

新型可信计算平台体系结构研究

张珂

(陕西师范大学网络信息中心, 陕西 西安 710062)

摘 要: 现行通用个人计算机基于开放架构, 存在诸多攻击点, 然而传统可信计算平台在解决个人 PC 安全问题的同时暴露出可信引导过程存在不可恢复的不足。针对这些安全问题, 基于可信密码模块(TCM)提出一种新型可信计算平台体系结构。该结构具有可信引导失败时的自恢复机制, 同时提供低于操作系统层的用户身份验证功能, 通过基于 TCM 芯片的完整性度量、信任链的传递以及可信引导等技术, 进而保证可信计算平台能够完成更安全的计算和存储工作, 使可信计算平台达到更高的安全性、可信性和可靠性, 同时该体系结构具有可信引导失败时的自恢复机制, 可解决现有可信计算平台引导失败时无法正常启动的不足。

关键词: 可信密码模块; 可信计算; 可信引导; 系统恢复

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2011)07-0153-05

New Trusted Computing Platform Architecture

ZHANG Ke

(Network Information Centre, Shaanxi Normal University, Xi'an 710062, China)

Abstract: For the open architecture of personal computer and security issue of attacks, the traditional personal computing can solve the security issues, but it had lack of recovery mechanism in trusted boot process, a new trusted computer architecture based on trusted cryptography module (TCM) is proposed, the new architecture can achieve self-recovery while the trusted bootstarp failed and provide the identity authentication below operation system level. Through integrity measurement of TCM, trusted chain pass, trusted bootstarp and the identity authentication below operation system level, the reliable security computing and storage circumstance can be achieved. By this mechanism the higher security and dependability is given to the personal computer. The new architecture has the recovery mechanism in trusted boot process, it can also start the trusted computing platform when you trusted boot process failure.

Key words: trusted cryptography module; trusted computing; trusted bootstarp; system rejuvenation

0 前 言

Internet 作为通信与信息传播的途径处于快速发展并且广为人们所接受, 与此同时, 安全与隐私逐步成为 Internet 的一个关键问题。文献[1]中的民意调查表明用户使用 Internet 时感到最大的障碍就是担心自己的隐私被发现, 对于目前大部分计算机终端而言, 保护措施一般都由防火墙、入侵检测和病毒防范等组成, 采取堵漏洞、筑高墙、防攻击等老三样, 防护者只能将防火墙越砌越高、入侵检测越做越复杂、恶意代码库越做越大, 误报率也随之增多, 维护与管理变得更加复杂和难以实施, 终端使用效率大大降低, 而成本却大幅度上升, 最终的结果是防不胜防。

现行通用个人计算机终端基于开放架构, 防火墙、入侵检测和病毒防范等安全防护策略均以软件形式实

现, 并且是建立在操作系统的基础之上, 但是以软件为根基的安全防护机制有其固有的漏洞与缺陷, 即操作系统密钥的安全级别较低, 而当前的操作系统均以密钥作为进入系统的通行证, 因此攻击者即可使用常见的黑客工具暴力破解出密钥, 假冒合法用户登录系统进行破坏性操作。由此可见, 依靠操作系统的安全性来保护的用户秘密数据及重要文件就根本没有安全性可谈, 同时应用程序在这样的环境下运行其安全功能也不可能发挥出其真正的作用。

可信计算平台的提出在一定程度上缓解了计算机平台所面临的问题, 但是传统的体系结构尚且存在一些不足, 文中针对这些不足基于可信密码模块(Trusted Cryptography Module, TCM)提出一种新型可信计算平台体系结构。

1 传统可信计算平台的不足

1.1 引导过程的不可恢复性

传统的可信计算平台(Trusted Computing Platform,

TCP) 正常启动后, TCP 将 BIOS 引导块作为完整性度量的可信根, 安全芯片 (如 TCM) 作为完整性报告可信根, 从 TCP 加电开始, BIOS 的完整性由 BIOS 引导模块负责度量, 并在安全芯片上存储度量值, 同时将度量日志记录在可写的内存中, 接着继续度量硬件和 ROM 的完整性, 在安全芯片中存储度量得到的完整性值, 在内存中记录日志, 接着 OS Loader 度量操作系统 (Operation System, OS), OS 度量应用和新的 OS 组件。当启动 OS 后, 是否继续信任这个平台系统是由用户所决定, 系统平台的可信性是由一个信任链的建立过程所保证。但是在整个过程中, 一旦度量值出现异常, 就立刻发出警报, 并终止系统运行, 这时如果无法解决度量值与安全芯片中摘要值不相匹配的问题, 系统将无法正常启动, 这仅仅只是就问题提出了应对之策^[2,3]。

