文章编号: 1001- 2486(2003) 01- 0021- 05

面向大规模网络的入侵检测与预警系统研究*

胡华平[1], 张 怡[1], 陈海涛[1], 宣 蕾[1], 孙 鹏[2]
(1. 国防科技大学计算机学院, 湖南 长沙 410073; 2. 北京科技大学信息工程学院, 北京 100083)

摘 要: 开展面向大规模网络的入侵检测与预警系统的研究, 对于提高我国网络系统的应急响应能力、缓解网络攻击所造成的危害、提高系统的反击能力等具有十分重要的意义。首先对国内外的研究现状进行综述; 然后, 提出了面向大规模网络的入侵检测与预警系统的体系结构与组成; 最后, 着重对与本系统研制相关的关键技术与难点进行论述。

关键词: 入侵检测; 战略预警; 数据融合; 数据挖掘; 威胁评测
中图分类号: TP393. 08 文献标识码: A

The Study of Large Scale Networks Intrusion Detection and Warning System

HU Hua-ping[1], ZHANG Yi[1], CHEN Hai-tao[1], XUAN Lei[1], SUN Peng[2]
(1. College of Computer, National Univ. of Defense Technology, Changsha 410073, China; 2. College of Information Engineering, USTB, Beijing 100083, China)

Abstract: It is very important to study Large Scale Networks Intrusion Detection and Warning System(LSNIDWS), which can increase the network systems reaction ability to catastrophe, slow down the harm of the network attack, enhance system counterattack ability. The summarization of studying situation in the world is first presented. Then, the structure and its component of LSNIDWS are presented. Finally, the key technology and difficulties related to building LSNIDWS prototype are discussed.

Key words: intrusion detection; strategic warning; data fusion; data mining; threat assessment

IDS 的研究始于 20 世纪 80 年代, 主要包括基于主机的入侵检测系统和基于网络的入侵检测系统。因为基于主机的入侵检测需要在所有受保护的主机上均安装检测系统, 配置费用高, 所以实际应用较多的是网络型的入侵检测系统。但是高带宽网络、交换式网络、VLAN、加密传输的发展都对基于网络的入侵检测造成了很大限制, 所以最好的策略是两者相结合。现有的主流的基于网络的商业入侵检测系统都准备或已经增加了基于主机的检测功能。目前的主要研究为适用于大型网络的入侵检测系统, 主要有已经实现的 NADIR 系统和 CSM(合作安全管理), 以及正在研究中的 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances) 项目和 AAFID(the Autonomous Agents for Intrusion Detection) 。它们都在 IDS 体系结构、ID 技术和网络安全策略等方面展开了研究, 而相应有关预警技术的研究较少[1]。

国外早已开展了早期预警系统及入侵检测技术的研究, 在一些重要的政治、军事和经济网络上对非法入侵实施监控。这些系统在保障信息网络安全、尽早发现入侵攻击迹象、分析入侵攻击的技术手段方面发挥着重要的作用。美国国家安全局设有国家计算机安全中心, 系统与网络攻击中心, 负责网络信息战的战略情报预警、网络攻防技术开发和网络信息战指导; 国防信息系统局成立了网络战战术预警中心。自 1997 年以来, 美、英等国一直在进行网络安全预警技术的研究。1998 年, 美国针对各个信息基础设施提出了分三阶段、长达 15 年的实现预警系统的计划。美国战略司令部已经于 1999 年 9 月进行

* 收稿日期: 2002- 07- 05
基金项目: 国家 863 高技术资助项目(2001AA142030)
作者简介: 胡华平(1967—), 男, 副研究员, 博士后。

了新一代的入侵检测系统原型的“先期概念技术演示(ACTD)”,它能为美国国防部提供信息战的早期预警。英国 King′s College London 学院战争研究系的国际安全分析中心(International Centre for Security Analysis, ICSA)在信息战攻击威胁评测和预警方面进行了深入的研究,提出了智能化的预警决策支持系统[2]。

