一种基于移动代理的入侵检测系统

范西昆，　郑连清，　樊昌周，　霍文俊
（空军工程大学 电讯工程学院，陕西 西安　710077）

摘　要：在介绍移动代理的基础上，阐明了将移动代理技术应用于入侵检测系统的优势，并提出一种基于移动代理技术的入侵检测系统(MAB－IDS)。重点讨论了系统结构模型和系统检测入侵的方法及其原理。通过与其他系统进行比较，得出由于利用了移动代理技术，MAB－IDS 的入侵检测能力较强。

关键词：入侵检测；移动代理；Java
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009－3516(2001)06－0078－04

入侵检测技术作为防火墙技术的合理补充，近年来一直是网络安全领域研究的热点问题。现在，许多新型入侵检测系统被研制出来并应用到不同的领域，它是越来越多需要接入网络的计算机系统在安全上的迫切需求。

1994 年 Purdue 大学的 Crosbie 和 Spafford 在其论文[1]中首次提出将代理技术应用到入侵检测系统。现在，已有一些实用的基于代理的入侵检测系统，如 AAFID[2] 等。随着研究的深入，基于代理的入侵检测技术也逐渐显露出诸多不足。主要体现在：

1)代理功能的局限性，由于分布式系统拓扑结构的特点，代理一般处于网络结构的末端，节点的信息非常有限和单一，所以这些代理往往只能实现相对简单的功能，例如简单数据采集和转发等。

2)代理对网络数据整体认识能力低，因此很难准确地判断启动入侵跟踪的时间，容易受到 IP 分段等针对 IDS 的攻击。

移动代理技术为解决这些问题提供了可能[3]。为此，我们设计了一种基于移动代理的 IDS，简称 MAB－IDS。下面首先介绍移动代理的概念，然后讨论 MAB－IDS 的系统结构和工作原理，最后对系统的性能进行比较分析。

1　移动代理

移动代理是指能在异构网络主机之间自主地进行迁移的有名字的程序。程序能自主地决定什么时候迁移到什么地方。它能在程序运行的任一点上挂起，然后迁移到另一台主机上，并接着这一点继续往下执行。移动代理是运行在虚拟机环境中的特殊软件代理，具有迁移性、智能性、协作性和分布灵活性。

迁移性是指代理可以在运行期间直接进行主机间的迁移，即代理可以从一个场地采集所需要的数据并处理之后，不终止进程而直接迁移到另一台主机上继续运行，保留了原来进程的数据段和堆栈。这样，极大简化了数据的处理过程，从而使数据的可操纵性和全局性有了根本的改变。

智能性是指代理具有一定自适应能力，可对环境的变化做出适当的反应。它对网络环境的适应能力使它可以减轻网络负担和支持间断计算。

协作性是指通过虚拟机系统的通信机制，可以实现多个代理之间的合作。这种合作有多种模式。相同的代理之间相互协作，可以防止系统和代理失效。另外，异种代理之间也可以进行互补性合作，多个不同功

收稿日期：2001－04－03
基金项目：国家自然科学基金资助(69631020)
作者简介：范西昆(1976－)，男，陕西户县人，硕士生，主要从事网络安全研究.

能的代理协作完成共同目标。这样有利于将总体功能模块化,减少单个代理所完成的功能,从而降低代码的复杂度,缩短调试过程。利用这个特性,可以进一步增强代理的可靠性。

分布灵活性是指代理运行在整个分布式系统中,它根据所需将自己发送到主机现场,进行本地操作。这样,提高了操作的灵活性,消除了代理对复杂通信协议的依赖。

移动代理的体系结构包括代理本身、客户或服务程序、代理执行环境、代理移动支持模块、消息子系统以及通信底层等六大模块[4]。

在使用移动代理的IDS中,移动代理会自动转移到目标系统中,在系统日志中收集只与入侵有关的信息,无需将日志传送给检测服务器,这样降低了系统通信量,提高了工作效率。移动代理可用于路由追踪,这样就对网络数据有了全面的认识,可以更准确地把握入侵行为。移动代理的移动性和协作性使得代理功能大大增强。

2　MAB - IDS的结构模型

MAB - IDS的结构模型如图1所示。系统组件包括监视器、转换器、传输器、监视代理、移动代理以及用户界面。

该系统可分布在网络中任意数量的主机上。每一个主机可以包含多个移动代理,它们是用于监视主机系统资源某一方面的软件实体,如文件系统、网络系统和用户系统等,还可以直接监视日志。移动代理使用独立于系统的方式,利用转换器收集数据。移动代理发现可疑行为,将向特定的传输器报告,由传输器决策如何处理移动代理的配置信息。传输器根据移动代理的报告,启动其进行路由追踪。移动代理能加入或从系统中移出,而不会改变系统中其他组件,它能在运行时进行动态配置而无须重新启动。