1.2 设置 BIOS 密码的安全漏洞

BIOS 是计算机中最基础也是最重要的程序。它为计算机提供最底层的、最直接的硬件控制。BIOS 作为固化在主板 ROM 芯片中的一段软件代码, 主要包括基本硬件驱动与初始化启动及引导部分代码, 计算机的原始操作都是依照固化在 BIOS 里的内容来完成的, BIOS 可以看作是计算机启动和操作的基石。如果 BIOS 的完整性遭到破坏, 计算机的启动过程就无法正常进行, 可见保证 BIOS 的完整性是构建可信计算平台环境时必须重视的问题, 所以众多用户喜欢在 BIOS 下设置密码保护作为资料保密的第一道防线, 但这却为计算机终端安全带来了隐患, 厂商设置的主板 BIOS 通用密码可以绕过用户设置的 BIOS 密码, 另一方面, 利用 DEBUG 命令向特定地址写入特定字节可以清除用户 BIOS 密码, 最后还可以通过给 CMOS 放电使 BIOS 的所有设置恢复到默认状态从而清除用户设置的 BIOS 密码。综上所述设置 BIOS 密码来实现用户认证和系统保护, 其安全性不堪一击^[4]。

2 基于 TCM 的新型可信计算平台

由于当前的可信计算平台尚且存在上述不足, 文中基于 TCM 提出一种新型可信计算平台体系结构。如图 1 所示为带有恢复机制的可信计算平台体系结构示意图。

在原始计算机体系结构基础上进行安全体系架构设计即可形成可信计算平台, 其中, 关键部件安全芯片 TCM 是一个基于密码学的芯片, 通过 LPC (Low Pin Count) 总线集成在计算机主板上, 为使安全芯片能在系统动态生成过程中对各模块进行信任度量, 需对主板固件 BIOS 进行重新设计。文中所提出的新可信计算平台体系结构是在此基础上添加了初始化安装模块, 使可信计算平台系统实现出错时的自恢复机制和

低于操作系统层的用户身份验证功能。

如图 1 所示, 安全硬件层主要由安全芯片 TCM、初始化安装模块、可信 BIOS 和安全模块构成; TCM 服务模块 (TSM) 主要包括完整性报告、身份证明、密码学服务、密钥管理、平台安全管理; 安全应用层则包括关键的可信应用, 各层次安全模块通过相互支撑来构建统一的可信计算平台体系结构。

