加强计算机终端信息安全的两种解决方案

李 超[1],王红胜[1],陈军广[1],孙 蕊[2]
(1.军械工程学院 计算机工程系,河北 石家庄 050003;
2.军械工程学院 信息与管理分院,河北 石家庄 050003)

摘 要:目前,各种信息安全问题的不断发生,证实了操作系统和信息安全管理已不能适应信息私密性与完整性的要求,并且大多数安全问题发生在单位内部。因此,人们越来越意识到终端信息安全的重要性。针对计算机终端安全问题,总结并提出了两种主要的解决方案:一是基于可信平台模块的终端信息安全体系结构;二是操作系统安全信息防护体系的设计。这两种解决方案根据各自特点,满足不同用户的需求,共同构建计算机终端安全防护体系。

关键词:终端;信息安全;可信计算;可信平台
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)01-0165-03

Two Solutions to Strengthen Computer's Terminal Information Security

LI Chao[1], WANG Hong-sheng[1], CHEN Jun-guang[1], SUN Rui[2]
(1. Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;
2. Communication and Management College, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: At present, the occurrence of all kinds of information security problems verifies the fact that operation system and information security management be disabled to meet the privacy and integrality of information. Besides, many questions happened inner company. therefore, more and more people aware of the importance of terminal informations security. In order to solve this question, there are two solutions are provided in this paper: one is the architecture of terminal security based on trusted computing model. The other is the new system that defends operation system to information security. Used the two solutions with cooperation each other to build secure terminal by various requirements.

Key words: terminal; information security; trusted computing; trusted platform

0 引 言

随着信息与网络时代的到来,人们享受着便捷的办公与电子信息传递。然而,网络病毒、木马程序、黑客攻击等安全问题愈演愈烈,信息遭到篡改或窃取,其完整性和私密性面临着威胁。文中正是在这种情况下,针对为什么要加强终端信息安全,并对其解决方案进行研究与分析,最后分析了解决方案中存在的问题。

1 信息安全的基石——终端安全

1.1 信息安全面临的威胁

信息安全系统包括三个方面:网络传输、终端安全、服务器安全。人们更多地关注了网络传输,因为信息毕竟是在非控制的外部公共设备传输,一系列的加密措施、数字签名、VPN等方案收到了较好的效果。而对于终端信息安全却一直没有得到根本解决,安全事件的发起者在终端,最终造成失泄密的往往也是终端。我国公安部的统计数据也表明,70%的泄密犯罪来自单位内部。另外从我军近来通报的几起重大泄密事件来看,都是机密文件的处理不当(如被私自拷贝回家,在联接互联网的计算机上使用)造成的。

信息安全事关国防安全、社会稳定和经济发展。近一两年,国内外泄密事件的频频发生,究其根本原因,终端信息安全防护能力相差太远。对于相关重要单位和个人来说,计算机终端安全防护建设还是个空白。在如此不安全的终端上进行数据处理,怎能放心?

1.2 终端安全的提出

随着个人对信息私密性要求越来越高,操作系统已经漏洞百出了:比较弱势的身份验证;计算机软、硬件结构简化;资源可任意使用;操作系统对执行代码不检查一致性;敏感数据处理、存储安全措施不够;用户

收稿日期:2008-04-29
基金项目:全军重点科研计划项目(2007HZ4307001)
作者简介:李 超(1981-),男,陕西西安人,硕士研究生,研究方向为军事信息安全;王红胜,硕士,副教授,硕士生导师,研究方向为装备信息系统工程和系统安全。

权限没有严格的访问控制，可造成越权访问[1]；计算机输入输出设备存在安全缺陷。安全管理相对滞后：移动存储设备公私混用；私自接连互联网；在连接互联网的终端处理机密数据；私自复制秘密数据等等。

由此可见，终端安全是解决信息安全问题的核心和起点。终端信息安全的解决方案大致可分为两类：一是基于可信平台模块的可信计算技术的发展；二是加强操作系统安全软件防护体系。这两种解决方案可因需求和安全等级不同做出选择。从长远的发展考虑，第一种方案更适合信息安全的要求，以硬件作支撑，从根部"治疗"安全问题，信息的完整性和私密性得到了保护。第二种方案主要是应用软件技术给操作系统加上一层"防护罩"，应用方便，代价较少。下面是对这两种方案的研究设计。

2 操作系统信息安全防护体系

针对 Windows 操作系统在身份验证、文件系统安全、审计等三个环节存在的重大隐患，对终端操作系统信息安全防护体系作了如下设计：

2.1 高强度的身份认证

采用软硬件结合的强制性登录机制，通过 Windows 操作系统图形化认证接口(GINA)与操作系统无缝结合，可支持多种方式的身份认证，如 USB Key，指纹，视网膜等具有不可复制性的生物特征。在身份认证基础上结合恰当的授权体系，为终端树立一个坚固的大门。

