文章编号：1000-5889(2004)06-0082-04

基于 Mobile Agent 的入侵检测系统模型的研究

袁占亭，张秋余，米国治，包广斌

(兰州理工大学 计算机与通信学院，甘肃 兰州 730050)

摘要：提出了一个基于 Mobile Agent 技术的入侵检测系统模型.该模型采用传送 Agent 实现关键主机的隐藏，提高系统的抗攻击性；采用分区域管理增强系统的扩展性及适应性；在 CIDF 通信协议下，采用协作 Agent 实现多个入侵检测系统的协同工作.此外，还对模型的优缺点做了分析，为将来 Mobile Agent 在入侵检测系统中的应用提供一定的依据.

关键词：网络安全；移动 Agent；入侵检测

中图分类号：TP393.08 **文献标识码**：A

Investigation of intrusion detection system based on Mobile Agent technique

YUAN Zhan-ting, ZHANG Qiu-yu, MI Guo-zhi, BAO Guang-bin

(School of Computer and Communication, Lanzhou Univ. of Tech., Lanzhou 730050, China)

Abstract: On the basis of Mobile Agent technique, a model of intrusion detection system is presented. In this model transmitting agents are adopted to implement the concealment of key hosts so that the anti-attacking ability of the system is improved. Regional administration is used to improve scalability and availability of the system, and cooperative Agents are used to implement multi-IDS cooperated operation under CIDF communication protocols. Additionally, the advantages and disadvantages of the model are also discussed by the authors, providing certain basis for the application of Mobile Agent in intrusion detection system in the future.

Key words: network security; mobile agents; intrusion detection

随着网络技术的飞速发展，网络安全事件日益增多，这使得人们利用入侵检测系统(intrusion detection system, IDS)来保护他们的敏感信息变得必要.入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前发现和响应入侵.目前入侵检测还处于发展阶段，各种新的技术、新的思想不断得到应用，包括移动智能体(Mobile Agent)技术.

1 入侵检测系统及其发展

Anderson 在 1980 年第一次建立了入侵检测的概念，1986 年 Denning 给出了入侵检测的定义[1].此后，出现了两种入侵检测系统(IDS)，即基于主机和基于网络的 IDS.

基于主机的 IDS 是从一台主机内部资源收集本地数据，一般是审计日志，它的优点是可以直接从信息源收集完整的数据、实时监视可疑的连接、对入侵事件立即做出反应，还可针对不同操作系统的特点判断应用层的入侵事件，但它无法检测涉及多台主机的分布式攻击，而且基于主机的 IDS 会占用主机的资源.

基于网络的 IDS 通过在线路上设置网络接口来监视网络数据包并进行网络事件的分析.但它只能监视本网段的网络活动，在交换网络环境中难以配置而且容易受到入侵欺骗.

后来发展的混合型(同时基于主机和网络)分布式结构是将 IDS 探测器分布设置到网络中的关键节点，探测器收集数据后进行预处理，再将处理后的数据传送到一个能关联这些数据的中心分析节点.但这种 C/S 结构有单点失效、网络规模有限、灵活性有限等缺点.

收稿日期：2004-01-16
基金项目：甘肃省自然科学基金(ZS022-A25-027)
作者简介：袁占亭(1961-)，男，陕西扶风人，教授，博导.

解决这些问题的一般方法是采用分层结构和中间组件. 如 Emerald 的 State-of-the-art ID 系统和 AAFID. 层次化的入侵检测结构没有中心处理节点,信息收集在叶节点(叶节点为基于网络或基于主机的收集点). 事件信息被传送到内部节点,内部节点聚集从多个叶节点来的信息,进一步聚集、抽象和数据精简发生在更高层的内部节点直至根节点. 根节点为一命令和控制系统,它评估攻击状况并发出响应. 根节点通常向操作员控制台报告,管理员可在操作员控制台上进行人工估计攻击状态和发送命令. 一般地,层次化的体系结构能使通信效率提高,对于中央控制管理的可扩展分布式 IDS 非常适合[2].

2　基于 MA 技术的 IDS

自治性软件代理,特别是具有移动性的自治软件代理,给入侵检测技术的应用提供了一种新型的设计思路,是现在入侵检测应用研究的一个热点. 1994 年 Purdue 大学的 Crosbie 和 Spafford 在其论文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 等. 移动代理为入侵检测系统提供了一种不同于 C/S 结构的新的分布式计算方法,它的应用改善了 IDS 的许多功能[3~5].

