具有协作代理功能的分布式入侵检测系统

刘冰寒,张 建,刘宝代
(山东建筑大学,山东 济南 250101)

摘 要:入侵检测作为保护信息系统安全的一项重要技术,特别是在信息商业化的今天显的特别重要。文中在分析了传统的入侵检测系统的优缺点之后,在保留分布式层次结构的基础上,采用移动代理技术来克服信息采集节点地址固定,容易遭受入侵者攻击的缺点,并对代理间通信机制和数据共享加强了管理,从而增强了代理之间协同工作能力。针对系统误报率高的缺点进行了研究改进,从而减轻了管理员的负担,希望能对将来系统的研究改进提供一个借鉴模式。

关键词:入侵检测;移动代理;通信管理;警报过滤
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)09-0149-04

Distributed Intrusion Detection System with Collaborative Agent Functions

LIU Bing-han, ZHANG Jian, LIU Bao-dai
(Shandong Jianzhu University, Jinan 250101, China)

Abstract: Intrusion detection is an important technology to protect security of information systems, especially in the days of commercialization of information. Used the mobile agent technology to overcome the shortcomings of fixed collection of nodes address and vulnerable based on the hierarchy of distributed after analysis of the traditional advantages and disadvantages of intrusion detection system. Also strengthen management for communication mechanism and data sharing to enhance the collaboration among agents the ability to work. At last, study the high rate of false positives for the system, thereby reducing the burden on administrators, hoping for future study and improvement of the system to provide a reference model.

Key words: intrusion detection; mobile agent; communication management; alarm filter

0 前 言

随着信息技术和网络技术在各行各业的迅速普及和不断深入,信息系统的安全问题便成为人们关注的焦点。各种网络入侵、网络病毒以及信息系统自身的各种缺陷和漏洞给信息系统的安全性提出了严峻的挑战。特别是20世纪90年代以后,国内外网络技术的迅速发展,尤其是电子商务系统的迅速兴起,随之而来的网络入侵事件的数量也成倍增长,因此,保障网络系统和信息系统的安全便成为目前网络发展的重要课题。

传统的防火墙技术能够成功地拦截大多数外部的入侵,但是对于内部的攻击却无能为力。有统计资料显示,现在大多数的系统攻击都是由内部系统引起的,员工有意或者无意的操作造成信息的泄密,入侵者绕过防火墙从内部实施攻击都可能造成系统的崩溃,这就要求我们要有一款能够检测出内部攻击的检测系统。入侵检测作为一项能够检测出内部攻击的网络安全的重要技术,从90年代开始便有一些专门针对具体的入侵过程进行的入侵检测的研究,1994年以后逐渐出现一些入侵检测的产品,发展到现在入侵检测系统已经成为网络安全中的一个重要研究方向。

1 入侵检测系统及其分类

入侵检测系统(Intrusion Detection System, IDS)是一种主动的安全防卫技术,它是从系统内部或者各种网络资源中主动采集信息,并从中分析出可能的入侵行为,然后向管理员发出警报并在系统受到危害之前进行拦截防卫,其目的是保护计算机系统的完整性、可用性和机密性等[1]。现有的入侵检测系统大多数是采用概率统计、专家系统、神经网络、模式匹配、行为分析等技术来实现系统的检测机制,以分析事件的审计记

收稿日期:2009-12-20;**修回日期**:2010-03-09
基金项目:山东省教育科技计划项目(J07JY14)
作者简介:刘冰寒(1984-),男,山东济南人,硕士研究生,从事信息风险研究;张 建,博士,教授,从事信息系统风险控制、工作流系统方面的研究。

