一种分布式协同入侵检测系统的设计与实现*

段海新，吴建平

(清华大学 信息网络工程研究中心，北京 100084)

E-mail: dhx@bjnet.edu.cn; jianping@cernet.edu.cn

http://www.nrc.tsinghua.edu.cn

摘要：提出了一种能够精确描述入侵检测技术的综合分类方法，针对多管理域环境设计了一个分布式协同入侵检测系统(distributed cooperative intrusion detection system，简称 DCIDS)，通过不同管理域 IDS(intrusion detection system)之间高效安全的通信，实现协同检测. 介绍了 DCIDS 的系统结构和 4 个组成部分：传感器、分析器、管理器以及用户界面，并讨论了系统实现中的安全通信、入侵检测点的选择等关键问题.

关键词：网络安全；分布式协同入侵检测；网络管理；认证；访问控制

中图法分类号：TP393 **文献标识码**：A

在 20 世纪 80 年代，Anderson 的报告[1]和 Denning 的论文[2]引发了入侵检测系统(intrusion detection system，简称 IDS)的研究与开发，近年来逐渐成为研究的热点. IDS 的发展大致经历了 4 个阶段[3]：Host Based，Multi-Host Based，Network Based 和 Distributed IDS. 每个阶段中典型的系统是 IDES[4]，AID(adaptive intrusion detection system)[5]，NSM(network security monitor)[6]，DIDS(distributed intrusion detection system)[7]. 其他正在进行的入侵检测研究项目详见文献[3]. 商业化的入侵检测产品已经开始面世，如 ISS 公司的 Real Secure，Cisco 公司的 NetRanger 等.

基于网络的 IDS 规模仍限制在企业网范围之内，多数系统是封闭的. 然而 Internet 是没有集中管理权威的多域互连网络，因此多管理域间 IDS 的协作是必需的. DARPA 与 IETF 正在制定入侵检测的标准 CIDF(common intrusion detection framework)[8]，但这些标准还未成熟.

本文讨论多管理域网络环境中分布式 IDS 间协同工作的框架结构以及实现中的关键问题. 第 1 节对现有的入侵检测技术提出了一种综合分类方法. 第 2 节给出了一个分布式协同入侵检测系统(distributed cooperative intrusion detection system，简称 DCIDS)的结构设计，并讨论了各组成部件的工作原理. 第 3 节讨论了 DCIDS 实现中的关键问题，包括部件间通信的效率与安全性、检测点的选择等.

1 入侵检测技术的综合分类

IDS 一般要经过数据收集与归纳、行为的分析与分类、报告与响应等过程. 根据数据来源的不同，IDS 可以分为基于主机(host-based)检测和基于流量(traffic-based)检测，如图 1(a)所示；根据分析方法的不同，又可以分为异常(anomaly)检测和误用(misuse)检测如图 1(b)所示. 在综合上述分类方法的基础上，我们提出了一种新的综合分类法，如图 1(c)所示. 其中 S 表示入侵检测技术的

* 收稿日期：1999-11-17；修改日期：2000-05-08

基金项目：国家 863 高科技发展计划资助项目(863-306-ZD08-01-3)

作者简介：段海新(1972—)，男，山东金乡人，博士，讲师，主要研究领域为计算机网络安全，网络管理；吴建平(1953—)，男，山东巨野人，教授，博士生导师，主要研究领域为计算机网络体系结构，协议测试，网络管理.

全集,H 代表 Host-Based,T 代表 Traffic-Based,A 代表 Anomaly,M 代表 Misuse.

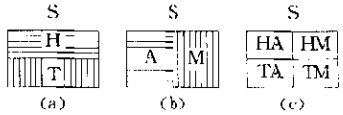


Fig. 1 Integrative taxonomy for IDS
图1 入侵检测技术综合分类

在综合分类方法中,基本入侵检测技术有以下 4 类:

HA=H∩A,数据来源于主机,使用异常检测方法,如 IDES;

HM=H∩M,数据来源于主机,使用误用检测方法,如 AID(adaptive intrusion detection system);

TA=T∩A,数据来源于网络,使用异常检测方法,如 NSM(network security monitor);

