一个基于 Multi-Agent 的分布式入侵防御系统模型

谢赞福[1] 李吉桂[2]

(广东技术师范学院计算机科学系 广州 510665)[1] (华南师范大学计算机科学系 广州 510631)[2]

摘 要 从入侵防御技术的基本概念出发,讨论了入侵防御系统构造所涉及的关键技术,提出了一个基于 Multi-Agent 的分布式入侵防御系统模型。该系统模型结合目前几种主要的入侵检测、入侵防御、免疫原理和数据挖掘技术,实现了入侵检测和实时响应防御的分布化,同时增强了入侵防御系统的灵活性、可伸缩性、鲁棒性、安全性以及入侵防御的全面性。

关键词 Multi-Agent,信息网络安全设施,入侵检测系统(IDS),入侵防御系统(IPS)

Research on Distributed Intrusion Prevention System Based on Multi-Agent

XIE Zan-Fu[1] LI Ji-Gui[2]

(Computer Science Dept., Guangdong Technology Normal University, Guangzhou 510665)[1]

(Computer Department of the South China Normal University, Guangzhou 510631)[2]

Abstract Based on the concept of intrusion prevention techniques, some key techniques for intrusion prevention system are discussed, and a distributed model of intrusion prevention system based on Multi-Agent is proposed in this paper. In this system the main detection methods, prevention methods, immunity principle and data mining technology are used to realize the distribution of intrusion detection and real-time response prevention, and improve the system's flexibility, expansibility, robustness, security and the prevention maturity.

Keywords Multi-Agent, Information network security infrastructures, IDS, Intrusion Prevention System(IPS)

1 引言

入侵防御系统也称入侵防护系统(Intrusion Prevention System,IPS)是一种主动的、积极的入侵防范、嵌入式的阻挡系统,它部署在网络的进出口处,当它检测到攻击企图后,它会自动地将攻击包丢掉或采取措施将攻击源阻断。IPS 的检测功能类似于 IDS,但 IPS 检测到攻击后会采取行动阻止攻击,它对检测的内容提供实时的保护。IPS 实时地阻止攻击,而不是在攻击到达的同时或之后,简单地发出告警。可以说 IPS 是基于 IDS 的、建立在 IDS 发展的基础上的新生网络安全产品。IPS 弥补当今防火墙、防病毒、IDS、补丁管理等响应式的安全解决方案的不足,已成为网络安全中一支生力军。

IPS 一般工作在 in-line 模式,它串接在网络中,可以阻断部分攻击行为。由于大部分攻击行为具有相对固定的特征和变形方式,提高检测的准确性、实用性和实时性是研究重点。与 IDS 一样,IPS 也分成基于主机的 IPS(HIPS)和基于网络的 IPS(NIPS),前者预防黑客对关键资产,如对关键服务器、数据库的攻击,后者预防对关键网段的攻击(NIPS 的工作原理示意图如图 1 所示)。与 IDS 的基于异常行为库匹配检测方法相反的是,IPS 是对基于正常行为的匹配检测,即系统设立正常行为库,符合正常行为的访问才允许进入,而不符合的则拒绝,从其原理中可看出,IPS 将能防御以往未知的攻击。

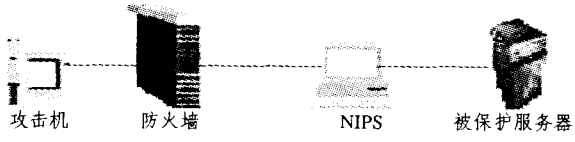

图 1 NIPS 工作原理示意图

入侵防御技术已经成为目前动态安全工具的主要研究和开发的方向,入侵防御是分层式网络安全性的关键,研制开发入侵防御系统已成为一项具有极大应用价值的计算机工程。在技术发展上,IPS 将朝下列方向发展:(1)精简规则并提高系统的自适应防御免疫能力;(2)与防火墙紧密结合;(3)实时关联分析技术;(4)简单易用方面的提高。

2 入侵防护系统的发展需求

实践证明,单一功能的产品已不能满足客户的需求,安全产品的融合、协同、集中管理是网络安全重要的发展方向。大型企业需要一体化的安全解决方案,需要细粒度的安全控制手段。中小企业一边希望能够获得切实的安全保障,一边又不可能对信息安全有太多的投入。从早期的主动响应入侵检测系统到入侵检测系统与防火墙联动,再到最近的入侵防御系统,是一个不断完善的解决安全需求的过程。

