第42卷 第12期 西 安 交 通 大 学 学 报 Vol. 42 №12
2008年12月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Dec. 2008

网络安全协同防卫系统研究与实现

安喜锋，李伟华，刘尊
（西北工业大学计算机学院，710072，西安）

摘要：为了解决防卫体系中各安全模块缺乏协同控制以及不能有效发挥整体效应的问题，提出了一种基于代理的协同控制框架.将各个安全模块关联起来，以实现相互通信和协同工作.在此基础上，构建了包括预警定位、协同安全审计及态势评估、协同事故恢复、网络伪装等功能的网络安全协同防卫系统(NSCDS).以基于机器学习的系统调用序列审计模型为例，对关键技术模块进行了分析和验证，结果表明NSCDS软件在百兆级带宽下，安全审计预警漏报率小于6%，误报率小于8%，各功能模块工作稳定且配合正常，充分显示出系统的综合优势，实现了网络安全多层次、全方位的协同防卫目标.

关键词：协同控制；预警定位；安全审计；事故恢复
中图分类号：TP393.08 **文献标志码**：A **文章编号**：0253-987X(2008)12-1495-05

Research and Implementation of Network Security Cooperative Defense System

AN Xifeng, LI Weihua, LIU Zun
(College of Computer Science, Northwestern Polytechnical University, Xi′an 710072, China)

Abstract: A novel network security cooperative defense technology is studied and a cooperative control framework based on agent mechanism is proposed to solve the lack of cooperative control and whole effect in traditional defense systems. The technology supports both IPv4 and IPv6 protocols and security modules in the framework are associated with each other to accomplish communication and work together. Furthermore, a network security cooperative defense system is composed and the key functions that support the early-alert, audit, accident recovery, network camouflage and so on are also achieved. The pivotal research is emphasized on the key technologies of system call sequences audit model based on machine learning and cooperative accident recovery. Under the condition of 100 M Data flow speed, the NSCDS software's false negative is less than 6% and its false positive is less than 8%. Besides, all module functions work normally and the system can be used to carry out cooperative defense capability.

Keywords: cooperative control; early-alert and orientation; security audit; accident recovery

随着因特网的深入应用，网络安全事故愈演愈烈.据报道，2003年安全事故仅有2 557起，而2006年则高达26 476起[1]，可见网络安全事故呈迅速增长态势.

传统的安全措施，如加密认证、防火墙和入侵检测系统(IDS)等，在保护信息的机密性、完整性和鉴别、控制访问方面虽有成效[2-3]，但网络终因其缺陷及新型攻击方式层出不穷而受到种种威胁.因此，研究网络安全防卫的新模型、新方法，全面保障网络的正常运转，已是一个亟待解决的现实问题.

本文结合研究实践，以IPv4现役网为基础，构建了IPv6环境，研究了新老协议并存环境下的网络

收稿日期：2008-04-09. 作者简介：安喜锋(1973—)，男，博士生；李伟华(联系人)，男，教授，博士生导师. 基金项目：国家高技术研究发展计划资助项目(2006AA01Z406)；西北工业大学研究生创业种子基金资助项目(Z200651).

安全协同防卫技术，编制了相应的软件，实现了网络安全协同防卫系统.

1 网络协同防卫系统

基于 P2DR 模型，开发和完善了具有安全事件检测、实时动态监控、协同控制、事故恢复、电子取证、主动安全服务等功能的动态自治的网络安全协同防卫系统(NSCDS)，结构如图 1 所示.

NSCDS 的操作系统开发平台为红帽子 Linux 9.0，并采用基于特征的入侵检测方法，同时支持 IPv4/IPv6 协议，包括预警定位、审计及安全态势评估、协同电子取证、隔离控制、协同事故恢复、网络伪装、IPv6 环境下入侵检测和防冒等 8 个相关模块，如图 2 所示.