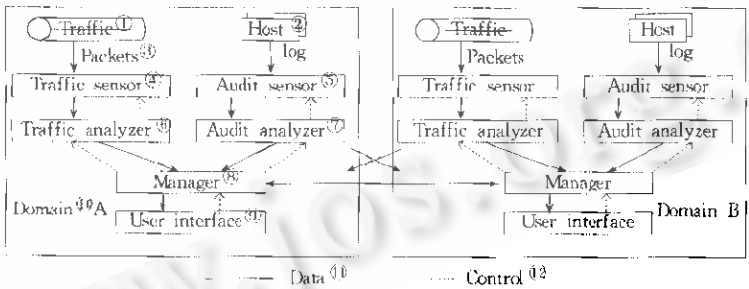
TM=T∩M,数据来源于网络,使用误用检测的方法,如 RealSecure.

这样,〈HA,HM,TA,TH〉构成了 S 的一种新的划分,可以精确地描述特定检测技术的特征.

以上各种检测技术各有优缺点.比如,HA 便于检测对应用系统的攻击,但是对性能影响大、不易扩展到大规模网络;TA 和 TM 能够方便地检测出利用网络协议的缺陷对攻击系统的攻击,然而对于应用层的攻击却无能为力.下文即将讨论的入侵检测系统是 HA,HM,TA,TM 的综合使用.

2 分布式协同入侵检测系统(DCIDS)体系结构及其组成

为了适应大规模、多管理域网络的入侵检测需求,我们设计了一个分布式协同入侵检测系统(DCIDS),如图 2 所示.DCIDS 使用多种检测技术,同时处理不同类型的原始数据(如 syslog,SNMP trap,traffic 等);分布在不同管理域的 DCIDS 之间可以交换信息,以协同检测.



①流量,②主机,③包,④流量传感器,⑤审计传感器,⑥流量分析器,
⑦审计分析器,⑧管理器,⑨用户界面,⑩管理域,⑪数据,⑫控制.

Fig. 2 The architecture for DCIDS
图2 分布式协同入侵检测体系结构

整个系统由 4 种功能部件组成:传感器(sensor)、分析器(analyzer)、管理器(manager)和用户界面(user interface).在数据流程中,前一个部件的输出是下一个部件的输入;在控制流程中,后一个部件通过相应的协议操作和控制前一个部件.

(1) 传感器(sensor)用于采集原始数据(如主机审计日志、流量数据等),这些数据是入侵检测的第一手资料.在 DCIDS 中有主机型和网络型两种传感器:(1) 主机审计传感器,分布在主机和路由器中,将安全相关事件(如 telnet)通过 syslog 发送给审计型分析器;(2) 网络流量传感器,是一种具有过滤功能的流量侦听设备,数据包经过滤以后交给流量分析器.

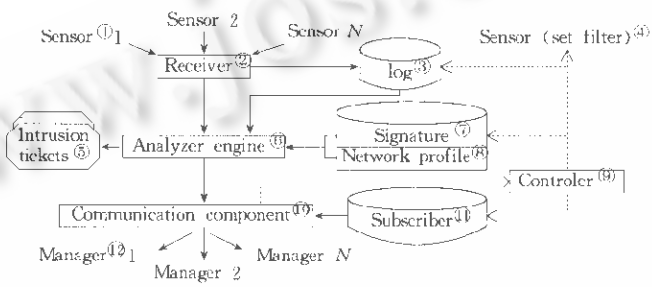
(2) 分析器(analyzer)是整个入侵检测系统功能的核心,对应于两种传感器有审计(audit analyzer)和流量(traffic analyzer)两种分析器,具有如图 3 所示的相同的结构,包括消息接收、分析引擎、通信和控制这 4 个功能组成模块. 分析引擎从消息接收模块收到消息或 IP 包后,首先根据特征库(signature)中的规则进行误用检测. 对于上下文无关的事件,比如流量分析器收到一则"源地址=目标地址"这样的 IP 数据包(极有可能具有攻击性),根据规则 j 的规定:

MessageType=SRC EQ DST, pattern="bit_compare_eq(IP[96], IP[128],32)", Count=1, Level=EMERG,

分析器直接向通信模块发送紧急告警信息;对于上下文相关事件,如审计分析器收到登录失败事件,根据规则 i:

MessageType=LOGIN FAILED, Pattern="/login failed/", Count=3, Level=ALARM,

分析引擎需要检查 Intrusion Tickets 中的事件卡片,根据当前状态来判断响应动作.