信息安全产品的发展趋势是不断地走向融合,走向集中管理。但防火墙加入侵检测产品互动的方式也有一些不足。首先使用两个产品防御攻击会使系统很复杂,任何一个产品发生故障都会导致安全防范体系的崩溃,而且两个产品的维护成本也比较高。最重要的问题在于防火墙和入侵检测产品的互动并没有一个被广泛认可的通用标准。这样,用户在采购安全产品的时候,不得不考虑到不同产品的交互性问题,从而限制了用户选择产品的范围。为了解决不同安全产品难于协作的问题,人们考虑将两个产品的功能集成到一个产品内,这样就产生了 NIPS(网络入侵防御系统)。

对于 IDS 系统,人们很自然地会有这样的想法:既然可以检测到攻击行为,为什么不去阻止它呢?实际上,IDS 系统的开发人员也确实是这样去做的。在早期,开发人员试图在网

谢赞福 副教授,从事计算机科学技术研究,主要研究方向:面向对象的软件工程环境、数据库技术与信息网络安全等。李吉桂 教授。

络层对攻击行为进行阻断，这样就产生了所谓的主动响应的网络入侵检测系统。但是这种主动响应的网络入侵检测系统只针对 TCP 流和 UDP 连接进行阻断。显然，IDS 向 IPS 的发展，就是一个寻求在准确检测攻击基础上防御攻击的过程，是 IDS 功能由单纯的审计跟踪到审计跟踪结合访问控制的扩展和延伸。

3 入侵防护解决方案的特点

真正的入侵防护解决方案可使用户不必进行分析即可采取措施保护系统；同时，它可防止攻击对操作系统、应用系统和数据造成的损失。通过使用防御系统来主动预防攻击，而不会产生检测攻击、确定攻击最后采取措施阻断攻击过程的间断。同时，对于安装软件补丁以在操作系统和应用程序中安装软件补丁的方式来堵塞漏洞，并阻断类似蠕虫病毒和缓冲区溢出等攻击方面，入侵防护可帮助企业更好地控制这一高成本和费时的过程。一个理想的入侵防护解决方案应该包括以下几个特点：

(1)主动、实时预防攻击。提供对攻击的实时预防和分析是入侵防护解决方案核心所在，应该在任何未授权活动开始前发现攻击，并防止攻击进入重要的服务器资源。基于防御免疫原理是实现这个特点的可选择技术方案。

(2)保护重要的服务器。服务器中有最敏感的企业信息，是大多数黑客攻击的主要目标。所以，拥有专门为服务器保护订制的入侵防护解决方案十分重要。

(3)补丁等待保护。补丁管理是一个复杂的过程。在补丁被开发和安装之间，狡滑的黑客会对服务器和重要数据造成恶意破坏，优秀的入侵防护方案应为系统管理员提供补丁等待期内的保护和足够的时间，以测试并安装补丁。

(4)签名和行为规则。检测入侵最有效的方法是采取混合方式，即整合针对具体攻击的签名和行为规则的力量。这一混合方式可提供已知和未知攻击保护，而同时将误报率降至最低，从而无须做出任何损失性让步。

(5)分层防护。强大的安全都是基于深度防御的概念：拥有多层保护。应该具有冗余机制，当攻击通过一层阻挡时，总有其他的阻挡在等待它们。

(6)多种环境同时保护。使用不同运行环境的企业需要确保选择的入侵防护在所有重要的服务器中保持一致。它也可进行连贯、可靠的跨平台保护。

(7)可管理性。理想的入侵防护解决方案应可使安全设置和策略被各种应用程序、用户组和代理程序利用，从而降低安装与维护大型安全产品的成本。

(8)可升级。可升级体现在可支持众多受保护的服务器、支持大流量和支持分散型安全管理，以满足大型分散式企业的需求，与时俱进地保持最高水平的安全，及时采用经受考验的预防技术。

(9)低总体拥有成本。用户所投资的系统最好能降低监控和管理全面服务器安全的成本。减少为确保系统安全而花费在清毒、补丁和监控等方面的成本。

目前，市面上已有一些成熟 IPS 产品推出，如 NAI 公司推出的基于主机的 IPS 系统 Entercept 和基于网络的 IPS 系统 McAfee IntruShield；Top Layer 网络公司推出的网络入侵防御最新产品 Attack Mitigator IPS 套件；NetScreen 公司推出的 NetScreen-IDP 系列产品等。美国网络联盟的 McAfee IntruShield 网络入侵防护解决方案拥有可编程安全硬件，可以成倍地提升几乎每个功能的处理速度，如协议分析、统计分析、字符串匹配和可视化。IntruShield 在对已知攻击、未知攻击和 DoS 攻击进行防护时，可以迅速支持成千上万的特征，而不会丢失任何数据包。IntruShield 方案提供了综合的防护体系，可以跨越企业核心网络，企业边界网络，以及分支机构的网络。IntruShield 的体系结构集成了多项技术，包括：特征检测、异常检测和拒绝服务分析技术，能在几千兆的网络流量下进行准确和智能的检测和防护。