3　基于 MA 的网络安全模型

3.1　模型分析

基于移动代理的入侵检测系统模型如图1所示. 模型采用分布式层次化结构,结合基于主机和基于网络的混合式入侵检测. 模型在叶结点对采集到的数据进行预处理及分析,将无法进行判断和系统请求的数据发送到网络控制管理台进行进一步的处理,以此来减少过多数据传输消耗带宽和主机资源,保证 MA 的移动性和反应能力,并均衡网络负载. 模型中的 MA 主要用于传送、协作和响应功能. 系统可分布在网络中任意数量的主机上,规模取决于每个网络控制管理台的处理能力. 由于使用了 MA,此模型的特点包括可扩展性、可动态配置、集成性、有效性、协作性,便于维护、升级,并可实现自动响应等,同时通过隐藏关键主机技术增强了系统的稳定性及抗攻击性.

从功能角度,此模型分为事件采集、入侵分析、入侵响应和安全控制 4 个部分,每部分包含若干组件,分布于各个主机上. 系统内的每个主机可以包含多个移动代理,它们分别用于实现监视主机系统资

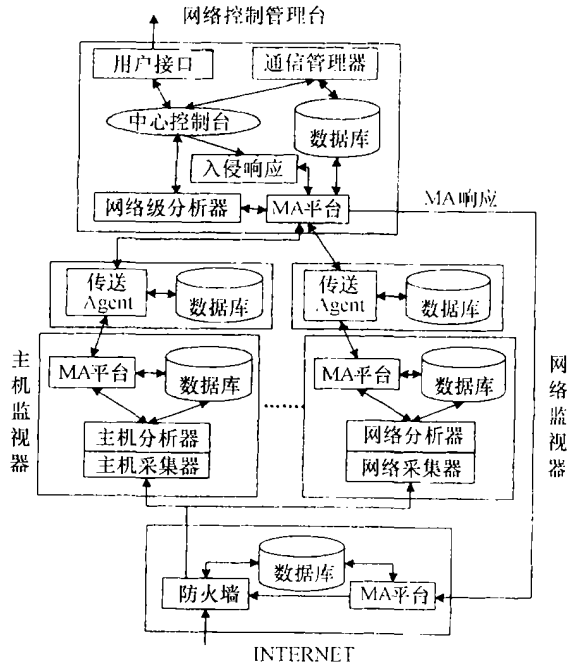

图 1　MAIDS 系统模型设计

Fig. 1　Model designing of MAIDS system

源的某一个方面或完成某一特定的任务. 移动代理的使用独立于系统,它的控制、配置、运行及恢复依赖于存在不同主机上的 MA 平台,MA 平台还控制移动代理的加入和移出,在不影响其它组件的情况下实现对移动代理的动态配置而无须重新启动系统.

主机监视器和网络监视器实现主机事件和网络事件的采集和预处理任务. 采集的数据以标准的数据格式 GIDO 传给位于主机监视器或网络协议监视器中的分析组件. 它们同时采用基于异常检测和基于误用检测的方法对采集的数据进行分析,将无法判断的数据通过传送 Agent 发送到网络级分析器进行进一步的处理,将已分析数据的分析结果存入数据库等待系统调用.

传送 Agent 模块是主机的对外通信接口. 它以 GIDO 标准数据格式向网络级分析器传送数据,并向各主机监视器或网络监视器发送系统请求,它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. 它通过产生相应的信息或执行所要求的行为,来响应系统的命令. 它是确保网络控制管理台安全通信的关键.

网络控制管理台是整个入侵检测系统的核心部分,也是系统中最高层的实体. 与传送 Agent 模块相比,网络控制管理台可以控制不同主机上的实体,而传送 Agent 模块只能控制本主机中的移动代理. 网络控制管理台接收各个传送 Agent 发送的入侵报

告、各种待处理数据以及请求数据，通过入侵分析器的分析、核实、互补和互纠(CIDF 提出的组件协同方式)，将分析结果报告给中心控制台，由它决定要采取的行动. 中心控制台是网络控制管理台的核心组件，它通过入侵分析器的分析结果决定系统是采取入侵响应、向管理员报告还是向其它网络控制管理台发送协助请求等行动.

入侵响应包括安全策略更新和 MA 自动响应. 安全策略更新包括防火墙规则和攻击特征库的更新，是让 MA 携带的安全策略移动到网络节点中对已有的规则进行更新. 可以在发现一个网络入侵时采取这样的措施以屏蔽入侵者，或者定时更新整个网络系统的安全策略. MA 自动响应机制包括自动追踪入侵者、入侵证据收集和隔离目标主机等. 自动追踪入侵者是指派遣追踪 MA 追踪入侵来源，主要用于追踪内部入侵者和确定外部入侵者的首闯入点. 追踪 MA 可以在被入侵主机上激活信息收集 MA，或者由中心控制台根据需要派遣信息收集 MA 来收集相关的入侵信息. 通信管理器进行的网络控制管理台间协作包括发送请求、身份认证、派遣 MA 和回收数据.

