浅谈分布式入侵检测系统

成汶洲，张　亮
（福建宁德核电有限公司，福建 宁德 355200）

【摘　要】在当前互联网信息数据安全问题备受业内人士关注与重视的背景下，网络计算机技术发展非常迅猛。互联网已经全面触及人们工作、生活的方方面面，同时也导致信息安全面临巨大威胁。互联网平台下的数据及各种应用功能多以分布式方式部署于各个网络与地区，承受的入侵攻击呈现分散性、复杂性特点。为了应对这一问题，必须尝试构建分布式入侵检测系统，以达到保障系统安全的目的。文章在概述分布式入侵检测系统产生背景的基础上，重点探讨该系统的设计与实现方案，希望有助于入侵检测系统性能的优化与提升，并为网络信息安全提供可靠保障。

【关键词】分布式；入侵检测系统；技术
【中图分类号】TP393.08　【文献标识码】A　【文章编号】1674-0688(2018)07-0093-02

0 引言

众所周知，在计算机网络迅速发展的背景下，网络在各行业领域中的重要性不断凸显，网络安全问题开始受到业内人士的关注与重视。防火墙作为网络安全的第一道关卡，属于网络安全的被动防御模式。对于典型的局域网网络而言，防火墙设置于局域网边界，可以对内网与外网进行隔离，对流经网络的数据包进行访问控制，但对于内网而言，防火墙无法有效抵御来自内网用户的攻击行为，而且还有部分攻击行为可以绕过防火墙，对信息数据安全产生影响。为了弥补这一局限性，本文提出了在防火墙后部署入侵检测技术的操作方法，利用入侵检测的方式对流经网卡的数据包信息进行实时性检测，对所捕获的数据包进行处理，与入侵数据特征库信息进行对比分析，实现对各种入侵行为的合理检测，并根据检测结果及时报警响应，通过这种方式确保网络安全与可靠。

1 分布式入侵检测系统概述

所谓入侵检测是指在计算机系统或计算机网络辅助下，利用若干关键点对信息进行收集与分析，以评估网络或主机中是否存在对安全策略产生影响的行为，了解网络或主机是否存在被攻击的可能性。根据不同的分类方法，可以将入侵检测技术分为多种不同类型：根据数据来源进行分类，有主机入侵检测技术、混合型入侵检测技术及网络入侵检测技术；根据时效性进行分类，有脱机分析入侵检测技术、联机分析入侵检测技术；根据模块运行方式进行分类，有分布式入侵检测技术集中式入侵检测技术。

对于集中式或分布式入侵检测技术而言，集中式入侵检测系统集中在一个检测点上完成所有的数据分析工作，导致单一检测点的工作压力巨大。若检测点对处理速度或储存能力存在较高要求，或出现数据量较大的情况，就会导致集中检测点的处理压力巨大，甚至发生丢包，无法对入侵行为进行可靠检测。换言之，集中式入侵检测系统无法完全满足网络安全发展的要求。在这一背景下，提出了更具适应性的分布式入侵检测系统建设方案。面向网络数据安全所构建的分布式入侵检测系统是指：策略定义与管理由控制台统一实现，在分发协议原则支持基础之上，通过控制台实现 Agent 客户端对策略的接收，并根据所接收信息由客户端展开实施操作。通过这种方式能够很好地解决集中式入侵检测系统运行中存在的问题，因此逐步发展成为当前计算机网络系统入侵检测领域的研究热点。

2 分布式入侵检测系统设计与实现

整套分布式入侵检测系统采用 C/S 结构模式，通过配置服务器端的方式，实现对局域网范围内全部客户机的控制，入侵检测的覆盖范围包括 DoS、特洛伊木马等多种入侵与攻击行为，根据检测结果对入侵行为进行合理检测与控制，以确保网络信息安全可靠。一旦客户机检测到入侵行为，可以及时将该事件上报至服务器端，也可通过发送邮件的方式进行报警，以确保服务器端能够实现面向整个局域网网络的实时性监控，系统结构如图 1 所示。

2.1 服务器端设计方案

整个分布式入侵检测系统服务器端主要由全局策略设置模块、客户机通信模块、身份认证模块 3 个部分构成。全局策略设置模块是指自控制台实现对整个分布式入侵检测系统全局策略的设置功能；客户机通信模块是搭建与客户端之间的连接载体，并根据分布式入侵检测系统全局配置策略，将相应操作指令下达至客户机中；身份认证模块是指面向分布式入侵检测系统管理员用户提供身份认证功能，为不同用户分配相应权限，

【作者简介】成汶洲，男，四川眉山人，本科，福建宁德核电有限公司工程师，研究方向：安保技防系统；张亮，男，湖北天门人，本科，福建宁德核电有限公司工程师，研究方向：安保技防系统。