①传感器,②接收器,③日志,④传感器(设置过滤器),⑤入侵卡片,⑥分析引擎,⑦特征库,⑧网络轮廓,⑨控制器,⑩通信部件,⑪订阅者,⑫管理器.

Fig. 3 The structure of analyzer
图3 分析器结构

异常检测是定期执行的,分析引擎定期地从消息日志中统计网络和主机的行为模式,并与 Profile 中存储的该对象的正常模式相比较,对于异常的行为模式(比如主机负载过高、夜间网络流量过高)向管理器告警.

通信模块通过下文将要讨论的入侵告警与控制协议(IACP)向管理器发送入侵事件,接收管理器的查询和控制命令. 控制模块执行管理器发来的控制命令,负责分析器的配置管理和维护,主要包括消息日志的维护和归档,Signature 库的增、删、改,Profile 的更新以及订户列表的配置.

(3) 管理器(manager)是 DCIDS 的决策与响应部件,由通信模块、决策与统计模块和响应与测试工具组成. 通信模块接收分析器的告警事件,在管理员控制下,向分析器发送配置和控制命令. 决策与统计模块一方面根据网络的配置知识和既定的响应策略来决定告警事件的响应动作,包括忽略、报警、向其他管理器转发、终止当前的连接、自动配置防火墙或路由器访问控制链表等,并可以执行用户配置的响应程序;另一方面,从分析器中获取原始的数据信息,整理、归并到关系数据库中,并定期分析,将分析结果以图形化的形式提交管理员,生成新的 Profile,经管理员确认后更新分析器中的 Profile 库.

(4) 用户界面以直观的形式显示告警事件,并且指示入侵事件类型和侵害程度;反映当前的网络活动和被检测对象的当前状态,并给管理员相应的处理意见. 为了便于远程管理和控制,DCIDS 采用了基于 Web 浏览器的管理界面.

3 实现中的关键技术问题

(1) CDIDS 各组成部件之间的通信问题. CDIDS 各组成部件可能分布在不同的网络甚至不同的管理域中,考虑到对效率、安全性、可靠性的不同需求,各部件之间的通信机制应该作不同的考虑:

(1) 传感器-分析器之间的通信主要考虑大量数据传输的高效性和实时性. 在实现时,主机型的传感器通过 syslogd 进程、路由器通过 SNMP trap,向分析器的 Receiver 发送消息;流量传感器,通过 100M 网卡与分析器直接相连,目前可以处理 100Mbps 的以太网流量,对于 100Mbps 以上的高速网络,我们正在研制专用的流量侦听设备. 以上协议都是基于 UDP,减少了通信开销并提高了实时性.

(2) 分析器-管理器之间的通信主要考虑通信开销、可靠性和安全性问题,特别是在涉及多管理域时,IDS 的通信开销可能会影响到正常的通信业务;告警事件和控制命令有可能丢失,基于 UDP 的 SNMP 不能满足要求. 分析器和管理器之间需要双向认证机制、访问控制机制和数据源发认证以防非授权访问和 DoS 攻击. 在 CDIDS 中,我们采用了以下方法:

① 分析器在其订户列表(subscriber list)中对每个管理器保留一个事件过滤器,只发送该管理器预定的告警事件,大大减少了通信流量. 订户列表中保存了管理器的认证信息与授权信息,用于认证管理器的身份,控制管理器的访问权限.

② 分析器和管理器的通信部件之间通过一种专门设计的入侵告警与控制协议(intrusion alarm and control protocol,简称 IACP)通信,以实现双向的身份认证、可选数据的完整性和保密性服务. IACP 基于 TCP,由告警协议与控制协议两部分组成. 告警协议由分析器发起,首先由分析器向管理器发起一个 TCP 连接,经过双向的认证之后,再协商会话密钥(可选). 协议操作步骤如下:

TCP Connection: Aanlyzer——(tcp port 8110)——→Manager

Security Handshake: Analyzer←--authentication,negotiation——→Manager

Alert_Transmit: Analyzer---Alert_Message——→Manager

Alert Terminate: Analyzer——Alert_Terminate——→Manager

控制协议由管理器发起,用于向分析器发送控制命令和主动轮询,类似于 SNMP GET 的作用. 控制协议的操作与上述告警协议相同.

