网络安全态势感知研究进展

李 硕, 戴 欣, 周渝霞
(中国人民解放军第三零二医院, 北京 100039)

摘 要: 首先指出了网络安全态势感知研究的必要性,介绍了网络安全态势感知的概念、含义和主要任务;其次,详细阐述了网络安全态势感知国内外的研究现状和涉及到的关键技术;最后,总结和展望了网络安全态势感知当前存在的难题和今后的研究方向。

关键词: 态势感知; 网络安全态势感知; 数据融合; 态势值计算; 态势预测
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)09-3227-06
doi:10.3969/j.issn.1001-3695.2010.09.006

Research progress of network security situation awareness

LI Shuo, DAI Xin, ZHOU Yu-xia
(302 *Military Hospital of China*, *Beijing* 100039, *China*)

Abstract: Firstly, this paper indicated the necessity to research network security situation awareness(NSSA), and provided the concepts, meanings and main tasks of NSSA. Secondly, it surveyed the research progress of NSSA, and elaborated key technologies involved in the research field of NSSA. Finally, put forward the existing difficult problems of NSSA at present and research directions of NSSA in the near future.

Key words: situation awareness; network security situation awareness(NSSA); data fusion; situation value computation; situation prediction

随着计算机和通信技术的迅速发展,伴随着用户需求的不断增加,计算机网络的应用越来越广泛,其规模也越来越庞大。同时,网络安全事件层出不穷,使得计算机网络面临着严峻的信息安全形势,传统的单一的防御设备或者检测设备已经无法满足安全需求。网络安全态势感知(NSSA)技术能够综合各方面的安全因素,从整体上动态反映网络安全状况,并对安全状况的发展趋势进行预测和预警,为增强网络安全性提供可靠的参照依据。因此,针对网络的安全态势感知研究已经成为目前网络安全领域的研究热点[1,2]。

1 网络安全态势感知相关概念

1.1 网络安全态势感知的概念

态势感知(situation awareness)这一概念源于航天飞行的人因(human factors)研究[3],此后在军事战场、核反应控制、空中交通监管(air traffic control,ATC)及医疗应急调度等领域被广泛研究。Endsley 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"[3~5],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。

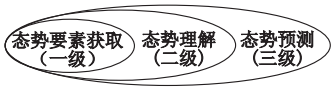

图1 态势感知的三级模型

网络安全态势感知源于 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,Bass[6] 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,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。网络安全态势感知包含了两层含义:a)实时地根据网络安全设备的告警信息及其他信息,进行关联归并、数据融合等操作,实时反映网络实际的运行状况;b)根据历史数据进行一定的离线分析,采用一定手段对潜在可能的威胁进行预测。

目前,对网络安全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。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。网络安全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。

1.2 网络安全态势感知的主要任务

网络安全态势感知的任务至少应包括以下七方面的内容[7~9]:

a)当前状态感知,亦称态势觉察(situation perception),包括态势识别(situation recognition)和态势确认(situation identification)。态势确认包括攻击类型、攻击源、攻击目标等的确认。

b)攻击影响感知,亦称影响评估(impact assessment),包括当前影响评估(即损害评估)和将来影响评估(如果攻击者继续攻击的话)两个部分。脆弱性分析(vulnerability analysis)是影响评估的一大方面,提供了己方知识,促进将来影响的预测。

收稿日期: 2010-03-09; **修回日期**: 2010-04-30

作者简介:李硕(1982-),女,河北保定人,助理工程师,博士研究生,主要研究方向为计算机网络安全、计算机应用技术等(llss69c@126.com);戴欣(1984-),男,主要研究方向为计算机应用技术;周渝霞(1965-),女,高级工程师,硕士,主要研究方向为计算机网络安全、计算机应用技术.

将来影响评估还涉及到威胁评估(threat assessment)。

c)态势演化感知。态势追踪(situation tracking)是其重要组成部分。

d)行动者(敌手)行为感知。其重要组成部分是攻击趋势(attack trend)和意图分析(intent analysis),更关心行动者(敌手)的行为,而不是态势本身。

e)感知当前态势形成原因和过程,包括因果关系分析(causality analysis)(通过事后追踪)和事后分析(forensics)。

f)感知收集到的态势感知信息项,以及从这些信息项中得到的知识—智能—决策(knowledge-intelligence-decisions)的质量(可信性)。质量度量包括可信性(trustfulness)、完全性(completeness)和新鲜性(freshness)。

