网络态势感知系统研究综述*)

王慧强 赖积保 朱 亮 梁 颖
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 开展网络态势感知系统 NSAS(Network Situation Awareness System,也称 Cyberspace Situation Awareness System)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,发现潜在恶意的入侵行为,提高系统的反击能力等具有十分重要的意义。本文首先给出了态势感知的概念及发展 NSAS 的必要性;其次介绍了网络态势感知的概念,并对相关概念以及 NSAS 与 IDS(Intrusion Detection System)的区别与联系进行了讨论,详细综述了国内外 NSAS 的研究现状。以此为基础提出了 NSAS 的框架,并着重对相关的关键技术与难点问题进行了论述。最后给出了 NSAS 今后的发展方向。

关键词 态势感知,网络态势感知系统,数据挖掘,数据融合,态势可视化

Survey of Network Situation Awareness System

WANG Hui-Qiang LAI Ji-Bao ZHU Liang LIANG Ying
(College Computer Science & Technology, Harbin Engineering University, Harbin 150001)

Abstract The study of NSAS(Network Situation Awareness System or Cyberspace Situation Awareness System) has great importance in improving abilities of responding to emergences, reducing losses of network attacks, revealing abnormally intrusions and enhancing system abilities of fighting back. At first, the definition of situation awareness and the necessity of developing NSAS were given. Then, the definition of NSAS was presented and relationships of NSAS and IDS were discussed. The summarization of studying situation in the world is presented. The architecture of NSAS was proposed in the following. The key technology and difficulties related to building NSAS prototype are discussed. In the end, the future development of NSAS was described.

Keywords Situation awareness, Network situation awareness system, Data mining, Data fusion, Situation visualization

1 引言

态势感知(Situation Awareness)这一概念源于航天飞行的人因(Human Factors)研究[1],此后在军事战场、核反应控制、空中交通监管(Air Traffic Control, ATC)以及医疗应急调度等领域被广泛地研究。态势感知之所以越来越成为一项热门研究课题,是因为在动态复杂的环境中,决策者需要借助态势感知工具显示当前环境的连续变化状况,才能准确地做出决策。1988 年,Endsley 在文[2]中把态势感知定义为"在一定的时空条件下,对环境因素的获取、理解以及对未来状态的预测",整个态势感知过程可由如图 1 所示的三级模型直观地表示出来。

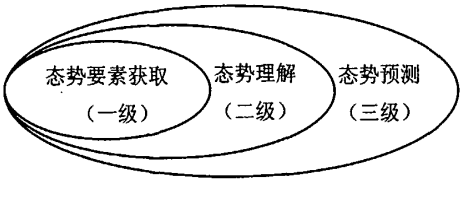

图 1 态势感知的三级模型

目前随着 Internet 的发展普及,网络的重要性及其对社会的影响越来越大,网络安全问题也越来越突出,并逐渐成为 Internet 及各项网络服务和应用进一步发展所亟需解决的关键问题。此外,随着网络入侵和攻击行为正向着分布化、规模化、复杂化、间接化等趋势发展,势必对安全产品技术提出更高的要求。国家计算机网络应急技术处理协调中心(CNCERT/CC)在发布的《2004 年网络安全工作报告》中提到了 2004 年 4 月 11 日发生的全国性断网事件,再次向我们敲响警钟,也充分暴露了我国网络安全体系的脆弱。而现有安全产品(如 IDS)也无法监控防御此类事件。因此迫切需要研究一项新技术来实现大规模网络的安全态势监控。基于上述原因,提出了 NSAS 的研究,旨在对网络态势状况进行实时监控,并对潜在的、恶意的网络行为变得无法控制之前进行识别,给出相应的应对策略。

2 网络态势感知系统

2.1 网络态势感知概念

网络态势感知源于空中交通监管(Air Traffic Control, ATC)态势感知,是一个比较新的概念,并且在这方面开展研究的个人和机构也相对较少。1999 年,Tim Bass 在文[3]中首次提出了网络态势感知(Cyberspace Situation Awareness)这个概念,并对网络态势感知与 ATC 态势感知进行了类比,

*)高等学校博士学科点专项科研基金项目(20050217007)、国防预研重点资助项目(413150702)、武备预研基金资助项目(51416060104CB0101)。王慧强 博士、教授、博导,研究方向为可靠性理论、计算机网络;赖积保 博士研究生,研究方向为计算机网络、信息安全;朱 亮 硕士研究生,研究方向为信息安全;梁 颖 博士研究生,研究方向为计算机网络、数据融合。

旨在把 ATC 态势感知的成熟理论和技术借鉴到网络态势感知中去。

目前，对网络态势感知还未能给出统一的、全面的定义。所谓网络态势是指由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势。值得注意的是，态势是一种状态，一种趋势，是一个整体和全局的概念，任何单一的情况或状态都不能称之为态势。网络态势感知是指在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

