第32卷 第18期 计 算 机 工 程 2006年9月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0172—03 文献标识码：A 中图分类号：TP393.08

一种基于自治 Agent 的分布式入侵检测系统

王丽辉，李 涛，杜 雨，郭 京，胡晓勤，卢正添
（四川大学计算机系，成都 610065）

摘 要：设计并实现了一个基于自治 Agent 的分布式入侵检测系统。系统采用层次化的管理控制结构，自上而下包括监控器、收发器和 Agent 3 种功能实体。使用基于 publish/subscribe 的通信模式减少了 IDS 系统的通信开销，提高了通信效率。
关键词：分布式入侵检测；自治 Agent；协同工作

A Distributed Intrusion Detection System Based on Autonomous Agent

WANG Lihui, LI Tao, DU Yu, GUO Jing, HU Xiaoqin, LU Zhengtian
(Department of Computer, Sichuan University, Chengdu 610065)

【Abstract】 A distributed intrusion detection system based on autonomous agent is presented. The architecture of the system is layer-based, with monitor, transceiver, and agent as the three functional entities. The system employs publish/subscribe communication paradigm to reduce the overhead and improve the efficiency of the communication.
【Key words】 Distributed intrusion detection; Autonomous agent; Cooperation

随着网络使用的增长，入侵技术也在不断发展和演化，这表现在攻击手段的多样化和复杂化，入侵规模的扩大以及攻击的分布化[3]。现有的IDS系统已越来越不能满足实际应用的需要，这表现在以下几个方面：(1)局限于单个主机或网络架构，IDS系统之间缺乏协作；(2)单一的检测手段和检测数据来源；(3)对大规模及分布式攻击缺乏检测能力；(4)可扩展性和灵活性差。由此，分布式入侵检测技术应运而生。传统的分布式IDS大多采用sensor/manager框架[3]，sensor的监控和数据分析都集中在manager上，不仅加大了manager的处理负担，还会因为manager的失效造成整个系统的瘫痪[4]。

目前，Emerald等典型的分布式IDS系统[5]，使用层次式的体系结构，中心控制系统位于层次树的根节点，sensor位于叶结点，检测信息从叶结点逐一上传到根结点，这会导致大量的数据传输，增加网络负荷，同时也存在单点故障问题。Purdue大学提出的基于自治Agent的入侵检测框架AAFID[1]为分布式入侵检测提供了一个高效的系统架构，但它并没有具体考虑系统中的各个实体结构和实体间通信、协作的实现方式。

鉴于以上情况，本文对AFFID系统进行了改进和完善，实现了一个基于自治Agent的分布式入侵检测系统[1]。系统采用层次式的管理控制结构，由监控器控制一个自治域中的所有收发器，收发器控制一台主机上的所有Agent。由于控制权分散到自治域和主机上，防止了单点故障。Agent可以根据不同的需求进行实现和扩展，增加了系统的灵活性。本文采用基于publish/subscribe的通信模式，减少了实体间的通信开销，提高了通信效率。

1 系统结构

整个系统主要由入侵检测 Agent、收发器(transceivers)、监控器(monitors)和用户管理界面 4 部分组成。图 1 示出了系统的结构。从 monitor 到 Agent 形成一种自上而下的层次式控制机制。上层实体可以对下层实体进行控制，同层实体之间可以互发事务消息。

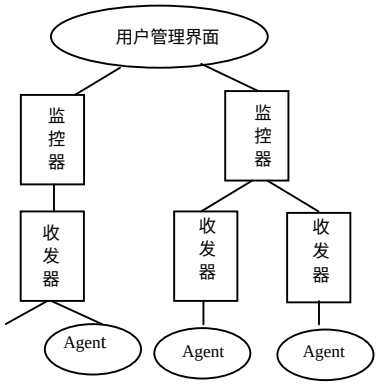

图 1 系统结构

Agent 是系统的数据采集和事件分析单元，它采集主机或网络数据进行分析，并将结果报告所在主机的 transceiver，由其进行统一的处理。

transceiver 是主机之间通信和联系的接口。每个受监控的主机上有一个 transceiver，它控制该主机上所有 Agent，处理 Agent 的报警数据，并与 monitor 交互。

