面向混合入侵检测策略的应用模型研究

王 峰,宗 平
(南京邮电大学 物联网学院,江苏 南京 210003)

摘 要:入侵检测是为了确保计算机系统和网络系统的安全而设计和配置的,其设置意图是为了能够及时发现并报告系统中的异常现象或未授权行为,主要用于检测计算机网络中违反安全策略的行为。入侵检测系统通过寻找恶意行为的迹象来监控计算机网络。基于入侵检测的准确性和完备性考虑,给出了一种面向标志入侵检测和异常入侵检测的混合入侵检测系统模型,并说明了相关的设计与实现技术。分析表明该模型相对于单策略的检测手段,具有更好的检测效果。

关键词:网络安全;入侵检测;模型
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)07-0149-04

Study of Mixed Model Oriented Intrusion Detection

WANG Feng,ZONG Ping
(College of Internet of Things,Nanjing University of Posts and Telecommunications, Nanjing 210003 ,China)

Abstract:Intrusion detection technology is designed and configured to ensure the computer system and network system security, its purpose is to discover in time and report abnormal phenomenon or unauthorized act in system, mainly used in the detection of behavior which breaches security strategy in computer network. Intrusion detection system monitors computer network by looking for signs of malicious behavior. It gives a kind of mixing intrusion detection system model oriented the sign intrusion detection and abnormal intrusion detection, and illustrates the related technologies of the design and implementation. The analysis shows that the model has better detection effect than the single strategy detection means.

Key words:network security;intrusion detection;model

0 引 言

依赖于互联网的公司越来越多,他们逐渐将其核心业务向网络转移,从而使网络安全问题的重要性愈发明显。一般情况下,公司使用防火墙之类的工具作为其安全防护的第一道防线。然而,随着攻击工具的获得日趋方便,攻击手法的日趋复杂,只是使用防火墙策略无法保障对安全高度敏感的公司和部门的网络安全,必须采用纵深的、多样的新手段来加强网络的安全防护。在互联网高度普及的今天,网络环境也愈加复杂,设备变得复杂多样,系统需要不断升级、查漏补缺,这样使得网络管理员的管理工作变得愈发沉重,一不小心的大意便有可能造成严重的安全问题。在此背景下,入侵检测系统 IDS(Intrusion Detection System)已成为构建网络安全体系中不可或缺的组成部分。但是现有的入侵检测机制基本上是基于单一策略的,在特定应用环境下是有效的,却很难适应复杂多变的安全需求。因此,研究混合入侵检测系统模型是十分有意义的。

收稿日期:2010-11-29;**修回日期**:2011-03-20
基金项目:江苏省科技支撑项目(BE2009157)
作者简介:王 峰(1983-),男,硕士研究生,研究方向为计算机网络;宗 平,博士,教授,研究方向为计算机网络、信息安全等。

1 入侵检测机制

入侵检测按照通常的习惯标准可以分为两类:一类采用基于标志的入侵检测(signature-based),另一类采用基于异常的入侵检测(anomaly-based)[1]。

在基于标志的入侵检测中,需要指出违背安全策略的事件的特征是什么,例如网络数据包的一些头信息。入侵检测机制的主要工作是判断在所收集到的数据中是否出现了这类特征,这有些类似于杀毒软件的工作原理。这类入侵检测技术工作的准确性建立在不断更新的知识库之上,需要不断收集并分析新的违背安全策略的入侵方式和手段,并提取出特征[2]。如果单独采用这种入侵检测技术,则会有很多新出现的入侵方法不能够被有效地检测出来,从入侵检测系统的完备性角度考虑,仍就存在极大的安全隐患。

在异常的入侵检测技术中,首先定义一组系统在"正常"情况下的数值,例如文件校验和、CPU 利用率、内存利用率等等,可以人为地定义这类数据,亦能通过

对系统的观察，利用统计的方法得出，然后把系统工作时的数值和在此之前定义的“正常”值进行比较，进而得出系统是否被攻击的结论。怎样准确定义所谓的“正常”情况是这种检测方式的核心所在[3]。这种入侵检测技术无法准确地判别出攻击的类型和手法，往往需要和多个正常的系统参数进行比较，看其是否符合正常的参数区间，并综合各方面因素做出判断，这样，往往会使系统增加额外的实时处理任务，系统的实时响应处理能力会受到很大影响，特别是对于那些处理能力不高的系统环境，这种入侵检测技术可能会成为系统的瓶颈，进而影响整个系统的性能。