2.2 相关概念比较

下面从网络态势研究的角度出发，对态势评估(Situation Assessment)、威胁评估(Threat Assessment)以及态势感知(Situation Awareness)三者之间的关系进行简单阐述。三者关系如图 2 所示。态势评估和威胁评估分别是态势感知过程的一个环节。威胁评估是建立在态势评估的基础之上的。

态势评估包括态势元素提取、当前态势分析和态势预测，涵盖以下几个方面：1)在一定的网络环境下，提取进行态势估计要考虑的各要素，为态势推理做准备；2)分析并确定事件发生的深层次原因，例如网络流量异常；3)已知 T 时刻发生的事件，预测 $T+1, T+2, \cdots, T+n$ 时刻可能发生的事件；4)形成态势图。态势评估的结果是形成态势分析报告和网络综合态势图，为网络管理员提供辅助决策信息。

威胁评估是关于恶意攻击的破坏能力和对整个网络威胁程度的估计，是建立在态势评估的基础之上的。威胁评估的任务是评估攻击事件出现的频度和对网络威胁程度。态势评估着重事件的出现，威胁评估则更着重事件和态势的效果。

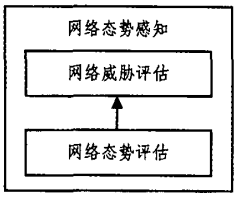

图 2 网络态势感知、态势评估与威胁评估关系图

2.3 NSAS 与 IDS 比较

NSAS 与现有的 IDS 之间有区别也有联系。二者的区别主要体现在：

(1)系统功能不同。IDS 可以检测出网络中存在的攻击行为，保障网络和主机的信息安全。而 NSAS 的功能是给网络管理员显示当前网络态势状况以及提交统计分析数据，为保障网络服务的正常运行提供决策依据。这其中既包括对攻击行为的检测，也包括为提高网络性能而进行的维护。

(2)数据来源不同。IDS 通过预先安装在网络中的Agent 获取分析数据，然后进行融合分析，发现网络中的攻击行为。NSAS 采用了集成化思想，融合现有 IDS、VDS(Virus Detection System)、FireWall、Netflow(内嵌在交换机和路由器中的流量采集器)等工具提供的数据信息，进行态势分析与显示。

(3)处理能力不同。网络带宽的增长速度已经超过了计算能力提高的速度，尤其对于 IDS 而言，高速网络中的攻击行为检测仍然是有待解决的难点问题。NSAS 充分利用多种数据采集设备，提高了数据源的完备性，同时通过多维视图显示，融入人的视觉处理能力，简化了系统的计算复杂度，提高了计算处理能力。

(4)检测效率不同。IDS 不仅误报率和漏报率高，而且无法检测出未知攻击和潜在的恶意网络行为。NSAS 通过对多源异构数据的融合处理，提供动态的网络态势状况显示，为管理员分析网络攻击行为提供了有效依据。

同时，NSAS 与 IDS 也存在一定的联系。其中 IDS 便可作为 NSAS 的数据源之一，为其提供所需数据信息。

2.4 相关工作

自 Tim Bass 提出了网络态势感知概念后，随即在文[4]中提出了基于多传感器数据融合的入侵检测框架，并把该框架用于下一代入侵检测系统和 NSAS。采用该框架能够实现入侵行为检测、入侵率计算、入侵者身份和入侵者行为识别、态势评估以及威胁评估等功能。Stephen G. Batsell[5]、Jason Shifflet[6]等人也提出了类似的模型。开展这项研究的个人还有 A. DeMontigny-Leboeuf[7]、伊利诺大学香槟分校(University of Illinois at Urbana- Champaign)的 William Yurcik[8]等。接下来简单介绍几种现有的 Internet 级网络态势感知工具。

美国劳伦斯伯克利国家实验室(Lawrence Berkeley National Labs)的 Stephen Lau 于 2003 年开发了“The Spinning Cube of Potential Doom”[9]系统，该系统在三维空间中用点来表示网络流量信息(在笛卡儿坐标系中，即 X 轴代表网络地址，Y 轴代表所有可能的源 IP，Z 轴代表端口号)，极大地提高了网络态势感知能力。卡内基梅隆大学 SEI(Software Engineering Institute)所领导的 CERT/NetSA(The CERT Network Situational Awareness Group)开发出 SILK[10](the System for Internet-Level Knowledge)，该系统采用集成化思想，即把现有的 Netflow 工具集成在一起，提供整个网络的态势感知，便于大规模网络的安全分析。美国国家高级安全系统研究中心(National Center for Advanced Secure Systems Research, NCASSR)正在进行的 SIFT[11](Security Incident Fusion Tool)项目，欲通过开发一个安全事件融合工具的集成框架，为 Internet 提供安全可视化。目前该机构已开发的 Internet 安全态势感知软件有：NVisionIP，VisFlowConnect-IP，UCLog+等。NVisionIP[12,13]通过系统状态可视化来获取 Internet 的安全态势感知；VisFlowConnect-IP[14,15]通过连接分析可视化来获取 Internet 的安全态势感知；UCLog+[16]是安全态势感知数据库系统，用于事件存储、事件查询以及事件关联。