录、识别特定的模式、生成检测报告和最终分析结果。

入侵检测系统在实际发展过程中主要分为以下几种：

* 基于主机的入侵检测系统(HIDS)。

基于主机的入侵检测系统是对给定的主机用户、系统活动和攻击进行监视，通过分析、提取被保护系统的运行数据进行入侵分析来实现入侵检测的功能。基于主机的入侵检测系统具有检测效率高，分析代价小，分析速度快的特点，非常适合发现内部的入侵。但是它在一定程度上依赖系统的可靠性，要求系统本身应该具备基本的安全功能并具有合理的设置[2]，然后才能提出入侵信息。随着网络的发展与普及，发现它不能够很好地应用于网络之中，因此受到了网络发展的冲击。

* 基于网络的入侵检测系统(NIDS)。

基于网络的入侵检测系统是监视网络中各个主机之间传输的信息，通过抓取网络中的数据包进行分析，从而发现入侵行为的检测系统。基于网络的入侵检测系统的优点是：能够及时地监视通信流量而不影响服务器平台的变化和更新，配置简单，能够检测出多种类型的攻击并且具有实时性，但是对于加密了的数据不能很好地做出判断[3]，防入侵欺骗的能力通常较差。

* 分布式入侵检测系统。

随着信息技术的发展，人们发现基于主机的入侵检测系统和基于网络的入侵检测系统都不能很好地适用于对现在系统的检测，于是出现了分布式的入侵检测系统。分布式入侵检测系统是将基于主机的入侵检测系统和基于网络的入侵检测系统结合起来的一种入侵检测系统，它结合了两种技术的优点，并且相互补充，从而大幅度地提高了对入侵检测的能力。分布式入侵检测系统(DIDS)采用多个检测点在网络不同位置分别进行检测，并且协同处理可能的入侵行为[4]，是目前主流入侵检测系统普遍采用的架构，但是这种静态分层的结构缺乏灵活性，底层的检测节点在网络中的位置是固定的，很容易遭到入侵者的攻击[5]，另外各个检测部件之间缺乏通信管理，不能很好地配合。

2 系统共同的缺点

缺乏信息共享是现在所有入侵检测系统一个天生的缺陷，较早出现的分布式入侵检测系统只是简单地扩大了数据源的范围，能够更好地检测到入侵，但是它没有有效地对信息共享进行细化，也没有对数据共享进行严格的控制访问[6]。还有就是数据的采集虽然分布在不同的主机上，但最终的数据分析却集中进行，如果该中心失效将导致整个系统瘫痪。

另外还有一个问题就是过高的误报率使得入侵检测系统每天产生成千上万的报警，其中相当一部分是误报或者是对本系统产生不了威胁的无关紧要的报警[7]，或者是重复的报警或者相似的报警，如分布式入侵检测系统检测点在网络的不同位置可能检测到同一个入侵行为，并分别发出了警报信息，这就要求系统把这些相同或相似的入侵行为进行融合过滤，减少报警的数量进而减轻管理员的负担。

3 系统的改进

针对以上问题在保留了分布式层次结构的同时，使用了移动代理的检测节点来提高节点的抗攻击能力。移动代理能够在网络各个节点之间自主地、有目的地进行移动，实时地针对环境的改变作出相应的变化，从而减少了受攻击的可能性。要求检测代理们共同使用一个数据库，并且严格审查他们访问数据库的权限，代理之间的通信也将受到严格的控制[8]，保证了代理之间的协作能力和抗攻击能力。代理们使用同一的数据库可以保障他们及时地分享最新的数据，发现最新的入侵行为。严格审查代理的权限，这样可以保障系统的安全，防止入侵者使用一个伪代理对系统发起攻击，进而造成系统的瘫痪。

4 移动代理在入侵检测中的优点

代理是指能够在特定地环境中可以自主地移动并工作的软件实体，可以根据环境的改变而改变自己的参数，从而适应环境的变化[9]。

移动代理通常具有以下特点：

(1)动态性，代理们可以在主机之间动态地移动，这样就可以使代理的运行不再局限于某一特定的位置，从而减少了受攻击的次数。他们还可以根据环境的变化和自身的需要，自主地在网络中采集不同节点的信息，从而扩大了信息的采集量。

