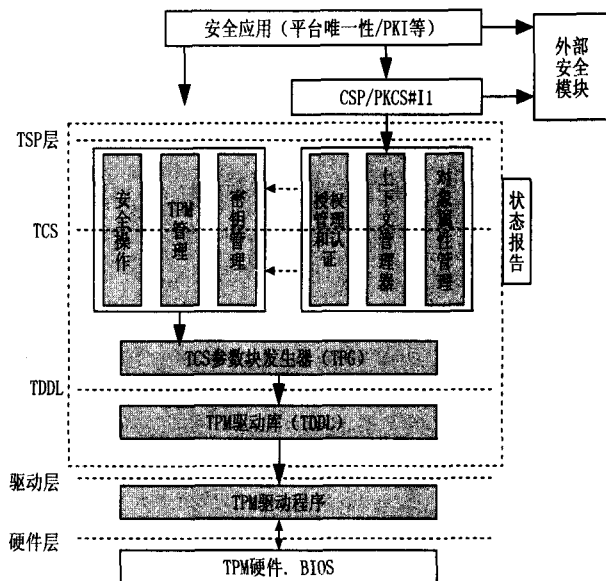


图4 TSS 总体结构

3 可信计算研究的发展

美国国防部于1983年制定了世界上第一个《可信计算机系统评价准则 TCSEC (Trusted Computer System Evaluation Criteria)》。同时,可信计算机和可信计算基TCB(Trusted Computing Base)的概念第一次在TCSEC中被提了出来,这就是可信计算的初现。接着,TCPA和TCG的出现形成了可信计算的新高潮。2006年初,欧洲开展了“开放式可信计算”的研究。在国内,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,它是国内第一款自主研发的可信计算平台,并已在我国公安、电子政务、军队、银行得到实际应用。2005年初,我国可信计算标准工作组成立。同年,由联想集团研制的“恒智”芯片和可信计算机陆续研发成功。与此同时,兆日公司也相继研发了TPM芯片。武汉大学、中科院软件所等各高校以及研究机构也开展了对可信计算的研究计划。另外,方正、天融信、同方、浪潮等公司也都纷纷加入可信计算的研究行列。并且,国家发改委、信息产业部、科技部、国家自然科学基金委等政府部门对可信计算的研究给予了高度的重视。2006年成立可信计算密码专项组,于2008年12月正式更名为中国可信计算工作组(China TCM Union,简称TCMU),并正式推出了TCMU官方网站,为更多的人了解和研究可信计算提供了一条绿色通道。2009年瑞达公司的“可信计算密码模块安全芯片”通过国家密码管理的认证,基于这一芯片的可信计算也推出上市。至此,我国的可信计算事业进入蓬勃发展的阶段。

4 可信计算对产业的影响

目前,产业界认为可信计算可能给产业带来以下几点重要的影响:

1) 有利于认证市场的开拓,各个公司都首先申请一个合法身份,以便让自己的程序可以在可信计算机上识别,进而给与权限运行。

2) 有利于规范软件版权,所有破解版将不能通过可信计算机的可信身份的识别。

3) 对开放源码的产品将有巨大的影响,因为在可信计算机上,理论上不应该允许用户随意更改代码、编译、运行软件(尤其对内核或驱动这种允许在特权级上的代码)。这样所谓的“自由”软件,将不再自由了。

4) 由于程序之间需要双方的合作,所以具有垄断地位的产品将更容易垄断,其它软件很难通过兼容已有产品来开拓市场。

5) 由于不能用自由软件的用户只能选择少数系统认可的软件,整个市场将失去竞争性。

5 可信计算研究的几点思考

5.1 可信计算标准亟待制定

业内人士表示,中国错过了发展具有自主知识产权的 CPU 和操作系统的机会,TCM 将是我国信息安全最后的防线。而当前面对的问题是,计算机操作系统的核心未能掌握,芯片的核心也不在国内。因此,是否在许多关键领域沿用国外标准值得思考。那么如何保证我们的信息安全呢?只有制定了国家可信计算平台标准,才能掌握产业发展的主动权,保障国家的利益。

