局域网 Agent 网络结体系 包过滤 6

计算机科学 2000Vol.27№.8

2-22

局域网环境中基于 Agent 的网络安全体系研究

A Research of Network Security Architecture Based on Agent Technology under LAN Environment

吕双双 刘培玉

TP393.1

（山东师范大学计算机系 济南 250014）

Abstract Network security has become the hot issue of current network technology field. The paper first discusses the existing security technology, especially the firewall technology, then, proposes a kind of new-style network security architecture under LAN environment, combining with Agent technology.

Keywords Network security, Agent technology, Multi-Agent system, Network security architecture

一、引言

在网络技术迅速发展和普及的同时，网络的安全性问题也日益突出，越来越多的人已经意识到网络上存在着大量的安全威胁。一个用户或一个局域网络连接到 Internet 或其他外部网络后，虽然可方便地进行信息的共享，但是由于网络开放性的体系结构，用户或局域网络自身的信息和数据，包括某些具有不同程度保密性要求的信息和数据，也全部暴露在外部网络用户面前。面对网络上飞速发展和迅速传播的计算机病毒及恶意的黑客入侵攻击等安全隐患，人们迫切需要一种有力的网络安全工具，以保护政府、国防、金融、保险、电信及军工企业等具有获取信息和严格保证数据安全的双重要求的局域网络的安全性。在这种情况下，许多网络安全技术应运而生。

二、网络安全技术

针对网络上存在的各种安全隐患，人们已经研制了许多安全防范措施，提出了许多解决网络安全问题的思想。已有的网络安全技术有：防火墙技术；信息保密技术；信息认证技术；在工作站上部署防病毒软件；利用操作系统、数据库、电子邮件、应用系统本身的安全性，对用户权限进行控制；或其他方法。其中，防火墙技术是当前比较广泛地用于局域网络安全防护的安全技术。

防火墙是近几年发展起来的重要安全技术，已广泛应用于网络安全防护，它是设置在被保护网和外部网之间的一道屏障，用来检查网络入口点通讯，根据客户设定的安全规则，对通过防火墙的数据流进行监测、限制和修改，以实现不安全的公共网络环境下的局部网络的安全保护。防火墙可以是一个独立的系统，也可以在一个进行网络互连的路由器上实现。防火墙采用的基本技术有如下两种：

◇包过滤技术 是基于路由器的技术，包过滤型防火墙位于网络层，它根据在系统内部设置的访问控制表，对通过网络层的 IP 数据包进行选择和过滤。通过对数据包包头信息中的源 IP 地址、目的 IP 地址、源端口号、目的端口号的检查，来确定该数据包是否合法，以决定是否允许它通过。

◇代理(Proxy)服务技术 这种防火墙实际上是一组代理程序的集合，对于每种应用服务，如：Http，WWW，Ftp 等都由相应的代理程序提供服务。这种技术在应用层上实现。当外部网络上的用户要与内部网络进行通讯时，它发出的请求，都要先经过防火墙，由防火墙上的代理程序对它进行安全性或合法性检查，之后根据检查结果决定与目的客户建立连接或拒绝该请求。内部网络与外部网络的通讯与此类似。

到目前为止，防火墙技术仍只是处于发展阶段，还有许多问题有待于解决：①传统的防火墙产品和目前市场上流行的多种安全设备都需要人工来实施和维护，不能主动跟踪入侵者；②完全不能防止内部攻击，它针对的是来自系统外部的攻击，一旦入侵者绕过了防火墙，他就成了系统内部人员，防火墙对他就不再起作用；③防火墙在对网络数据流量进行深入检测和分析的同时，网络的传输速度势必就要受到影响，防火墙的使用是以牺牲整个网络效率为代价的；④不能防止受病毒感染的软件或文件的传输，内部人员下载软件时，其中隐藏着致病模块，如：特洛伊木马，病毒等；⑤另外，其透明性也不够理想。

三、Agent 技术及多 Agent 技术

Agent 技术及多 Agent 技术是近年来分布式人工

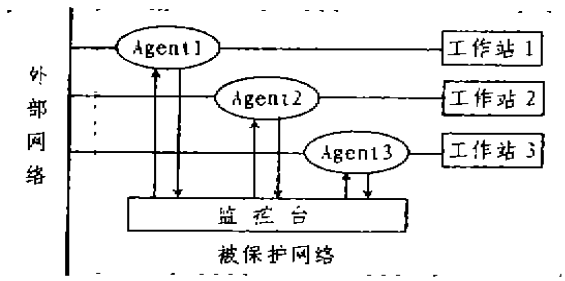
智能(DAI)研究的一个十分活跃的领域，Agent是一个反应的、自治的、内部驱动的实体，能以主动服务方式完成一组操作，具有智能性、自主性、交互性和可移动性，能作用于自身和环境，并能对环境做出反应。多Agent系统MAS(Multi-Agent System)是由一组独立的、但又协同工作的Agent构成的计算系统，Agent是其基本组成单元。各Agent之间可以相互通讯，以协调完成某一共同任务。在多Agent系统中，Agent应能够认识变化的过程流并进行相应的自适应调整。在理想情况下，系统的Agent能够动态重配置自身以适应负载的变化。因此，Agent具有易扩展、易维护、可重用等优点。