目前我国还只具备适用于局域网的入侵检测系统与预警系统,还没有适用于大规模网络的入侵检测与预警系统。为了保障我国信息系统支持和适应信息战的要求,开展网络入侵检测与预警系统的研究是十分必要的,它对于提高网络系统的应急响应能力、缓解网络攻击所造成的危害、提高系统的反击能力等均具有十分重要的基础意义。在现代信息战与维护国家信息安全中,它是有效抵御敌方的信息攻击,维护自身网络体系的正常运作,并进行追踪和反击所必不可少的[3]。

1 面向大规模网络的入侵检测与预警系统[4]

面向大规模网络的入侵检测与预警系统的组成如图 1 所示(图中所画的应急响应中心不在本文讨论范围之内),它主要由基于网络的入侵检测系统、区域预警中心、总预警中心等三部分组成。入侵检测代理是分布于不同网段的攻击检测程序,在检测到可疑事件或入侵后,立即向中心服务器报告。当中心服务器收到从各个代理上报的可疑事件或入侵时,除采用一定的响应策略(如发出警报、切断 TCP 连接等)外,立即将可疑事件或入侵上报给区域预警中心,以便对其做出进一步的检测和预警。

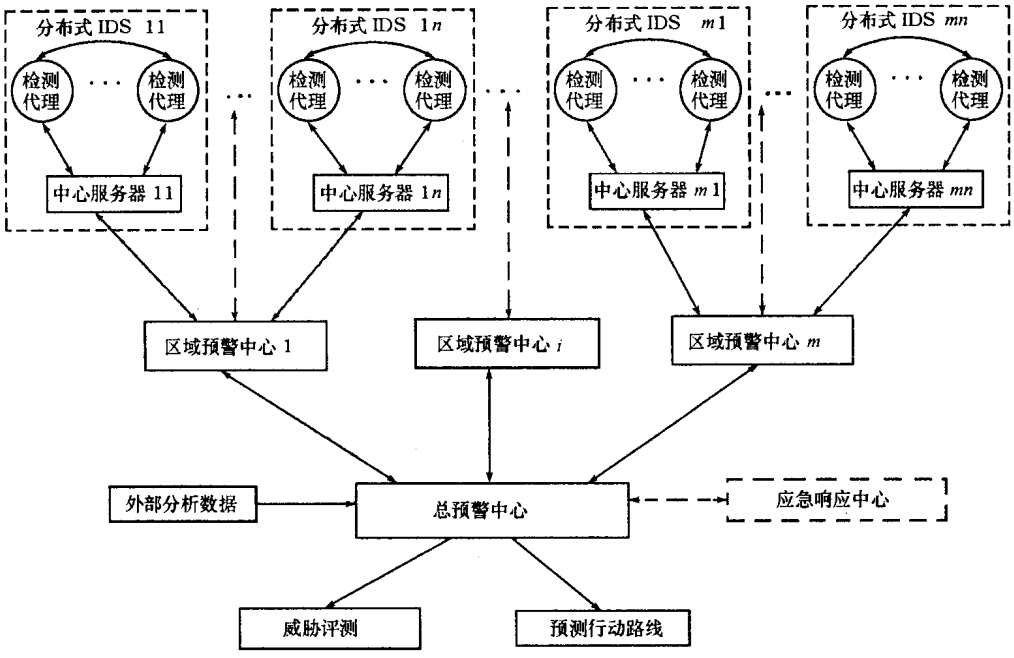

图 1 面向大规模网络的入侵检测与预警系统的组成

Fig. 1 The compose of large scale networks intrusion detection and warning system