4 基于 Multi-Agent 的分布式入侵防御系统模型

本文提出的基于 Multi-Agent 的分布式入侵防御系统模型(简称 MAgentDIPS)如图 2 所示。在这个模型中，包括：SMTP-Agent 防护群、HTTP-Agent 防护群、FTP-Agent 防护群、DNS-Agent 防护群、IAS-Agent 审计跟踪群及事件数据库。各类防护群以 Agent 形式出现，而事件数据库是以数据仓库的形式出现。各个 Agent 分布自治，又相互协作，共同完成检测防护的任务。

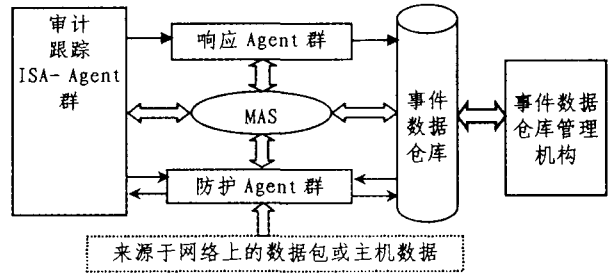

图 2 基于 Multi-Agent 入侵防御系统(MAgentDIPS)模型

在网络的全部通信中，98%都由 HTTP、FTP、SMTP 和 DNS 构成，因此所有这些协议都可能被黑客用来发动攻击。作为入侵防御的核心工作方式，Agent 防护群在应用层中阻挡大范围的攻击，保护网络的安全。在 MAgentDIPS 这个模型中，Agent 防护群的作用是：

SMTP-Agent *防护群* 监控接收和发送的邮件的内容，以保护网络的安全。其中的一些功能包括：防止邮件服务器超载及受到邮件炸弹袭击，并依据邮件的类型和名称来辨别邮件是否携带有蠕虫或者特洛伊木马之类的病毒。当黑客对邮件攻击的时候，SMTP Proxy Agent 能够自行阻击攻击行动，拦截所有隐瞒“回邮地址”的邮件，并提供能隐藏或改变内部的 IP 地址，以及隐藏更多的内部资料，避免一切受到攻击的可能性。

HTTP-Agent *防护群* 检测由用户接入万维网时进出网络的流量。它选择性地过滤内容，保护网络浏览用户和其他依赖互联网的应用免受基于 HTML 的攻击。它的主要功能包括：有效检测和控制内部用户接入 Internet 时的网络流量，同时有选择性地过滤内容，过滤 Java 和 ActiveX 控制，删除客户连接的信息，删除 cookies，避免一切基于 HTTP 浏览而受到攻击的可能。

FTP-Agent *防护群* 提供的保护包括，把进入连接或者出去连接都限制为“只读”，设定有效连接的时间，禁止利用 FTP 登录站点命令，从而避免黑客进行恶意的连串攻击，有效保护企业资源。

DNS-Agent *防护群* 通过确保协议的一致性和有选择性地过滤包头内容，全面保护企业的网络。

IAS-Agent 审计跟踪群　协助各类 Agent 防护群，保存异常现场数据，分析安全现状，协助改进安全策略和防护系统。

MAgentDIPS 中的 Agent 防护群都具备多种的配置功能和设置，且能通过人机界面轻松控制。Agent 群由多智能体系统(Multi-Agent System，MAS)统一管理，MAS 主要是针对行为的管理，包括如何协调各智能体的知识、目标、策略和计划，以采取联合行动或解决问题。当发现有可疑入侵行为出现时，Agent 群在防御免疫机制下，根据在线防护策略(如：SBD 策略[8]，即 Strategy-Based-on-Disorganization，SBD 策略在 MAgentDIPS 的作用是：能够有效地瓦解分布式入侵者有组织的协作，从而提高分布式入侵防御系统的整体对抗防御能力)，自动激活防护规则，形成 Agent 联邦和 Agent 联盟，执行防御措施。

在 MAgentDIPS，Agent 具有如下基本特征：

① 自主性　Agent 具有属于其自身的计算资源和局部于自身行为控制的机制，能在无外界直接操纵的情况下，根据其内部状态和感知到的(外部)环境信息，决定和控制自身的行为。

② 交互性　能与其他 Agent 进行多种形式的交互，能有效地与其他 Agent 协同工作，寻求协同刺激。

③ 反应性　能感知所处的环境，并对相关事件作出适时的反应。

④ 主动性　能遵循承诺采取主动行动，表现出面向目标的行为。

⑤ 移动性　Agent 可以在信息网络上移动。

Agent 的一般逻辑结构见图 3。Agent 设计的基本内容主要包括：Agent 数据类型和数据结构；Agent 信息处理的种类和机制；Agent 行为；Agent 方法；方法条件及完整性条件等。