其他研究机构还有美国国防部计算机安全中心(National Computer Security Center of Department of Defense)、美国空军(US Air Force)、加拿大国防研究与开发中心(Defence R&D Canada)，以及瑞士联邦技术院(Swiss Federal Institute of Technology Zurich, ETH Zurich)等。

鉴于当前网络的现状、发展以及入侵与攻击行为所造成的巨大损失，有关政府部门已经意识到开展网络态势感知研究的必要性。美国国防部在 2005 年的财政预算报告[17]中就包括了对网络态势感知项目的资助，并提出分三个阶段予以实现，分别为：第一阶段完成对大规模复杂网络行为可视化新算法和新技术的描述和研究，着重突出网络的动态性和网络数据的不确定性；第二阶段基于第一阶段所研究的工具和方法，实现和验证可视化原型系统；第三阶段实现可视化算法，提高网络态势感知能力。美国高级研究和发展机构(Advanced Research and Development Activity, USA)[18]在 2006 年的预研计划中，明确指出网络态势感知的研究目标和关键技术。研究目标是以可视化的方式为不同的决策者和分析员

提供易访问、易理解的信息保障数据——攻击的信息和知识、漏洞信息、防御措施等等；关键技术包括数据融合、数据可视化、网络管理工具集成技术、实时漏洞分析技术等等。

国内对网络态势感知的研究才刚刚起步。冯毅在文[19]中从我军信息与网络安全的角度出发，阐述了我军积极开展网络态势感知研究的必要性和重要性，指出了两项关键技术——多源传感器数据融合和数据挖掘。国内其它相关研究主要是围绕网络安全态势评估、大规模网络预警等来开展的。在网络安全态势评估方面，西安交通大学实现了基于 IDS 和防火墙的集成化网络安全监控平台[20]，该系统实现了态势评估；并在文[21]中提出了一个基于统计分析的层次化安全态势量化评估模型，该模型从上到下分为系统、主机、服务和攻击/漏洞 4 个层次，并且采用了自下而上、先局部后整体的评估策略及相应计算方法。北京理工大学信息安全与对抗技术研究中心研制了一套基于局域网络的网络安全态势评估系统[22]，由网络安全风险状态评估和网络威胁发展趋势预测两部分组成，用于评估网络设备及结构的脆弱性、安全威胁水平等。在大规模网络预警方面，国防科技大学的胡华平等人[23]提出了面向大规模网络的入侵检测与预警系统的基本框架及其关键技术与难点问题。从以上的阐述，我们不难发现国内在网络安全态势评估和大规模网络预警所开展的研究，还存在诸如实时性不强、数据源单一等问题。

3 通用的 NSAS 框架

通过对美国国防部 JDL[24]（Joint Director of Laboratories）给出的 JDL 模型和 Endsley 所给出的态势感知模型[25]的分析研究，本文提出了 NSAS 的总体框架结构，如图 3 所示。NSAS 主要包括多源异构数据采集、数据预处理、事件关联与目标识别、态势评估、威胁评估、响应与预警、态势可视化显示以及过程优化控制与管理等 7 个部分。