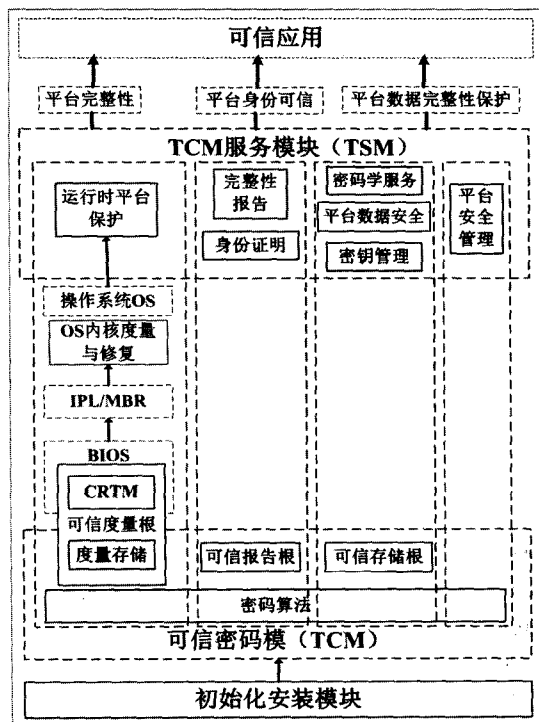


图 1 基于 TCM 的新型可信计算平台体系结构

可信密码模块是可信计算平台的可信根, 通过如下三类度量机制及 TCP 的自身安全管理功能, 实现 TCP 的安全功能。

(1) 系统起点—可信度量根, 计算 TCP 系统平台的完整性度量值, 为计算机系统建立平台信任链, 以信任链为基础确保系统平台的可信。

(2) 平台身份的可信性由可信报告根所标识, 其具有唯一性的特点, 以可信报告根为基础, 构建 TCP 的身份证明和完整性报告机制。

(3) 以 TCP 的可信存储根为基础, 实现 TCP 的密钥管理、平台数据安全保护等功能, 并且提供相应的密码服务功能。

2.1 初始化安装模块的作用

当计算机第一次启动时处于安全可信状态, 系统检测出是第一次使用 TCM 芯片, 初始化安装模块首先将提供用户身份验证的代码嵌入到主引导扇区 (MBR) 中, 提供低于操作系统层的用户身份验证功能, 然后对 MBR 进行 HASH 计算, 并将计算所得的哈希值存储到 TCP 指定的位置, 之后以相同的方式计算 BIOS、OS Loader 以及 OS 的哈希值, 同样将哈希值存储

到 TCP 指定的位置。它们将作为标准的 HASH 值在 TCP 可信引导过程中对启动时的各步骤进行完整性检验,通过与计算出的值进行比较,从而判断 TCP 启动的可信性。

同时初始化安装模块对此刻处于可信环境下的 BIOS、MBR、OS Loader 和 OS 进行备份,将备份值存入系统指定的位置,以备在进行完整性度量过程中出现错误时进行恢复操作。

2.2 用户身份验证功能的实现

OS 中低于操作系统层的更可靠、更安全的身份认证功能是由用户身份验证所提供。

2.2.1 代码安装功能的实现

MBR 获得执行权后,OS 会执行系统的 13 号中断操作 (INT13H),通过 INT13H 所提供的磁盘读写功能,OS 从硬盘中读入各种配置即可完成初始化设置及 OS 的引导。文献[5]正是使用该原理,在 INT13H 中加入口令检查代码,在主引导扇区调用 INT13H 中断时,同时完成用户身份检验操作。

2.2.2 用户身份验证功能的实现

在 MBR 中的加入用户身份验证代码,不但可以提供比操作系统更底层的用户身份认证功能,同时其安全性比 BIOS 密码更可靠、更安全,同时由于 MBR 受字节限制,编码相对精简,对嵌入的修改代码要求很高,一般不易被恶意修改。

首先口令检查代码将由代码安装程序写入主引导记录,口令检查代码主要负责替换 INT13H 的中断程序入口地址,用提前设计好的带有口令检查功能的中断程序替换原有的中断程序,替换后的 INT13H 中断主要完成两个功能:1)验证用户口令;2)用户口令验证通过后,恢复默认的 INT13H 中断程序入口地址,恢复 OS 对 INT13H 的正常使用。

这样,系统原 BIOS 中断 INT13H 就被新设计的中断程序所接管,当机器启动时会调用中断 INT13H 读写硬盘,进行各种参数的配置,完成初始化操作,新的 INT13H 中断程序中由于添加了口令检查代码,会对用户口令进行验证,只有持有正确口令的用户才能通过验证而获得机器的操作权。

2.3 可信系统的备份

可信计算平台系统提供可信环境的系统备份功能,用户可以将备份文件存储到移动设备中如移动硬盘等,由用户自行保存,若要为备份数据提供安全的保存环境,则可以将其保存到具有高安全级别的移动设备上,如指纹加密移动硬盘等,利用设备的安全防护措施,对可信系统的备份文件提供安全保护。我国联想、方正等企业均已生产出具有高安全性能指纹加密移动硬盘。

3 新型可信计算平台实现机制

3.1 可信密码模块(TCM)

在可信计算中密码支撑平台必备的关键基础部件是可信密码模块^[6](TCM),其具有独立的密码算法。TCM 是硬件和固件的集合,可以采用独立的封装形式,也可以采用 IP 核的方式和其他类型芯片集成在一起,提供 TCM 功能,其基本组成结构如图 2 所示^[7]。

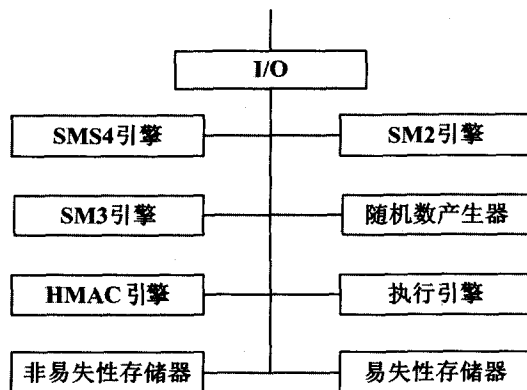


图2 可信密码模块结构

I/O:TCM 的输入输出硬件接口;

