一种基于智能代理的分布式入侵检测系统设计*

A Framework Design on the Agent-Based on Distributed Intrusion Detection System

李陶深，葛志辉

Li Taoshen，Ge Zhihui

（广西大学计算机与电子信息学院，广西南宁 530004）

(School of Comp.，Elec. and Info.，Guangxi Univ.，Nanning，Guangxi，530004，China)

摘要：在CIDF(Common Intrusion Detection Framework)模型的基础上，提出一个基于智能代理的分布式入侵检测系统结构框架，并介绍该系统结构框架中的组成模块。该系统框架具有实现机制与策略分离、控制安全可靠、扩展性好等特点，能适应于分布式入侵检测的需要。

关键词：入侵检测 分布式系统 代理 CIDF 模型

中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1002-7378(2005)04-0272-03

Abstract：Based on CIDF(Common Intrusion Detection Framework)model，a framework of an agent-based on distributed intrusion detection system is presented. Its main components are also introduced. This system framework is possessed of some good characteristics，such as segregation of control and strategy，control safety and reliability，good expansibility. It can meet the need of distributed intrusion detection.

Key words：intrusion detection，distributed system，agent，CIDF model

入侵检测(IDS)是当前网络安全研究热点之一。传统的入侵检测系统，由于局限于单一架构，无论是基于网络数据源，还是基于主机数据源，无论采用误用检测技术，或是异常检测技术，在面临异构系统及大规模网络的时候都显得有些力不从心。面对这种挑战，需要各个入侵检测系统之间能够实现高效的信息共享和协作检测，在大范围网络中部署有效的入侵检测系统，以克服传统IDS的不足。

分布式入侵检测系统是由遍布整个网络的多个检测组件组成[1]。它们之间可以交换信息并向中心监控器报告以便可以全局监控。分布式入侵检测系统由于采用非集中的系统结构和处理方式，相对于传统的IDS具有明显的优势[2,3]。然而，在实现分布检测组件的信息共享和协作上，却存在着一些技术难点。另外，现在的分布式入侵检测系统大多是从原来的基于网络或基于主机的入侵检测系统不断改进而来的，在体系结构方面还不能满足分布、开放的要求。本文主要研究分布式入侵检测系统的体系结构问题，并在CIDF(Common Intrusion Detection Framework)模型的基础上，提出一个基于智能代理的分布式入侵检测系统结构框架。

1 CIDF模型[1,4]

CIDF模型提供一个入侵检测系统的基础框架，它将一个入侵检测系统分为以下组件：事件产生器、事件分析器、响应单元、事件数据库。CIDF将IDS需要分析的数据统称为事件，它可以是基于网络的IDS从网络中提取的数据包，也可以是基于主机的IDS从系统日志等其它途径得到的数据信息。CIDF各组件之间以通用入侵检测对象的形式交换数据，其数据格式由通用入侵规范语言来定义。

CIDF中的事件产生器负责从整个计算环境中获取事件，但它并不处理这些事件，而是将事件转化为入侵检测对象标准格式提交给其它组件使用。CIDF中的事件分析器接收并分析入侵检测对象，然后以一个新的入侵检测对象形式返回分析结果。CIDF中的事件数据库负责入侵检测对象的存贮，

收稿日期：2005-06-27

作者简介：李陶深(1957-)，男，广西邕宁人，教授，主要从事网络计算与信息安全，分布式数据库，CAD等领域的研究。

*广西留学回国人员科学基金(桂科回0342001)和广西科技攻关(桂科攻0385001)项目联合资助。

它可以是复杂的数据库,也可以是简单的文本文件。CIDF 中的响应单元根据入侵检测对象做出反应,它可以是终止进程、切断连接、改变文件属性,也可以是简单的报警。

目前CIDF 还没有成为正式的标准,也没有一个商业IDS 产品完全遵循该规范,但各种IDS 的结构模型具有很大的相似性,各厂商都在按照CIDF 进行信息交换的标准化工作,有些产品已经可以部分地支持CIDF。可以预测,随着分布式IDS 的发展,各种IDS 互操作和协同工作的迫切需要,各种IDS 必须遵循统一的框架结构,CIDF 将成为事实上的IDS 的工业标准[5]。由于CIDF 在系统扩展性和规范性上的优势,已经被许多研究人员用作构建分布式入侵检测系统的基本框架。

