基于资源的分布式入侵检测系统模型研究*
A Model of Resource-based Distributed Intrusion Detection System

邹 莹,李陶深
Zhou Ying,Li Taoshen
(广西大学计算机与电子信息学院,广西南宁 530004)
(Coll. of Comp. & Info. Engi. ,Guangxi Univ. ,Nanning,Guangxi,530004,China)

摘要:提出一个基于资源的分布式入侵检测系统模型。该模型由智能的资源代理组成,每个智能代理都是独立的实体,拥有解决问题的不完全的信息或能力。该模型通过协同工作实时检测网络入侵行为,跟踪网络入侵者,有效地维护网络安全。

关键词:网络安全 入侵检测 分布式 代理 资源
中图法分类号:TP393.08

Abstract: A model for resource-based distributed intrusion detection system is presented. The system model consists of intelligent resource agent. Each agent is an independently running entity, which can real-timely detect the network intrusion and trace network intruder through operating cooperatively, and maintain network safety effectively.

Key words: network security, intrusion detection, distributed, agent, resource

目前,对入侵检测系统IDS(Intrusion Detection System,简称IDS)的研究逐渐成为网络安全的研究热点之一。按照获取原始数据的方法,入侵检测系统可以分为基于网络的入侵检测系统和基于主机的入侵检测系统[1,2]。基于网络和基于主机的入侵检测系统各有自己的优势,它们都能发现对方无法检测到的一些入侵行为。例如,从某个重要服务器的键盘发出的攻击并不经过网络,因此就无法通过基于网络的入侵检测系统来检测,只能通过使用基于主机的入侵检测系统来检测;基于网络的入侵检侧系统可以研究负载的内容,查找特定攻击中使用的命令或语法[3],这类攻击可以被实时检查包序列的入侵检测系统迅速识别,而基于主机的系统无法看到负载,因此也无法识别嵌入式的负载攻击。基于主机的入侵检测系统使用系统日志作为检测依据[3],因此在确定攻击是否已经取得成功时与基于网络的检测系统相比具有更大的准确性。

本文融合基于网络的入侵检测系统和基于主机的入侵检测系统的优点,提出了一个基于资源的分布式入侵检测结构模型。

2004-05-12 收稿。
*广西留学回国人员科学基金(桂科回0342001)和广西科技攻关项目基金(桂科攻033008-9)联合资助项目。

1 基于资源的分布式入侵检测模型

入侵者必然会访问系统的一些关键资源[4]。这里所说的资源范围很广,既包括内部网中的服务器、路由器以及防火墙和用户工作站,同时还包括文件系统、注册表、用户数据库、引导区、文件分配表、磁盘扇区、系统日志以及系统进程、网络端口和内存空间等,以及各种应用程序和系统服务。例如数据库服务可以将自己的会话(session)定义为关键资源。

入侵的目的就是要实现对系统的非授权使用和进行破坏,那么,入侵的过程或最终结果一定会涉及到一些入侵者无权访问的资源。例如,企图通过密码尝试攻击系统的入侵者必然要访问系统的用户数据库,而企图通过同时建立过多网络连接从而导致系统无法正常运转的入侵必然要占用系统的端口资源。尽管存在这样一些入侵手段,它们几乎只需要发送一个数据包就可以造成系统的瘫痪,但这种情况是非常少的,而且其危害性也很小,只能使系统暂时运行不正常。绝大多数的入侵都可以视为一个过程,入侵者逐步获得系统的信任,进而窃取他希望得到的东西或达到期望的目的[5]。

基于资源的分布式入侵检测系统结构模型(如

图 1 所示)的设计思想是:对于整个网络系统中的关键资源,按照它们各自的特点为它们设计出专用的入侵检测实体。其中,对于诸如防火墙、网关等网络连接资源,采用基于网络的入侵检测的思想,设计出基于网络的入侵检测实体;对于诸如客户工作机、数据库等系统资源,采用基于主机的入侵检测的思想,设计出基于主机的入侵检测实体。这样,综合利用网络入侵检测和主机入侵检测的优点,提高系统的准确性。