5.2 可信操作系统亟待研制

因为可信操作系统是可信计算平台中的基石,并且可信计算平台同可信操作系统之间必须相互配合,因此可信计算平台的发展必然同时带动拥有自主知识产权的国产操作系统的发展,从而当今计算机中广泛采用国外不安全操作系统的局面就会被打破。所以,随着可信计算技术的研究及其相关产业成为一个热门的研究领域,在当前和今后一段时期内,构建基于可信计算平台的高可信操作系统是可信计算技术的研究重点。

5.3 企业、用户的安全意识需要提高

据 IDC 之前的预测,在 2010 年全球搭载可信计算芯片的电脑就要基本普及,然而目前在国内市场搭载可信计算的电脑率还很低。这是由于在国内市场对可信计算的认知度不够,以及企业和个人的普遍忧患意识不足。据业内人士分析,可信计算的市场前景广阔,所以国内必须抓住机遇发展具有我国自主知识产权的可信计算机。沈昌祥院士也曾指出,可信计算技术在

中国的发展势在必行。这就需要提高企业、用户的安全意识,以加强可信计算机的推广。

5.4 对可信计算的重点研究问题及研究方法的思考

可信计算组织 TCG 用实体的预期性来定义可信计算,这种以研究行为的信任问题应该是我们研究可信计算的重点。而行为本身属于理论范畴,TCG 有着强烈的工程背景,为行为的抽象提供了依据。

我国著名信息安全专家屈延文提出了“软件行为学”的理论,推动了可信计算的研究与发展。那么具体行为产生之后,效果如何判断与评估就需要建立信任模型。但信任模型并非当前 TCG 所提出的可信模型可以概述,TCG 所提出的可信模型中引入“信任根+信任链”是因为计算机的启动本身就是一个顺序的过程,在这个过程中引入认证机制并确定其源头可信是可行的。但诸如人类社会行为、网络运行行为等就不是这样一个线性的过程了,它们没有信任根与信任链可言。可信计算平台为工程实践提供了基础,属于工程范畴,所以行为信任问题的研究完全可以脱离可信计算平台进行。

参考文献:

- [1] 沈昌祥. 坚持自主创新加速发展可信计算[J]. 计算机安全, 2006(6): 2-4.
- [2] Denning P J, McElcalf R M. Beyond calculation: the next fifty years of computing [M]. New York: Springer-Verlag New York inc, 1997: 26-27.
- [3] 张焕国, 罗捷, 金刚, 等. 可信计算机技术与应用综述[J]. 计算机安全, 2006(6): 8-12.
- [4] Trusted Computing Group. TCG Specification Architecture Overview [EB/OL]. [2005-03-01]. http://www.trusted-computing-group.org/groups/TCG_1_0_Architecture_Overview.pdf.
- [5] Pearson S. Trusted Computing Platform, the next Security Solution[R], Bristol UK: HP Laboratories, 2002.
- [6] 林闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005(5): 751-757.
- [7] 张焕国, 罗捷, 金刚, 等. 可信计算研究进展[J]. 武汉大学报(理学报), 2006(5): 513-518.
- [8] 王勇, 徐小琳, 吕慧勤. 可信计算研究综述[J]. 信息网络安全, 2008(8): 34-36.
- [9] 肖政, 韩英, 叶蓬, 等. 基于可信计算平台的体系结构研究与应用[J]. 计算机应用, 2006(8): 1807-1812.
- [10] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学(E辑), 信息科学, 2007(2): 129-150.
- [11] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2): 139-166.
- [12] 陈建勋, 侯方勇, 李磊. 可信计算研究[J]. 计算机技术与发展, 2010, 20(9): 1-4.