2.2 安全文件系统研究

Windows 应用程序请求某种服务时调用 win32 API，通过 win32 子系统使用系统服务接口，I/O 管理器创建 IRP 请求并传给设备驱动程序，从而调用硬件抽象层使硬件工作。这里可以有多个驱动程序上下链接形成驱动程序堆栈(实际数据结构是由这些驱动程序创建的设备对象所构成的设备堆栈)，共同为此设备服务。IRP 依次通过各过滤驱动程序，直到某个驱动程序完成此 IRP 请求的操作[2]。

文件系统过滤驱动程序截获 IRP，在转发给原文件系统驱动程序之前，根据用户需求进行加、解密操作，确保了文件都以加密形式存储。并且能实现加、解密操作透明性，从而最大程度上保证用户界面友好易用。

简单示意图如图 1 所示。

2.3 计算机设备及接口监控

主要是监控计算机的外设接口或端口接入的设备。包括打印监控、接口监控、通信类设备监控。接口监控可详细监控记录本机外设端口(USB，1394 等)的设备接入情况，并可按类别屏蔽 USB、1394 等接口插入的设备，确保只有授权的或无安全隐患的设备才可以通过此接口接入计算机。

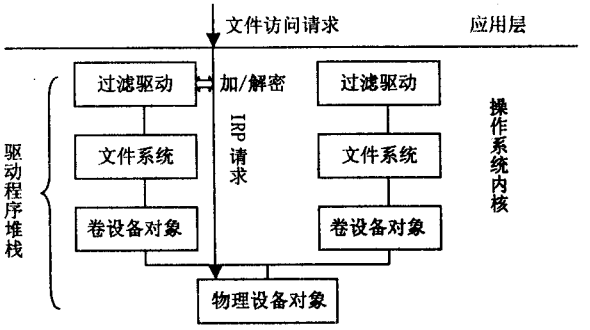

图 1 文件系统过滤驱动程序示意图

3 构建可信计算平台确保终端安全

操作系统安全防护体系毕竟是一个软件系统，有着软件系统共有的软肋，存在 BUG、易受攻击和破解等弱点。那么可以试着从硬件与软件的结合方面考虑终端安全问题。这就是下面要谈到的可信计算。

3.1 可信计算研究现状

根据 ISO/IEC 15408，可信计算的概念：所谓一个模块、操作或进程可信，即任何操作条件下，它们的行为是可预测的，并且能非常高效地抵抗应用软件、病毒的攻击和一定级别的物理干扰[3]。1999 年 10 月，由 HP、IBM 等大型公司联合成立了可信计算平台联盟(TCPA)。2003 年 3 月，TCPA 被改组为 TCG(The Trusted Computing Group)[3~6]。TCG 就是专门的发布可信计算规范的一个非赢利性组织。

我国着手可信计算研究不算晚，而且进展迅速。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 月研制出国内第一款自主研制的可信计算平台。2005 年，联想集团的 TPM (Trusted Platform Module)芯片和可信计算机相继研制成功，兆日公司的 TPM 芯片也研制成功[4]。

3.2 可信计算平台的构建

(1)可信计算平台的根本思想是通过在通用计算机主板中嵌入一块 TPM 芯片，结合安全芯片软件协议栈(TCG Software Stack，TSS)等软件接口，架设新的安全体系结构。本安全体系结构可以完成平台软硬件可信度量、文件加密、本地和远程平台认证、私密数据隔离存储等功能。TPM 的主要功能是证明平台配置是否可信和存储核心数据及相关密钥。前者是通过一组平台配置寄存器(Platform Configuration registers，PCR)来存储平台完整性度量后的度量报告。所谓度量报告即将软、硬件当前状态的完整性度量值连同

PCR 中当前值连接成一串,计算这个连串的 SHA－1 Hash 函数值,并将结果存入 PCR 中,这是一个不可逆转的更新方式。平台证明时一般重新度量平台信息并与 PCR 中的数据进行比较,以确定平台的可信性。为安全期间,用户可以将核心数据存储在 TPM 中。加密存储数据实际是复杂密码加速器的扩展,能够执行 SHA－1 哈希操作、RSA 操作、HMAC 鉴别、保护密钥以及可编程。TPM 将存储数据与具有特定配置平台绑定,通过指定 PCR 以及提供 20 字节长的认证码来封装数据,并将加密后的数据返回。解密时,平台将数据提交给 TPM,只有指定的 PCR 拥有和数据封装时相同的值,并且调用者提供正确的认证码,才能解密[7]。TPM 的硬件体系结构如图 2 所示。