SMS4 引擎:执行 SMS4 对称密码运算的单元,该对称密码算法是一个分组算法,该算法的分组长度为 128 比特,密钥长度为 128 比特,加密算法与密钥扩展算法都采用 32 轮非线性迭代结构,解密算法与加密算法的结构相同,只是轮密钥的使用顺序相反,解密轮密钥是加密轮密钥的逆序;

SM2 引擎:产生 SM2 密钥对和执行 SM2 加/解密、签名运算的单元,SM2 算法包含:系统参数、密钥对生成、数字签名算法(SM2-1)、密钥交换协议(SM2-2)和加密算法(SM2-3)共五个部分;

SM3 引擎:执行杂凑运算的单元,SM3 是 TCM 内的密码杂凑算法,对于给定的长度为 $k(k < 264)$ 的消息,SM3 密码杂凑算法经过填充、迭代压缩和选裁,生成杂凑值,经预处理过的消息分组长度为 512 比特;

随机数产生器:是生成随机数的计算单元;

HMAC 引擎:基于 SM3 引擎的计算消息认证码单元,该消息认证码算法对于给定的消息和验证双方共享的秘密信息产生长度为 t 个字节的消息验证码,消息认证码产生过程采用 FIPS PUB 198 中的消息认证码产生过程;

执行引擎:TCM 中的运算执行单元;

非易失性存储器:TCM 中永久数据的存储单元;

易失性存储器:TCM 运行时临时数据的存储单元。

文献[8]提出了一种 TCM 符合性测试的形式化方法,采用基于扩展有限状态机模型与测试向量相结合的方式对 TCM 的标准进行形式化建模,通过测试结

果分析以及与其他相关工作的对比,表明该方法能够有效地产生测试用例,并提高 TCM 符合性测试的错误检测率。文献[9]提出了一种有效的 TCM 符合性测试方法,给出了衡量指标,并按照该指标对测试进行了测试分层,利用 TCM 内部命令的依赖关系建模获取测试用例,测试结果表明:与其他 TCM 测试方法相比,文献[9]提出的测试方法具有较高的测试效率,能够发现更多产品不符合标准带来的问题。

文献[6]对 TCM 各组成模块的功能、TCM 服务模块(TSM)、可信计算密码支撑平台、完整性度量以及传统的信任链传递过程进行了详细的介绍,这里不再赘述。

3.2 新的信任链传递体制

信任链建立在信任根的基础上,通过可信度量机制来收集那些影响平台可信性的性能参数,然后通过度量所获得的值和预期的值进行比较,来判断系统是否可信。信任链的建立必须遵循以下三条规则^[10,11]:

(1)除了信赖度量核心根(Core Root of Trust for Measurement, CRTM)之外,所有部件在未经度量前,都认为是不可信的,只有经过可信度量并符合预定义期望的部件,才可以划入可信边界。

(2)平台不允许运行可信边界以外的部件实体,只有可信边界内的部件才可以获得相应平台控制权。

(3)只有可信边界内部件才可以作为验证代理对未验证部件进行完整性验证。

结合以上三条规则,制定出带恢复机制的信任链建立模型如图 3 所示。

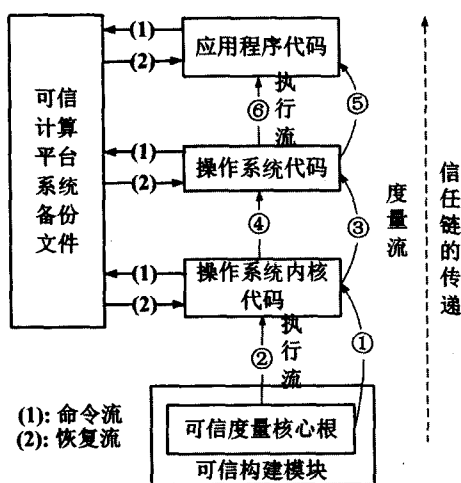


图 3 带恢复机制的信任传递模型及可信边界的扩展

1) PC 被加电,可信度量的核心信任根的代码开始执行,CRTM 负责度量 BIOS 的完整性,将完整性度量值存储到 PCR 中,并将度量过程记录到相应的事件日志中,将控制权传递给 BIOS。