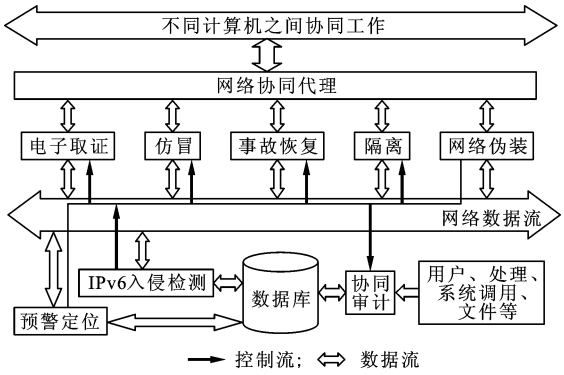

图 1 网络安全协同防卫系统体系结构图

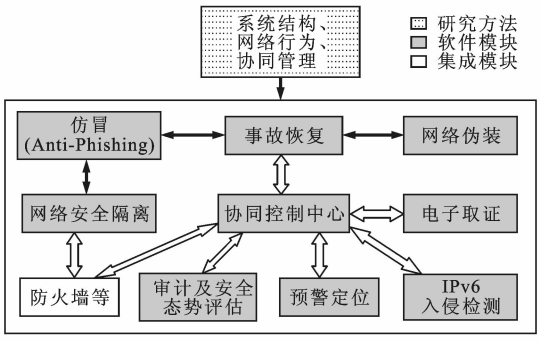

图 2 系统模块组成及模块之间的关系

NSCDS 主要采用 C 语言以及 PHP、Perl 脚本和 MySQL 数据库来实现. 其中：协同控制中心采用了基于Agent的图形化方式，使得预警定位、审计及安全态势评估、电子取证、隔离控制、事故恢复、网络伪装等模块可协同工作，从而构成了对现役网(IPv4 协议网)安全实施的多层次全方位防卫，而 IPv6 环境下的入侵检测模块是针对下一代互联网(IPv6 协议网)的；防冒模块可与现役网/下一代互联网的安全措施协同工作，对仿冒、盗窃等一些特殊网络入侵行为实施防卫；网络协同代理是构造内部网协同安全体系的基础，负责与其他主机进行通信、控制等协同工作. 网络安全协同防卫系统的 8 个功能模块由网络协同控制中心统一协调.

2 关键技术及模块

审计及安全态势评估是对透过防火墙进入网络系统的各种访问建立快速、准确的审计机制，它能对整个系统的安全态势进行分析和评估，与预警[4]定位模块配合，可为电子取证提供信息激励，结构如图 3 所示. 入侵者进入系统后，会通过执行程序或命令达到进攻的目的，而系统程序的运行会产生系统调用序列. 因此，对于系统调用序列的审计是甄别系统安全状况的重要依据. 综合相关工作并根据协同安全的需要，本文提出了一种基于机器学习的系统调用序列审计模型.

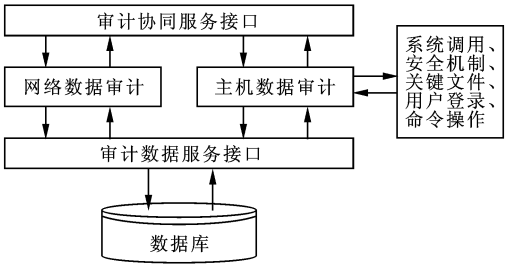

图 3 审计功能结构图

2.1 基于机器学习的系统调用序列审计模型

模型在对程序行为进行监视时，首先应该获得当前运行程序的系统调用情况. 本文在 Linux 中采用 PTrace 检测程序来截获系统调用情况，即通过对攻击行为(缓冲区溢出攻击)的分析，来发现溢出攻击发生后可能出现的情况：①被攻击进程异常退出，用户权限发生变化，攻击成功；②被攻击进程异常退出，用户权限没有发生变化，攻击失败；③被攻击进程正常，用户权限发生变化，攻击失败；④被攻击进程正常，用户权限发生变化，攻击成功. 审计系统通过分类器学习系统进行审计规则的训练和异常行为判定.

分类器学习系统的主要算法采用了针对审计序列的桶队列算法(Bucker Brigade Algorithm). 假设分类器 $c \in L_C$，其权值为 $p(c,k)$，k 为学习次数(时间参数)，L_C 为分类器列表，那么实际使用的信任分配算法描述如下.

(1)检测器从环境信息中获取训练例子集，并将其编码成二进制字符串的消息，多个消息构成消息

列表 L_M.

