基于自治代理的分布式入侵检测系统框架设计

付湘琼，胡建华，王清心，周海河
(昆明理工大学 信息工程与自动化学院，云南 昆明 650051)

摘要：入侵检测是继“防火墙”、“数据加密”等传统安全保护措施之后新一代的安全保障技术.文中分析了传统入侵检测的不足，在公共入侵检测框架的基础上，提出了一种基于自治代理的分布式入侵检测模型框架，并在此模型下讨论了这个模型具体实现的细节.

关键词：入侵检测；自治代理；分布式；网络安全
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1007-855X(2003)02-0073-04

Frame Design of Distributed Intrusion Detection System Based on Autonomous Agents

FU Xiang-qiong, HU Jian-hua, WANG Qing-xin, ZHOU Hai-he
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China)

Abstract: The intrusion detection is a new security technology, apart from the traditional security protection technologies, such as firewall and data crypt. The disadvantages of the traditional intrusion detection system are pointed out, and according to the analysis of common intrusion detection framework, a frame model based on autonomous agents is proposed, This paper also gives a detailed description how to realize the model.

Key words: intrusion detection; autonomous agent; distribution; network security

0 引言

互联网的迅速发展给网络安全技术的发展带来了挑战和机遇.目前网络安全系统主要采用的是以防火墙为主的被动管理.但防火墙本身容易受到攻击，而且对内部网络出现的安全问题经常束手无策.近些年来，作为一种主动的安全防护技术，入侵检测已经成为当今计算机动态安全模型 PPDR(Policy, Protection, Detection, Response)[1]的重要组成部分，也是动态安全技术最核心的技术之一.

1 入侵检测(IDS)技术及目前存在的问题

入侵检测是检测计算机网络以发现违反安全策略事件的过程[2].按照 DARPA 提出的 CIDF(Common Intrusion Detection Framework)构架[3]，入侵检测系统主要由四个部分组成：①事件产生器，信息的收集和过滤；②事件分析器，对数据进行分析，如模式匹配等，并作出判断；③事件数据库，模式库管理；④响应单元，根据分析结果进行响应.

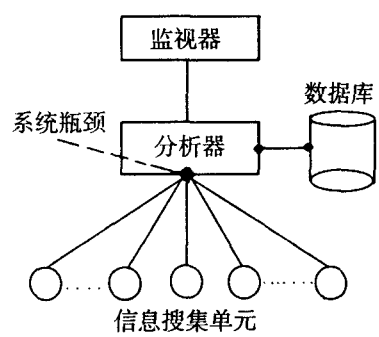

图1 集中式检测模型

在体系结构上，现今的 IDS 存在着一些问题[4,5]，例如许多现存的 IDS 采用集中统一搜集和分析数据的体系结构，即由单一或分布的主机搜集数据，数据的分析由一台独立的主机进行集中处理.这种体系有着单点失效、可扩展性差、重新配置和增加功能困难等缺陷，同时这种系统还存在通讯和计算的瓶颈，如图1.

收稿日期：2002-09-20.
第一作者简介：付湘琼(1977~)，男，硕士；主要研究方向：信息网络集成.

在数据采集上,目前有基于网络和基于主机的.基于网络的是通过将网卡设置成混杂模式来捕获网络上的数据包,基于主机的通常是分析系统日志或系统调用.基于网络的检测由于具有配置低、隐蔽性好、不依赖被检测系统的操作系统、不占用被检测系统的系统的资源,因此目前基于网络的入侵检测系统的商业化产品较多.如今比较流行的ISS公司的Realsecure、Cisco公司的NetRanger,以及开源代码的Snort等.但我们知道现今入侵大部分发生在主机上,虽然攻击可能是通过网络进行的,但攻击最终发生在主机上.同时,基于主机的检测还有着这些优点[6]:①能够准确知道主机上发生什么;②在高速网络中,基于网络的检测可能发生丢包;③可以处理主机数据加密的情况.由于初期的入侵检测系统的研究多以基于主机为主,因此这类技术研究比较成熟,市场上也存在大量产品,如Kane Security Monito以及Stalker等等.