2) 执行 BIOS 代码,BIOS 度量 OS Loader 的完整

性,将完整性度量值存储到 PCR 中,并将度量过程记录到相应的事件日志中,将控制权传递给 OS Loader。

3) 执行 OS Loader 代码,OS Loader 度量 OS 的完整性,并将完整性度量值存储到 PCR 中,并将度量过程记录到相应的事件日志中,将控制权传递给 OS。

4) 执行操作系统代码,装入系统内核等。

5) 操作系统对装入的应用程序进行度量,将完整性度量值存储到 PCR 中,并将度量过程记录到相应的事件日志中,将控制权传递给应用程序,执行应用程序。

在度量过程中,若完整性遭到破坏,则可以通过可信计算平台的恢复机制将系统恢复到可信的状态,带恢复机制的信任传递模型在原有的度量流和执行流的基础上,增加了恢复流,使可信计算平台系统在度量失败时,具有恢复到可信状态的能力。

3.3 带恢复机制的可信引导过程

可信计算平台从核心可信度量根开始执行一系列的度量操作,TCP 中已经或将要执行软件的完整性即通过这些度量操作来记录^[12]。度量过程基本是从开机加电开始监控:度量 BIOS 是否是可信任的;度量由 BIOS 引导装载的 OS 是否是可信任的;度量 OS 加载的应用程序是否是可信任的,同时在 OS 运行过程中可监控关键部件是否被修改。

新型可信计算平台引导过程如图 4 所示,具体过程为:首先,由初始可信边界中的 CRTM 代码度量 BIOS 可信性,并将可信度量值报告给 TCM;信任根将完整性度量的控制权交给 BIOS;BIOS 度量 MBR 的可信性,并将度量值报告给 TCM;BIOS 将完整性度量的控制权交给 MBR;MBR 度量操作系统加载程序的可信性,并将度量值报告给 TCM;MBR 将完整性度量的控制权交给操作系统加载程序;操作系统加载程序度量操作系统的可信性,并将度量值报告给 TCM;操作系统加载程序将完整性度量的控制权交给操作系统;操作系统度量应用程序的可信性,并将度量值报告给 TCM;TCM 对所有部件的完整性度量值进行检查,验证各个部件的完整性,同时对 TCM 中的完整性度量序列进行检查,验证是否被非法修改过。

在新的可信引导过程中任一步的完整性检验出现异常,可信计算平台系统都会终止启动过程,将询问用户是否采取进一步的恢复措施,用户可以通过指定备份文件的路径使出错文件恢复到可信的状态,否则将给出详细的出错信息,指出系统的完整性遭到破坏。

新型可信计算平台在可信引导过程中,对出错文件的恢复机制进行检测,若无法正常的恢复,即平台无法对出错文件进行恢复时,新型可信计算平台则启动传统的开机方式,确保系统的正常运行。

