网络安全预警系统的研究

谢振国，凌 捷
（广东工业大学 计算机学院，广东 广州 510006）

摘 要：网络安全预警技术是实现网络安全检测和预警的一种新技术。对它的研究有助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和提高系统的反应能力等。首先对国内外的预警研究现状进行综述分析；然后，提出了网络安全预警系统的系统结构和工作流程图；最后分析研究构成网络安全系统的检测域、预警代理、区域预警中心等重要组成部分，同时对实现该设计方案所涉及的相关技术和方法进行了研究，这将为下一步网络安全预警系统的实现奠定理论基础。

关键词：网络安全；入侵检测；威胁评估；攻击识别；信息融合
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-629X(2011)11-0250-04

Study of a Network Security and Early-Warning System

XIE Zhen-guo, LING Jie
(College of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Network security warning technology is a kind of new technology in network security. The research on network security warning technology will increase the network systems reaction ability to catastrophe, alleviate the damage of network attack and enhance the system response ability, etc. The summarization of warning studying situation in the world is first presented. Then, the structure and its flow charts of NSES are presented. Finally, analyze the main elements such as detection domain, warning agent and local warning center in advance. Meanwhile study the related technologies and methods for realizing this design scheme, which establishes the academic base for the realizing of NSES.

Key words: network security; intrusion detection; threat assessment; attack recognition; information fusion

0 引 言

随着社会信息化的不断发展，人们对计算机网络的依赖程度也不断提高。与此同时网络本身的安全性也逐渐成为网络应用的重要问题。为了最大程度确保网络安全，传统的网络安全防御采用防火墙、杀毒软件、入侵检测等安全设施。面对日益复杂的网络结构，网络病毒、DDos攻击等构成的威胁和损失不断加大，传统的安全防御措施已满足不了目前网络安全的要求。因此需要更加积极主动的防御技术对网络状况进行保护和预警。网络安全预警技术就是当前一段时间内实时监测和预警的新技术。

鉴于预警技术的重要性，国外已有一些研究机构开展了早期预警系统及入侵检测技术的研究。英国的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)从1997年至2000展开了对信息战攻击评估系统(Information Warfare Attack Assessment System, IWAAS)[1]的开发研究，提出了开发性信息源决策支持系统的框架[2]。

2003年美国在《确保网络空间安全的国家战略》中明确强调需要进一步对网络攻击和网络脆弱性进行战术与战略分析和评估，扩展“网络预警和信息网络”，以支持国土安全部方面协调危机管理，其目的在于加强其网络安全预警与响应能力[3]。

在预警体系结构研究上，Kijewski在文献[4]中给出一个早期预警与攻击识别的信息流程，给出了攻击分析、早期预警单元、检测发生器、知识库之间的流程。胡华平在文献[5]中提出了一个网络安全预警模型，在理论上解决了网络威胁量化的问题。

论文研究工作主要是结合相关的研究成果[6~12]，分析设计了网络安全预警系统模型和网络安全预警系统的检测域、预警代理、区域预警中心等重要组成部

收稿日期：2011-04-01；**修回日期**：2011-07-10
基金项目：广东省自然科学基金(915100900 1000043)；广东省科技计划项目(2009B060700002)；广州市开发区科技计划项目(2009Q-P178)
作者简介：谢振国(1984-)，男，湖南桂阳人，硕士研究生，主要研究方向为网络安全、数据挖掘；凌 捷，教授，主要研究方向为网络与信息安全技术。

分,同时对实现该设计方案所涉及的相关技术和方法进行了研究。

1　网络安全预警系统结构

网络安全预警系统采用分布式结构,主要由检测域、预警代理、区域预警中心这三部分组成。每个检测域中分布多个预警代理,来进行数据包获取、预处理和检测分析。区域预警中心对报警信息进行数据融合分析。

网络安全预警系统的拓扑图如图 1 所示,它主要由检测域、预警代理和区域预警中心三部分组成。检测域包括多个网段,其中包含若干个预警代理。预警代理由分布在不同网段的网络检测机制组成。