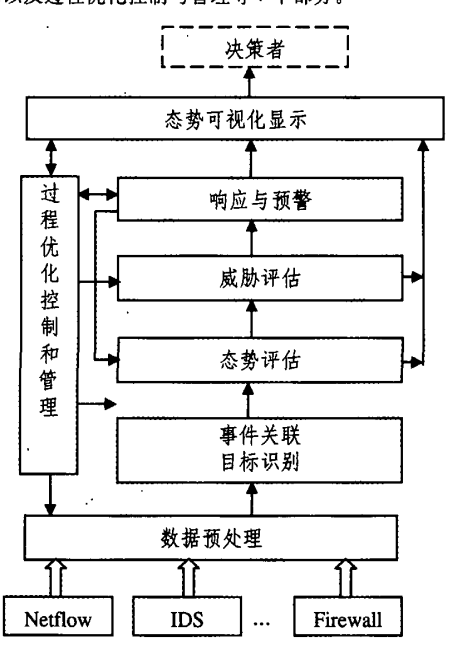

图 3 NSAS 框架

多源异构数据采集是通过分布在各个企事业单位现有的 Netflow 采集器、IDS、Firewall、VDS 等来实现的。如果有特殊需要，也可在相应的关键节点布置新的采集设备。数据预处理主要完成数据筛选、数据简约、数据格式转换以及数据存储等功能。事件关联与目标识别采用数据融合技术对多源异构数据从时间、空间、协议等多个方面进行关联和识别。态势评估和威胁评估在前面已有较为详细的介绍，在这就不重复该部分内容。响应与预警主要依据事件威胁程度给出相应的响应和防御措施，再把响应预警处理后的结果反馈给态势评估，来辅助态势评估。态势可视化为决策者提供态势评估结果（包括当前态势及未来态势）、威胁评估结果等信息的显示。过程优化控制与管理主要负责从数据采集到态势可视化的全过程优化控制与管理工作，同时将响应与预警和态势可视化的结果反馈到过程优化控制与管理模块，实现整个系统的动态优化，达到网络态势监控的最佳效果。

4 关键技术

大规模网络节点众多，分支复杂，数据流量大，并且包含多个网段，存在多种异构网络环境和应用平台。随着网络入侵和攻击正在向分布化、规模化、复杂化、间接化的趋势发展，为了实时、准确地显示整个网络态势状况，检测出潜在、恶意的攻击行为，NSAS 必须解决相应的技术问题。

4.1 数据挖掘

针对网络日益增长的数据量与要求快速分析数据之间的矛盾，采用数据挖掘技术，旨在从海量数据中发现有用的、可理解的数据模式，便于检测未知攻击和自动构建检测模型。

数据挖掘是指从大量的数据中挖掘出有用的信息，即从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中发现隐含的、规律的、人们事先未知的，但又有潜在用处的并且最终可理解的信息和知识的非平凡过程（Nontrivial Process）[26]。所提取的知识可表示为概念（Concept）、规则（Rules）、规律（Regularities）、模式（Pattern）等形式。数据挖掘是知识发现（Knowledge Discovery in Database，KDD）的核心环节。

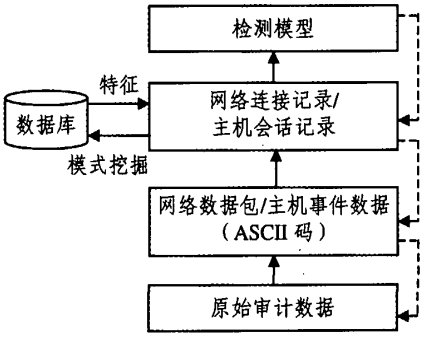

图 4 入侵检测的数据挖掘框架

数据挖掘是在 1989 年 8 月举行的第 11 届国际联合人工智能学术会议上首次提出，并从 1995 年加拿大召开的第 1 届知识发现和数据挖掘国际学术会议后开始掀起研究的热潮。该技术现已逐步应用到网络安全领域。美国哥伦比亚大学的 Wenke Lee[27,28] 等人最早将数据挖掘引入到入侵检测领域，并系统提出了用于入侵检测的数据挖掘框架，如图 4 所示。其它将数据挖掘技术应用到入侵检测领域的成果还有 MADAMID[29]（Mining Audit Data for Automated Models for Intrusion Detection），IDDM[30]（Intrusion Detection Using Data

Mining)等。在网络态势感知方面，K. Lakkaraju[12]、Yin Xiaoxin[14]等人虽然在各自的研究中把数据挖掘作为一项关键技术提到，但均未展开阐述。

从数据挖掘应用到入侵检测领域的角度来讲，目前主要有4种分析方法[26,31]：关联分析、序列模式分析、分类分析和聚类分析。关联分析用于挖掘数据之间的联系，即在给定的数据集中，挖掘出支持度和可信度分别大于用户给定的最小支持度(minimum support)和最小可信度(minimum confidence)的关联规则，常用算法有Apriori算法、AprioriTid算法等。序列模式分析和关联分析相似，但侧重于分析数据间的前后(因果)关系，即在给定的数据集中，从用户指定最小支持度的序列中找出最大序列(maximum sequence)，常用算法有DynamicSome算法、AprioriSome算法等。分类分析就是通过分析训练集中的数据，为每个类别建立分析模型，然后对其它数据库中的记录进行分类，常用的模型有决策树模型、贝叶斯分类模型、神经网络模型等。与分类分析不同，聚类分析不依赖预先定义好的类，它的划分是未知的，常用的方法有模糊聚类法、动态聚类法、基于密度的方法等。关联分析和序列模式分析主要用于模式发现和特征构造，而分类分析和聚类分析主要用于最后的检测模型。