(2)逐一处理 L_C 中的每个分类器，检查 L_M 中是否存在与分类器的条件部分相匹配的消息. 如果存在匹配关系，则将相应分类器置于集合 M.

(3)计算匹配分类器 c 的投标值

$$B(c,k)=\frac{R(c)}{b}p(c,k) \tag{1}$$

式中：b 表示条件部分的位长；$R(c)$为条件部分非冗余码的位数.

在 M 中，按各分类器的投标值确定中标者(胜者). 胜者因中标需支出，但其权值减少，即

$$p(c,k)=p(c,k-1)-B(c,k) \tag{2}$$

而在前一次学习中向分类器 c 发送消息的分类器 s 的权值为

$$p(s,k)=p(s,k-1)+B(c,k)/n \tag{3}$$

式中：n 为发送消息的分类器数目.

(4)进行交易.

(5)计算测试表 L_T 中各分类器支出的投标值，即将投标值在匹配的分类器中平均分摊，激活 L_T 中的分类器，生成新的结论，并将结论作为新的消息置入 L_M 中.

(6)将 L_T 得到的结论通过作用器施于环境.

基于机器学习的系统调用序列审计模型的要点是审计规则可自动更新[5]，这对于识别新类型的攻击是十分重要的. 当模型第一次运行时，可以提前截取一些非法序列来训练审计规则，这样可以加速模型规则成型.

本文模型在一台 Linux 的主机上进行了运行测试，测试用例为针对 Sendmail 的溢出攻击[6]，攻击过程共为 4 段，在每一段中真实攻击 10 次并夹杂一些虚假攻击(不成功的攻击)作为扰动. 表 1 为攻击过程中审计模型的运行情况.

表 1　模型运行验证情况

检测率/%			
第 1 段	第 2 段	第 3 段	第 4 段
13	72	90	93

由表 1 可以看出，在最初阶段，模型对攻击并不能进行有效识别，随着时间的延续，模型对于攻击的识别率逐渐提高，而当识别率到达一定范围时将趋于稳定. 在模型配置时还发现，不宜使模型的规则演化收敛得过快，收敛过快的模型规则集很容易受到外界的干扰.

经过一系列的实验对比可知，该模型对于未知攻击具有一定的识别能力.

2.2　安全态势评估技术

为了在含有大量噪声的审计结果中对网络安全状态进行准确评估，本文提出了基于模糊推理的综合审计技术. 这种审计可建立在现有任何一种检测器的基础之上，并采用分布式运行模式，通过多个检测器的输出对网络数据进行初步审计[7]，然后将审计结果传递给推理器进行综合审计，最后保存、输出审计结果，并对网络安全状态做出评估. 实时审计的对象包括：网络数据流、主机操作、操作系统安全机制的行为模式[8]、关键文件完整性、用户登录情况等. 在网络环境中，操作系统安全性的缺陷分析、审计是重点所在，主要采用静态和动态相结合的分析方法. 静态分析采用基于源代码和二进制代码分析的脆弱点识别技术，以判断操作系统中可能存在的缓冲区溢出、隐通道等缺陷. 由于该审计结合了网络协同代理技术，所以可为内部网提交其他主机的审计结果，并将审计和安全态势评估结果(根据威胁等级)返回给安全功能模块.

2.3　基于网络备份联盟的自动恢复技术

协同事故恢复子系统由监测模块、控制模块、文件信息模块和通信代理组成，如图 4 所示. 在协同事故恢复系统中，源主机将需要保护的关键数据纳入实时监控，并在备份联盟中进行备份. 为了提高处理速度，该系统使用了差量备份和恢复技术. 一旦监测到关键数据文件遭受攻击或非法篡改，事故恢复系统将从多个备份点传送未被非法改动的关键数据，以恢复数据.

