综述与评论 Review and Comment

入侵检测系统研究进展

张振国[1]，巩林明[1,2]
（1.陕西科技大学，陕西 西安 710021；2.石河子大学，新疆 石河子 832000）

摘 要：入侵检测系统是信息安全领域研究的热点问题。在阐述入侵检测系统概念和类型的基础上，指出了当前入侵检测系统的优点及局限性。神经网络、遗传算法、模糊逻辑、免疫原理、机器学习、专家系统、数据挖掘、Agent等智能化方法是解决IDS局限性的有效方法。介绍并着重分析了2种基于智能方法的IDS，提出了IDS在今后发展过程中需要完善的问题。

关键词：IDS;入侵检测专家系统;人工神经网络;异常检测;智能体
中图分类号：TP393 **文献标识码**：A

Review of research progress on intrusion detection system

ZHANG Zhen Guo[1], GONG Lin Ming[1,2]
(1. Shanxi University of Science Technology, Xi'an 710021, China; 2. Shihezi University, Shihezi 832000, China)

Abstract: IDS is the hot topic in the field of information security. On the elaborated concept and types of IDS, the merit and limitation of the current IDS are pointed out. The intellectualized neural network, genetic algorithm, fuzzy logic, immunity, machine learning, expert system, data mining, Agent and so on are effective approaches to overcome the limitation of IDS. Two kinds of IDS based on intelligent method are introduced and analyzed. Finally, issues about IDS that will be consummated in the next developing are put forward.

Key words: intrusion detection system; intrusion detection expert system; artificial neural network; anomaly detection; agent.

在当今信息化的时代，随着网络的高速发展，信息安全问题引起了世界各国的高度关注。国外在信息安全方面的研究比较早，而我国相对较晚，虽然近几年发展迅速，但仍处在发展的初级阶段。

传统上，用户大都采用被动的静态防护技术，诸如防火墙、身份认证、访问控制、加密、安全路由。然而，随着攻击者知识体系的日趋完备，攻击工具和攻击技术的日趋复杂，单纯的被动防御已经无法满足对信息安全高度敏感部门的需要，因此，信息防御还应采用主动的动态防御技术，即应该重视提高系统的入侵检测能力、系统的事件反应能力以及当系统遭到入侵引起破坏时的快速恢复能力。在此境况下，入侵检测技术及入侵检测系统成为了信息安全领域的新热点。

1 入侵检测系统的发展历程

1980年4月，JAMES P.A.为美国空军做了一份题为“Computer Security Threat Monitoring and Surveillance”的技术报告。该报告提出了一种对计算机系统风险和威胁的分类方法，并将威胁分为外部渗透、内部渗透和不法行为3种，最重要的是它提出了利用审计数据来监视入侵活动的思想，即入侵检测系统的思想[1]。1984年到1986年，乔治敦大学的Dorothy Denning和SRI/CLS公司计算机科学实验室的Peter Neumann研究出了一个名为入侵检测专家系统IDES (Intrusion Detection Expert Systems)的实时入侵检测系统模型[2]。该模型的六部件理论为构建IDS提供了一个通用框架。1988年，Teresa Lunt等人针对当时爆发的莫里斯蠕虫，基于Dorothy Denning提出的入侵检测模型[3]开发出了用于检测单机上入侵企图的入侵检测专家系统IDS。1995年又推出了它的改进版本，名为下一代入侵检测专家系统NIDES（Next-generation Intrusion Detection Expert System）[4]。1989年，加州大学戴维

斯分校的Todd Heberlein写了一篇题为《A Network Security Monitor》的论文，文中提出了用监控器用于捕获TCP/IP分组报文，第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机，网络入侵检测从此诞生。

时至今日，IDS的发展大致经历了3个阶段：第一代IDS包括基于主机日志分析、模式匹配，这个阶段的IDS基本是试验性的系统。第二代IDS出现在于20世纪90年代中期，它主要采用网络数据包截获，主机网络数据分析和审计数据分析等技术。代表性的产品有早期的ISS Real Secure(V6.0之前)、Snort等。国内的绝大多数IDS厂家的产品都属于这一类。第三代IDS是近几年才出现的，其特点是采用协议分析、行为分析等技术。协议分析技术的采用极大减小了计算量，减少了误报率；行为异常分析技术的采用赋予了第三代IDS系统识别未知攻击的能力。第三代IDS可以分为基于异常检测的IDS和基于误用(滥用)检测的IDS两大类。异常检测IDS是根据异常行为和计算机资源的使用情况来判断的，其代表性产品有Network ICE(2001年并入ISS)、Rea1Secure(V7.0)、NFR(v2.0)等。

2 入侵检测系统的定义

入侵检测的目标是在不影响网络性能的情况下，通过检查系统的审计数据或网络数据包信息来检测，从而提供对内部攻击、外部攻击和误操作的主动的实时保护。

入侵检测的前提是用户或者程序的行为是可以被观察的，而且正常行为和入侵行为之间存在着明显的不同。

入侵检测系统IDS（Intrusion Detection System）是通过分析与安全相关联的数据进行检测入侵活动的系统[6]。IDS的作用：(1)能够在入侵攻击对用户产生危害前，发现入侵，并利用报警与防护系统阻止入侵行为的实现；(2)在入侵攻击实施过程中减少入侵所造成的损失；(3)在遭到入侵攻击后收集入侵攻击的相关信息，在分析提取后添加到作为防范系统的知识库内，进而增强系统的防范能力。