经过误用检测和异常检测,把可疑事件和入侵信息发送到区域预警中心,区域预警中心对报警信息进行冗余归并、数据融合,预测当前网络或未来网络可能发生的攻击和进行网络威胁评估,对入侵行为采取一定的安全策略,如发出警报、切断网络等。

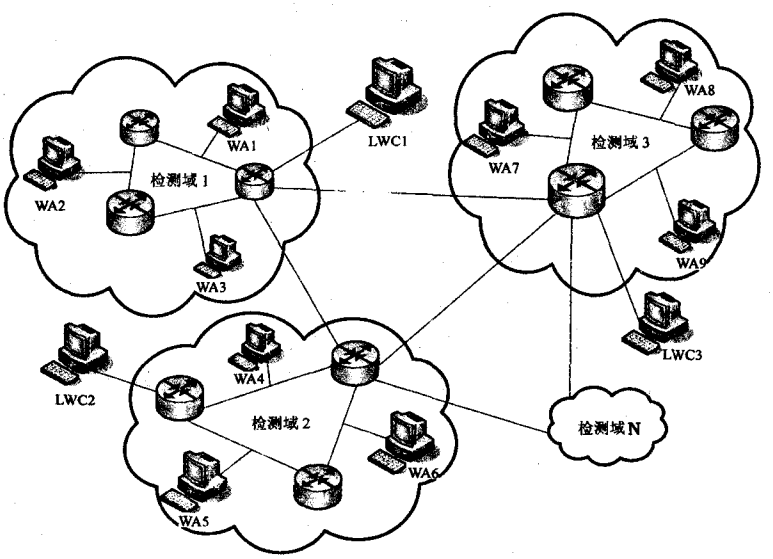

图 1　网络安全预警系统拓扑图

2　系统的工作流程

图 2 给出了系统的工作流程图。首先由检测域采集处理网络数据包,然后将报警信息数据发送到预警代理,对其进行误用检测和异常检测,再经过区域预警中心的冗余归并和关联融合后将确定的入侵事件发送给控制响应模块进行处理,而异常信息根据融合结果进行攻击识别、威胁评测和更新入侵特征,并把报警信息发送给控制响应模块。控制响应模块负责更新入侵模式库和过滤规则库等。

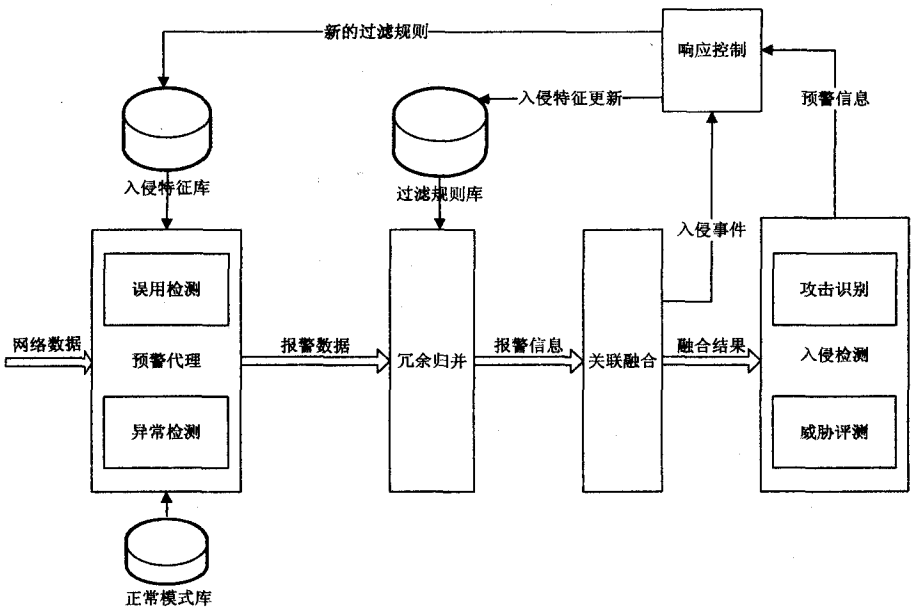

图 2　网络安全预警系统流程图

3　关键模块分析

在网络安全预警系统中,检测域、预警代理、区域中心是三大核心模块,分别代表了网络安全预警的几个不同阶段。数据挖掘、数据融合、模式匹配、神经网络等技术大量地运用于这些模块中,下面对这几个核心模块进行详细的介绍。