(2)平台无关性。现在大多数的代理们都采用与平台无关的语言编写，这样就可以摆脱对环境的依赖性，可以跨平台运行，从而扩大了入侵检测的使用范围。

(3)代理之间的合作功能。现在的系统越来越庞大，仅仅只靠单个检测系统是无法完成对系统的保护的，而采用了代理的结构后，代理之间可以相互配合合作，增强检测的能力，还能使检测具有了扩展能力。

根据以上分析，提出的系统模型如图 1 所示。

可以看到系统模型主要分为 3 个层次，最底层的是由一系列的入侵检测代理(IDA)组成，他们的主要任务是负责收集、分析数据，并且把他们的分析结果上

报给管理他们的 manager。为了保障系统的效率和安全性,在这里我们扩大了代理的功能:代理们不仅可以独立地采集网络中的数据,而且还可以分析出数据中的原始警报信息,这样就把分析入侵信息功能的活动分散在各个代理上完成,减轻了原系统中分析部件工作强度,还能加强系统的安全性,当某个代理遭到入侵的攻击瘫痪后,其它的代理仍然可以正常工作,并不断地收集分析数据,改变了原系统分析部件一旦瘫痪,整个系统便无法工作的缺点。

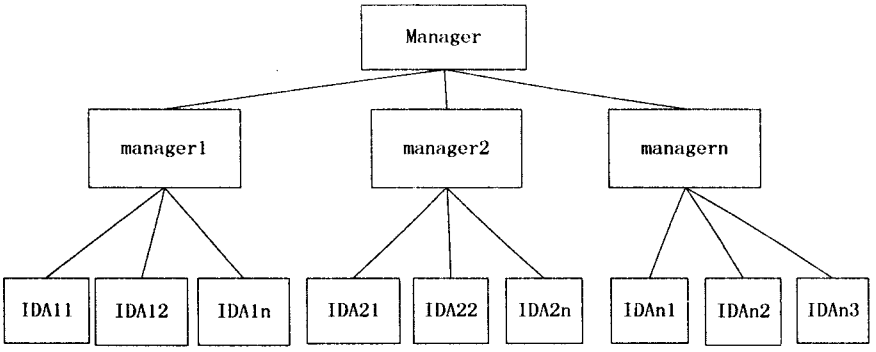

图 1　入侵检测系统模型

为了实现代理的自主功能和防止攻击者假冒代理从系统内部进行攻击,各个代理之间的通信必须受到严格的控制[10]。在这里使用一个专门的模块对代理们的权限和通信认证机制进行管理,以加强系统的安全性。

代理之间的通信过程如下:

(1)IDA1 向 IDA2 发送通信请求。

(2)IDA2 向他们共同的管理者 manager 发送请求要求验证 IDA1 身份及通信请求是否合法。

(3)管理者 manager 通过认证数据库检查 IDA1 的身份认证文件和控制文件是否合法,如果合法就允许他们之间进行通信,否则就禁止他们之间通信,并加强对 IDA1 的监控。

通信管理如图 2 所示。

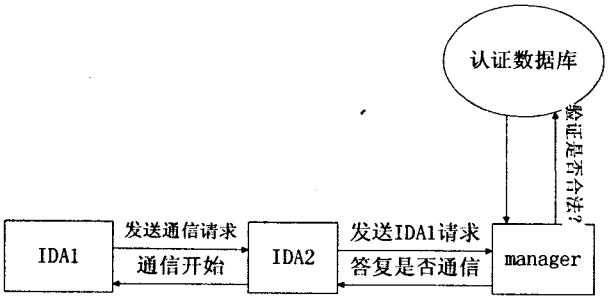

图 2　代理通信机制

在这里每个代理都有唯一的能够证明自己身份的标识,这些标识是代理向他们的管理者注册时管理者分配的,这些标识不仅能够证明自己身份的合法性,保证 IDA 之间的正常通信,并且这个标识在 IDA 访问他们共同的数据库分析数据时极为重要,IDA 在访问数据库时,数据库管理系统首先检查这些代理的身份是否合法,如果合法就允许他们访问数据库进行数据分析,如果不合法就拒绝访问。在我们的系统中通过增加一个身份认证的数据库,加强了对代理身份的管理,从而增强了系统的认证功能,同时也就增加了系统本身的安全性,防止了入侵者假冒系统本身对计算机系统进行的攻击。