在分析上,目前主要采用的检测方法是将审计事件同特征库中得特征相匹配,即误用检测.这种方式很大程度上依赖特征库的完备,而现在的特征库组织简单,导致漏报和误报率较高,难以实现对分布式、协同式攻击等复杂攻击手段的准确检测.另外一种分析方法是采用异常检测技术.例如,系统维护一个系统对象(如用户、文件、目录和设备等)组成的知识库,每隔一段时间(通常为一天)统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)并加入到知识库中.这些属性的平均值将被用来与当前网络、系统的行为进行比较,任何观察值在正常值范围之外时,就认为有入侵发生.

代理是执行一定安全监视和入侵检测功能的软件代理,它可以在有或无其他代理的条件下工作,可以接受更高层其他实体的控制指令,如启动、停止、运行参数的改变等等.Mark Crosbie 和 Gene Spafford 提出了在IDS种使用自主代理的概念[7],其基本思想是利用分布的独立模块完成对入侵检测的数据采集和数据分析,通过所有模块的相互协作实现对整个系统监控.

本文根据以上传统IDS系统的不足,同时参照CIDF来实现一种基于代理的分布式入侵检测系统.

2 系统总体设计

如图2所示的基于代理的分布式入侵检测系统.由中心服务器监管各个代理,内部代理监视内部网络,主机代理监视关键服务器.其中代理是分布于不同的主机和网段的一个符合于CIDF的微IDS检测系统,它可以是基于主机(在关键的服务器上)的也可以是基于网络的(在内部局域网中).

对比传统的IDS系统,这种体系结构有以下优点:

1) 用自治代理组织为相互独立的子集可以减少单点失效的问题.

2) 可扩展性好,利用代理的自治性,保证IDS规模的可扩展;采用统一的框架设计入侵检测模块,其规则可以扩展,可以引用其他同标准的IDS协同工作.

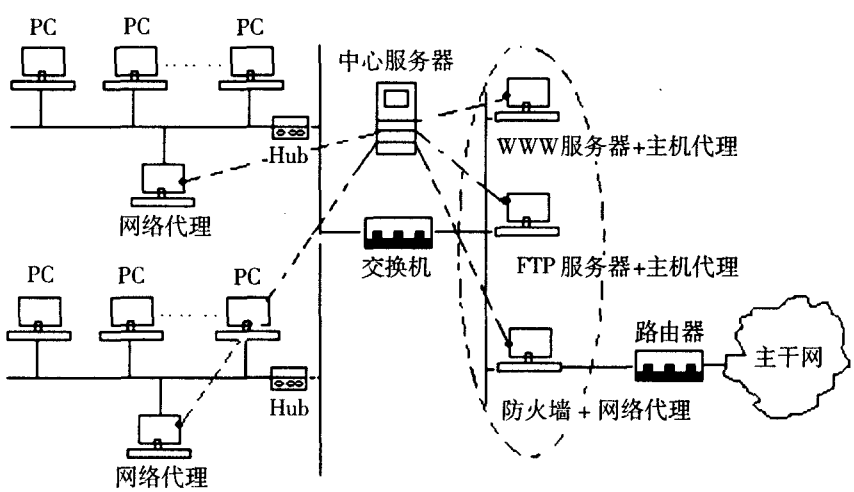

图2 物理结构图

3) 不必重启就可以重新配置IDS(或部分IDS),也可独立配置一个代理,添加数据;可以针对具体的环境进行特殊配置,增加检测的效率和性能.

4) 可以打破基于主机和基于网络之间存在的传统界限,将它们结合起来,已获得更好的检测效果.