此外，系统中各部分还包括不同的数据库来保存相关信息.

在大型网络中，可以按区域划分主机及网络监视器，每个区域有一个网络控制管理台，各区域间通过网络控制管理台进行协同工作(见图 2)，区域可以按照不同的要求(如操作系统)[6]进行划分. 这样就可以分摊检测的功能，增强此检测模型的可扩展性，同时也提高了检测系统的效率和实时性. 从安全的角度出发，模型中的网络控制管理台为检测系统的最高实体，在层次结构中它相当于根节点，在其之上没有更高级别的网络控制管理器，以此来防止层次结构中单点失效对整个检测系统造成影响.

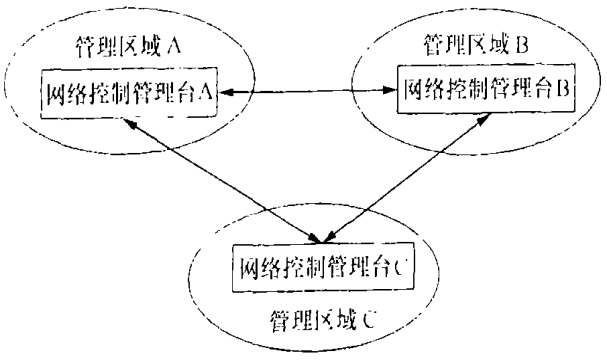

图 2 区域管理框架

Fig. 2 Regional management framework

3.2 服务请求机制

在本模型中，各个部件所提供的功能都是以服务的形式表示出来的. 一个部件在加入系统时需要进行相应的注册，将其所提供的服务注册到管理它的注册管理器中. 各个主机监视器或网络监视器在传送 Agent 模块上进行注册；各个传送 Agent 模块在网络控制管理台上进行注册，网络控制管理台之间可以进行相互注册. 每个部件将其所能够提供的服务注册到管理它的注册管理器当中，在其它部件需要时进行申请调用. 一个部件只需要在一个上层注册管理器中注册，如果有多个注册管理器，则这几个注册管理器按照一定的算法决定在哪个注册管理器中注册.

当一个部件需要某服务时，它向上层管理器发出请求，请求可以直接是服务提供部件的 IP 地址或是所需要的服务，上层管理器根据情况决定是否接受请求. 如果接受，则向部件发出服务接受消息；否则发出服务拒绝消息.

3.3 组件间的安全通信

3.3.1 通信机制

通信的安全性要求在通信机制中是很重要的. 因为可能包括公共网络或 Internet，所以对传输的信息进行验证和加密是必要的[7]. 本模型中共包括 3 种类型的通信.

1) 主机监视器或网络监视器间的通信及与传送 Agent 模块之间的通信：在同一个区域的主机监视器或网络监视器可以相互通信，它们之间的通信是由 MA 通过传送 Agent 模块来完成的. 传送Agent 模块也可以直接与和它相连的主机监视器或网络监视器通信. 由于主机监视器或网络监视器是容易受到攻击的，为了防止攻击的传播，避免暴露网络控制管理台中关键主机的位置，禁止主机监视器或网络监视器与网络控制管理台直接进行通信，这样在主机监视器或网络监视器受到攻击时，攻击者仅能知道与其通信的传送 Agent 的位置，加强了模型的安全性. 另外，还禁止主机监视器或网络监视器与其他区域的主机监视器或网络监视器通信，以避免暴露其他区域安全主机的位置.

2) 传送 Agent 模块与网络控制管理台之间的通信：传送 Agent 模块相当于代理主机，它的作用是路由网络通信. 网络控制管理台可以派遣 MA 与传送 Agent 进行数据交换，而传送 Agent 模块中的 MA 不可以移动到网络控制管理台，防止恶意Agent 的攻击，有效隐藏关键主机.

3) 网络控制管理台之间的通信：它是不同区域

间数据交换的唯一方法,它的安全通信主要依靠防火墙有效地阻止攻击数据包.攻击者可以切断它们之间的通信,但不会影响每个区域内的通信.若某个网络控制管理台受到攻击也不会影响其它的网络控制管理台,之后可以利用备份机制进行自恢复.

3.3.2　安全机制

由于发往网络控制管理台的信息都通过传送 Agent,攻击者即使攻破了主机监视器、网络监视器或传送 Agent 也无法得到网络控制管理台关键主机的位置,而主机监视器、网络监视器和传送 Agent 都有备份,在受到攻击后可由备份进行恢复.只要在 TCP/IP 层加入简单的过滤规则就可以阻止绝大部分主动 probing 攻击和 sniffing 攻击[8].