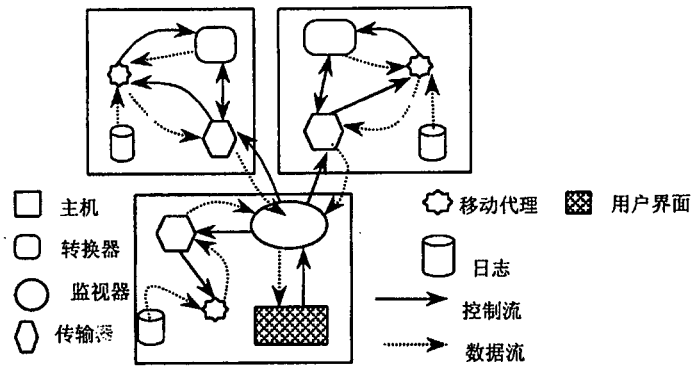

图1　MAB - IDS的结构模型

传输器是主机中的对外通信接口。它有两个职能:控制和数据处理。传输器的控制功能包括:跟踪和控制本主机移动代理的执行,启动和中止主机上运行的移动代理。启动和中止命令可能来自配置信息,也可能来自某一个监视器或对特殊事件的响应(如:某一个移动代理的报告可以触发其他移动代理对本主机的细节进行监视)。它通过产生相应的信息或执行所要求的行为,来响应监视器的命令。传输器的控制功能还包括如同文献[5]中信息板的功能。传输器的数据处理功能与AAFID[2]传输器的数据处理功能类似。

监视器是系统最高层的实体。与传输器相似,它的功能也是进行控制和数据处理。但监视器可以控制不同主机上的实体,而传输器只能控制本主机中的移动代理。监视器的数据处理功能:它将不同主机中传输器的信息进行综合处理,确定入侵所包括的主机。监视器有权检测传输器未标明的事件。控制功能主要是控制传输器。监视器是一个接口,用户界面可以访问监视器数据或给监视器提供命令,同时它向较低层实体发送命令。

转换器的主要功能是为移动代理提供经过选择和分离的数据。在独立的系统中,多个监视代理可能需要从同一个数据源中获取数据。这种情况在具有多功能日志文件(如:var、adm和messages)的Unix系统中普遍存在[2]。监视代理通过不同的方式从这些日志文件中获取数据,对其进行分析并获取有用记录。在不同版本的Unix,甚至在不同结构的系统中(如:Windows NT)运行的移动代理可以提供非常有用的信息。但是,监视代理所需的数据可能存储在不同区域或以不同格式存储。转换器为移动代理提供预约服务。每个数据源包括一个转换器,多个监视代理向其提出预约申请,提出申请时需要标明需要何种类型的纪录(通过使用通用表述的标准)。转换器只向移动代理发送符合标准的纪录,这样就减少了不必要的信息传送。

一个性能优良的监测系统必须具备与用户进行交互的良好机制。系统将用户界面和数据采集和处理单元分离,用户界面必须和监视器交互,获取信息和发送指令。这种分离模式允许系统使用不同用户界面。例如,一个图形用户界面(GUI)可被用于交互式地访问检测系统;同时,一个命令行式的界面,可以以脚本的形

式来实现维护和报告功能的自动化。

3 MAB - IDS 的工作原理

MAB - IDS 依据移动代理所监视的系统资源对其进行配置。监视网络资源的移动代理是通过分析数据包中的入侵特征来检测入侵。针对不同攻击手段的移动代理加入不同的特征文件。如针对 WinNuke 攻击[6],移动代理通过检测发往主机 139 端口的数据包,检验 TCP 头标志中的 URGENT 位设置是否为 1,如为 1 即向传输器报告。移动代理发现数据包中含有字符串"/cgi - bin/phf",即判定发生了 Web 服务器攻击[6]。对于监视其他系统资源的移动代理可从操作系统提供的日志中获取信息。当操作系统产生一个新的审计记录时,由一个代理读取此条目并进行处理。系统还可指派一个移动代理扫描值得注意的系统事件,如改变系统文件、CPU 的利用率、低层网络事件等,如发现异常,即向传输器报告。

现在,入侵手段趋向于复杂化,从针对特定主机的攻击上升为针对网络的全面攻击。攻击者利用不同身份登录分散在网络中的主机,利用它们对特定主机进行协同式攻击。这样的攻击方法包括分布式拒绝服务攻击[6](DDOS)等。位于单一节点的代理获取的信息已无法获得满意的检测效果,所以,必须利用移动代理的迁移性进行路由追踪,代理通过在路由路径上的信息积累,可以更准确地检测出入侵行为。

