第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·安全技术· 文章编号：1000—3428(2007)06—0139—02 文献标识码：A 中图分类号：TP393.08

分布式自治型入侵检测系统研究

陈蜀宇，吴庆佺，周辉毅
（重庆大学计算机学院，重庆 400030）

摘 要：传统分布式入侵检测系统大都采用多层次型结构，存在层次控制复杂及通信瓶颈等问题。该文提出了一种分布式自治型入侵检测系统，采用 2 层结构框架减少了控制层次，通过结合了协议分析和模式匹配技术的自治性检测节点来实现分布式检测，用自定义通信协议及标准 SSL 协议来保障系统内部通信安全，通过 B/S 模式实现在任意节点浏览告警信息，方便了用户使用。

关键词：入侵检测系统；分布式；自治型

Research of Autonomous Model of Distributed Intrusion Detection System

CHEN Shuyu, WU Qingquan, ZHOU Huiyi
(College of Computer, Chongqing University, Chongqing 400030)

【Abstract】The traditional distributed intrusion detection systems mostly use multilayer architecture, which results in complicated management and communicational bottleneck. This article introduces an autonomous model of distributed intrusion detection system. It has only two layers so it can reduce the complicate of layer control. It makes up of autonomous detection node, which integrates the protocol analysis technology and the pattern matching technology to achieve distributed intrusion detection. It uses user-defined protocol and the standard SSL protocol to ensure security of the communications within the whole system. For the convenience of the custom, it can browse the alarm in any detection node by browse/server model.

【Key words】 Intrusion detection system; Distributed; Autonomous model

入侵检测[1]（Intrusion Detection，ID）通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。实现入侵检测功能的软件与硬件的结合就是入侵检测系统（Intrusion Detection System，IDS）。

分布式入侵检测系统[2](Distributed Intrusion Detection System，DIDS)关键技术是检测信息的协同处理与入侵攻击的全局信息的提取。在入侵检测体系结构基本框架上引入了分层次过滤、分布处理、分层管理等思想，有效地解决了网络带宽不足、主机性能瓶颈、单点失效、可扩展性差、重新配置或增加功能困难等问题，可实现对入侵行为的实时检测。

1 分布式自治型入侵检测系统

传统的分布式入侵检测结构是一种自顶向下树状的分级多层次结构，它把各个子系统安排到不同的节点上，各节点充分发挥自身性能、相互协调地完成任务，能够适应网络通信的需要，方便进行扩充与缩减。但是在这种分级多层架构中，所有的节点都是静态的，系统遵循自顶而下的控制流程，存在层次控制复杂、容易产生通信瓶颈等问题，且一旦某个节点失效，则该节点所控制部分将无法正常工作。入侵者还可以通过分析失效节点与其他节点之间的通信进一步破坏整个系统，从而使其不能对网络进行保护。

为了解决传统分布式入侵检测系统的上述问题，本文采用具有自治性的检测节点来组成仅有 2 层的分布式系统，每个自治性检测节点均能独立的完成检测，各个节点之间仅相互传递必要的信息，且采用安全认证形式传递。这样整个系统不再是一个多层次的结构，控制简单方便，不易产生通信瓶颈，且各节点相互平等，一旦某个节点失效，不会影响到其他节点。系统整体结构如图 1 所示。

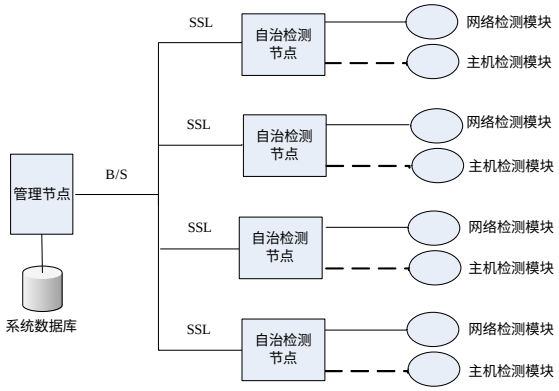

图 1 总体系统结构

2 自治检测节点

每个自治检测节点均能单独实现基于主机和基于网络的入侵检测功能，其模块组成如图 2 所示，符合通用入侵检测框架(Common Intrusion Detection Framework，CIDF)规范[3]。

数据采集模块完成对不同数据源数据的采集和数据信息格式化表示，并将处理后的数据（事件）送分析模块，完成事件产生器功能。分析模块分析送来的事件，依据给定的规则判断是否出现违规或异常，完成事件分析器功能。本地数

基金项目：教育部“ 新世纪优秀人才支持计划 ”基金资助项目(NCET-04-0843)；重庆市自然科学基金资助项目(2005BB2192)
作者简介：陈蜀宇(1963－)，男，教授、博导，主研方向：网络安全，网格计算，容错与诊断；吴庆佺、周辉毅，硕士生
收稿日期：2006-03-30 **E-mail：**wuqingquan@163.com