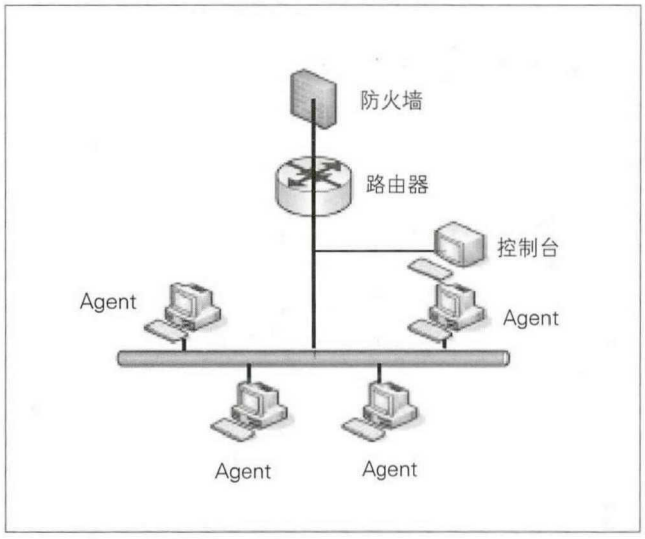

图 1　分布式入侵检测系统网络结构示意图

在数据库表中包含用户名、用户登录密码 2 个字段，管理员在登录分布式入侵检测系统服务器终端时与数据库表中信息建立匹配关系，当匹配关系成立后，可允许该用户对分布式入侵检测系统服务器端进行访问与相应操作。

2.2　客户端技术实现

首先，通过 Windows 系统进程与端口映射，结合木马端口库来检测特洛伊木马。参考计算机 TCP/IP 协议定义端口，在定义过程中明确规定以端口及 IP 地址作为套接字，与 TCP/IP 协议方式连接下连接端呈对应关系，可将其简称为“Socket”。换言之，在计算机系统客户端模块中，每个端口均与某个应用程序或服务保持对应关系，主机运行过程中的计算操作进程可以通过搭载［IP：端口］的方式实现，其主要目的是方便两台计算机能够搜寻对方进程并展开相应的通信。本文构建的分布式入侵检测系统，搭载 Windows 系统操作平台，在计算机操作进程与端口之间形成对应的匹配关系，并匹配系统正常进程状态下的数据库信息，以对比发现进程中存在的问题，当检测发现可疑进程后，需要立即终止该进程的运行，从而实现对入侵攻击行为的防范。

其次，当检测到入侵行为后需要立即面向分布式入侵检测系统客户端发送报警指令，以邮件方式发送至指定邮箱，同时需要将检测所得入侵行为数据信息写入分布式入侵检测系统远程服务器端数据库中。本文构建的分布式入侵检测系统，客户端若检测到扫描，需要对入侵事件进行及时记录，并将其记录于数据库中备份保管，入侵事件记录参数按照一定的时间间隔发送至指定邮箱地址并进行保存。

2.3　入侵检测流程

整套分布式入侵检测系统参考特洛伊木马通信中的主动连接技术模式，展开对网络入侵行为的监测与防范工作，在主机安装分布式入侵检测系统客户端后，一旦上线会直接按照服务器端要求进行配置，读取指定参数，并获取管理端 IP 地址列表，与分布式入侵检测系统服务器端进行连接，可以通过服务器端与客户端所建立的对应关系，在局域网网络系统中展开实时性监督控制。客户机方面，可以通过灵活配置的方式实现对主机运行状态的实时性监督控制，及时将所检出的入侵事件写入服务器端数据中，以作为计算机系统防范攻击行为的重要标准。

3　结语

现阶段计算机网络入侵行为与攻击开始呈现多样化、复杂化的发展特点，网络安全形势是非常严峻的。为了有效预防入侵行为对网络安全产生影响，本文简述了一种基于分布式入侵检测系统的网络入侵行为防御工作机制。在概述分布式入侵检测系统产生背景的基础上，重点探讨该系统的设计与实现方案，希望能优化与提升入侵检测系统性能，并为网络信息安全提供可靠保障。

参　考　文　献

[1] 王秀英. 分布式网络时序关联入侵攻击行为检测系统设计[J]. 现代电子技术，2018，41(3)：107-110.
[2] 庄夏. 基于局部参数模型共享的分布式入侵检测系统[J]. 计算机工程与设计，2017，38(11)：2935-2939.
[3] 刘萍萍，周求湛，徐昊，等. 混合型分布式入侵检测系统模型[J]. 吉林大学学报：工学版，2004(4)：666-670.
[4] 彭国星. 基于分布式数据入侵检测模型研究[J]. 中南林业科技大学学报，2010，30(3)：147-151.
[5] 吉根林，凌霄汉，程学云. 神经网络集成的分布式入侵检测方法[J]. 南京航空航天大学学报，2007(2)：231-235.

[责任编辑：钟声贤]