事实上，因采用的检测方法不同，可能得出的结论也会有所不同。对于基于标志的入侵检测技术来说，其核心工作是维护一个知识库。一般来说，如果是已知的攻击类型，该种检测技术可以给出详细、准确的报告，然而，对于未知的攻击类型却束手无策，并且需要不断地更新知识库。基于异常的入侵检测技术可以判别出更加广泛、甚至是新类型的攻击，却无法准确地区别出攻击类型和攻击手法[4]。

为了解决上述两种入侵检测技术的缺陷，使入侵检测系统能够更加迅速、有效、全面地检测出系统中面临的各种安全隐患，文中给出一种结合基于标志入侵检测机制和异常入侵检测机制的混合入侵检测系统模型—MixSA Model 的设计方法。

2 MixSA Model 的设计

MixSA Model 将入侵检测过程分为三个阶段来处理。首先在网络或计算机系统中安装一些感应器或者一些信息采集的应用程序来收集数据，并在集中安全管理中心配置便于实现标志入侵检测功能的攻击特征规则和便于实现异常入侵检测功能而定义正常行为规则。这样，信息收集环节收集了必要的信息，定义了相关的规则。其次，依据攻击特征规则，建立了攻击特征库，按照攻击特征库进行模式匹配，快速准确发现入侵行为，对于不符合攻击特征的行为，同时依据定义的正常规则建立的正常行为模板进行相关参数的匹配，看其是否位于正常区间。最后，按照系统事先设计的对各种可能入侵行为的相应响应规则，依据系统的分析结果，做出对应的告警与响应。混合入侵检测系统模型—MixSA Model 如图1所示。

MixSA Model 实现了标志入侵检测和异常入侵检测的有效结合，既具备了标志入侵检测的准确性，又因为结合了异常入侵检测，进而解决了标志入侵检测在完备性方面的缺陷，同时也因标志入侵检测部分功能的引入，克服了异常入侵检测在准确性与及时性方面的缺陷。

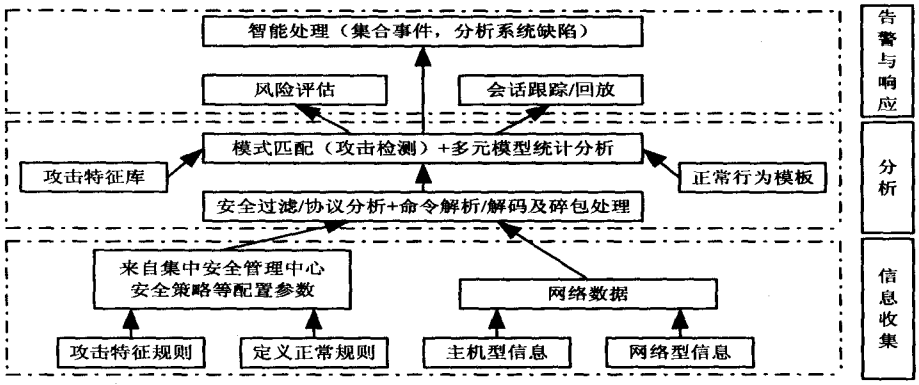

图1 混合入侵检测系统模型—MixSA Model

2.1 信息收集

在入侵检测系统模型中，信息收集的内容主要包括网络、数据、系统以及用户活动的行为和状态。通过在计算机网络系统的不同关键点设置感应器来收集信息，这样一方面可以尽可能扩大检测范围，另一方面从几个信源来的信息的不一致性判断可疑行为或入侵标识，因为有时候从一个信源来的信息有可能检测不出疑点[5]。同时在集中安全管理中心配置两方面的安全策略：一是标志入侵检测的攻击特征规则；二是定义用于异常入侵检测的正常访问规则。信息收集模型如图2所示。