区域预警中心采用数据融合技术对来自多个入侵检测系统中心服务器的数据进行分析处理,根据不同子网所发生的入侵信息来判断该区域网络可能发生的入侵事件,对其做出实时的检测,进行及时的报警,并将数据上报总预警中心。总预警中心是一个决策支持系统,主要由威胁评测系统构成。当预警中心收到可疑事件或入侵的报告后,对它们进行威胁评测,判断威胁级别、发出预警并预测敌方可能的行动路线。与此同时,总预警中心将预警结果反馈给各区域预警中心,以便及时作出响应。

2 关键技术与难点

2.1 分布式入侵检测协同模型的研究

随着黑客入侵手段的提高,尤其是分布式、协同式、复杂模式攻击的出现和发展,传统的单一的、缺

乏协作的入侵检测技术已经不能满足需求, 需要有充分的协作机制。所谓协作主要包括事件检测、分析和响应能力的协同以及各部分所掌握安全相关信息的共享等两个方面。

尽管现在最好的商业产品和研究项目中也只有简单的协作, 如 ISS 的 RealSecure 入侵检测产品可以和防火墙协作, 在 AAFID 中同一网段上各主机型代理之间可进行简单的信息共享, 但很难满足实际需求。协作的程度主要有以下层次:

- 同一系统中不同入侵检测部件之间的协作, 尤其是主机型和网络型入侵检测部件之间的协作, 以及异构平台部件的协作;
- 不同安全工具之间的协作;
- 不同厂家的安全产品之间的协作;
- 不同组织之间预警能力和信息的协作。

要实现协同, 首先要考虑两个问题: 一是信息表达的格式和信息交换的安全协议; 二是协作的模型。信息表达的格式有两个发展中的标准: DARPA 的通用入侵检测框架中提出了 CISL(Common Intrusion Specification Language) 语言[5]; IETF 的入侵检测工作组(IDWG) 中提出了在 IAP 中使用的另一套方案[6], 两者各有长短。分布式入侵检测协作模型应充分利用 Agent 研究现有的技术和进展, 将其应用到入侵检测和攻击防护中, 其主要研究内容包括:

- 研究检测代理(基于主机、基于网络的) 之间的信息交换格式和协作模型, 以形成统一的入侵检测表达格式;
- 研究各实体之间的分布结构和逻辑从属关系, 以及安全的互操作系统模型。

2.2 基于数据挖掘的入侵检测技术研究

模式匹配方法仅适用于检测已知的攻击, 而不能用于检测未知的攻击; 概率统计方法虽然根据用户对象的动作为每个用户都建立一个用户特征表, 通过比较当前特征与已存储定型的以前特征, 从而判断是否是异常行为, 并具有一定的预测特性, 但是在如何选择系统特征时要使用直觉和经验, 因而仍具有一定的局限性。而基于数据挖掘的入侵检测技术, 它利用形式语言、数据挖掘技术的方法和理论, 对从网络中和主机系统中采集到的数据、安全日志和审计信息进行分析和过滤, 从“正常”的数据中发现“正常”的用户和程序的使用模式, 利用这些模式来检测网络上的入侵行为, 从而提高系统对用户异常行为的识别能力和未知模式攻击的检测能力。它涉及到的主要技术包括:

- 数据泛化与聚类技术;
- 分类函数或分类模型(也称作分类器) 的生成技术;
- 关联规则发现与合并技术;
- 序列模式发现技术。

2.3 数据融合技术研究

研究数据融合模型, 对来自多个入侵检测中心的数据进行分析处理与汇总, 做到从不同子网所发生的入侵来判断区域网络可能发生的入侵事件。数据融合系统可以分析多个入侵检测系统采集的数据, 从中发现单个入侵检测系统无法确定的攻击, 以进一步核实入侵检测系统发现的攻击, 并作为决策支持系统提供入侵报警信息, 以提高报警的准确性。

数据融合系统的输入可以从许多分布式入侵检测代理、用户的轮廓数据库、系统消息和操作者的命令中得到数据。融合后的数据输出将对入侵者的身份、位置、入侵者的行动、可观察到的威胁及攻击级别进行评测。图 2 为数据融合系统的层次模型[7]。