目前数据挖掘在网络安全领域有着很好的发展前景，但仍有一些问题有待解决。如数据挖掘前期所需要的训练数据来之不易；从大量数据中进行挖掘，很费时间和资源，很难保证实时性等。如何将数据挖掘与机器学习、模式识别、归纳推理、统计学、数据库、数据可视化和高性能计算等相关领域有机结合，达到挖掘有用信息的最佳效果，还有待进一步研究。

4.2 数据融合

数据融合技术出现于20世纪80年代，真正得到发展则是在90年代。该项技术发展之初就在军事领域得到了广泛的重视和应用。目前所说的数据融合这一概念来源于早期军事领域，主要研究在现代战场中对多源信息的快速有效处理。美国国防部JDL[24]从军事应用角度给出了数据融合的定义。目前数据融合的应用已拓展到图像融合、机器人传感处理、网络安全等领域。

为了保证网络空间的安全性，针对当前IDS系统误报率高和对时间及空间上分散的协同攻击无法有效检测的缺陷，引入了数据融合技术。在文[32]中，Christos Siaterlis和Basil Maglaris运用该技术设计出检测DDoS攻击的模型，验证了数据融合是一种可以有效增加DDoS检测率、降低虚警率的方法。这里所研究的数据融合技术是指对来自网络环境中的具有相似或不同特征模式的多源信息进行互补集成，从而获得对当前网络状态的准确判断。Tim Bass在文[33]中首次提出将JDL模型直接运用到网络态势感知领域，这为以后数据融合技术在网络态势感知领域的应用奠定了基础，是该技术在此领域应用的一个起点。Jason Shifflet[6]运用数据融合技术构造了一个网络入侵检测模型，实现了网络空间的态势感知。国内也有一些科研机构尝试把数据融合技术应用到网络安全领域，提出了应用数据融合技术的网络安全分析评估系统[34]、入侵检测系统[35]等。

目前用于数据融合领域的典型算法有贝叶斯网络和D-S证据推理[36]。贝叶斯网络是神经网络和贝叶斯推理的结合。它使用节点和弧来代表域知识，节点之间可通过弧来传播新的信息。网络中保存的知识可以由专家指定，也可以通过样本进行学习。贝叶斯网络还使用了具有语义性的贝叶斯推理逻辑，它更能反映容易理解的推理过程，因此也在具有内在不确定性的推理和决策问题中得到了广泛的应用。作为一种知识表示和进行概率推理的框架，将贝叶斯网络应用于态势感知，具有广阔的发展前景。

D-S证据理论是Dempster于20世纪60年代提出的，试图用概率上下限来表示实际问题中的不确定性。Shafer对它做了进一步的发展，并使之系统化、理论化，形成了一种不确定推理理论，即D-S证据理论。它允许人们对不精确和不确定性问题进行建模、推理，为融合不确定信息提供了一条思路；另外，它不要求融合信息具有同类性，因而在融合处理异类、同步、异步信息方面优势也很明显。但是，在证据严重冲突的情况下，组合结果往往与实际情况不相符。

基于上述知识我们不难发现，设计出高效、快速的融合算法是数据融合技术快速发展的关键。这就要求我们综合运用多学科的知识，进一步设计出完善的算法，将有利于数据融合技术更好地用于网络态势感知。

4.3 态势可视化

态势生成是依据大量数据的分析结果来显示当前状态和未来趋势，而通过传统的文本形式，无法直观地将结果呈现给用户。可视化技术正是通过将大量的、抽象的数据以图形的方式表现，实现并行的图形信息搜索，提高可视化系统信息处理的速度和效率。

从计算机安全领域的角度来看，可视化技术最初是用来实现对系统日志或者IDS日志的显示。T. Takata和H. Koike开发的Mielog[37]可以实现日志可视化和统计分析的交互式系统，依据日志的分类统计分析结果，进行相应的可视化显示。H. Koike和K. Ohno专门为分析Snort日志以及Syslog数据开发的SnortView[38]系统，可以实现每2min对视图的一次更新，并可以显示4h以内的报警数据。R. Danyliw的ACID(the Analysis Console for Intrusion Databases)系统[39]也是为分析Snort日志而设计，使用基于Web的接口，在HTML中以图标的形式表示报警信息。R. Bacher基于Hummer IDS采集的日志实现了Erbacher's Hummer IDS可视化系统[40]。