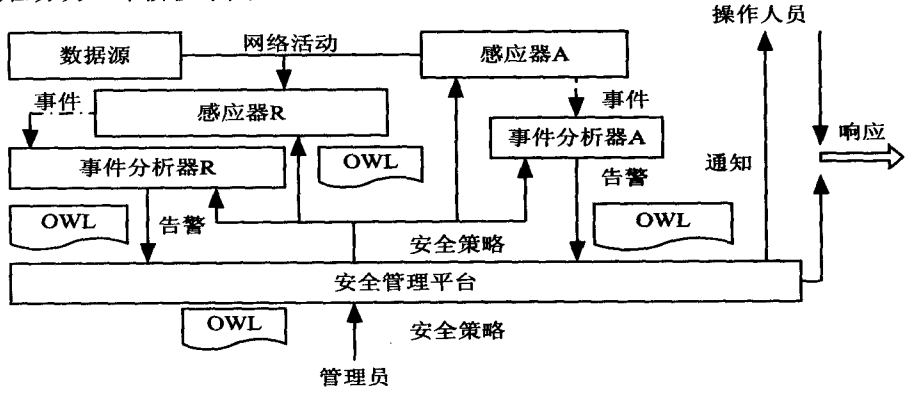

图2 信息收集模型

系统日志、程序执行中的异常行为、目录以及文件中的异常改变、物理形式的入侵信息是入侵检测使用的四个主要的信息源[6]。

一般情况下,黑客很难抹除他们在系统日志中留下的踪迹,所以,检测入侵的必要条件就是充分利用系统日志。各种各样的行为类型,每种类型的各种信息都包含在日志文件的记录中,自然地,对于正常的使用来说,不期望的或不正常的行为就是非授权的企图访问重要文件、重复登陆失败、登陆到不期望的位置等等。

在网络系统中,程序的执行通常情况下包括操作系统、用户启动的程序、网络服务和特定目的的应用。一般情况下,通过一到多个进程实现一个在系统上执行的程序。各个进程执行的环境可能有所不同,在这种情况下,环境控制着进程可访问的数据文件、程序和系统资源等。当黑客入侵你的系统的时候,通常都会有进程出现不期望的行为。黑客一般采用分解运行的程序或者服务的手段进行攻击,进而使用户正常运行失败,使其自身以非用户或非管理员意图的方式进行操作,达到入侵的目的[7]。

很多软件和数据文件包含在网络环境中的文件系统中,黑客修改和破坏的目标时常锁定在这些包含重要信息的文件和私有数据文件中。

物理形式的入侵通常采用两种形式,一是未授权访问物理资源;二是对网络硬件的未授权连接。

2.2　数据分析

数据分析通常采用如下三种技术手段:统计分析、模式匹配和完整性分析。在进行实时入侵检测的时候通常采用前两种技术,而事后分析则采用完整性分析技术。MixSA 模型采用模式匹配和多元模型统计相结合的分析方法。在模式匹配环节把收集的信息与攻击特征库中的攻击模型进行匹配,如果匹配成功,则证明入侵存在,直接进入告警与响应环节;如果匹配不成功,则进行多元模型统计分析,与正常行为模板相比较,比对其相关参数是否在正常范围内,并向系统报告是否异常,进入相应的告警与响应环节。

模式匹配是把前期信息收集阶段收集到的有关信息与已知的入侵类型、系统误用模式数据库中的误用模式相比较,通过比较,找出违背安全策略的行为。模式匹配的好处是仅仅需要收集与之有关的数据集合,使系统的负担显著的减少,并且技术手段已经很是成熟,检测准确率和效率都很高。该技术的缺陷是为了对付不断出现的黑客攻击手法需要不断地升级系统,对于新型的攻击类型和攻击手法也无能为力。MixSA 混合入侵检测系统通过运用多元模型统计分析方法来解决未知的入侵行为,能够有效地提高入侵检测的功效。

统计分析方法首先需要给诸如用户、目录、文件和设备等系统对象创建一个统计描述,据此了解正常使用时的操作失败次数、访问次数和延时等基本测量属性。比较网络、系统的行为与测量属性的平均值,当有超过了正常值范围的观察值出现时,就可以理解为发生了入侵行为[8]。统计分析方法能够检测到未知的入侵类型和新型的入侵手法,可是很多时候也会误报、漏报,对于用户正常行为时常发生较大改变的情形则不适用。

基于统计分析的模型有多种,诸如多元模型、马尔柯夫过程模型、操作模型、时间序列分析和方差等。其中多元模型作为操作模型的扩展,它通过同时分析多个参数实现检测。具有较高的检测效能。

统计分析方法可以“学习”用户的使用习惯,正是这一优点使其拥有了可用性和较高检出率的特点。有利有弊,入侵者则有机会利用这种“学习”能力,通过不断“训练”,把入侵事件变成符合正常操作的统计规律,轻松地骗过入侵检测系统,但是,具有明显规律的标志入侵检测可以通过前期的模式匹配环节加以解决,这正是 MixSA 混合入侵检测系统的优势所在。