入侵检测系统主要由如下4个部分组成[7, 8]，系统结构如图1所示。

(1)数据收集装置:收集反应状态信息的审计数据，传给检测器；

(2)检测器:负责分析和检测入侵，并发出警告信息；

(3)知识库:提供必要的数据信息支持；

(4)控制器:根据警报信号，人工或自动做出响应动作。

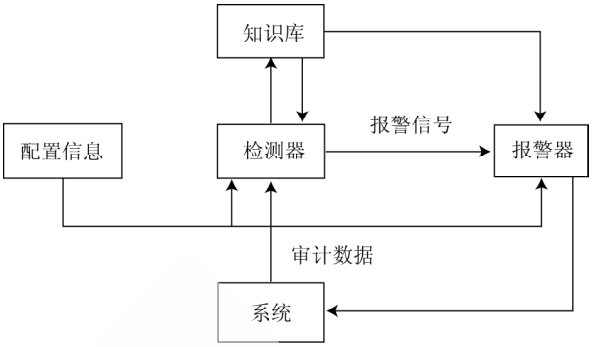

图1 入侵检测系统结构图

3 入侵检测系统的分类

基于信息来源的不同，网络入侵检测系统可分为网络基IDS、主机基IDS和混合基IDS 3类，其中混合基IDS是综合了网络基IDS和主机基IDS的入侵检测系统，它既可以发现网络中的入侵信息，又可以从系统日志中发现异常情况。

基于检测分析方法的不同，网络入侵检测系统可分为滥用检测IDS（基于知识）与异常检测IDS（基于行为）2类。前者通过收集入侵攻击特征和系统缺陷构成知识库，利用已有的知识来识别攻击行为；后者的理论基础是假设入侵者活动异常于正常主体的活动中，通过对系统审计踪迹数据的分析建立起系统主体的正常行为特征轮廓，将当前主体的活动状况与已建立的特征轮廓进行比较，若有很大偏差，就认为该活动可能是“入侵”行为。

4 传统入侵检测系统的局限性及克服方法

入侵检测系统在结构上的发展是与信息系统的结构变化密切相关的，但入侵检测的方式没有多少变化，时至今日入侵检测系统还是异常检测、误用检测或是二者的结合。传统入侵检测系统的可扩展性和适应性都受到限制。在实际应用中，入侵检测模型仅能处理一种特殊的审计数据源，更新费用较高，速度也较慢。

为了克服传统入侵监测系统的局限性，在原来的基础上引入了用于对入侵的特征进行辨识的人工神经网络、遗传算法、模糊逻辑、支持向量机、免疫原理、机器学习、专家系统、数据挖掘、Agent等智能化方法。入侵检测系统发展趋势为同时采用多种检测技术的综合型智能入侵检测系统。下面就基于人工智能领域分支技术的IDS进行阐述。

4.1 基于神经网络的入侵检测系统[5, 12, 13]

人工神经网络的优点是具有较强的容错性，能够识别带噪声或变形的输入模式，具有很强的自适应能力；可以进行并行分布式信息存储与处理，识别速度快，能把识别处理和若干预处理融为一体进行。而入侵检测系统的异常检测技术实质上是一种模式识别或分

类问题，因此有很多学者将神经网络技术应用到了入侵检测系统中，发展成为今天的基于神经网络的入侵检测系统。

4.2 基于专家系统的入侵检测系统

专家系统是最经典的智能检测技术之一，它克服了简单模式匹配的一些弱点，被许多经典的入侵检测系统IDS所采用，如MIDAS、IDES、NIDES、DIDS和CMDS等。将专家系统应用于IDS，充分利用安全专家的知识，通过有效的推理，将所获取的网络数据与专家知识进行匹配，判断是否为入侵行为。

4.3 综合型入侵检测系统：基于专家系统的滥用检测系统IDES

入侵检测专家系统IDES（Intrusion Detection Expert System）是SRI公司CSL实验室20世纪80年代开始研究的一个综合入侵检测系统，同时采用专家系统（滥用检测）和统计分析（异常检测）[4]两种检测技术。

IDES原型系统采用的是一个混合结构，包含了一个异常检测器和一个专家系统。异常检测器采用统计技术刻画异常行为；专家系统采用基于规则的方法检测已知的入侵行为。IDES系统结构如图2所示。

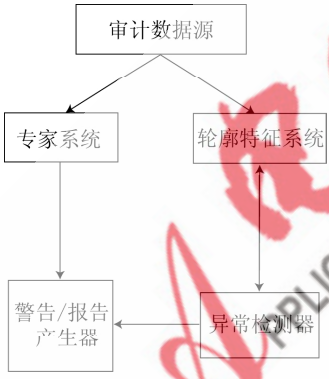

图2 IDES系统结构

IDES检测用户行为审计数据是否与该用户的历史活动相一致。专家系统组件包含描述可疑行为的规则，规则建立在入侵行为的过去知识、已知的系统脆弱性漏洞及特定系统安全策略基础上。