当前，基于计算机的活动越来越多，绝大部分自动体都要求用户明确启动所有任务，并监视所有事件，或者说，用户必须直接操纵这些活动，这就要求用户必须事先经过适当的培训，否则用户就会有一种不适应计算机的感觉。这实际上增加了用户工作的复杂性，给他们带来了不便。自治的Agent可以用来补充"直接操纵"的人机交互模式，实现"间接管理"的人机交互方式，即用户从事于与Agent的协作过程，用户和Agent既启动通讯，监视事件，又执行任务。这样，Agent与用户协作完成任务时，就隐藏了任务的复杂性，而且它还能像用户一样，监视事件和过程。

因此，可以考虑将Agent技术应用于网络安全，构造一种新的网络安全体系结构。

四、基于Agent的网络安全体系

结合Agent技术，我们提出一种新的局域网环境下的网络安全体系，如下图所示：



其中，局域网环境中的每个工作站，都配置一个Agent，各Agent具有报警和简单的控制功能。它们根据建在本地的规则库，负责对流入或流出该工作站的数据流进行采集，分析，并根据分析结果生成本地安全日志；必要时，向监控台报警。各Agent都具有一定的独立性，但又协调工作以共同完成网络安全的维护工作。

监控台负责监视各工作站上的Agent，收集它们发来的警报信息，根据设置在此地的中心规则库，采取相应的措施；或进一步分析，或向发来警报的工作站Agent发送指示，必要时向局域网环境中的所有工作站报警，并进行相应的安全记录。如：某工作站发现一带病毒文件，而该文件已经发出，有可能在网络上传播，这时，监控台就需要向各工作站上的Agent发出报警信息，通知该文件名及所带病毒名或病毒特征，以便各工作站上的Agent采取预防措施，减少发生危害的可能性。监控台上的中心规则库需要根据情况不断更新。

引入这种新的网络安全体系的好处有：

1)在上述体系结构中，监控台负责从总体上监视流入和流出局域网环境中各工作站的数据流，但它并不是将所有通过的数据流都机械地记录下来，而是通过监视各工作站上的Agent，间接地对各工作站实施监控。各工作站上的Agent负责对该工作站进行监视，对一些简单的任务，Agent可自行处理，只有当发现它处理不了的复杂任务时，才向系统监控台发出报警信息，由控制台做进一步的判断分析。这种有选择地向系统监控台发送报警信息的体制，减少了系统监控台处理的信息流量，减轻了它的负荷，有利于加快网络上信息传输的速度，进而提高整个系统的效率。

2)与流行的防火墙技术体系相比，该体系不但能对来自外部网络的攻击实施监控，还能对来自内部的攻击进行记录，为最终查找到实施攻击的用户提供依据，从而对内部用户起到警告和威慑作用，有效减少来自内部的攻击，这对于有70%的攻击来自于内部网这一事实，具有重大意义。

3)由于Agent具有易扩展、易维护、可重用等优点，可以方便地对系统进行扩充和维护。现代科学技术的发展日新月异，同时，新的病毒、新的入侵攻击手段也不断出现，这就需要对系统进行不断的更新和改进，以适应形势的需要，维护网络的安全。

4)由于局域网络又可能根据地理位置或其他因素划分成不同的网络片段(network segment)即子网，而每个子网又有不同的安全性要求，所以越来越多的企业倾向于根据安全等级，将内部网划分成多个子网。在每个子网上配置一个维护该子网安全的Agent，可以降低网络安全维护人员的工作复杂性，方便管理。

参考文献

1 吴坪，徐时新，张信成. 应用层次化Agent构造网络安全辅助系统. 计算机工程与应用，1999，6
2 张晔，刘玉莎 防火墙技术的研究与探讨. 计算机系统应用，1999，9
3 孙玉冰，林作铨. 软件Agent. 计算机技术与自动化，2000，19(1)
4 赵战生，冯登国，等. 信息安全技术浅谈. 科学出版社，1999
5 吴建林，姜丽红，薛华成. 专家系统与多Agent协作系统. 计算机科学，1998，25(4)
6 刘海燕，王献昌，王兵山. 多Agent系统研究. 计算机科学，1995，22(2)