2 基于智能代理的分布式入侵检测系统的设计

基于智能代理的分布式入侵检测系统由中心控制台和多个代理组成,其功能模块如图1 所示。所谓代理,实际上可看作是在执行某项特定监视任务的软件实体。代理既可以基于网络,也可以基于主机,它可以综合运用误用检测和异常检测技术。代理的这种独立性和灵活性为系统提供了良好的扩展性和发展潜力。

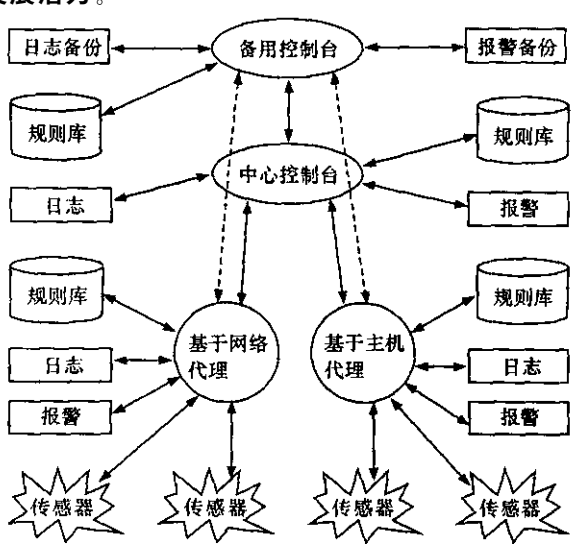

图1 系统结构

2.1 系统的主要功能模块

(1)传感器数据采集模块。传感器可以在本地主机上设置一个到多个。按照代理的不同,其数据源可以是系统产生的日志,也可以是某一网段的网络通信。传感器将采集到的数据发送给代理处理。

(2)代理数据处理模块。代理负责处理传感器采集到的数据,按照与规则库的比较结果产生报警,向中心控制台实时发送检测情况,并记录日志。代理还负责执行本地的安全策略,从中心控制台获得反馈信息,以便急时调整策略和监控焦点。

(3)中心控制台。中心控制台负责策略的形成和指挥。中心控制台对攻击者的意图和过程分析,对检测到的攻击报警,并预测攻击者的下一步可能活动,将信息发送到各个代理以便调整安全策略。

(4)备用控制台。备用控制台是中心控制台的一个备份,它实时地监测中心控制台的运行状态,并备份报警及日志,一旦中心控制台失去响应,备用控制台立刻接管各个代理。

2.2 系统结构的设计特点

(1)实现机制与策略分离。传感器采集到数据后并未直接处理,而是交由代理处理。因为系统要处理大量的通信数据,在不同的时刻系统可能需要对不同类型的通信采取监听及响应方法进行适当的调整,如果传感器在采集到数据后就直接处理的话,改动起来就很复杂。而代理的安全策略是高度可定制的,实现起来会容易得多。

(2)采用备用控制台。中心控制台是一个单点故障,如果使它瘫痪的话,整个系统也就失效了。因此我们提出采用一个备用控制台的方法,以保证系统自身的安全性和可靠性。其代价是需要额外的一台机器运行备用控制台。

(3)具有可扩展性。因为中心控制台只是在抽象层次上进行预计和指挥,其负载并不大,如果所监视的网络扩展,只要增加新的代理和传感器。

2.3 系统实现的关键技术

2.3.1 事件的产生

(1)主机信息。基于主机的传感器可以将系统产生的日志文件作为数据源,如 Linux 下的 utmp,wtmp 日志文件等,以及主机上的敏感文件和目录内容。这些信息可以通过直接访问相应的文件内容或者利用系统提供的系统调用接口来获得。

