基于P2P的移动Agent入侵检测系统

孙名松[1],李 卿[2],刘 鑫[2]
(1.哈尔滨理工大学 网络信息中心,黑龙江 哈尔滨 150080;
2.哈尔滨理工大学 计算机科学与技术学院,黑龙江 哈尔滨 150080)

摘 要:传统入侵检测系统的能力在迅猛发展的互联网面前日显薄弱。探讨了将P2P技术、Mobile-agent技术引入到传统入侵检测系统中,构建一个基于P2P的Mobile-agent入侵检测系统。组成该系统的Agent在网络的各个节点间流动,实时监测网络状况,同时Agent能够互相识别各自的行为并能根据潜在的策略采取适当的反应。该系统与传统系统相比具有灵活性、分布式、智能化等特点,能全面、深入地实现入侵的检测和防御。

关键词:P2P;Mobile-agent;入侵检测
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)04-0166-04

Mobile-Agent Intrusion Detection System Based on P2P Theory

SUN Ming-song[1],LI Qing[2],LIU Xin[2]
(1.Network Information Center of Harbin University of Science & Technology, Harbin 150080,China;
2.School of Computer Science & Technology, Harbin University of Science & Technology, Harbin 150080,China)

Abstract:Facing the fast developing Internet, the ability of traditional intrusion detection system becomes weaker. Focuses on introducing P2P and Mobile-agent technology into the traditional intrusion detection system to design a Mobile-agent intrusion detection system based on P2P. These agents can mutually recognize each other's actives and can take appropriate action according the underlining security policies. Compared with the traditional system, this system is flexible, distributed and intelligent, and so on. It can finish the intrusion detection and prevention completely.

Key words:P2P; mobile-agent; intrusion detection

0 引 言

网络安全问题的日益突出对入侵检测技术提出了更高的要求,然而现有的入侵检测技术面对攻击技术的飞速变化仍然存在一定缺陷,入侵检测系统在很多地方还有待改进,如分布式、灵活性、效率等方面,需要探索新的技术来提高入侵检测的整体性能[1]。迄今为止,最为流行的用作分布式Agent网络来处理大型网络数据的是C/S模型。C/S模型是一种中心化的网络结构,过分依赖于中心服务器,而P2P模型中各实体是对等的,可以不经过服务器和其他实体进行连接,从而有效地解决传统C/S网络结构中频繁访问服务器端单一资源造成的瓶颈问题,并且消除了服务器端出现故障造成的网络瘫痪情况的发生。因此,将P2P技术应用于入侵检测系统不但降低了网络流量,而且优化了网络性能。移动代理技术作为一种新的分布式智能化技术,由于其特殊的优势,决定了它的广泛应用前景[2]。对于入侵检测技术,利用移动Agent的分布式应用这一特点,弥补了传统的入侵检测系统局限于一个网段、彼此协同差的缺点[3]。文中通过借鉴P2P的成果,并结合移动Agent技术,提出了一种新型的入侵检测系统APIDS。

1 移动代理

移动代理(Mobile Agent,简称MA)[4]是一个能在异构计算机网络中的主机间自主地迁移的程序,它在汲取传统分布计算技术的有益经验的基础上,为分布计算提供了一个全新的范型。可以将Mobile Agent定义为:具有跨平台持续运行、自我控制移动能力,模拟人类行为关系,并能够提供一定人工智能服务的程序。其突出特征就是Agent实体的运行不是固定在一台机器上,而是可以在多台机器上。移动代理的特点在于移动上,它可以选择何时进行迁移,移动到何地。主要表现在每个代理可以在执行的任意点上挂起并将自己

收稿日期:2008-07-17
作者简介:孙名松(1963-),男,教授,研究方向为网络应用与网络安全。

传送到另一台主机上,然后在该处继续执行,任务结束后将执行结果返回给原主机。它还可以执行克隆等操作,产生子代理共同完成任务。

移动代理是能够自主地从网络中的一个结点移动到另一个结点的自治程序。移动代理可以在运行期间直接进行主机间的迁移,就是说,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。极大地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。由于移动代理可以自由地在主机之间进行迁移,使得代理的运行场地不再局限在某一个特定位置,从而比较容易获得全面和有针对性的数据,使移动代理具有智能性。

1.1 移动 Agent 的系统结构

移动 Agent 的系统结构如图 1 所示。

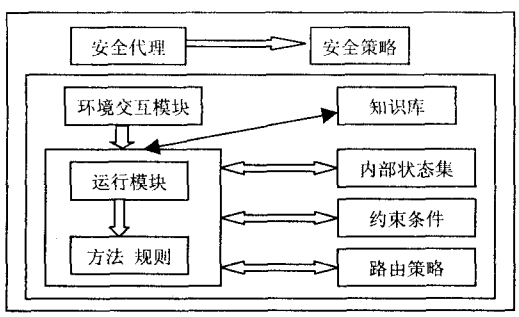

图 1　移动代理的结构模型

1) 安全代理模块。

移动 Agent 与外界环境通信的中介,保护移动 Agent 自身,执行移动 Agent 的安全策略,阻止外部环境对移动 Agent 的非法访问,保证数据的正确性和合法性。它通常需要完成数据加密和数字签名等任务。