对数据融合模型的特征识别和模式的识别过程比较困难, 因为该推断的级别比较高, 它通常需要从源数据层提取特征值, 模式识别的基本参数要被模板化, 模板最基本的形式被用于当前的入侵检测系统中。未来协同多因素的信息战攻击的追踪需要群分析技术、可适应性的神经网络和基于规则的专家系统的支持。

2.4 基于入侵检测的预警模型研究

预警模型是评测攻击的威胁程度, 攻击的本质、范围和起源, 同时预测敌方可能的行动的基础。图

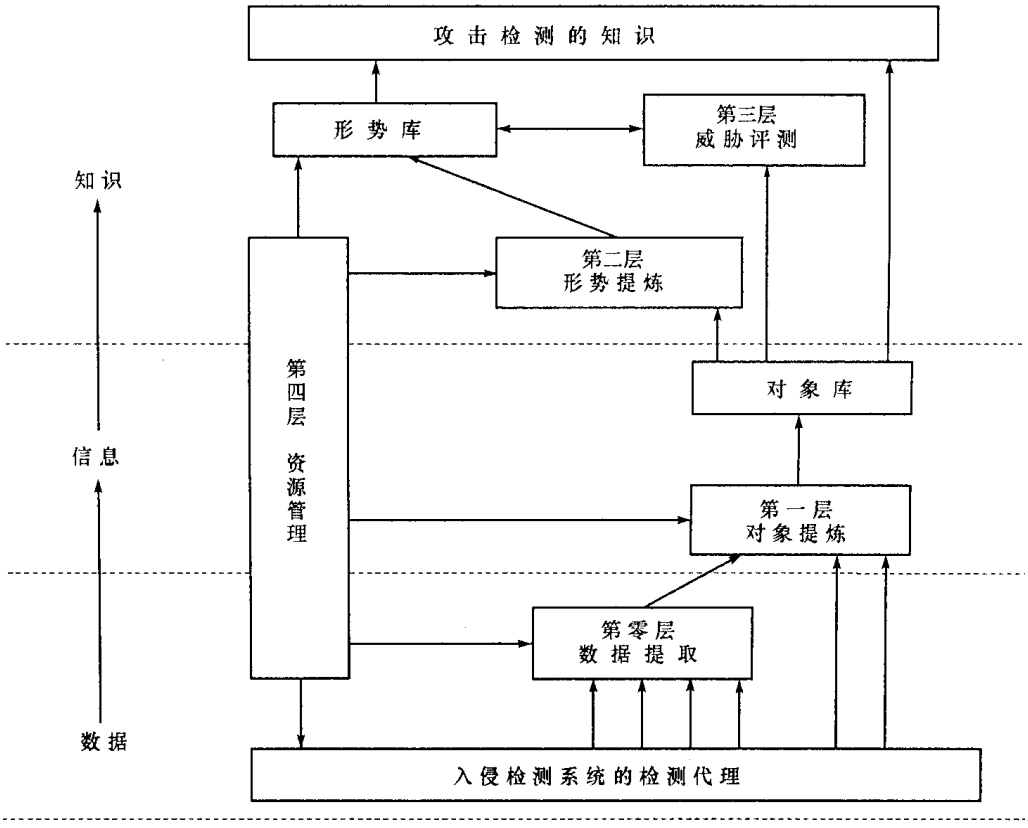

图 2 数据融合系统的层次模型

Fig. 2 Hierarchical model of data fusion system

3 给出了预警系统的体系结构。其中,短期知识库代表了指示各子网之中及其周围的异常活动的检测报告,即入侵检测数据汇总系统报告的数据。长期知识库由与信息战威胁相关的融合数据组成,威胁评测系统由威胁数据库和智能融合系统组成。中期知识库代表对发展势态的评测,其内容在异常事件被入侵检测系统检测出来、通过威胁评测系统过滤,再以威胁评测、预警和预测敌方行动路线的形式提交之后形成的[8]。