监测模块通过文件改动监测器 (File Alteration Monitor，FAM)监测关键文件列表，并将事件消息传递给控制模块. 控制模块的核心是传输控制进程，以用于控制各种消息的传输、各个列表的更新维护，

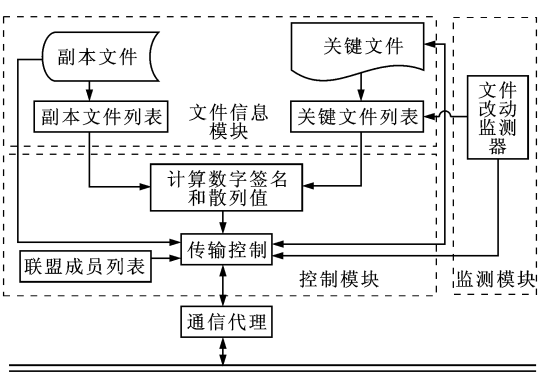

图 4　协同事故恢复各模块关系图

并计算数字签名值和散列值. 文件信息模块包括关键文件、副本文件及文件列表. 关键文件库由监测模块检测,而副本文件库存放着来自其他节点的关键文件备份. 多个节点组成一个备份联盟,在联盟各节点上,通信代理负责完成事故恢复系统之间的副本维护、文件恢复等过程的安全通信. 控制模块和通讯代理是事故恢复模块的关键,它们与协同控制中心进行交互协调.

基于网络备份联盟的恢复模块,主要是为安全性需求高的数据文件提供容灾功能,它采用多源数据快速备份恢复方式,保障关键数据的可用性. 备份联盟中各主机的监测模块一旦发现文件(文件夹)有所改动,将启动多源数据快速备份恢复模块,从备份联盟中的多个备份点传送数据. 在监控中心的备份主机状态栏中可以选择备份主机,并显示历次与该备份主机的通讯记录,包括恢复文件的大小、传输的字节数、传输的速度和加速度.

2.4 基于代理的协同控制技术

在网络安全协同防卫系统中,基于代理的协同控制框架如图 5 所示. 协同控制中心的任务是:负责代理通信的对称加密密钥的分发、加密认证算法的选择、各系统运行状态的提供、系统协同工作的查询、各个主机之间报文交换协议定义文件(DTD)的一致性维持等[9]. 在每台主机上必须运行且只能运行一个代理,其作用是:对传输的数据进行加密认证,并对本机运行的安全系统提供协同控制功能. 代理之间的通信可采用客户/服务器点对点模式,发起对话者为客户端. 每个代理开放一个服务器端口,这样每台主机相对于安全系统只有一个开放端口,从而最大限度地减小了入侵者通过不同端口攻击的可能性,同时有利于建立统一的加密认证机制.

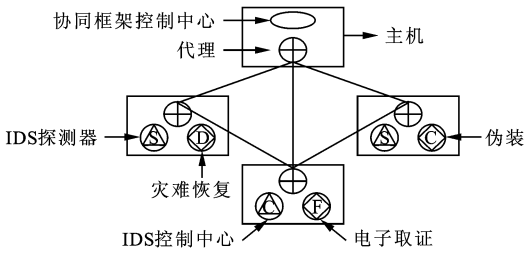

图 5 协同控制框架示意图

各个安全模块只能与本机代理进行通信,包括安全模块与主机内其他系统通过代理进行通信,安全模块与其他主机安全模块通过代理进行通信. 通过代理关联,各个安全功能模块实体可以建立自己的控制中心.

全网的安全控制中心部署在协同控制中心之上,负责配置统一的安全策略,设置系统中各模块性能参数. 各安全模块可与协同控制中心进行交互,并受协同控制中心的控制,其相互配合可共同完成网络安全防卫工作. 图 6 是预警定位模块在协同控制中心协调下工作的可视化[10]示例.

图 6 软件系统可视化界面示例

3 系统测试平台及测试结果

考虑到校园网实验环境受到校园网整体安全策略的限制,为了对网络安全协同防卫系统的功能、性能等指标进行全面测试,我们选择了比校园网更加开放、安全策略相对较弱的电信公众网络平台建立了测试环境. 测试平台基于中国电信 ADSL 网络,网络连接方式如图 7 所示.