虽然隐藏了关键主机,但攻击者还是可以选择随机的 IP 地址进行 flooding DoS 攻击,有可能恰好为关键主机,从而使 IDS 系统瘫痪.本模型中的解决办法是备份网络控制管理台中关键主机上的 MA,在关键主机受到攻击之后就会用替代 MA 取代原 MA.对于原 MA,如发现自己瘫痪时间过长就会进入自消除程序.如果时间不长,则查看自己是否已被代替,若没被代替,原 MA 继续运行.

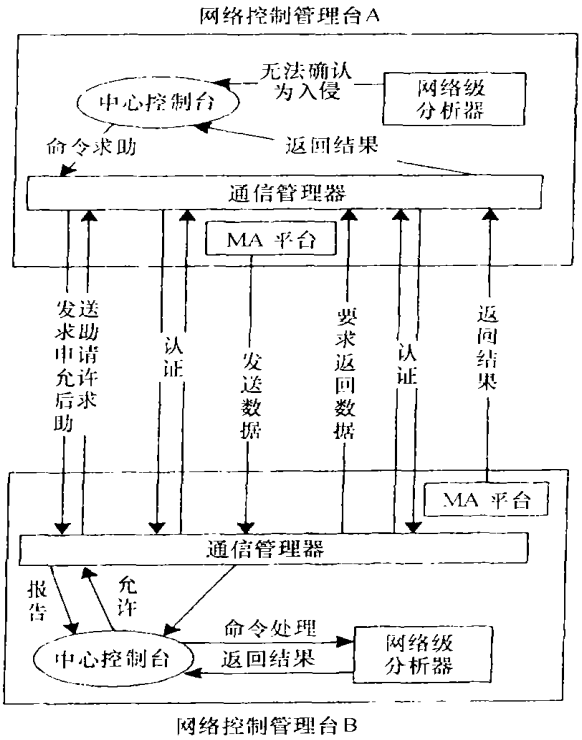

图 3　控制台间的求助过程

Fig.3　Appealing process among console

3.4　通信管理器间的求助过程

当网络控制管理台无法独立完成检测任务,它会按照注册管理器中注册的信息向其它网络控制管理台发送协助请求,若有某个网络控制管理台接受请求则发回接受信息,否则发回拒绝信息.求助由通信管理器完成,其过程如图 3 所示.

4　结语

本模型通过隐藏关键主机提高了 IDS 的抗攻击性,并充分利用移动代理技术,克服目前入侵检测系统之间的通信和协作方面的弱点,加强了入侵检测系统的整体功能.但还存在一些缺点:

1) 区域独立.因为区域之间通信包括类似 Internet 之类的不安全网络,攻击者可能切断区域之间的通信.

2) 切断控制台与监视器间的通信.区域中的网络控制管理台通过传送 Agent 通信,当传送 Agent 受到攻击瘫痪,其再恢复需要一段时间,这个间隙网络控制管理台与监视器之间是完全断开的.

由于基于 MA 的技术起步较晚,发展还不完善,在通信协议、远程配置和管理、负载以及在性能、安全性和可靠性等方面还有许多工作要做.

参考文献:

[1] DOROTHY E D. An intrusion detection model [J]. IEEE Transactions on Software Engineering, 1987, 13(2): 222-232.

[2] WAYNE J, PETER M, TOM K. Mobile agents in intrusion detection and response [EB/OL]. http://citeseer.nj.nec.com/jansen00mobile.html, 2000-06-30/2003-08-25.

[3] CHRISTOPHER K, THOMAS T. Applying mobile agent technology to intrusion detection [EB/OL]. http://citeseer.nj.nec.com/kr01applying.html, 2001-03-15/2003-08-25.

[4] WAYNE J, PETER M, TOM K. Applying mobile agents to intrusion detection and response [EB/OL]. http://citeseer.nj.nec.com/jansen99applying.html, 1999-05-20/2003-08-25.

[5] 赵　铭,罗军舟.基于 Agent 的入侵检测系统框架研究 [J].计算机工程与应用,2002(18):176-181.

[6] 张仕山,庄镇泉,狄晓龙.基于移动智能体的入侵检测系统 [J].计算机应用研究,2003(3):63-67.

[7] 张秋余,袁占亭,冯　涛.IDESA 数据加密算法的设计与实现 [J].甘肃工业大学学报,2002,28(2):73-76.

[8] 李宏权.一种基于移动 Agent 的抗攻击性 IDS 模型 [J].计算机工程与设计,2003,24(4):57-59.