2) 环境交互模块。

移动 Agent 通过它感知外部环境,并和其他移动 Agent 交换数据以达到准确传输,作用于外部环境的目的。它实现了 ACL 语义,保证使用相同 ACL 的 Agent 和服务器间的正确通信和协调,其通信内容语义与 ACL 无关。

3) 任务求解模块。

它由移动 Agent 创建者初始化,存储与执行任务相关的特征知识和其他合法移动 Agent 共享信息。它是为求解任务而构造的外部或自身的知识数据库,用以保存移动过程中获取的知识和任务求解结果。

4) 内部状态集。

它和移动 Agent 任务求解模块相互作用,用以存储移动 Agent 执行过程中的状态信息,即 Agent 执行的当前状态,保证移动 Agent 的记忆功能和连续性。

5) 约束条件。

它是 Agent 创建者为保证 Agent 行为和性能而设置的约束参数的集合,如返回时间、站点停留时间及任务完成程度等。一般只有创建者拥有对约束条件的修改权限。它由移动 Agent 来实现,通过移动 Agent 外部环境保证。

6) 路由策略。

它是决定移动 Agent 迁移路径的有序主机列表,即路由表。它定义了移动 Agent 在设计初期需要事先初始设置的路由信息,并将其存放在路由表中。它保证了移动 Agent 可以自主迁移,并且可以提高传输速率和避免网络拥塞。它可以是静态的 Agent 服务器列表,适用于简单、明确的任务求解情况,也可以是基于规则的动态路由,用以满足复杂和非确定任务的求解的需要。

1.2 将 Agent 应用于对等模式 IDS 的优势

移动代理是一个能在异构网络中自主地从一台主机迁移到另一台主机,并可与其它 Agent 或资源交互的程序,它可以自主地决定去哪儿,做什么,存活多久。在层次化协作模型中引入移动 Agent 可以解决和优化原有网络中的许多问题和方面:

1) 在 P2P 网络中,信息查询会产生巨大的通信流,并且大部分信息是冗余的。而移动 Agent 能移动到每个节点上,通过本地化的运行来减少这些情况的发生。

2) 移动 Agent 存储它所需要的所有数据,当产生它的机器不在网络时,仍能继续执行搜索任务,搜索完后,携带结果返回原始节点,或等待原始节点再次入网。

3) 它可以巡行到原始节点不知道的节点上,发现更多的资源。而接受它的节点也可以得到它曾访问过的其它节点的资源信息。但如果不想或不能容纳它,也可以拒绝接受。

4) 移动 Agent 可以通过克隆在网络上的不同方向上分派,并行运行,从而可以更快地发现资源并提高容错性。

2 P2P 原理

P2P(peer－to－peer),即对等网络或对等计算,网络的参与者共享他们所拥有的一部分硬件资源(处理能力、存储能力、网络连接能力、打印机等),这些共享资源通过网络提供服务和内容,能被其它对等节点(Peer)直接访问而无需经过中间实体[5]。在此网络中的参与者既是资源(服务和内容)提供者(Server),又是资源获取者(Client)。P2P 体现在对等性,它是一种网络模型,由大量高度动态的节点组成。网络中的节点

都是对等的,同时是动态的,可随时加入或退出,并具有相同的能力。与传统的 C/S 网络结构的本质区别是,整个网络不存在中心节点。在 P2P 网络中,每一个 peer 都是平等的参与者,同时扮演着使用者和提供者的角色,网络的每一个节点拥有资源的所有权和控制权。服务使用者和服务提供者之间进行直接通信,可充分利用网络带宽,减少网络的拥塞状况,使得资源的有效利用率大大提高。同时由于没有中央节点的集中控制,系统的伸缩性较强,也能避免单点故障,提高系统的容错性能。

P2P 网络不同于 C/S 模型的相互作用。C/S 的一个实例如 WWW,依靠单一的服务器存储信息以及用分发的方式响应客户请求,信息存储在服务器上本质上是静态的、集中式的,且主题仅仅由提供者更新,用户只接受而不提供信息,因此充当被动的角色。而 P2P 对等体之间可以不经过中间实体而直接访问,因此,这种网络的参与者既是资源的提供方又是资源的请求者。在另一方面,一个 P2P 网络在和其他网络成员分配信息上,所有的节点都处于平等的地位。每个用户构成一个可以访问的分布式信息仓库,与任何一个参加网络的能力相结合,导致一个由分布式信息仓库组成的网络的快速增长。一个没有中心服务器,系统的任何参与者之间都能够相互作用[6]。