在图 1 所示的模型中,网络资源检测单元(Network Resource Detection Unit,简称 NRDU)和系统资源检测单元(System Resource Detection Unit,简称 SRDU)是关键部分。NRDU 单元检测通过网络防火墙的数据包,从而发现网络中存在的网络入侵行为。然后由关键主机上的 SRDU 单元来发现非授权的访问行为,并定义行为主体。最后,通过 NRDU 和 SRDU 的通信来跟踪入侵者的攻击过程。

这里假定外部网络(Internet)和内部网络之间仅有 2 条链路。NRDU 为网络入侵检测代理,对于更多链路的情况,由于各个 NRDU 之间相对独立,所以只需在其他链路上添加 NRDU 并配置。

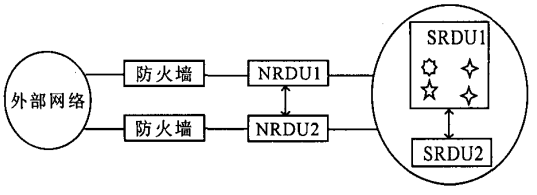

图 1 系统框架高层视图

☼:通信代理 TA;☆:状态检测代理 SA;✧:资源检测代理 SA。

2 NRDU 单元和 SRDU 单元的设计

2.1 网络检测单元 NRDU

NRDU 是网络入侵检测的核心功能部件,具备网络入侵检测所需要的一切功能和机制。各个 NRDU 是相对独立的。每个 NRDU 都可以独立于其他 NRDU 作为一个自治的 IDS 系统存在。当若干个 NRDU 组成一个网络入侵检测系统共同执行网络入侵检测功能时,它们相互通信,分工协作,协同完成入侵检测任务。这些操作对用户来说都是完全透明的,用户只需做简单而少量的配置工作。

图 2 给出 NRDU 在整个 IDS 系统中的逻辑视图。NRDU 分为三层,即分析决断层、交换层和报文过滤层。层次化的设计便于系统的实现、维护和拓展,而且使 NRDU 和数据报文在系统中的处理过程一致,取得了较好的处理效率。由于 NRDU 位于内部网络的一侧,并通过连接内部网络的接口交换信息,其通信速度和带宽以内部网络的指标衡量,因此完全可以保证 IDU 之间的交换效率和 IDS 整个系统的入侵检测效率。在实际情况中,内部网络和 Internet 之间的链路一般不会太多,以保证 NRDU 之间的通信量不会太大,从而不会对内部网络的通信造成过量的负载,影响内部网络的正常通信。

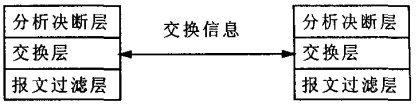

图 2 NRDU 的系统逻辑视图

图 3 给出单个 NRDU 的逻辑结构图。它是由交换引擎、报文处理器、分析器、判定器、响应器组成。每个 NRDU 监控经由本链路出入网络的通信数据流,掌握所监控各个会话及整个网络的状况,通过分析器及时发现并记录可疑事件。判定器根据记录的可疑事件,进行综合分析判断是否有入侵行为发生。响应器则根据预定的应对措施对入侵行为做出反应,阻止入侵行为的进一步实施。同时,每个 NRDU 利用交换引擎与其他 NRDU 交换信息,对整个网络中的会话进行分工监控,同时维护各个 NRDU 监控会话信息的完整性,以提高判断的正确性。

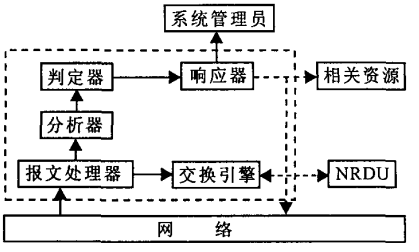

图 3 单个 NRDU 的逻辑结构

2.2 系统资源检测单元 SRDU

系统资源检测单元 SRDU 位于关键资源所在的主机,它是由通信代理(Transmission Agent,简称 TA),自身验证代理(State Agent,简称 SA)和资源检测代理(Resource Agent,简称 RA)等子代理组成。