2.3　完整性分析

MixSA 混合入侵检测系统在事后定期地进行完整性分析。在 MixSA 设计中,对一个计算机系统或者计算机网络系统,通过在系统中设计安装一款完整性检查小型软件来实现,该软件主要实现文件和目录的内容及属性的检查,同时,为了不增加系统和系统管理人员的负担,从入侵检测系统运行效率的角度考虑,该软件需要被设计为可以在特定时间自动运行。这样,对于每一个计算机系统或者网络系统,可以根据自身系统的业务特点,设定为在固定的某一闲时自动进行完整性检查,在大大提高系统安全性的基础上,尽可能地降低入侵检测对于系统自身处理性能的影响。

完整性分析关注的重点是对象或者文件是否被非法的篡改,这主要包括文件和目录的内容以及属性,该种方法特别擅长于被修改成类似特洛伊木马的应用程序的发现,它能够发现因入侵行为导致的文件或其他对象的任何改变。因为实现方式是批处理的,故其不足之处在于不利于实时响应。然而在 MixSA 混合入侵检测系统中,完整性分析是在基本入侵检测手段运用之后,作为对标志入侵检测和异常入侵检测的有效补充增加的,大大提高了 MixSA 混合入侵检测系统的检测能力。

2.4　实时记录、报警或有限度反击

IDS 的根本任务是要对入侵行为做出合适的反应,这些反应包括详细日志记录、实时报警和有限度的反击攻击源[9]。

在 MixSA Model 的分析环节中,如果模式匹配成功,则直接进入告警与响应环节,依据事先制订的攻击

特征等级，如果攻击等级一般，则进行日志记录并实时报警请求系统处理；如果攻击等级严重，则进行详细日志记录、实时报警请求系统管理人员实时干预、系统自动拒绝访问源的所有处理请求直至危险解除。在分析环节，如果按照正常行为模板进行多元模型统计分析，则依据正常行为的一系列参数，设置正常区间—无入侵，稍微偏离参数正常区间—轻度入侵，严重偏离正常区间—重度入侵，并对不同的入侵等级制定相应的响应策略，在无入侵情况下，系统不做任何处理，在轻度入侵的情况下，进行日志记录并实时报警请求系统处理，在重度入侵情况下，进行详细日志记录、实时报警请求系统管理人员实时干预、系统自动拒绝访问源的所有处理请求直至危险解除。在事后入侵检测的完整性分析过程中，也可以依据检查的结果，设置无攻击、攻击等级一般、攻击等级严重等多个等级，并依据不同的等级采取相应的处置响应策略，如：无攻击则日志记录，攻击等级一般则日志记录并报警请求系统处理，攻击等级严重则进行详细日志记录、报警请求系统管理人员实时干预、系统自动拒绝访问源的所有处理请求直至危险解除。

3 MixSA Model 的性能分析

准确性（Accuracy）是 IDS 的一个特别重要的能力，准确性的高低标志着 IDS 从各种行为中识别入侵的能力的强弱，IDS 检测能力低，则很有可能把合法活动看成是入侵的行为并进行异常处理[10]。处理性能（Performance）的优劣表示 IDS 处理数据源数据时速度的大小，自然地，在具有较差处理性能的 IDS 中，实现实时处理是不可能的，处理性能将制约 IDS 的性能，甚至影响整个网络系统的运行性能[11]。完备性（Completeness）表示 IDS 具备检测出所有攻击行为的能力，如果一个 IDS 具有检测的完备性，则表示任何一个攻击行为，都将被 IDS 检测出来，无一例外[12]。由于网络的飞速发展，黑客的攻击类型和攻击手段也在不断的变化，对于攻击行为，很难掌握所有相关知识，所以很难进行 IDS 的检测完备性评估。

关于入侵检测 Debar 等又增加了两个评价标准：及时性和容错性[13]。对于 IDS 来说，所谓的及时性，就是要求尽快地分析数据并把分析的结果尽早地传播出去，这样系统安全管理者可以及时地做出反应，避免入侵攻击给系统造成更大的危害，使损失降低到最小。这则同时对 IDS 的处理速度、传播速度、对检测结果信息的反应速度都提出了更高的要求。由于 IDS 承担了系统检测入侵的任务，使其成为了入侵者攻击的首选目标，所谓入侵检测的容错性（Fault Tolerance）就是要求 IDS 自身必须具有较强的抵御攻击的能力，特别是拒绝服务攻击。由于 IDS 运行在操作系统和硬件平台上，使其很容易遭受到来自各方的攻击，在这种情况下，IDS 的容错性就显得愈发重要。

在 MixSA 模型中，采用了基于标志入侵检测和异常入侵检测的混合机制。首先在信息收集阶段，集中安全管理中心定义了基于标志的攻击规则和基于异常的正常规则；其次在信息的分析阶段依据来自集中安全管理中心的攻击规则，定义了符合这一规则的攻击特征库，依据来自集中安全管理中心定义的参数正常规则，定义了正常行为模板。