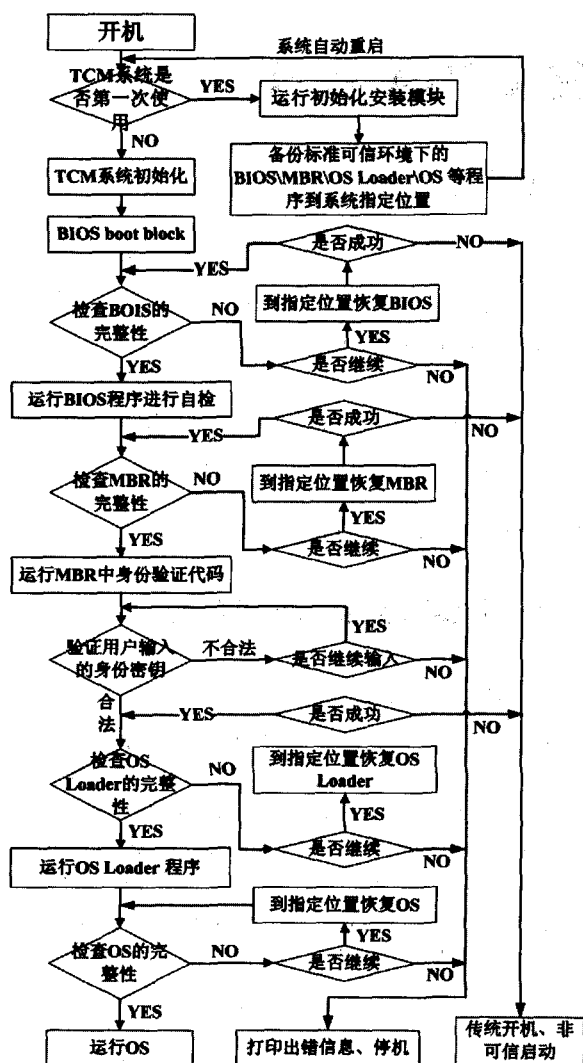


图4 带有恢复机制的可信引导过程

安全启动过程中完整性度量出错时的系统恢复功能。这在一定程度上解决了目前传统可信计算平台在出错时无法正常启动的问题,同时防止了用户设置 BIOS 密码的安全隐患。

参考文献:

- [1] Claessens J, Diaz C, Goemans C. Revocable anonymous access to the internet[C]// In: Internet Research: Electronic Networking Application and Policy. [s. l.]: [s. n.], 2003: 13-25.
- [2] 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: 139-166.
- [3] 张焕国, 严飞, 傅建明. 可信计算平台测试理论与关键技术研究[J]. 中国科学: 信息科学, 2010, 40: 167-188.
- [4] 李佳蕾. Linux 系统的开机认证和可信引导的设计与实现[D]. 北京: 北京交通大学, 2006.
- [5] 车生兵. 硬盘启动前口令检查的实现[J]. 计算机应用研究, 1998, 15(2): 81-83.
- [6] 中国可信计算工作组. 可信计算密码支撑平台功能与接口规范[EB/OL]. [2009-10-06]. <http://www.tcmu.org.cn/>.
- [7] 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.
- [8] 李昊, 胡浩, 陈小峰. 可信密码模块符合性测试方法研究[J]. 计算机学报, 2009, 32(4): 654-663.
- [9] 李昊, 冯登国, 陈小峰. 可信密码模块符合性测试方法与实施[J]. 武汉大学学报(理学版), 2009, 55(1): 31-34.
- [10] 李超, 王红胜, 陈军广, 等. 加强计算机终端信息安全的两种解决方案[J]. 计算机技术与发展, 2009, 19(1): 165-168.
- [11] 李熊达, 何利. 基于自动信任协商的可信网络研究[J]. 计算机技术与发展, 2010, 19(9): 150-153.
- [12] 张颖, 周长胜. EFI 下基于便携式 TPM 的可信计算平台研究[J]. 计算机技术与发展, 2010, 20(1): 167-170.

4 结束语

基于 TCM 所提出一种新型新可信计算平台体系结构, 提供了低于操作系统层的用户身份验证功能和

(上接第 152 页)

- Computation. Piscataway: IEEE Press, 2002.
- [5] Weeksl. Understanding Trust Man Agent System[R]. [s. l.]: Inter Trust STAR Lab, 2001.
- [6] Johnson T, Newman-Wolfe R. A Comparison of Fast and Low Overhead Distributed Priority Locks[J]. Journal of Parallel and Distributed Computing, 1996, 32(1): 74-89.
- [7] Bace R, Mell P. Intrusion detection systems. NIST Special Publication on Intrusion Detection Systems[M]. [s. l.]: National Institute of Standards and Technology, 2004.
- [8] Arbaugh W A, Fithen W L, Hugh J M. Windows of vulnerability: A case study analysis[J]. IEEE Computing, 2000, 33(12): 52-59.

- [9] 王琢, 赵永哲, 姜占华. 网络处理模式匹配算法研究[J]. 计算机应用研究, 2007, 24(12): 310-312.
- [10] Kemmerer R A, Vigna G. Intrusion Detection: A Brief History and Overview[J]. Supplement to IEEE Computer (IEEE Security & Privacy), 2002, 35(4): 27-30.
- [11] 喻飞, 朱妙松, 朱森良, 等. 入侵检测系统中特征匹配的改进[J]. 计算机工程与应用, 2004, 40(29): 32-35.
- [12] 纪详敏, 连一峰, 许晓利, 等. 入侵检测技术的研究与进展[J]. 计算机仿真, 2004, 21(11): 130-131.
- [13] 柏海滨, 李俊. 基于支持向量机的入侵检测系统的研究[J]. 计算机技术与发展, 2008, 18(4): 137-139.