预警模型的核心是威胁评测系统,它作为决策支持工具,目的是对由敌方或授权代理引起的信息战威胁的级别产生定量的指示。智能融合系统使用层次化规则集合来组织问题答案,利用威胁数据库量化来自每个角色的风险因子。由于信息战的威胁不像常规军事威胁那么容易被量化,因此需要研究多种规范以发展建立专家系统及其相关数据库。由于智能融合系统合并了能改变威胁指数的所有的引发因素,为适应现实输入数据的变化,威胁指数应该是动态变化的[9]。

主要研究内容包括:

- 研究威胁评测模型,对由敌方或授权代理引起的入侵威胁的级别给出定量的指示;
- 研究建立威胁数据库的方法与技术,以量化来自不同角色的风险因子。

3 结束语

为了保障我国信息系统支持和适应信息战的要求,开展网络入侵检测与预警系统的研究是十分必要的,它对于提高网络系统的应急响应能力、缓解网络攻击所造成的危害、提高系统的反击能力等均具有十分重要的基础意义。在国家 863 计划的资助下,我们在原型系统的搭建、基于入侵检测的预警模型的建立、分布式入侵检测协同模型的研究、数据融合技术研究、通用网络通信库的研制等方面开展了卓有成效的工作。

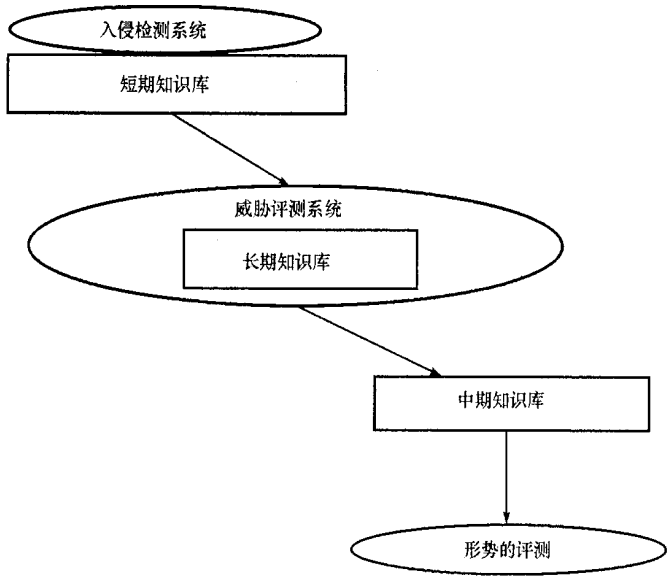

图 3 预警系统的体系结构

Fig. 3 The structure of warning system

参 考 文 献:

[1] 胡华平, 陈海涛, 黄辰林, 唐勇. 入侵检测技术的研究现状与发展趋势[J]. 计算机工程与科学, 2001, 23(2): 20- 25.

[2] US Infrastructure Assurance Strategic Roadmaps. Strategies for Preserving Our National Security[R]. August 1998.

[3] 胡华平, 等. 网络安全深度防御与保障体系研究[J]. 计算机工程与科学, 2002, 待发表.

[4] 胡华平, 等. 网络入侵检测、预警和安全管理技术(863-104-02-02) 申请书[R]. 2001.

[5] Chen S S. Common Intrusion Detection Framework[R]. http://seclab.cs.ucdavis.edu/cidf/.

[6] 入侵检测工作组(IDWG). http://www.ietf.org/html.charters/idwg-charter.html.

[7] 苗青. 网络安全战略预警系统设计及关键技术的研究[D]. 长沙: 国防科技大学, 2002.

[8] Rathmell A, et al. Information Warfare Attack Assessment System(IWAAS)[R]. Information Warfare Seminar, 1997.

[9] 苗青, 宣蕾, 苏金树. 网络安全战略预警系统的攻击检测技术研究[J]. 计算机工程与科学, 2002, 24(1): 14- 17.