3 系统各部件设计

3.1 中心服务器

中心服务器由系统管理员在对高层对整个系统进行监控.中心服务器的结构如图4[8],它可以由通信

部件、响应部件、代理监控和配置部件、报警显示界面，规则库管理部件等五个部分组成．为了提高整个系统安全，可以考虑增加一个冗余中心服务器．中心服务器主要完成以下功能：

1）对自治代理进行控制，可以改变局部或全部的系统配置．

2）保持最新的攻击特征数据库信息，可更新各个代理的特征数据库．

3）协调各个代理的之间的协作．

4）报警的接收和显示．

3.2 自治代理

自治代理是整个系统的最核心的部分，其效率与性能决定了整个 IDS 的价值．各个自治代理都遵循相同的结构，其结构如图 4 所示．其中，信息收集部件主要完成信息的收集，包括捕获网络数据包、关键系统配置文件的改变、生成审计事件等等任务．事件分析部件根据收集到的信息、入侵规则数据库、误用检测方法来判断是否有入侵．响应部件是在判断有入侵行为后采取一些主动的行为，例如检测到一个可疑的连接时，它可以先是使连接减慢甚至停止，以防止在等待中心报警和操作员采取相应措施的过程中造成损失，这解决了一般分布式 IDS 响应延时的问题．心跳线是用作代理保护方面，一旦中心服务器发现自治代理没有“心跳“了，就可以重新启动代理．通信部件负责与中心服务器通信，这个部件我们在下面单独讨论．自治代理主要完成以下功能：

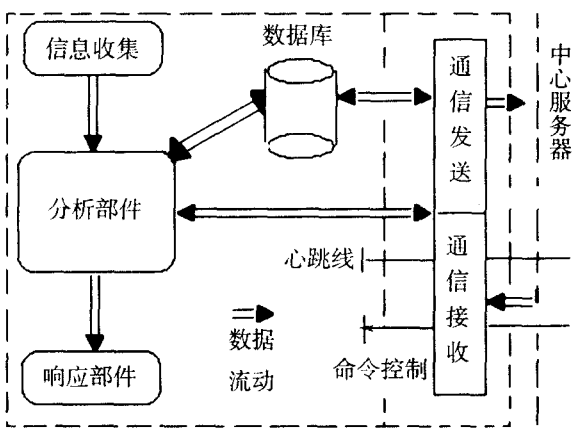

图 3 自治代理结构

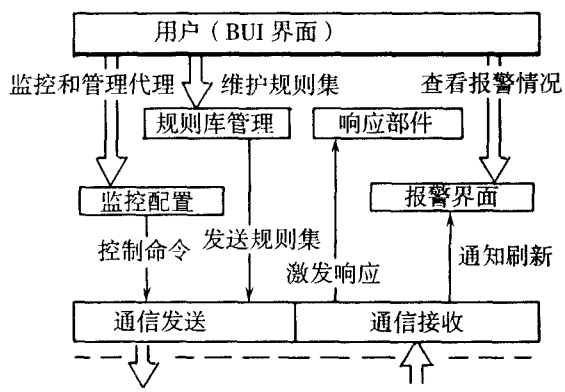

图 4 中心服务器结构

1）对入侵行为进行实时检测．

2）更新攻击数据库．

3）过滤大量次要的事件，报告重要的事件．

4）对入侵做初步响应．

3.3 通讯部件的设计

通讯部件主要完成可靠的信息传送功能，是整个系统的消息传送部件．它可以采用软总线方式，这样任何符合其标准部件都可以挂在上边和其他部件进行通讯，其结构如图 5[9]．这个结构包括一个通讯协议和该协议的具体实现，以及向上层提供一组编程接口．通讯协议规定了各个部件间通信消息的具体格式、部件间的身份认证方式、消息的加密/解密算法等．中心服务器和各个自主代理通过调用 API 函数来完成相互的通讯．