3.1　检测域

分布式网络安全预警系统把要保护的网络划分为不同的检测域,每个检测域包含若干个网段。在检测域确定后,其所包含网络的主机 IP 地址也确定了,从而检测域可以与主机 IP 地址范围进行绑定。检测域中包含主机、交换机、路由器、防护墙和各种应用服务器等。在检测域中,还加入了两大安全主件预警代理(Warning Agent,WA)和区域预警中心(Local Warning Center,LWC)从事报警信息分析和响应。

3.2　预警代理模块

预警代理模块的设计如图 3 所示,在每个网段中都有一个预警代理,它负责对本网段数据的获取、预处理和检测分析。经过检测分析后把报警信息传送到区域预警中心。将数据检测分析放在预警代理而不是放在区域预警中心,因为这样可以减少网络数据传送到

区域预警中所带来的网络开销，平衡各个检测域的数据检测效率，从而提高实时性和并行性[6]。

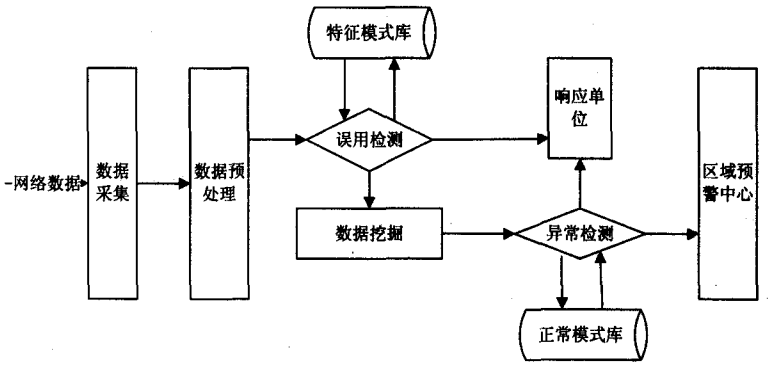

图 3 预警代理模块设计

数据的获取可以通过将网卡设置为混杂模式的方式得到。对捕获的数据包先进行预处理，将数据转换为相应的数据处理格式，然后进行检测分析。

由于对已知的攻击类型的检测，误用检测有较高的检测率，但是对于未知的、新的攻击误用检测的效果不是很理想，所以先进行误用检测再进行异常检测。这里采用误用检测和异常检测相结合的检测方法。这样就可以从中发现网络攻击和可疑信息，并对攻击行为进行报警响应。

对于误用检测，由于数据包中存在一部分冗余的信息，不能直接用于预测，需要进行特征提取，然后运用分类算法如 C4.5 和 RIPPER 算法进行分类，建立分类模型。而异常检测的关键在于正常行为模式的建立，在现有的几种异常检测的算法，研究表明基于数据挖掘的密度聚类和层次聚类检测率较高，误报率较低，缺点是不能够分辨各种攻击类型[7]。可以将几种检测算法融合使用，利用原有的优点，并加以改进，各取长处提取出正常情况下网络用户行为模式。

3.3 区域预警中心

区域预警中心对预警代理传送的报警数据先进行冗余归并，然后进行数据融合分析，发现事物之间的因果联系，实现报警关联。预测网络可能遭受的攻击和对本区域的网络进行威胁评测，对攻击行为进行响应并向检测域发送预警信息。区域预警中心的设计如图 4 所示。