然而，基于日志数据的可视化显示受到日志本身特性的限制，实时性不好，需要较长的时间才能上报给系统，无法满足实时性要求高的网络需求，因此提出了基于数据流的可视化工具。The spinning cube of the potential doom工具[9]是由Stephen Lau开发的，为了能在三维空间中尽可能多地显示网络中实时存在的信息，首次采用了"点"表示连接的方法，在一定程度上消除了视觉障碍的影响，起到了比较好的效果。由Gregory Conti和Kulsoom Abdullah开发的可视化工具[41]通过对网络流量的实时监控，能够提取出网络攻击行为的特征。由Sven Krasser等人开发的SecViz[42]在三维的可视化视图中，以离散的、平行的点表示捕获的数据，使得一些网络攻击行为在视图中显示得十分明显，易于发现。

对于大规模的网络，主机间的数据交换以及连接的建立活动非常频繁，仅依靠流量数据无法准确地判断网络态势，于是提出了基于多数据源、多视图的可视化系统。C. P. Lee等人提出的Visual Firewal系统[43]基于Model View Controller(MVC)的事件驱动结构，有两个数据源：IDS警报以及防火墙事件数据。系统使用Java语言实现，借助于JOGL和JFreechart实现图形的可视化。系统中采用了4种视图：real-time traffic view；visual signature view；statistic view；IDS a-

larm view,分别显示了 network traffic、packet flow、throughput、可疑行为的视图显示,为网络的整体态势提供了一个全面的显示。NCSA 的 SIFT(Security Incident Fusion Tools)也着重于将安全信息可视化,开发了 NVisionIP[12]、VisFlowConnect[14]等工具,它们都是基于 NetFlow 设计的。在实现时使用了两个数据源:一个是由 CISCO 路由器上得到的 NetFlows,另一个是从 tcpdump 数据中得到的 Argus NetFlows。在显示结果上,二者都不仅仅针对入侵行为的显示,而是对整体态势的显示。二者最大的区别是 NVisionIP 提供的是基于主机的视图,VisFlowConnect 提供的是基于连接的视图。

随着可视化技术在安全态势领域的应用,有人提出应将可视化应用于网络态势感知的整个过程。如图 5 所示,Anita D'Amico 和 Michael Kocka 在文[44]中详细阐述了可视化技术在安全态势每个阶段的重要作用,并对今后的发展提出了展望。

目前,可视化技术可以按近实时地显示多达 2.5 个 B 类 IP 地址空间内主机(约 65532×2.5=163830)的网络行为[45]。但随着网络规模的不断扩大,攻击行为的隐蔽性日益提高,对可视化技术又提出了许多新的要求。如何将基于主机的数据和基于网络的数据显示方法进行有机的结合,确定态势显示的统一规范,提高显示的实时性,增大系统可显示的规模,增强人机交互的可操作性等都是可视化技术需要进一步解决的问题。

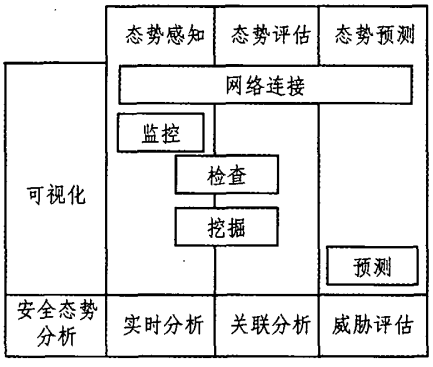

图 5 安全态势与可视化技术的关系

4.4 其它技术

其它 NSAS 技术包括数据校准、数据格式统一、数据简约、响应与预警技术、入侵追踪等。数据校准是为了在时间和空间上将多源异构采集器校准到统一参数点。数据格式统一是为了将多源异构数据经数据格式转换,形成统一的数据格式,便于随后的事件关联、目标识别等进行高效处理。数据简约主要是去除数据中包含的冗余信息,防止大规模网络中的数据泛滥,减少数据的传输总量,提高后续数据分析的效率。响应与预警技术主要研究灵活高效的响应政策、响应机制以及防御措施等。入侵追踪的研究重点是发现攻击者的数据传输路径和真实 IP 地址,实现对攻击者的定位;网络入侵的追踪是对网络入侵进行正确响应的重要前提。

5 难点问题

NSAS 要达到实用化水平,监控整个网络的态势状况,还必须考虑如下难点问题:

(1)跨机构的扩展性。由于很多机构组织采用不同厂商的网络设备,使得要监控整个网络的安全态势状况变得非常困难。应该建立一套机制,达到不同厂家安全产品之间的协作以及不同组织之间信息的协作。

(2)不断增长的网络复杂性。目前网络之间依赖的程度越来越大,网络体系结构日益复杂,黑客实施的攻击行为造成的后果也越来越严重。这就要求系统应该具有高度灵活性,能够适应网络结构的变化,迅速对全网的态势做出判断。