模型的第二层是一系列的管理者 manager。manager 在这里主要有两个作用:

1)控制 IDA 之间的通信,能够掌握向他注册的 IDA 的位置,从而控制 IDA 的移动。当某个 IDA 受到攻击时可以及时采取相应的措施,及时地移动或者关闭 IDA,以保护整个系统。

2)对 IDA 分析出的原始警报进行过滤,去掉一些可能引起误报的警报信息。

由于环境噪音或者人为干扰等因素的影响,检测器获得的原始警报信息常常是不精确、不完整的,甚至还有可能是不同的代理收集到了同一条入侵信息并分别发出了警报,或者是一些网络包确实包含攻击的特征,但是对具体的目标和环境没有作用或不会成功的攻击,也被网络入侵分析部件判定为攻击,从而产生了误报[11]。因此,原始的警报信息中含有大量的不精确、相同的、无关紧要的警报信息,这就需要系统对这些警报进行过滤操作,减少系统的误报率。文中针对警报数据的一些参数建立警报知识库,通过一定的条件来对原始的报警数据进行过滤,这些条件具体包括:

a)较低安全级别的入侵信息或者是对系统不会造成任何影响的入侵行为;

b)被攻击的对象不存在或本系统不关心的行为;

c)被攻击端口本系统已关闭或不使用的;

d)攻击操作系统与本系统不匹配;

e)攻击名称错误的。

过滤过程如图 3 所示。

代理们分析出原始的警报信息并把它们发送到所属的 manager 时,manager 就开始把这些信息与知识库中可能引起误报的信息进行匹配操作,过滤掉原始警报信息中的无关紧要的信息,从而减少误报次数,提高系统的检测率。长期以来误报率一直是系统管理员最头疼的一件事情,过高的误报率使管理员浪费大量的时间与精力来处理这些引起误报的数据,经过我们的

改进可以减轻管理员的工作量。

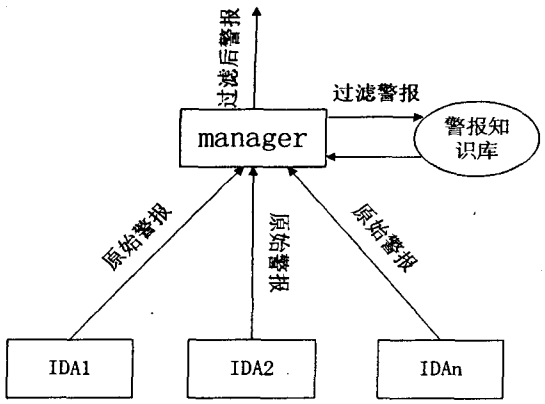

图 3 警报过滤模块

模型的第三层是 MANAGER,它的主要作用是向用户提供检测结果并管理、维护整个系统。检测结果中还包括受系统保护的特殊信息,这些系统数据在发现被攻击造成损坏的区域时非常有用,收集的数据类型包括使用的网络带宽、CPU 使用情况、网络数据包、内存使用情况、连接的数目、试图连接数目、协议、源端口与目的端口的比率和数据包的长度等。这些数据还有利于对系统内部的信息进行检测处理,可以根据这些信息的使用情况与平时的使用情况进行比对,如果发现异常就极有可能是内部发生入侵行为。