基金项目：国家自然科学基金资助项目(60373110)；教育部新世纪优秀人才基金资助项目；教育部博士点基金资助项目(20030610003)；四川大学创新基金资助项目
作者简介：王丽辉(1981—)，女，硕士生，主研方向：网络安全，人工智能；李 涛，教授、博导；杜 雨、郭 京，硕士生；胡晓勤、卢正添，博士生
收稿日期：2005-10-10 **E-mail：**gailya@sohu.com

monitor 是系统中最高层控制处理单元，monitor 也可以以层次式的方式进行扩展。它控制多个 transceiver，接收报警数据并进行分析，从而发现单个 transceiver 不能发现的入侵行为；它还可以接收来自其他 monitor 或用户的控制信息。

2 系统设计与实现

2. 1 通信机制

系统中的通信消息主要包括控制信息和数据信息。控制信息包括系统各个实体之间的协作消息；数据信息主要包括特征库、策略库数据和报警数据。系统所采用的通信机制需要达到以下要求：

(1)不能增加过多的网络流量；

(2)满足主机内和主机间通信两种方式；

(3)保证通信安全性。

2.1.1 通信模式

本系统采用基于 publish/subscribe 模式的通信模型来完成多个实体的通信和协作。在这种模式中，publisher 相当于消息的发送方，而 subscriber 相当于接收方。所不同的是模型提供了一个事件注册服务(Event Service, ES)。subscriber 将感兴趣的事件向 ES 申请注册，ES 用一个注册信息表专门维护这些注册信息。当 publisher 发送信息时，它不是直接发给 subscriber，而是将信息发布给 ES，ES 在注册信息表里查找对该信息感兴趣的 subscriber，然后将消息发送给它们。图 2 示出了通信模型的逻辑结构。

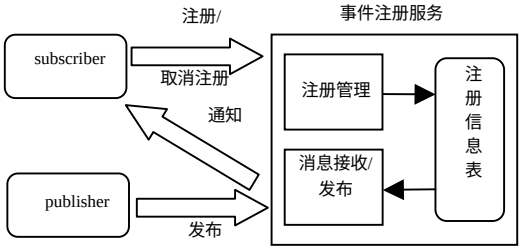

图 2 通信模型逻辑结构

比起传统的分布式环境下的通信模式，如应答式、RPC 等，基于 publish/subscribe 的通信模式具有很好的时间、空间的松耦合性：在时间上，它不需要通信双方同时参与消息传递过程，publisher 发布消息时 subscriber 可以不在场，反之亦然。这样就消除了同步不同实体相互通信的负担。空间上，消息发送方和接收方不必知道对方的信息和状态，减少了信息维护的难度，并消除了每个实体都要保存其他相关实体的信息的开销。这为实体间的相互协作带来很大的灵活性。

事件注册服务可以运行于 monitor 上，称为 MES(Monitor Event Service)，为不同的 transceiver 提供服务，ES 还可以运行于 transceiver 上，称为 TES (Transceiver Event Service)，为同一主机上的 Agent 提供服务。

2.1.2 消息发布

系统中的通信分为主机间和主机内两种方式。主机间的通信包括transceiver之间、monitor之间和transceiver与monitor之间的通信。MES采用多播的方式发布消息，即对于所有注册了同一事件的subscriber，使用多播方式将该事件通知给每个subscriber。这需要MES运行于多播模式下。同时，这些subscriber需要位于同一多播组中。这样，对同一事件的发布不需要建立多个网络连接，而且不需要多次传送同一消息的拷贝，节省了网络资源。多播的可靠性传输协议和加密认证机制可以保证数据的完整性和安全性[7]。

主机内的通信包括 Agent 之间的通信和 transceiver 与 Agent 之间的通信。TES 采用逐一通知的方式发布事件消息。

2.2 监控器(monitor)的实现

monitor 控制和协调不同主机上的 transceiver。一个系统中可以有多个 monitor，分别控制不同的自治域。monitor 模块间的相互关系如图 3 所示。