3 基于 P2P 原理 Agent 入侵检测模型 APIDS

根据对移动 Agent 技术的介绍,我们已知道在入侵检测系统中引入移动 Agent 技术具有的优点:减轻网络负担、缩短网络等待时间、异步自治执行、动态自适应、异构环境运行以及健壮性和容错能力[7]。通过比较可以发现,P2P 原理和移动 Agent 系统虽然是两种不同的技术,但两者组织结构之间有许多相似之处:都是分布式系统;都具有多个自主实体;都具有局部和全局任务;都是自适应的并且都能通过自身经历进行自我学习;都能够感知外界环境的变化并做出相应的反应;系统中各个实体都能进行相互交流和协作;实体都拥有进行智能决策的知识[8]。如果把 P2P 的机理与 Agent 技术融合在一起,就可以构造出一个具有 P2P 特征的 Agent 模型——APIDS。图 2 描述了基于 APIDS 的入侵检测系统物理结构框架。

各个域又可分为物理上的多个逻辑检测区域(局域网),每个检测区域内包含一个分析器和多个智能代理(主机代理、布于各网段上的网络代理及监控代理)。主机代理域中,每个智能代理监测系统资源的一部分,如文件系统、网络系统、用户系统等;服务器代理域中,每个智能代理监视经过路由器的数据包;子网代理域中,每个智能代理检测并记录流经子网的数据流[9]。主机代理域、服务器代理域和子网代理域的工作过程基本相同。如下所述:

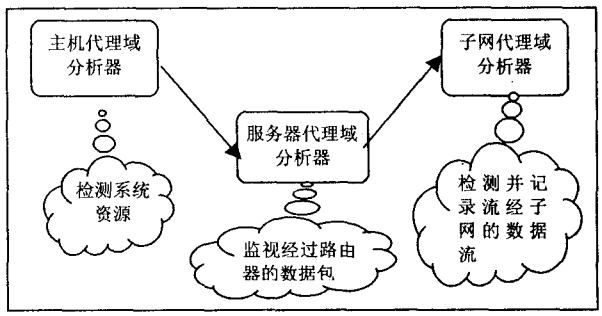

图 2 模型体系框架

1) 采集进出主机、服务器或子网的信息流;

2) 按照规则库中的规则分析这些信息,并把分析结果作为安全日志存入事件库;

3) 分析并确定入侵阈值,如果超出预先所规定的阀值,则智能代理向系统管理员汇报检测结果或发出报警并采取相应的措施;

4) 如果入侵事件比较复杂,单个智能代理不能处理,则通过监控代理与其它智能代理合作,共同完成入侵检测任务;

5) 如果区域内的分析器不能确认攻击类型,则向其它域中的分析器发出协查请求,通过与其它分析器之间的协作共同完成入侵检测任务;

6) 使用数据挖掘引擎,对事件库中的数据进行分析,维护并更新规则库,同时记录该用户信息[10]。

4 模型与分析

通过描述一个复杂入侵的检测过程来简单阐述 APIDS 系统的工作流程和原理,这个实验是有关分布式目标的扫描行为的,假设攻击者对 3 个局域网内的主机发起了端口扫描。

如图 3 所示,每个局域网所在的检测区域内的网络代理 S1,S2,S3 通过对各自网络数据流的分析,就会检测到对本检测区域内主机大量端口的连接请求。S1,S2,S3 分别向所属的分析器 A1,A2,A3 报告异常端口连接事件 E1,E2,E3。假设分析器 A2 首先收到 S2 提交的 E2,然后向分析器 A1 和 A3 发出协查请求消息,并给出 E2 的描述信息。A1 和 A3 接收到 A2 的协查请求后,提取 E2 的特征,与本分析器得到的各事件报告进行相关分析,各自发现与 E2 在时间、来源等特征属性上存在紧密相关的事件 E1 和 E3,分别向分析器 A2 返回协查回复消息。A2 通过对 E1、E2、E3 三个事件进行综合,确认在监控网络内发生了一次分布