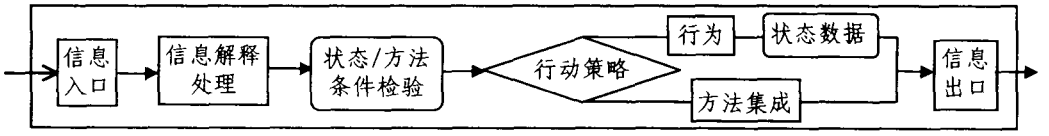

图 3　Agent 逻辑结构简图

5　入侵防御系统的组成及功能要求

入侵防御系统由事件分析单元、响应单元、审计单元和控制管理单元组成。各单元功能由其相应的 Agent 群完成。

5.1　事件分析单元(MAgentDIPS_ANL)

采用相关的分析检测技术，对经过的信息进行分析，提取信息中所包含的事件特征。事件分析单元组件功能要求：

(1)对通信协议进行分析、译码并提取特征信息。

(2)从网络通信数据包中提取字符串信息进行分析。至少应分析以下内容：事件主体；事件客体；协议特征(类型和标志位)；内容特征；事件描述。

(3)事件分析单元应提供特征库升级功能，允许用户及时更新特征库。

(4)事件分析单元应具备身份鉴别能力，除具有明确访问权限的用户外，事件分析单元应禁止其他用户对事件分析单元的访问。

5.2　响应单元(MAgentDIPS_RSP)

根据定义的策略对事件分析单元发送的消息进行响应。有以下三种响应手段：记录、报警和阻断。响应单元组件功能要求：

(1)当策略中被定义为报警的事件产生时，响应单元应将报警信息以消息或邮件等形式提交给管理员。报警信息至少应包括以下内容：事件标识；事件主体；事件客体；事件发生时间。

(2)响应单元应将事件信息以文件或数据库记录等形式记录下来。记录信息至少应包括以下内容：事件标识；事件主体；事件客体；事件发生时间。

(3)响应单元应将策略中定义为阻断的事件准确阻断。

5.3　审计单元(MAgentDIPS_FAU)

在违反安全策略的事件发生时，对事件发生的时间、主体和客体等信息进行记录和审计。审计单元组件功能要求：

(1)功能应为以下审计操作产生审计记录：审计功能的开启和关闭；符合基本级审计的所有下列可审计事件：修改安全属性的所有尝试、任何对鉴别机制的使用、所有对鉴别资料的请求访问、所有对审计数据读取不成功尝试、对角色中用户组的修改；其它在安全策略中定义的需要审计的事件。

审计功能生成的每一条审计记录至少应记录以下信息：事件时间，事件类型，主体身份和事件结果(成功或失败)。

(2)授权管理员应能对审计记录执行创建、储存和删除等操作。

5.4　管理控制单元(MAgentDIPS_MAN)

负责入侵防御系统定制策略、审阅日志、系统状态管理，并以可视图形化形式提交授权用户进行管理。

结论　入侵防御系统的研究还处于一个不完善的阶段，还有很多问题需要解决。如何有效地挖掘网络数据资源解决已知攻击检测及防御始终是 IPS 的基本功能，具备智能检测变异的、未知的入侵行为并采取有效的免疫防御措施是 IPS 的期望目标。入侵防御系统将向着智能化、标准化和特色化的方向发展，如何实现高速网络、集群系统的实时入侵防御已成为一个现实的问题。

参 考 文 献

1　[美]Pfleeger C P，等著. 李毅超，等译. 信息安全原理与应用(第三版)[M]. 北京：电子工业出版社，2004

2　刘文涛编著. Linux 网络入侵检测系统[M] 北京：电子工业出版社，2004

3　李涛著. 计算机免疫学[M]北京：电子工业出版社，2004

4　Jang H，Sangwook K. Intruder Tracing through dynamic extension of a security domain[J]. Journal of Network and Computer Applications，2002，25(2)

5　杨义先、钮心忻，等. 信息安全新技术[M]北京：北京邮电大学出版社，2002

6　戴英侠，等编著. 系统安全与入侵检测[M] 北京：清华大学出版社，2002

7　谢赞福，魏文国. 信息安全设施中入侵检测技术探讨[J]. 计算机工程与设计，2004，25(3)：390～393

8　彭 军，王文凤，张晓勇. SBD 策略在多智能体协作中的应用[J]. 计算机工程，2005，31(5)：186～187