5 结束语

入侵检测作为一种积极主动的安全防护技术,提供了对系统的实时保护,能够在系统受到入侵时成功地响应报警,受到用户的好评。发展到今天各种各样的入侵检测系统凭借自身的优点在市场上不断发展,文中在探讨了几种常见的系统的优缺点之后,在保留分布式层次结构的基础上采用移动代理技术来克服收集节点地址固定的缺点,并对代理缺乏通信管理、不能共享数据、误报率高的缺点进行了研究改进,取得了一定的成果。

面对日益发展的网络和网络攻击手段的多样化,单凭现在的检测系统是无法满足用户的需求的。随着智能技术的发展,比如神经网络、智能算法的发展,入侵检测系统也有必要借鉴这方面的技术[12],来扩大自己的检测能力。相信未来的入侵检测系统必将克服现在系统的缺点,更好地保护系统的安全。

参考文献:

[1] 陈雪斌,刘 峰,赵志宏,等.安全的分布式入侵检测系统框架[J].计算机工程与设计,2009,30(14):3266-3268.

[2] 徐国芹.基于 AGLET 的分布式入侵检测系统的研究[J].赤峰学院学报:自然科学版,2009,25(5):28-30.

[3] 李 生,邓一贵,唐学文,等.基于移动代理的分布式入侵检测系统的研究[J].计算机技术与发展,2009,19(9):132-135.

[4] 项 目,杨小平.基于移动代理的分布式入侵检测系统模型[J].计算机工程与应用,2006(19):140-143.

[5] 肖 昆,郑 记.一种新型的适应于 MANET 的基于移动代理的对等入侵检测系统[J].计算机应用与软件,2007,24(4):157-159.

[6] 张淑英,刘淑芬.基于移动代理的多层次分布式入侵检测网络预警系统[J].计算机应用研究,2006(5):13-15.

[7] 李旭晖,吕 慧,向剑文.移动代理系统的安全问题[J].计算机应用,2001,21(7):5-8.

[8] 安 娜,张 凡,吴晓南.一个基于移动 Agent 的分布式入侵检测系统[J].西北大学学报,2005,35(1):25-28.

[9] Athanasiades N, Abler R, Levine J, et al. Intrusion detection testing and benchmarking methodologies[C]//Proceedings of the IEEE Information Assurance Workshop. [s. l.]:[s. n.], 2003:63-72.

[10] Antonatos S, Kostas G, Anagnostakis, et al. Generating realistic workloads for network intrusion detection systems[C]// Proceedings of the fourth international workshop on Software and performance. [s. l.]:[s. n.], 2004:207-215.

[11] Lippmann R, Haines J, Fried D, et al. The 1999 DARPA off-line intrusion detection evaluation[J]. Computer Networks, 2000,34(4):579-595.

[12] 张雪芹,顾春华,林家骏.入侵检测技术的挑战与发展[J].计算机工程与设计,2004,25(7):1096-1099.

(上接第 148 页)

http://lxr.oss.org.cn/source/net/ipv6/.

[7] 孙冰心,张凤斌,江子扬. Linux 下内容过滤的实现[J].哈尔滨理工大学学报,2004,9(2):56-59.

[8] NetFilter project[EB/OL]. 2009-12-20. http://www.netFilter.org/.

[9] 严蔚敏,吴伟民.数据结构[M].北京:清华大学出版社,2002.

[10] 王一平,韦 卫.网络安全框架 NetFilter 在 Linux 中的实现[J].计算机工程与设计,2006,27(3):439-468.

[11] Iperf project[EB/OL]. 2009-12-20. http://sourceforge.net/projects/iperf/.

[12] 高鸿峰,王一波,傅光轩. NetFilter 框架下 IPv6 防火墙的设计与实现[J].电子科技大学学报,2007,36(6):1427-1429.

[13] 申凤兰.防火墙中透明模式和流过滤技术的研究与实现[D].广州:暨南大学,2003:22-23.