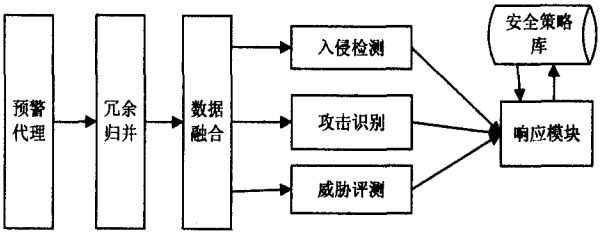

图 4 区域预警中心设计

区域预警中心对本检测域的所有预警代理传送的报警信息进行检测分析，同时结合本地知识库进行数据融合分析。每个区域预警中心都有一张检测域和其对应的主机 IP 地址映射表。如果区域预警中心产生预警，则根据检测到数据的检测域与 IP 地址的映射表，将报警信息发送到相应的检测域。

区域预警中心是网络安全预警系统的核心模块，它的主要功能是对报警信息进行冗余归并、信息关联融合、攻击识别、威胁评测和信息控制管理。

(1)报警信息冗余归并。

把预警代理模块传送的报警信息先进行初步处理，使具有明显特征且具有很高响应级优先级的报警信息及时响应。

(2)信息关联融合。

信息的关联融合处理，是对报警信息在冗余归并后的进一步分析，即报警关联分析和数据融合。对数据融合分析的三种结果(入侵、异常、正常)采取相应的分析响应模式：对于入侵信息直接发送至控制响应模块，并由控制响应模块向检测域发送预警信息；对于异常信息发送至攻击识别模块，根据攻击预测结果识别入侵行为，并由控制响应模块向对应的检测域发送报警信息；对于正常信息，则忽略本次报警信息。

(3)网络攻击识别。

对预警代理检测后的报警信息，经过冗余归并和数据融合处理，预测未来网络可能遭受的攻击，发出预警信息。

引入攻击轨迹链的方法，攻击轨迹链[8]是指攻击者从发起攻击到攻击结束的每一个环节按时序排列所构成的轨迹链。攻击轨迹链是攻击过程中从攻击者视角到防御者视角转换的对映物，它能清晰完整地反映攻击者的攻击逻辑步骤。攻击轨迹链在逻辑上表现出一种因果关系，攻击者往往通过一个因果关系的攻击序列体现出其攻击意图。例如，攻击者发动攻击 A 为攻击 B 做准备，则攻击 A 触发的报警 X 与攻击 B 触发的报警 Y 之间满足因果关系。挖掘出攻击行为的关联序列，对报警信息进行因果分析，从而发现攻击者的意图。

(4)网络威胁评测。

威胁评测的主要功能是以本区域内一段时间内的网络入侵攻击行为为基础，再结合本区域网络的控制策略和安全防护能力，得到局部攻击对区域网络安全的影响，并进行安全预警。

对于威胁评测，可以将网络划分为 LAN、主机、服务和主机/漏洞这四个层次。预警系统的安全状况可以通过服务、主机、系统 LAN 这三个方向进行评测。每个层次的安全状况可以分解为其下层各节点的安全

状况的“和”，这样将下层的各个节点联系起来，形成对上层节点的安全状况的评测，即威胁评测的结果[9]。

(5)信息控制管理。

对上传来的报警信息进行存储和管理，并建立相关的入侵行为的知识库，主要功能是描述当前的网络安全状况、攻击者的攻击历史等，为攻击识别和威胁评测提供依据。

4 结束语

开展对网络安全预警的研究，可以更加有效地保障网络信息安全。网络安全预警对于提高网络系统的应急响应能力，缓解网络入侵攻击所带来的危害，提高系统的反击能力等具有十分重要的意义。国内目前对于网络安全预警的研究最近才开始，相关理论和技术也才刚刚兴起。

文中在深入分析国内相关研究后，建立了网络安全预警系统的结构和工作流程图，分析研究网络安全预警系统的检测域、预警代理模块、区域预警中心模块等重要组成部分。网络安全预警技术中诸如基于数据挖掘的检测技术、数据融合、可视化等方面有许多问题需要研究。

参考文献：

[1] Rathmell A, Overill R, Valeri L. Information Warfare Attack Assessment System[EB/OL]. 2003. http://www.kcl.ac.uk/orgs/icss/Old/iwaasppr.PDF.

[2] Sandia National Laboratories. US Infrastructure Assurance Strategic Roadmaps-Strategies for Preserving Our National Security[R]. [s.l.]: Sandia National Laboratories, 1998.