(2)网络信息。由于基于网络的代理需要分析整个网段的数据包分组,所以要求基于网络的传感器可以直接对数据链路层进行访问。目前大多数操作系统都提供了访问数据链路层的手段。Unix 上最常用的数据链路层访问方法是 BSD 的分组过滤器(BPF)、SVR4 的数据链路提供者接口(DLPI)、Linux 的SOCK-PACKET 接口以及一个独立与平台无关的数据包捕获函数库libpcap。基于可移植性的考虑,可以采用libpcap 库。

2.3.2 事件的分析

基于主机的代理可以采用异常检测的方法。系统可以为用户的正常行为建立一个正常的特征文件,这样系统可以统计那些不同于系统已经建立的特征文件的所有系统状态的数量,然后用此来识别入侵行为。如根据系统日志,统计某个用户的登陆失败次数,如果超出3次,则系统认为其是异常行为。衡量每个用户的CPU使用时间以及I/O使用量等,如果超出正常范围,则认定为攻击。

对基于网络的代理,可采用协议分析与模式匹配相结合的方法,把传感器截获的网络数据包根据不同的网络协议进行解码,存入相应的数据结构,然后再与规则库中定义好的规则进行匹配。

中心控制台在对攻击者的意图和过程分析方面采用文献[1]提出的基于攻击树的策略分析方法来实现。使用该方法描述的一个窃取信息的攻击例子如图2所示[5]。从图2可以看出,使用该方法可以很好的对攻击者的意图进行预测,以便提前做出防范措施,尽可能的降低由攻击带来的损失。

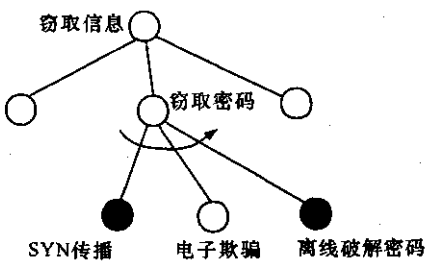

图2 窃取信息的攻击策略描述

●已检测到的事件;○需要进一步验证或者未完成的攻击事件。

2.3.3 代理与中心控制台间的通信

为了保证系统组件之间通信数据的真实性和完整性,系统采用安全套接层协议(SSL)作为通信双方的身份验证和保密传输。由于SSL协议建立在TCP协议之上,而且又独立与应用层协议,因此它可以保障通信不被攻击者窃听。

3 结束语

随着计算机技术和网络技术的不断发展,分布式计算环境的广泛采用,海量存储和高带宽传输技术的普及,传统的基于单机的集中式入侵检测系统已不能满足安全需求。而且由于黑客入侵形式具有多样性、隐蔽性和复杂性等特点,以及诱骗攻击和协同攻击等新手段的应用,传统的单纯的基于主机或基于网络的入侵检测系统已经不能胜任全局监控的需要,分布式入侵检测逐渐成为入侵检测乃至整个网络安全领域的研究重点。本文提出的基于智能代理的分布式入侵检测系统结构框架,具有实现机制与策略分离、控制安全可靠、扩展性好的特点,能适应于分布式入侵检测的需要。

参考文献:

[1] Huang Mingyuh, Robert J Jasper, Thomas M Wicks. A large scale distributed intrusion detection framework based on attack strategy analysis [J]. Computer Networks, 1999, 31(23/24): 2465-2475.

[2] 连一峰. 分布式入侵检测系统研究[D]. 合肥:中国科技大学, 2002.

[3] 连一峰, 戴英侠, 胡 艳, 等. 分布式入侵检测模型研究[J]. 计算机研究与发展, 2003, 40(8): 1195-1202.

[4] Vern Paxson Bro. A system for detecting network intruders in real-time[J]. Computer Networks, 1999, 31(23/24): 2435.

[5] 唐正军. 黑客入侵防护系统源代码分析[M]. 北京:机械工业出版社, 2002.

(责任编辑:邓大玉)