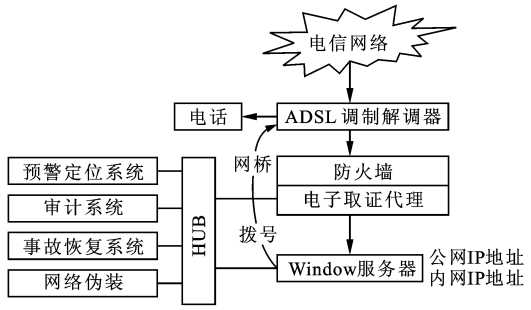

图 7 系统测试平台的网络连接方式

测试方式分为外网真实环境验证和模拟攻击演练. 根据测试数据统计,利用分布式安全事件预警分析和协同审计系统可检测出 31 类共 2 045 种(可扩充)攻击. NSCDS 在百兆位流量下对 IPv4/IPv6 攻击的入侵检测捕获率大于 99.7%,漏报率小于 6%,误报率小于 8%. 采取差量备份技术,事故恢复速度是正常拷贝的 2 倍以上,且可在线实时恢复,恢复程度达 100%. 根据需要,协同控制中心能够对所有的

IPv4/IPv6 攻击预警信息进行排序、分析和图形显示，并能够根据地址反查数据库，从而对地址来源进行追踪. 整个 NSCDS 系统易于操作和管理，人机界面良好.

4　结束语

本文构建了一种面向大规模网络环境的网络安全协同防卫系统，其关键技术实现方案的可行性得到了初步验证. 在基于代理的协同控制框架下，各功能模块工作稳定且配合正常，显示出了系统的综合优势，实现了网络多层次、全方位的协同防卫的目标. 下一步的工作是：继续深入研究预警分析算法，提高预警的准确性；实现协同控制中心和防冒系统的联动设计，使协同防卫系统更加规范、有效、完整；在有大量噪声的审计结果中，加强评估安全态势和 IPv6 特征规则提取的准确性研究.

参考文献：

[1] CNCERT/CC. 2006 annual report by CNCERT [EB/OL]. [2007-10-10]. http://www.cert.org.cn, 2007.

[2] BERK V H, GRAY R S, BAKOS G. Using sensor networks and data fusion for early detection of active worms [C]// Proceedings of the SPIE AeroSense: Sensors, and Command, Control, Communications, and Intelligence Technologies for Homeland Defense and Law Enforcement II. Orlando, FL, USA: SPIE, 2003: 92-104.

[3] 傅翀，王娟，秦志光，等. 宏观网络安全预警与应急响应系统 [J]. 电子科技大学学报，2006，35(4)：702-705.
FU Chong, WANG Juan, QIN Zhiguang, et al. Macro network security warning and emergency response system [J]. Journal of University of Electronic Science and Technology of China, 2006, 35(4): 702-705.

[4] 胡华平，张怡，陈海涛. 面向大规模网络的入侵检测与预警系统研究 [J]. 国防科技大学学报，2003，25 (1)：21-25.
HU Huaping, ZHANG Yi, CHEN Haitao. The study of large scale networks intrusion detection and warning system [J]. Journal of National University of Defense Technology, 2003, 25 (1): 21-25.

[5] BALEPIN I, MALTSEV S, ROWE J, et al. Using specification-based intrusion detection for automated response [C] // Proceeding of the 6th International Symposium on Recent Advances in Intrusion Detection. Berlin, Germany: Springer, 2003: 136-154.

[6] Nsfocus. Sendmail 异步信号处理竞争条件漏洞 [EB/OL]. [2007-10-10]. http://www.nsfocus.net/vulndb/8596.

[7] 王新昌，杨艳，刘育楠. 一种基于局域网络监控日志的安全审计系统 [J]. 计算机应用，2007，27(2)：292-294.
WANG Xinchang, YANG Yan, LIU Yunan. Security audit system based on LAN monitoring logs [J]. Journal of Computer Applications, 2007, 27(2): 292-294.

[8] 卿斯汉，刘文清，温红子. 操作系统安全 [M]. 北京：清华大学出版社，2004：25-26.

[9] 雷浩，黄建，冯登国. 协同环境中共有资源的细粒度协作访问控制策略 [J]. 软件学报，2005，16(5)：1000-1011.
LEI Hao, HUANG Jian, FENG Dengguo. A fine-grained coalition access control policy for jointly-owned resources in collaborative environments [J]. Journal of Software, 2005, 16(5): 1000-1011.

[10] HIRAISHI H, MIZOGUCHI F. Design of a visual browser for network intrusion detection [C] // 10th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Piscataway, NJ, USA: IEEE, 2001: 132-137.

（编辑　苗凌）