(3) DCIDS 采用了基于 Web 浏览器的管理界面. 为了解决管理器向浏览器主动发送(即 PUSH)信息问题,我们考察了 Server Push 和 Java Applet 两种技术. Server Push 要求整个管理过程中 TCP 连接一直要保持,一旦断开,所有的告警信息都会丢失. 后者需要在浏览器上运行一个 Java Applet,与管理器上的消息传递进程建立一个 TCP 连接,在意外终止时,applet 可以自动恢复连接. 由于控制的灵活性,我们选择了 Java Applet.

(2) 入侵检测点的分布和内容的选择结合 CERNET 运行情况,我们认为传感器设备分布在以下位置能够有效地检测大量的入侵活动:

(1) 网络边界(perimeter). 实验表明,在网络边界处安装流量传感器和流量分析器,可以发现大量 DoS 的攻击以及网络、端口扫描等;

(2) 骨干网路由器、交换机等互连设备以及服务器区(server farm). 将路由器或主机的日志信息和 SNMP TRAP 信息发送到主机型分析器,从中分析出端口扫描、非法登录企图、非法 SNMP 访问等. 另外,通过主机、路由器系统数据或配置信息的备份与校验,可以检测出被攻破的主机或路

由器.

4 结束语

本文提出的入侵检测技术的综合分类方法能够更为精确地描述入侵检测技术,所设计的DCIDS与其他企业网范围的IDS相比,具有网络结构上的可适应性、网络通信的安全性、对网络性能影响小等特点.

我们在CERNET骨干网环境中开发的DCIDS原型得到国家863高科技发展计划的资助.目前我们正在研究中高速(≥155M bps)网络流量传感器、分析引擎中的网络行为特征提取、入侵特征库设计等问题.在分布式入侵检测领域,仍有大量的研究工作和挑战性问题亟待解决.

References:

[1] Andersen, J. P. Computer security threat monitoring and surveillance. Technical Report, TR80904, Washington: Anderson Co., 1980.

[2] Denning, D. E. An intrusion-detection model. IEEE Transactions on Software Engineering, 1987,13(2):222~232.

[3] Biswanath, Mukherjee, Heberlein, L. Todd. Network intrusion detection. IEEE Network, 1994,8(3):26~41.

[4] Javitz, H. S., Valdez, A. The SRI IDES statistical anomaly detector. In: Teresa, F. L., ed. Proceedings of the Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1991.

[5] Sobirey, M. Adaptive intrusion detection system (AID). 1998. http://www-rnks. informatik. tu-cottbus. de/~sobirey/aid. e. html.

[6] Heberlein, L. T., Dias, G. V., Levitt, K. N., *et al*. A network security monitor. In: IEEE ed. Proceedings of the Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1990. 296~304.

[7] Snapp, S. R., Brentano, J., Dias, G. V., *et al*. A system for distributed intrusion detection. In: Teresa, F. L., ed. Proceedings of the Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1991.

[8] Clifford, K., Porras, P. A. A common intrusion detection framework. 1997. http://seclab. cs. ucdavis. edu/cidf.

Design and Implementation of a Distributed Cooperative Intrusion Detection System*

DUAN Hai-xin, WU Jian-ping

(*Network Research Center, Tsinghua University, Beijing* 100084, *China*)

E-mail: dhx@bjnet.edu.cn; jianping@cernet.edu.cn

http://www.nrc.tsinghua.edu.cn

Abstract: An integrative taxonomy for intrusion detection technologies is proposed in this paper, which can specify accurately existing intrusion detection methods. Aiming at multiple domain environments, a distributed cooperative intrusion detection system (DCIDS) is designed, which implements cooperative intrusion detection through efficient, secure information exchange among IDSes in different domain. The architecture of DCIDS is described, as well as its four components: sensor, analyzer, manager and user-interface. Some key issues are also discussed, including secure communication and selection of detection places.

Key words: network security; distributed cooperative intrusion detection; network management; authentication; access control

* Received November 17, 1999; accepted May 8, 2000

Supported by the National High Technology Development Program of China under Grant No. 863-306-ZD08-01-3