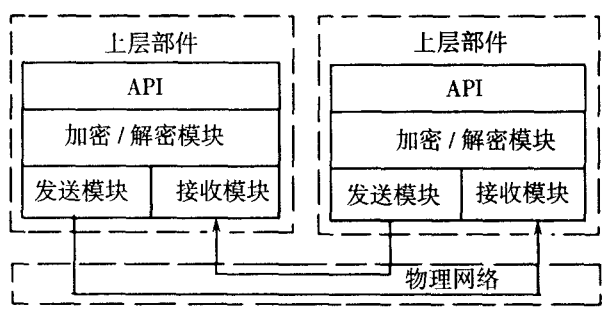

图 5　通信部件结构

4 小 结

网络的攻击与防护是一个长期复杂的过程，随

着网络攻击手段向分布式方向发展(如DDOS攻击),且采用了各种数据处理技术,其破坏性和隐蔽性也越来越强,相应地,入侵检测也应朝着分布式结构发展,以及综合采用多种检测方法.基于代理的分布式入侵检测就是适应这种发展,并已成为为当前入侵检测研究发展热点之一.本文据此设计了一个实现的框架,对其的具体实现也在进行当中.当然,这个设计也有其不足之处.例如,这种分布式的各个代理在协同检测上十分有限,要通过中心服务器的中转,解决的方法是,可以考虑扩展通信,使得各个代理能够相互通信,以达到减少中心服务器的负担、减少网络流量、以及加快的连动响应的能力.

参考文献:

[1] .S.M.Bellovin.Security Problems in the TCP/IP Protocol Suite[J].Computer Communication Review,1989,19(2):32~48.

[2] [美]Rebecca Gurley Bace 著,陈明奇,吴秋新,等译.入侵检测[M].北京:人民邮电出版社,2001.210.

[3] Phil Porras,Dan Schnackenberg, Stuart Staniford-Chen. The Common Intrusion DetectionFramework Architecture [EB/OL]. http://www.gidos.org.

[4] 胡化平,陈海涛,黄振林,唐勇.入侵检测系统研究现状及发展趋势[J].计算机工程与科学,2001,23(2):17.

[5] 何明耘,戴冠中.分布式入侵检测体系结构研究[J].计算机工程与应用,2001.15.

[6] 张铭来,金成鹏,赵文耘.分布式入侵检测系统的数据采集技术[J].计算机工程,28(2):10.

[7] Mark Crosbie,Gene Spafford. Defending a Computer System using Autonomous Agent[R].COAST Technical Report,1994.3.95~022.

[8] 唐勇,胡华平,陈海涛,余娜娜,张怡,岳虹.基于代理的网络入侵检测系统的研制[J].计算机工程与科学,2002,14(1):.

[9] 柴平,龚向阳,程时端.分布式入侵检测技术的研究[J].北京邮电大学学报,2002,2(25):15.

(上接第72页)

4 结论

(1) 对多相并流体系的实验时间序列进行了相空间重构,并考察了不同表观气速下的Poincare截面,研究结果表明,重构吸引子呈现不断伸展和收缩的变化,表现出整体稳定,局部无规的混沌特征.

(2) 多相流体系的压力波动信号具有重叠性,关联维将这种重叠性展露出来,在双对数坐标上关联积分随点距的变化曲线,明显存在三个饱和段,对应于高频分维、低频分维和低分形维.

(3) K 熵随操作条件的变化,存在与分维同样的变化趋势,K 熵均为正值,满足混沌特征的条件,K 熵越大,系统的混沌度越大,可预测性越小.

参考文献:

[1] Packard N H, et al. Geometry from a Time Series[J]. Phys Rev Lett, 1980,45(9):712~716.

[2] Grassberger P. Generalized Dimensions of Strange Attractors[J].Phys Letts, 1983,97A(6):227~230.

[3] Grassberger P, Procaccia I. Characterization of Strange Attractors[J].Phys Rev Lett, 1983,50(5):346~349.

[4] Ven don Bleek C M, Schouten J C. Deterministic Chaos: a New Tool in Fluidized Bed Design and Operation[J]. Chem Eng J, 1993,53:75~87.

[5] Daw C S, Halow J S. Evaluation and Control of Fluidization Quality Through Chaotic Time Series Analysis of Pressure-drop Measurements[J]. AIChE Symp Ser,1993,89(296):103~121.

[6] Franca F. The Rse of Fractal Techniques for Flow Regime Identification[J]. Int J Multiphase Flow,1991,17(4):545~552.

[7] Ben Mizrachi A, Procaccia I, Grassberger P. Characterization of Experimental(noisy) Strange Attractors[J].Phys Rev A, 1984,29:975~977.

[8] Bai D. Fractal Characteristics of Gas-solid Flow in a Circulating Fluidized Bed[J].Powder Technology,1997,90:205~212.