2.2.1 通信代理 TA

TA 专门用于通信服务,其任务就是数据的接收和转发,不具有检测能力和控制能力。

TA 在每台主机上都是唯一的,是主机内和协作主机间 RA 通信的桥梁。当 RA 要传送数据时,它指定目标 RA,然后将数据包转送给目标主机上的 TA,目标主机上的 TA 再将数据转送给目的 RA。

2.2.2 自身验证代理SAA

SA是为保证TA和RA的安全而设计的，它是Agent进行自身保护和验证的专门Agent。SA定时检查协作主机的TA和本机内RA的状态，并负责向系统管理员报告。

由于SA在每台目标主机上都是唯一的，它就成为整个安全系统的安全重点。一旦SA被破坏，整个目标主机中的RA之间和主机之间就无法进行协作。因此，检查和保证RA的正常运行状态是极其重要的。

2.2.3 资源检测代理RA

作为基于资源的基本检测代理，每个RA独立承担一定的检测任务，检测主机系统相关资源的安全，通常表现为主机系统安全的一个方面。在模型中，各个RA有独立的数据源、运行模式和响应方式，各个RA之间可以通过TA进行相互协作，对系统和网络用户的异常或可疑行为进行检测。不同的RA依据检测环境的不同，采用不同的检测方法和技术，这样就极大的增强检测的灵活性。

3 系统特点

(1)分布性。模型采用无控制中心的并行Agent检测模式，各个RA之间的协作是通过它们之间的通信来完成的。每个检测部件都是独立的检测单元，尽量降低各检测部件间的相关性，不仅实现了数据收集的分布化，而且将入侵检测和实时响应分布化，真正实现了分布式检测的思想，增强系统的抗攻击性。

(2)入侵检测机制。模型融合基于网络和基于主机2种检测机制的优点，使系统既有很强的检测能力，又有很高地检测效率。

(3)可扩充性。模型采用Agent技术，具有很好的可扩充性，易于加入新的网络资源和RA。另外，模型中的各个组件采用标准化设计，使得系统各个部分的升级和新的网络资源的加入变得简单。

(4)安全性。由于模型采用SA机制来进行状态检查和验证策略，保证SRDU的自身安全和通信安全。

(5)良好的系统降级性。当系统某一代理出现问题，不能完成自己的检测任务时，网络的监测工作会受到有限的影响，但整个系统的检测功能不会有明显的下降。

4 结束语

本文所提出的基于资源的分布式入侵检测模型是一个开放的系统模型，它综合基于网络的入侵检测系统和基于主机的入侵检测系统的优点，能够有效地检测入侵，并能够提供系统学习入侵者的攻击过程，为采取进一步的安全措施提供决策支持。该模型于特定的系统应用环境无关，提供了一个通用的入侵检测系统模型框架。

参考文献：

1 Smaha, Haystack S E. An intrusion detection system. Proceedings of the 4th Aerospace computer security applications conference. Washington D C: IEEE Computer Society press, 1988. 37～44.

2 Mukerjee B, Heberlein L T, Levitt K N. Network intrusion detection. IEEE Network, 1994, 8(3): 26～41.

3 唐正军，等编著. 网络入侵检测系统的设计与实现. 北京：电子工业出版社，2002.

4 夏春和，张 欣. 网络入侵检测系统RIDS的研究. 系统仿真学报，2000，(4)：375～379.

5 韩东海，王 超，李 群. 入侵检测系统及实例剖析. 北京：清华大学出版社，2002.

(责任编辑：黎贞崇)

海百合教育资源管理平台通过技术鉴定

南宁市平方软件新技术有限责任公司开发的“海百合教育资源管理平台”，2004年7月28日在南宁市通过了技术鉴定。

该平台由前台服务和后台管理两部分组成，其中前台服务包括网站公告服务、资源分类浏览、资源评论、用户服务等模块；后台管理包括教育资源元数据、用户、教育资源、网点维护、系统配置等管理模块。

该平台采用先进的文件传输技术和数据库设计方法，提高了文件传输及资源查询的速度；它的元数据能导出成XML标准文本，方便不同数据库之间的迁移；它有较强的站点维护功能，便于管理员根据需要进行个性化定制。“海百合教育资源管理平台”达到了国内同类技术的先进水平。

(广西科学院 罗海鹏)