据库存储生成的数据，供以后查询和进一步分析，完成事件数据库功能。告警模块依据分析模块产生的结果采取相应的动作，完成响应发生器功能。

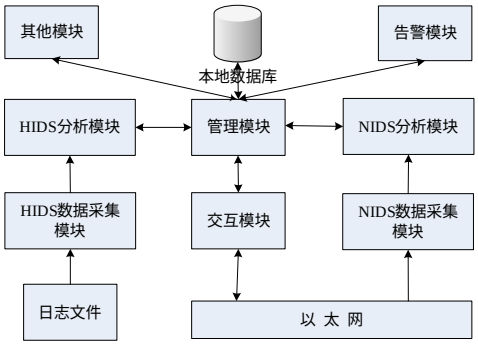

图 2 自治检测节点功能模块

2.1 数据采集模块

NIDS 数据采集模块用来捕获和解析网络上传输的数据包，并将其格式化表示为事件。在当前高速网络环境下，数据包的捕获关键是要保证高速度和低丢包率，这与硬件的处理能力及软件的效率有关。为了尽可能地保证高速度及低丢包率，本系统设计为让自治检测节点获取自身及其相邻部分节点的数据包，这样节点所处理数据量较小，不但可以保证不丢包，并且可以加快分析模块的处理速度，从而提高系统的攻击响应及时性。如果节点仅仅采集自身的数据包，当该节点遭受攻击而失效时便无法检测到攻击信息，而采用了获取相邻几个节点的数据包的冗余设计，这种攻击可以由其他节点检测出来。具体获取多少个相邻节点的数据包，可以根据节点硬件性能来决定。

HIDS 数据采集模块从操作系统日志中提取日志信息并格式化表示为事件。日志文件通常有应用程序日志、安全日志、系统日志、DNS 服务器日志、FTP 日志、WWW 日志等，不同操作系统的日志文件和记录格式不一致。该模块实现上因操作系统不同而不同，通过操作系统提供的 API 函数或自行编写日志数据读取函数来读取日志文件的数据并格式化表示为事件然后送分析模块。

2.2 分析模块

2.2.1 NIDS 分析模块

NIDS 分析模块采用误用检测中的模式匹配结合协议分析的分析方法，其主要工作是分析格式化表示后的网络数据包，即利用网络协议高度有效化的特点，快速地探测攻击，并在不丢包的情况下对包进行详细分析，将入侵行为的特征码归结为协议的不同字段的特征值，通过检测该特征值来决定入侵行为是否发生。分析提取数据包的特征值后，将其与特征库的特征码进行模式匹配，如果匹配成功，则表示攻击事件发生，产生告警信息。

协议分析方法充分利用了网络协议的层次结构，依次分解出各种协议的首部来匹配协议树，而且利用数据报文相应的数据部分来匹配协议入侵特征，最后用来与入侵规则匹配的报文比源报文的字节数成倍减少。协议分析方法与模式匹配方法原理一致，将二者结合起来检测入侵行为，能大大提高检测效率。

2.2.2 HIDS 分析模块

日志的事件类型一般包括：用户或进程的登录和退出，对系统相关的数据和设备的访问，改变用户账号和用户组，改变对系统数据和资源的访问权限，关闭或重启系统，注册可信的登录进程或者其他影响系统安全的活动，进程执行和跟踪，策略改变等。对需要关心的主机资源建立特征库并运用模式匹配方式实时分析日志事件检测出入侵信息。

2.3 管理模块

管理模块主要完成下面 3 个方面的功能：

(1)获取分析模块送来的报警信息，并将其发送到告警模块进行处理。

(2)获取交互模块从网络上读取的其他检测节点发送过来的特征码，然后搜索自身特征库，检查是否存在该特征码，如果不存在则添加到特征码链的首部，如果存在则直接交换到特征码链的首部。根据局部性原理（其他节点已经遭受的攻击，本机受到的相同攻击的可能性很大），这种方式能够提高匹配效率。

(3)获取文件完整性模块发送的数据并将其通过告警模块发送到数据库服务器进行保存。

2.4 告警模块

告警模块主要是对管理模块发送过来的数据进行处理。本模块将告警数据发送到远程数据库服务器保存，同时将告警信息特征码发送到通信模块，通信模块再将其发送给其他的节点，使各个节点间交互各自的检测情况，提高检测的效率和准确性。

2.5 通信模块

本系统采用分布式体系结构，各个自治检测节点的通信非常重要。系统采用如图 3 所示的应用层协议来实现各节点之间的通信并用 SSL 协议来保障传输数据通信安全。

图 3 通信协议数据格式

协议主要字段说明如下：

(1)报文类型：规则信息，设置为 0001；报警信息，设置为 0002；文件完整性检测时文件的 MD5 编码，设置为 0003。

(2)检测类型：NIDS 设置为 0001，HIDS 设置为 0002。

(3)发送方标识：数据报发送者的惟一标识，各节点统一编号。

(4)加密身份证书：发送方加密后的身份证书，由系统管理员生成。

(5)协议数据部分：数据部分包含 5 种数据：1)网络检测特征码；2)主机检测特征码；3)网络报警信息；4)主机报警信息；5)文件的 MD5 编码。特征码用于各个节点之间的交互，报警信息和文件的 MD5 编码直接发送到数据库服务器保存。特征码的发送采用广播方式，每个自治检测节点都可以接收到，但容易引起广播风暴。可通过设置阈值的办法来解决：每当检测到一个报警便把相应规则的计算器加 1，当达到阈值时便发送特征码，然后将计数器清零；其他节点收到特征码后，首先查看其身份证书是否合法，如果合法则交给管理模块处理，不合法则丢弃。这样既能够让其他节点了解当前节点的检测情况，又能调节自身的特征库提高匹配效率，同时还能有效地降低网络通信量。

为了在网络上更安全地通信，本系统还利用 Internet 上保密通信的工业标准——公开密钥技术的 SSL 协议对通信传

(下转第 194 页)