下面我们通过分析一次入侵检测实例来进一步了解 MAB - IDS 的工作过程。

如图 2,若某一入侵者登录主机 1、2、3 的路由顺序为从 1 到 2 再到 3。主机 1、2、3 中的移动代理分别通过各自主机的日志文件发现了可疑登录,并向各自主机的传输器报告。主机 2 和主机 3 中的移动代理 MA2、MA3 根据登录会话中的路由信息,分别向主机 1 和主机 2 迁移,并将自己的行踪记录在传输器中。MA2 和 MA3 到达目标主机后,向该主机的传输器报告。为了避免 MA2 和 MA3 路由追踪的重复,当 MA3 到达主机 2 后,传输器根据已有记录进行分析,命令 MA3 返回原主机而非继续追踪到主机 1。MA2 到达主机 1 后,在日志中继续收集信息并向主机 1 的传输器报告,然后返回原主机。各主机的传输器将数据处理结果发送给监视器,由监视器综合分析后得出入侵的路由为 1 - 2 - 3,并向用户界面报警。

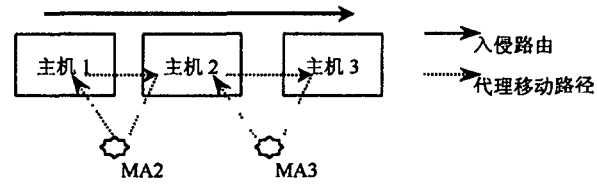

图 2 入侵检测实例分析

4 代理编程语言的选择

移动代理采用与平台无关的语言编写,这样的程序可以跨平台运行。主流的平台无关语言 Java, 在各种操作系统上都有其相应的实现,所以选用这种语言的移动移动代理可以很容易地完成跨平台的连接;而且,Java 的公共接口 CORBA(common object request broker architecture)也得到了广泛承认和支持;另外,在 Java 语言中已经直接集成了对象串行化的功能和 RMI(Remote Method Invocation)接口,为移动代理提供了强大的支持。鉴于 Java 语言的上述优点,本系统的移动代理采用 Java 语言编写。

5 与其他研究工作的比较

在文献[5]提出的基于移动代理的 IDS 中,被监视的每台主机均有一个传感器,由它来检测主机的日志文件,发现可疑行为后向管理器报告,由管理器向主机派遣跟踪代理。这种系统结构要求时刻保持网络连接,对网络的坚定性要求较高。同时,分布式系统中的主机可能会同时遭到入侵,频繁地向管理器请求会使网络开销增大,而且影响系统效率。对管理器的处理能力要求较高。

MAB - IDS 中,移动代理直接分布在各个主机,发现异常行为直接由传输器启动代理进行路由跟踪。在本地完成这些操作,既提高了系统效率,又减小了对网络坚定性的依赖。代理的特性表明,它适合作大规模信息搜集和动态处理。本系统直接采用移动代理检测日志,既发挥了移动代理的特长,又大大提高了系统的性能和整体功能。

AAFID[2]为了防止监视器在运行过程中突然失效,在每台主机中均设置一个监视器,并将所有监视器配制成层次结构。监视器间均有信息交换,网络的整体安全评估是由主监视器产生的。这样虽然提高了系统的稳定性,但是以增加网络通信量为代价的。MAB - IDS 采用了一个监视器,主要是从降低网络负担和提高系统效率方面考虑,这使得本系统在稳定性方面稍显不足。

移动代理是一种比较新的技术,将移动代理技术应用于入侵检测系统中,体现了诸多优良的特性。因此,MAB - IDS 将会有广阔的前景。目前,其原型正在进一步开发之中。

参考文献:

[1] Crosbie M , Spfford. E Defending a computer system using autonomous agents[R]. 95 - 022, COAST Laboratory , Purdue University IN 47907 - 1398, 1994.

[2] Eugene H. Spafford, Diego Zanboni. Intrusion detection using autonomous agents[J]. IEEE Computer Network, 2000,34(8): 547 - 570.

[3] Bradshaw J. Software Agent[M]. Cambridge MA: MIT Press. 1996.

[4] 任晓明,杨大鉴. 移动代理的体系结构分析[J]. 计算机工程与应用. 2001,(1):62 - 64.

[5] 李　江. 使用移动代理的网络入侵检测系统[EB/OL]. http://www. chinainfo. gov. cn/ peridical, 2001 - 02 - 04

[6] Stephen Northcutt. 网络入侵检测分析员手册[M]. 余青霓. 北京:人民邮电出版社,2000.

Mobile Agent Based Intrusion Detection System

FAN Xi - kun,　ZHENG Lian - qing,　FAN Chang - zhou,　HUO Wen - jun

(The Telecommunication Engineering Institute of the Air Force Engineering University, Xi'an 710077, China)

Abstract: Based on the introduction of mobile agent, the advantage of intrusion detection system using mobile agent technology is elucidated, and a mobile agent based intrusion detection system(MAB - IDS) is presented in this paper. The paper discusses the architecture of system in detail, as well as the means of intrusion detection and its working principle. By comparing with other systems in this area of research, It is concluded that the application of mobile agent technology makes MAB - IDS have a better capability of intrusion detection.

Key words: intrusion detection; mobile agent; Java