[3] The national strategy to secure cyberspace[EB/OL]. 2003. http://www.us-cert.gov/readingroom/cyberspace strategy.pdf.

[4] Kijewski P. ARAKIS-An earlywarning and attack identification system[C]//The 16th Annual First Conf. Dudapest, Hungary: [s.n.], 2004.

[5] 胡华平，何利民，肖枫涛，等. 网络安全预警模型的研究[J]. 计算机研究与发展，2006，43(z2)：353-359.

[6] 张险峰，秦志光，刘锦德. 网络安全分布式预警体系结构研究[J]. 计算机应用，2004，24(5)：42-49.

[7] 胡　亮，金　刚，于　满，等. 基于异常检测的入侵检测技术[J]. 吉林大学学报理学版，2009，47(6)：1264-1270.

[8] 刘上伟. 基于网络的分布式安全预警系统的研究与设计[D]. 成都：四川大学，2006.

[9] 陈彦德，赵陆文，王　琼，等. 网络安全态势感知系统结构研究[J]. 计算工程与应用，2008，44(1)：100-102.

[10] 彭云峰，沈明玉. 入侵防御系统在应急平台的应用研究[J]. 计算机技术与发展，2009，19(2)：162-164.

[11] 孙怿昉. 数据挖掘在入侵检测系统中的应用研究[D]. 大连：大连海事大学，2008.

[12] 李　生，邓一贵，唐学文，等. 基于移动代理的分步式入侵检测系统的研究[J]. 计算机技术与发展，2009，19(9)：132-135.

(上接第 249 页)

布系统、密码服务系统相互配合，部署在省级工商行政管理局电子政务外网中，通过互联网与电子商务网站相连，提供网络亮照服务。

3 结束语

网络身份识别系统是密码技术与工商行政管理业务相结合的产物，适用于工商行政管理行业，支撑工商行政管理部门颁发，具有权威性、防伪性和全国一致性的营业执照电子副本，有效保障工商行政管理部门对网络市场的监管和服务，有利于促进我国电子商务又好又快的发展。

参考文献：

[1] 范玉贞. 我国电子商务发展对经济增长作用的实证研究[D]. 上海：上海师范大学，2010.

[2] 王珏辉. 电子商务模式研究[D]. 长春：吉林大学，2007.

[3] 荆继武，林璟锵，冯登国. PKI 技术[M]. 北京：科学出版社，2008.

[4] 邓晓军. PKI 技术及其应用的分析[J]. 计算机技术与发展，2008，18(6)：144-147.

[5] 冯相忠. 基于 J2EE 技术的电子商务系统的开发[J]. 计算机技术与发展，2007，17(8)：33-36.

[6] Zhang Jinlong, Du Xiaofang. A Study on the Application Model of B2B E-Commerce in the Agricultural Sector[J]. Journal of Electronic Science and Technology of China, 2004(3): 134-139.

[7] Pei Songwen, Wu Baifeng, Zhu Kun, et al. Novel Software Automated Testing System Based on J2EE[J]. Tsinghua Science and Technology, 2007(s1): 51-56.

[8] He Xinwen, Wang Xuehua. Strategic Analysis and Choice for Forestry Enterprises Developing E-business[J]. Chinese Forestry Science and Technology, 2007(4): 80-88.

[9] 信息技术安全技术公钥基础设施在线证书状态协议[S]. 中华人民共和国国家标准，2005.

[10] 侯　灿，杨宗凯，刘　威. J2EE 架构下连接池技术的应用与改进[J]. 计算机技术与发展，2006，16(10)：8-10.

[11] 张登辉，高　济. 基于 Web Service 的可组合电子商务实验平台[J]. 计算机技术与发展，2006，16(2)：110-113.

[12] 网络商品交易及有关服务行为管理暂行办法[S]. 国家工商行政管理总局，2010.

[13] 张大强，殷世民，程家兴，等. 基于 Web Service 的电子商务体系结构[J]. 计算机技术与发展，2006，16(7)：23-25.