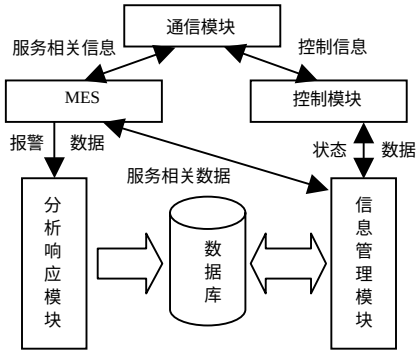

图 3 监控器模块结构

(1)事件服务模块(MES)。MES 是主机之间的通信和协作的基础。由于 monitor 监控不同主机的 transceiver，同时又要与其他 monitor 协调，因此，事件的注册和发布需要遵循一定的协议来满足通用性要求。MES 要处理注册/注销、发布、通知、反馈 5 种消息。

1)注册/注销。subscriber 需要提供自己的 IP 和注册/注销的事件，MES 收到请求后，修改相应的注册服务信息表。

2)发布。publisher 需要注明发布的事件 ID，事件相关数据。可以发布的事件有：特征库更新，策略更新，响应方式更新，报警。

3)通知和反馈。publisher、subscriber 和 monitor 处于同一多播组，publisher 在发布事件时，多播组中所有的主机都可以接收到事件，即所有活动的 subscriber 都可以接收到这一事件。接收到事件通知的 subscriber 向 monitor 发送反馈消息，monitor 由此修改 subscriber 的状态，将其对应的事件修改为已更新，并记录更新时间。对发布过程中不活动的 subscriber，由 monitor 在其变为活动时进行消息通知。

(2)控制模块。对用户界面发送的控制消息进行响应并完成相应操作，监控 transceiver 状态并向其发送控制消息。用户发送的消息有添加/删除一个 transceiver 或 Agent，启动、停止 agent，为 transceiver 或 monitor 注册/注销事件，更新某个多播组的特征库、策略库或响应方式，传递密钥等。monitor 向 transceiver 发送的控制消息与用户发送的消息类似。

根据以上的分析，通信协议和数据报设计如表 1、表 2 所示。

表 1 通信协议定义

动作	参数	数据	描述
subscribe	事件 ID	IP 地址	注册
unsubscribe			注销
publish/notify	supdate	特征数据	更新特征库
	sadd		添加特征
	sremove		删除特征
	pupdate	策略数据	更新策略库
	alert	报警数据	报警
	respose	响应方式	报警响应
feedback	事件 ID	IP 地址	通知反馈
control	动作	实体标识	发送控制信息

表 2 数据包格式定义

名称	长度(byte)	描述
Action	16	动作 ID
Param	16	参数内容
Length	16	数据包长度
Data	变长	数据内容

(3)信息管理模块。管理由 monitor 控制的 transceiver 的信息，注册服务信息表和事件通知状态表。transceiver 的信息可以采用以下几种方式获得：

1)transceiver 定时报告它的状态信息；

2)transceiver 状态改变时，报告 monitor；

3)由 monitor 直接向 transceiver 查询状态。

(4)分析响应模块。将各个 transceiver 的报警进行综合分析，可以采用的分析方法有概率统计、数据挖掘、数据融合、人工免疫等。从而发现在一台主机上不能检测到的网络攻击；它还可以按照指定的响应策略对攻击作出响应。

(5)通信模块。完成 monitor 与系统其他实体之间的通信。在收到消息后，它先对其进行解析，将解析的协议字段传递给对应功能模块，由它们进行处理。在发送消息时，它先对消息进行格式化封装，然后再进行发送。

2.3 收发器(transceiver)的实现

收发器的实现和 monitor 有所类似，其模块功能如下：

事件服务模块(TES)完成主机内 Agent 间的消息传递和 transceiver 对其他主机的消息发布，与 MES 不同的是，它采用逐个通知的方式发送事件消息。

控制模块控制 Agent 的启停，监控 Agent 的运行状态，删除或添加一个新的 Agent，并能更新 Agent 的特征库，策略库和响应方式。该模块还负责定时将 Agent 和 transceiver 的状态信息经由通信模块通知 monitor。