(3)多点事件关联。针对网络攻击行为分布性等特点,要求系统能够收集并关联多源异构数据,及时发现可疑事件,并准确地予以判断。

(4)态势可视化显示。在结果的可视化阶段,由于数据规模的原因,如何在全面而客观地显示库中数据的前提下保证具有良好的视觉效果,是一个难点问题。

(5)降低对新攻击行为的响应时间。

(6)网络额外负荷。由于网络在不断变化壮大,网络态势感知要具有一定的实时性,并且要尽量降低所带来的额外网络负载,与探测点的数目和探测的周期有关。

(7)系统容错性。当故障存在的情况下保障系统不失效,仍然能够正常工作的特性,在网络环境中具有十分重要的意义。

结论及展望 为了保障网络信息安全,开展大规模网络态势感知是十分必要的,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、发现潜在恶意的入侵行为、提高系统的反击能力等具有十分重要的意义。网络态势感知技术作为一项新技术,有很大的发展空间,同时在其发展过程中,应该把握好以下几个方面的内容:

(1)能对大规模网络进行实时或者近实时的态势感知,快速准确地判断出网络安全状态,实现实时的态势可视化显示,并能利用网络安全属性的历史记录,为用户提供一个比较准确的网络安全演变趋势。

(2)具有前向预测功能。在网络安全事件发生之前进行预测,为网络管理员制定决策和防御措施提供依据,做到防患于未然。

(3)自动响应。依靠人为干预对入侵进行反击是不可行的,需要 NSAS 自动阻止、反击入侵,而不是仅仅报警。

(4)智能化。通过采用诸如神经网络、遗传算法以及专家系统,使 NSAS 具有自学习和自适应能力。

(5)能检测和防御分布式攻击(如 DDOS),并能很好地检测出未知攻击和潜在的恶意网络行为。

(6)交互方便、易于使用。免去繁琐的配置与安装,便于推广。

相关研究成果对于民用关键网络或军事网络具有特别的意义,它能使网络管理员更好地了解整个网络态势,协助其分配网络资源,对潜在的威胁迅速做出实时响应,并为其进行决策支持和指挥控制提供有力的辅助信息。但是,国内目前对 NSAS 研究才刚刚起步,相关理论和技术还很不成熟,诸如海量网络数据的实时处理、多源传感器数据融合、态势评估、威胁评估、态势生成、态势可视化等方面均有许多问题需要研究。

参 考 文 献

1 Theureau J. Use of nuclear-reactor control room simulators inresearch & development. In:7th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of MAN-MACHINE SYSTEMS, Kyoto. 1998. 425~430

2 Endsley M R. Design and evaluation for situation awareness enhancement. Paper presented at the Human Factors Society 32nd