在 MixSA 模型中，因为采用了模式匹配的处理方式，将收集到的信息与定义的攻击特征库进行比较，如果收集到的信息符合攻击特征库的入侵特征，则可以快速做出反应，进入告警与反应环节，具备标志入侵检测的准确性和及时性；如果收集到的信息并不符合攻击特征库的入侵规则，但是依然可能是不符合安全策略的入侵行为，此时，在混合入侵检测系统模型中，入侵检测分析并没有结束，而是要依据正常行为模板的一系列正常参数进行多元模型统计分析，找出异常的入侵检测，进入告警与反应环节，能够检测出几乎所有的攻击入侵行为，则 MixSA 混合入侵检测系统的入侵检测能力具备了异常入侵检测系统入侵检测的完备性，同时由于前面的模式匹配已经对绝大部分的入侵行为进行了检查，并做出了响应，所以，MixSA 混合入侵检测系统又克服了单一的异常入侵检测系统在攻击方式确定和处理性能方面的缺陷。

4 结束语

入侵检测系统通过寻找恶意行为的迹象来监控计算机网络。基于入侵检测的准确性和完备性考虑，文中在论述入侵检测的基本机制的基础上，给出了基于标志入侵检测和异常入侵检测的混合入侵检测系统模型—MixSA，并说明了相关的设计与实现技术。分析表明该模型相对于单策略的检测手段，具有更好的检测效果。

参考文献：

[1] 蒋建春，冯登国. 网络入侵检测技术原理与技术[M]. 北京：国防工业出版社，2001.

[2] 蒋建春，马恒太，任党恩，等. 网络安全入侵检测研究综述[J]. 软件学报，2000(11)：29-31.

[3] 李仁发，李 红，喻 飞，等. 入侵检测系统中负载均衡研究与仿真[J]. 系统仿真学报，2004，16(7)：1444-1449.

[4] Bentleypj K. Toward an artificial immune system for network intrusion detection: An investigation of dynamic clone selection[C]//Proceedings of the 2002 Congress on Evolutionary

（下转第 157 页）

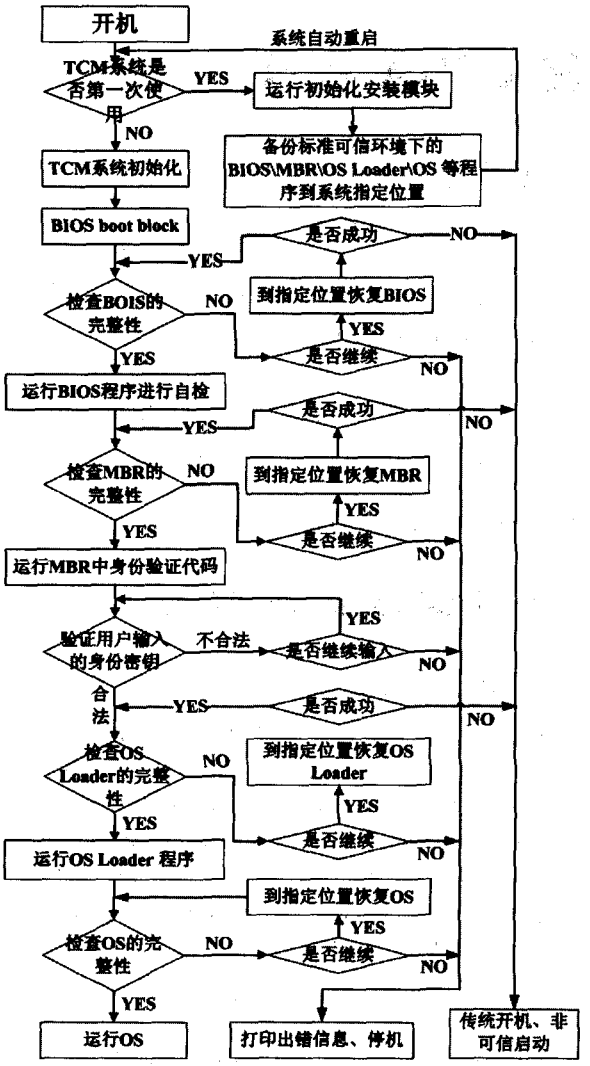

图4　带有恢复机制的可信引导过程

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.

(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 & Priracy),2002,35(4):27-30.

[11] 喻　飞,朱妙松, 朱淼良,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.