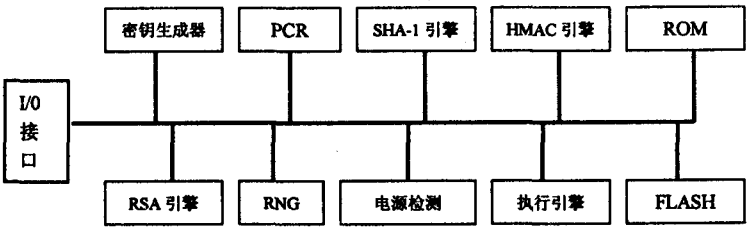

图 2　TPM 的硬件体系结构

(2)利用 RTM(Root of Trusted Measurement)作为可信根,构造一个可信环境。平台利用一个基于度量的可信根,通过可信引导方式完成每步的度量,用一条可信链,完成可信环境的构造。TPM 从计算机加电开始,PCR 会置零,平台完成度量后,就将度量报告与 BIOS 的 Hash 值写入 PCR 以记录当前 BIOS 的系统配置,如果这一步正确执行,BIOS 将下一步要执行的可信引导的代码(TSS)送到 TPM,TPM 按照同样的方式进行度量,并更新 PCR 值。依次加载 Operation System (OS)内核代码、OS 应用程序及 OS 相关组件等[8],分别进行度量,并更新 PCR 值。因此 TCG 将 BIOS 称为度量的信任根(RTM)。当然,内存的度量和检查不容忽视,敌手可以通过直接内存访问(DMA)技术绕过 TPM 的检查。可以在内存中存储加密公钥,没有 TPM 的私钥是不能访问内存的。

可信度量真正做的工作主要是检测软、硬件系统的环境是否改变或存在危机,因为 TPM 必须与指定的平台绑定,如果平台发生变化,TPM 会要求现在平台重新认证。

可信链的流程示意图如图 3 所示:虚线箭头表示完整性度量报告,实线表示完整性度量。

(3)TSS 提供了一个标准的软件接口访问 TPM 功能,以至于通过平台类型方便应用程序扩展和协同。TSS 内部包括三部分:最底层是 TDDL(TCG Device Driver Library),为上层提供 TPM 的设备驱动程序接口;中间层是 TCS(TCG Core Services),为上层提供核心服务接口,例如,完整性度量、加密存储信息等功能;最上一层是 TSP(TCG Service Provider),为应用程序提供服务接口。软件层的开发具有承上启下的作用,也是基于软、硬件结合构建可信平台的关键一步。

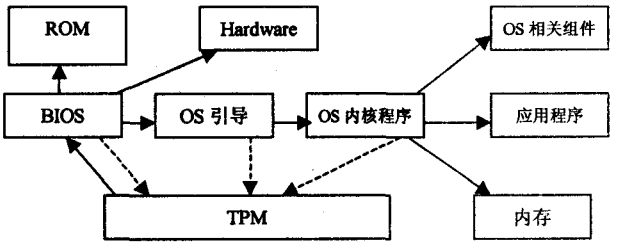

图 3　可信链流程示意图

TSS 也常常为现存的一些使用密码技术的 API 创建接口函数,例如:微软的 CAPI、CDSA、PKCS＃11 等。这样一来,TPM 就利用自己的这些 API 函数支持当前或以后的应用程序了。为了充分利用 TPM 的性能,文件备份密钥、移动密钥、平台证明和鉴定等,应用软件直接写入了 TSS 中[9]。

4　解决方案存在的问题

在解决终端安全的两个主要方案中,终端安全信息防护体系能够在短时间,依据操作系统或一些单位的特殊要求加强终端安全的防护,技术相对比较容易实现。但是存在软件系统自身的 BUG 问题,能解燃眉之急,却不是长久之策。

可信计算技术相对较新,理论还不成熟,还没有形成统一的规范,TPM 的体系结构也是不尽相同,动态信任链模型、可信操作系统、可信网络及可信数据库还有待研究。可信计算技术可以有效的加强计算机终端的安全水平,但是在目前看来,并不是所有的信息都需要高阶的安全保护,特别是考虑到成本要素。在未来的很长时间里,可信计算平台与终端安全信息防护体系仍将互相融合并共同朝着构建更加安全的计算机系统这个目标发展下去。

参考文献:

[1]　王　飞,刘　毅. 可信计算平台安全体系及应用研究[J]. 微计算机信息,2007,23(3):76－78.

[2]　Oney W. Programming the Microsoft Windows Driver Model [M]. 马少华译. [s.l.]:Microsoft Press,1999.