Annual Meeting. Santa Monica, CA, 1988
3 Bass T, Gruber D. A glimpse into the future of id. http://www.usenix.org/publications /login/1999-9/features/future.html, 1999
4 Bass T. Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness. Communications of the ACM, 2000, 43(4): 99～105
5 Batsell S G, Rao N S, Shankar M. Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security. http://www.ioc.ornl.gov/projects/documents/containment.pdf, 2005
6 Shifflet J. A Technique Independent Fusion Model For Network Intrusion Detection. Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mathematics, 2005,3(1):13～19
7 DeMontigny-Leboeuf A, Massicotte F. Passive network discovery for real time situation awareness. NATO/RTO Adaptive Defence in Unclassified Networks,Toulouse, France, April 2004
8 Yurcik W, et al. Two visual computer network security monitoring tools incorporating operator interface requirements. ACM CHI Workshop on Human-Computer Interaction and Security Systems(HCISEC), 2003
9 Lau S. The spinning cube of potential doom. Communications of the ACM, 2004, 47(6): 25～26
10 Carnegie Mellon's SEI. System for Internet Level Knowledge (SILK). http://silktools.source forge.net, 2005
11 Yurcik W. Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite. In:19th Usenix Large Installation System Administration Conference(LISA), San Diego, CA USA, Dec. 2005
12 Lakkaraju K, et al. NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness. In: ACM CCS Workshop on Visualization and Data Mining for Computer Security(VizSEC/DMSEC)held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004
13 Bearavolu R, Lakkaraju K, Yurcik W. NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows. FLOCON Network Flow Analysis Workshop(Network Flow Analysis for Security Situational Awareness), Sept. 2005
14 Yin Xiaoxin, et al. VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness. In: ACM CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC) held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004
15 Yin Xiaoxin, Yurcik W, Slagell A. The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness. In: Third IEEE International Workshop on Information Assurance(IWIA), 2005
16 Li Zhenmin, Taylor J, et al. UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection. In: 12th International Conference on Telecommunication Systems Modeling and Analysis(ICTSM), 2004
17 Office of The Secretary of Defense(OSD) Deputy Director of Defense Research & Engineering Deputy Under Secretary of Defense (Science & Technology). Small Business Innovation Research (SBIR)FY 2005.3 Program Description, USA. 2005
18 Advanced Research and Development Activity(ARDA). Exploratory Program Call for Proposals 2006, USA. 2005
19 冯毅.《中国信息战》我军信息与网络安全的思考. http://www.laocanmou.net/Html/20056 194115-1.html, 2005-06
20 张慧敏,等. 集成化网络安全监控平台的研究与实现. 通信学报, 2003,24(7)
21 陈秀真,等. 网络化系统安全态势评估的研究. 西安交通大学学报, 2004,38(4)
22 北京理工大学信息安全与对抗技术研究中心. 网络安全态势评估系统技术白皮书. http://www.thinkor.com/product/download/网络安全态势评估系统技术白皮书2.doc, 2005
23 胡华平,等. 面向大规模网络的入侵检测与预警系统研究. 国防科技大学学报, 2003;25(1)
24 Steinburg A N, Bowman C L, White F E. Revisions to the JDL Data Fusion Model. Joint NATO/IRIS Conference, Quebec, October 1998
25 Endsley M R. Toward a theory of situation awareness in dynamic systems. Human Factors,1995, 37(1): 32～64
26 张云涛, 龚玲. 数据挖掘原理与技术. 北京:电子工业出版社, 2004
27 Lee Wenke, Stolfo S. Data Mining Approaches for Intrusion Detection. In:Proceedings of the Seventh USENIX Security Symposium(Security'98). San Antonio,TX,Jan. 1998
28 Lee Wenke, Stolfo S, Mok K. A Data Mining Framework for Building Intrusion Detection Models. In:Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, CA, May 1999
29 Lee Wenke, Stolfo S, Mok K. Mining in a data-flow environment: Experience in network intrusion detection. In:Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining(KDD-99), August 1999
30 Abraham T. IDDM: Intrusion Detection Using Data Ming Techniques. DSTO Electronics and Surveillance Research Laboratory, Salisbury, Australia, May 2001
31 罗守山. 入侵检测. 北京:北京邮电大学出版社, 2004.82～87
32 Siaterlis C, Maglaris B. Towards Multisensor Data Fusion for DoS Detection. Network Management and Optimal Design Lab. National Technical University of Athens SAC '04, Nicosia, Cyprus,March. 2004
33 Bass T. Service-Oriented Horizontal Fusion in Distributed Coordination-Based Systems. IEEE MILCOM, 2004
34 刘超,谢宝陵,祝伟玲,等. 基于数据融合模型的网络安全分析评估系统. 计算机工程, 2005,31(13):7
35 闫飞,汪生,朱磊明. 基于数据融合和数据挖掘技术的入侵检测系统设计. 计算机工程与科学, 2004, 26(4)
36 Braun J J. Dempster-Shafer Theory and Bayesian Reasoning in Multisensor Data Fusion in Sensor Fusion: Achitectures, Algorithms, and Applications IV. Dasarathy B V,eds. In:Proceedings of SPIE, Vol 4051. 2000
37 Takata T, Koike H. Mielog: A highly interactive visual log browser using information visualization and statistical analysis. In:Proceedings of LISA XVI Sixteenth Systems Administration Conference, 2002.11
38 Koike H, Ohro K. SnortView: Visualization systems of snort logs. ACM, VizSEC/ DMSEC'04, Washington DC, USA, 2004.10
39 Danyliw R. ACID: Analysis Console for Intrusion Databases. http://acidlab.sourceforge.net, 2001
40 Erbacher R. Intrusion behavior detection through visualization. In:Proceedings of the IEEE systems, Man and Cybernetics Conference, Crystal City, Virginia, USA, 2003.10
41 Conti G, Abdullah K. Passive visual fingerprinting of network attack tools. VizSEC/DMSEC'04: Proceedings of 2004 ACM workshop on Visualization and Data Mining for Computer Security. New York, USA, 2004
42 Krasser S, Conti G, Grizzard J, et al. Real-time and forensic network data analysis using animated and coordinated visualization. 2005 IEEE Workshop on Information Assurance. IEEE Press, 2005
43 Lee C P, Trost J, Gibbs N, et al. Visual Firewall: Real-time network security monitor. Visualization for Computer Security VizSEC 2005, 2005
44 D'Amico A, Kocka M. Information Assurance visualizations for specific stages of situational awareness and intended users: lessons learned. Visualization for Computer Security VizSEC2005, 2005
45 Abdullah K, Lee C, Conti G, et al. IDS: Rainstorm: Visualization IDS alarms. Visualization for Computer Security VizSEC2005, 2005