5 引入智能化技术的入侵检测系统面临的主要难点及有待完善的问题

5.1 面临的主要难点[8, 9, 15]

(1) 实时检测难。由于智能入侵检测技术大都采用软计算方法，计算量大，占用系统资源大。随着网络技术的高速发展和吉比特高速网的出现，采用智能入侵检测技术的IDS将难以实现实时入侵检测。

(2) 正常使用模式的建立。智能入侵检测技术大部分都需要先对数据进行训练，从而建立正常使用模式，但要获得“纯净”的数据是比较困难的。在实际应用中获取的数据大都夹杂一些有攻击行为的数据，若将带有攻击行为的数据当成正常数据训练，则建立的模型将不会检测出该种攻击行为。

(3)缺乏精确性和完备性。由于网络系统的日益复杂化，以及各种攻击方法和攻击手段的快速更新，专家系统显得缺乏足够的完备性和准确性，导致根据专家系统建立的IDS缺乏准确性，进而容易造成误报和漏报。

(4)门限值的选定。智能入侵检测技术大都是通过对当前系统/用户行为与正常模型的偏离度来判断是否为入侵行为，每个度对应于一个门限值，若门限值选择过高，则漏警率高；若门限值选择过低，则误警率高。

(5)自防护性不强。由于IDS自身存在着脆弱点，而应对攻击者对IDS本身的攻击的防护手段与技术还不够成熟。

5.2 有待进一步完善的问题

由于智能入侵检测技术存在着或多或少的问题，使得这些技术难以应用于实际，因此大部分都还停留在研究阶段，但智能入侵检测技术所具有的自学习、自适应性的特点，恰是目前计算机安全软件所缺乏而又迫切需要的。有待进一步完善的问题主要有：(1)完善相关技术，对现有算法进行改进或提出新的更高效的算法，例如需要进一步研究数据挖掘的算法，以提高数据挖掘的效率，进而实现海量信息的高效处理；(2)将基于特征分类的检测技术与基于智能因素的检测技术结合，进一步提高IDS的性能；(3)采用数据融合技术，进一步提高IDS检测的准确性；(4)利用Agent及移动Agent技术从检测系统结构设计方面，实现对大型网络、高速网络、分布式异构平台环境的自适应性[10, 11, 16]；(5)综合多种技术构造更完美的混合型入侵检测系统，优化IDS系统各方面的性能；(6)发掘新技术与手段加强对IDS本身的防护。

参考文献

[1] JAMES P, ANDERSON C. Computer security threat monitoring and surveillance[R]. Fort Washington, PA, 1980.

[2] DENING D E, NEUMANN P G.Requirements and model for IDES—a real-time intrusion detection system[R]. Menlo Park, C A, USA: Computer Science Laboratory, Sri International, 1985.

[3] DINNING D E. An intrusion detection model[J]. IEEE Trans. On Software Engineering(Special Issue on Computer Security and Privacy),1987, 13(2):222-223.

[4] ANDERSON D, FRIVOLD T, VALDES S. Next-generation intrusion detection expert system (NIDES): A summary[R]. Menlo Park, California: Computer Science Laboratory, SRI International, 1995.

[5] CANNADY. Artificial neural networks for misuse detection [J].National Information Systems Security Conference, 1998:368-381.

[6] 胡昌振.网络入侵检测原理与技术[M].北京:北京理工大学出版社,2005.

[7] 唐正军,李建华.入侵检测技术[M].北京:清华大学出版社,2004.

[8] 郑成兴.网络入侵防范的理论与实践[M].北京:机械工业出版社,2006.

[9] 于志宏.基于协议分析的入侵检测规则智能匹配[J].吉林大学学报,2008,26(2):157-160.

[10]张云通.移动Agent及其应用[M].北京:清华大学出版社,2002.

[11]谷雨.基于支持向量机与移动Agent的入侵检测模型[J].云南民族大学学报,2008,17(1):68-70.

[12]LIU Yan Heng,TIAN Da Xin,WANG AiNuo. ANNIDS:Intrusion detection system based on artificial neural Network [R]. IEEE International Conference on Machine Learning and Cybernetics,2003,3(2):1337- 1342.

[13]汪兴东.基于BP神经网络的智能入侵检测系统[J].成都信息工程学院学报,2005,20(1):1-4.

[14]刘峰,胡昌振.一种基于系统调用序列的异常检测模型[J].计算机工程,2005,31(11):139-141.

[15]DASGUPTA D. Immunity-based intrusion detection system: a general framework [R]. Proceedings of 2nd National Information Systems Security Conference (NISSC), 1999:60-147.

[16]王海星.基于Mobile Agent的智能化分布式入侵检测系统模型[J].2007(2):57-60.

(收稿日期：2009-05-22)