[3]　Nie Xiao－Wei, Feng Deng－Guo, Che Jian－Jun, et al. Design and Implementation of Security Operating System Based

(下转第 171 页)

文档夹或文档组、单个文档或应用对象(如电子邮件或日历项目)。

3.3.3 恢复时间应用集成

在进行恢复时,CDP解决方案能够识别出该应用的先前历史中最优化或最重要的恢复点。这类应用集成是完全自动的,也是可扩展的。

3.3.4 数据库连续保护

CDP解决方案一般都支持常见数据库环境(如Oracle或SQL)的连续保护。支持的意思是该解决方案经过了厂商的全面测试和认证,而且还会向用户提供相关文档内容。

3.3.5 库架构

大多数CDP解决方案是将任何数据的变化存储在单独的地点,形成存储库架构,而且这种存储库是局域网、广域网或存储区域网上明确的专用节点。

3.3.6 库复制

一些CDP解决方案还提供将CDP库复制到另外一个远程库的能力。这样就能够提供更高的灵活性,防止主CDP库可能出现损坏或丢失对恢复能力产生影响。

3.4 CDP发展方向

随着CDP应用范围的扩大和人们认知的深入,CDP技术将会作为在线数据的重要保护手段而独立开辟一条新的通道。其发展方向概括为三点:

第一,CDP的连续和系统保护范畴将继续延伸,从目前基于微软的各类操作系统平台延伸到更多企业级所采用的UNIX平台。

第二,在精细点恢复的技术上,拉杆式日志恢复技术将使精细点的恢复超越最近的快照点。该技术将为一些高端的、以秒级错误恢复为目标的用户带来真正的数据保护方案。

第三,继续完善历史数据的存档机制、在线数据和离线数据的分级保护体系。可利用在线多时间点数据在后台自动提取的serverless备份技术,将近期各时间点数据在不影响应用的情况下存档到VTL虚拟带库中或者存档到物理磁带库中,从而实现数据的离线保存能力和长时间历史数据的保管。

4 结束语

今后,人们的信息系统将面临着越来越多的人为的或自然的不确定因素的威胁,因此,融合现有技术,不断发展新技术,构建更加安全、可靠的数据容灾系统,已经成为当今世界共同关注的课题。

参考文献:

[1] 崔可升,王玉春.建设容灾系统的几点思考[J].计算机系统应用,2003(7):26-29.

[2] 王树鹏,云晓春,余翔湛,等.容灾的理论与关键技术分析[J].计算机工程与应用,2004(28):54-58.

[3] 李兆玉,韦世红,李　鹏.容灾系统的建设方案研究[J].重庆邮电学院学报:自然科学版,2005(4):35-37.

[4] 杜　宁,姚玉坤,黄　伟.浅析基于SAN的容灾实现[J].山东通信技术,2006(2):9-11.

[5] 胡　勇,罗维荣.容灾备份技术架构浅析[J].电子政务,2006(9):15-16.

[6] 妙全兴,武海鹰.一种高性价比的网络容灾与高可用集群的设计[J].微机发展(现更名:计算机技术与发展),2003,13(9):41-42.

[7] Benjamin B, Shao M. Optimal Redundancy Allocation for Information Technology Disaster Recovery in the Network Economy[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 3:262-267.

[8] 颜　军.CDP带来存储新气象[N].计算机世界报,2006-04-03(12).

(上接第164页)

[D].青岛:中国海洋大学,2005.

[4] 云辽飞.基于角色的访问控制技术在统一设备管理中心系统中的应用[D].西安:西安电子科技大学,2007.

[5] 范玉顺.工作流管理技术基础[M].北京:清华大学出版社,2001.

[6] 杨冬梅,张亦军.基于角色的工作流模型研究与应用[J].电脑开发与应用,2006(11):22-24.

(上接第167页)

on Trusted Computing[C]//Proceedings of the Fifth International Conference on Machine Learning and Cybernetics. Dalian:[s.n.],2006:2776-2781.

[4] 魏　乐,叶剑新,黄　健.可信计算的初步研究[J].科技资讯,2007,13:166-167.

[5] 肖　曦,韩　军,汪伦伟.可信计算平台关键机制研究[J].信息工程大学学报,2007,8(2):217-220.

[6] 靳蓓蓓,张仕斌.可信计算平台及其研究现状[J].长春大学学报,2007,17(2):45-49.

[7] Smith S W. Trusted Computing Platforms: Design and Applications[M].冯登国,徐　震,张立武,译.北京:清华大学出版社,2006:148-151.

[8] 邢启江,肖　政,侯紫峰,等.一种基于TPM芯片的计算机安全体系结构[J].计算机工程,2007,33(15):152-154.

[9] Price A. More Secure Computing[EB/OL]. 2006. http:\\www.trustedcomputinggroup.org\TCGBackgrounder_revised_amp_oct_17_06.pdf.