信息管理模块和通信模块的实现与 monitor 里的一致，不过这里信息管理模块管理的是 Agent 的信息，并且它还要管理它向 monitor 注册的所有事件的信息和 Agent 向它注册的事件信息表。

由于 Agent 的检测分析方法的不同，得到的报警数据格式也不尽相同，因此需要将这些异构数据进行一致化，产生格式统一的报警信息。分析响应模块先将 Agent 的报警数据一致化，然后按照响应策略对报警进行响应，如有必要，它还要向上层 monitor 报告危险级别高的报警。

2.4 Agent 的实现

Agent 是独立运行于主机上的实体，自治系统对 Agent 的功能没有限制，Agent 可以是监控某个特殊事件的简单程序，也可以是复杂的软件系统。

根据数据采集方式的不同，Agent 主要分为主机 Agent 和网络 Agent。主机 Agent 对所监控的主机进行数据采集和分析，包括系统日志、用户行为、资源使用、主机网络通信等。网络 Agent 负责采集网络中的原始数据包，对这些包进行分片和流重组，并从中发现可能的入侵行为。

入侵检测的方式可以采用误用检测或异常检测两种[2]。基于误用检测的检测手段有专家系统、模型推理、状态转换分析等，而基于异常检测的主要手段有概率统计，神经网络和人工免疫。Agent的入侵检测特征库需要及时更新，特征库的更新有以下几种情况：

(1)发现新的特征库；

(2)用户加入或修改特征信息；

(3)Agent 通过自学习或相互协作等手段产生新的特征信息。

不同的 Agent 不直接通信，而是通过 MES 和 TES 相互协作。如某个 Agent 接收到某个入侵的新的特征信息，它将该入侵的标识、下载地址、更新事件等发布给 TES，TES 根据注册事件表，找到更新这类特征的组播地址，将该事件发布出去，所有关心这种入侵特征的 Agent 都会收到这个消息。这种方式避免了在层次式的控制结构中，不同主机间 Agent 的协作需要通过逐层消息传递才能达到的弊端。

2.5 用户管理界面的实现

用户管理界面提供的主要功能有：

(1)监控系统各实体的信息和状态；

(2)提供管理员管理配置接口；

(3)显示报警信息和图形化的分析报告。

3 结束语

本文设计并实现了一个基于自治 Agent 的分布式入侵检测系统。和传统的 IDS 系统相比，本系统具有以下优点：

(1)良好的互操作性和可扩展性。不同的检测 Agent 通过一个层次式的控制结构相互协作，系统对 Agent 的功能、数目没有限制，可以随时修改或添加新的 Agent，以满足不同场景的需要。

(2)支持多种检测手段。避免了检测手段单一造成的误报和漏报。

(3)控制和分析操作分散在多个自治域和主机之上，避免了单点故障。

(4)基于 publish/subscribe 的通信机制，使实体间的通信更为灵活，组播方式的消息发布减少了系统的通信开销，加密和认证机制保证了通信的安全性。

参考文献

1 Balasubramaniyan J S, Omar J. An Architecture for Intrusion Detection Using Autonomous Agents[Z]. http://www.cerias.purdue.edu/homes/zamboni/pubs/tr9805.pdf, 2005-07.

2 李 涛. 网络安全概论[M]. 北京：电子工业出版社，2004: 346-382.

3 Snapp S R, Brentano J, Dias G V, et al. DIDS(Distributed Intrusion Detection System)——Motivation, Architecture, and an Early Prototype[Z]. http://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf, 2005.

4 Li Chunsheng, Song Qingfeng, Zhang Chengqi. MA-IDS Architecture for Distributed Intrusion Detection Using Mobile Agents[C]. Proceedings of the 2nd International Conference on Information Technology for Application, 2004.

5 Porras P A, Neumann P G. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbance[C]. Proc. of National Information Systems Security Conference, Baltimore, 1997.

6 刘 璟, 周明天. 大型动态多播群组的密钥管理和访问控制[J]. 软件学报, 2002, 13(2).