式目标的端口扫描行为。通过实验分析,可以看出 APIDS 体系结构可以有效地检测分布式攻击。

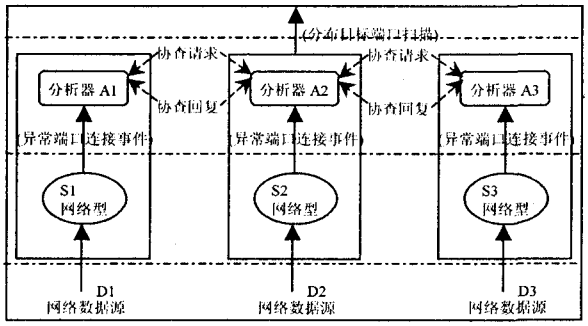

图 3　APIDS 模型

5　结束语

笔者创新点在于将移动 Agent 技术和 P2P 理论结合起来,构造出一个新型的入侵检测模型。移动 Agent 技术和 P2P 理论都是近年来的新兴技术,鉴于它们都具有自适应、自学习、分布式的特点,文中试图利用它们在技术上的优势来构建分布式入侵检测模型。它融合了两者的优势,是一个智能的、鲁棒的入侵检测系统,能同时进行多层次的监测和不同级别的响应。基于 P2P 的移动 Agent 入侵检测系统模型可以实时地检测基于网络和基于主机的入侵行为。该模型是个开放的系统,易于加入新的 Agent,扩充新的检测模式。模型充分利用了 P2P 分布式无中心和移动 Agent 的特点,各 Agent 间既分工又联合的协同作战,合作完成检测任务。另外模型采用一定状态的检查和验证策略,保证了系统自身的安全系统是完全分布式的,监视 Agent 生成后在网络上漫游,因此一个节点被攻破不会导致整个系统丧失检测功能。

下一步的研究工作主要集中在如何实现一个高效的算法,来保障 Agent 之间的通信以及它们在网络中移动的安全问题。

参考文献:

[1] Allen J, Christie A. State of the Practice of Intrusion Detection Technologies[R]. Technical Report, Networked Systems Survivability Program. [s.l.]:[s.n.],2000:47-83.

[2] 徐　峰,宋如顺,赵　洁,等. 基于 P2P 多 Agent 数据融合入侵检测模型研究[J]. 计算机工程与应用, 2004(17):159-161.

[3] The Intrusion Detection Message Exchange Format . draft-i-etf-idwg-id-mef-xml-12[S/OL]. 2005-04. http://www.ietf.org.

[4] 李　洛,李拥军. 基于 Agent 多媒体数据库模型的研究[J]. 计算机应用研究,2002(10):191-194.

[5] 黄道颖,黄建华,庄　雷,等. 基于主动网络的分布式 P2P 网络模型[J]. 软件学报, 2004(7):1081-1089.

[6] Zhu Y, Hu Y M. Efficient Proximity-Aware Load Balancing For DHT-Based P2P Systems[J]. IEEE Tran. Parallel and Distributed Systems,2005,16(4):349-361.

[7] 张云勇. 刘锦德. 移动 Agent 技术[M]. 北京:清华大学出版社,2003.

[8] Asaka M, Okazawa S. The Implementation of IDA: An Intrusion Detection Agent System[C]//Proceedings. North Falmouth:[s.n.],2001:81-92.

[9] Jansen W, Mell P, Karygiannis T, et al. Applying Mobile Agents to Intrusion Detection and Response[R]. National Institute of Standards and Technology Computer Security Division, NIST Interim Report (IR)-6461.[s.l.]:[s.n.],1999.

[10] 李　兵. 一种基于对等模型的网络入侵检测系统模型[J]. 计算机技术与发展,2008,18(3):172-176.

(上接第 156 页)

法——MAXQ-RLA,该算法可以轻便地找到最优的策略。但是,MAXQ 方法是利用先验知识对任务进行人工分层,自动分层的能力较弱,且分层粒度不够精细,如在出租车问题中,它难于进一步对导航子任务进行抽象,这些问题还有待于进一步的研究。

参考文献:

[1] Iima H, Kuroe Y. Swarm reinforcement learning algorithms - exchange of information among multiple agents[C]//SICE, 2007. Annual Conference. JAPAN: SICE, 2007:2779-2784.

[2] Erfu Y, Yang E. A Multiagent Fuzzy Policy Reinforcement Learning Algorithm with Application to Leader-Follower Robotic Systems[C]//Intelligent Robots and Systems, 2006 IEEE/RSJ International Conference. New YorK: IEEE, 2006:3197-3202.

[3] Handa H. Evolutionary Computation on Multitask Reinforcement Learning Problems[C]//Networking, Sensing and Control, 2007 IEEE International Conference. New York: IEEE, 2007:685-688.

[4] Watanabe T, Takahashi Y. Hierarchical reinforcement learning using a modular fuzzy model for multi-agent problem[J]. Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference. New York: IEEE, 2007:1681-1686.

[5] Dietterich T G. Hierarchical Reinforcement Learning with the MAXQ Value Function Decomposition[J]. Journal of Artificial Intelligence Research, 2000, 13:227-303.

[6] Dietterich T G. The MAXQ method for hierarchical reinforcement learning[C]//Proc of the 15th ICML. San Francisco: Morgan Kaufmann, 1998:118-126.