g)态势预测。预测敌手将来可能的行为和动作、可能采取的攻击路径,分析得出可能的态势。该部分需要对敌手意图、机会、能力以及自身脆弱性有全面了解。

不失一般性,网络安全态势感知可分为三个阶段:态势识别(包括 a)f)g)部分)、态势理解(包括 b)d)和 e)部分)和态势预测(包括 c)部分)。

2 国内外发展动态

国外在网络安全态势感知方面正做着积极的研究,比较有代表性的,如 Bass 提出应用多传感器数据融合[6]建立网络空间态势感知的框架,通过推理识别入侵者身份、速度、威胁性和入侵目标,进而评估网络空间的安全状态。Shifflet 采用本体论对网络安全态势感知相关概念进行了分析比较研究[10],并提出基于模块化的技术无关框架结构。其他开展该项研究的个人还有加拿大通信研究中心的 DeMontigny-Leboeuf、伊利诺大学香槟分校的 Yurcik 等。

与此同时,国外很多研究机构也已开始着手研制网络安全态势感知系统和工具。美国国家能源研究科学计算中心(NERSC)所领导的劳伦斯伯克利国家实验室(Lawrence Berkeley National Labs)于 2003 年开发了“The spinning cube of potential doom”系统[11],该系统在三维空间中用点来表示网络流量信息,极大地提高了网络安全态势感知能力。2005 年,CMU/SEI 领导的 CERT/NetSA 开发了 SILK[12],旨在对大规模网络安全态势状况进行实时监控,在潜在的、恶意的网络行为变得无法控制之前进行识别、防御、响应以及预警,给出相应的应对策略。该系统通过多种策略对大规模网络进行安全分析,并能在保持较高性能的前提下提供整个网络的安全态势感知能力。NCSA/SIFT 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 安全态势感知系统有 NVisionIP[13]、VisFlowConnect-IP[14]等。NVisionIP 通过系统状态可视化来获取 Internet 的安全态势感知;VisFlowConnect-IP 通过连接分析可视化来获取 Internet 的安全态势感知。还有美国国家高级安全系统研究中心(National Center for Advanced Secure Systems Research, NCASSR)的 SIFT 项目、Ambrosio 提出基于问卷调查方式的计算机攻击态势感知软件系统 SSAI;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)、加拿大国防研究与开发中心(Defence R&D Canada)、瑞士联邦技术院(Swiss Federal Institute of Technology Zurich, ETH Zurich)等。

国内在这方面的研究起步较晚,近年来也有单位在积极探索。冯毅[15]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,并指出了两项关键技术——多源传感器数据融合和数据挖掘;北京理工大学机电工程与控制国家重点实验室网络安全分室在分析博弈论中模糊矩阵博弈原理和网络空间威胁评估机理的基础上,提出了基于模糊矩阵博弈的网络安全威胁评估模型及其分析方法,并给出了计算实例与研究展望[16];哈尔滨工程大学提出关于入侵检测的数据挖掘框架;国防科技大学提出大规模网络的入侵检测;文献[17]中提到西安交通大学网络化系统与信息安全研究中心和清华大学智能与网络化系统研究中心研究提出的基于入侵检测系统(intrusion detection system, IDS)的海量报警信息和网络性能指标,结合服务、主机本身的重要性及网络系统的组织结构,提出采用自下而上、先局部后整体评估策略的层次化安全威胁态势量化评估方法,并采用该方法在报警发生频率、报警严重性及其网络带宽耗用率的统计基础上,对服务、主机本身的重要性因子进行加权,计算服务、主机以及整个网络系统的威胁指数,进而评估分析安全威胁态势。

其他研究工作主要是围绕入侵检测、网络监控、网络应急响应、网络安全预警、网络安全评估等方面开展的,这为开展网络安全态势感知研究奠定了一定的基础。

3 网络安全态势感知关键技术

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,网络安全态势感知必须解决相应的技术问题。

3.1 数据融合

网络是一个存在不确定性因素的环境,其存在各类安全设备,这些设备监控网络的不同内容,提供不同格式的安全事件信息来表征系统当前的状态。各类安全设备在事实上形成了一个多传感器的环境,为引入多传感器的数据融合技术提供了客观的应用环境[18]。如果能够将分处在网络不同位置的提供不同格式信息的安全设备看做是采集网络安全状态信息的传感器的话,那么采用相关技术,将各种信息进行预处理并在此基础上进行归一化、相关等融合操作,就可以获得精确的位置估计和身份估计,从而完成对网络当前状态的估计以及威胁重要程度的一些实时估计。目前,在网络安全的目标跟踪、识别、态势感知以及威胁估计方面,数据融合技术得到了相当多的应用[19]。在底层的数据融合实现了对数据的压缩、提炼之后,其输出结果可以作为高层次的态势感知和威胁估计的主要依据。

数据融合是一个多级、多层面的数据处理过程,主要完成对来自多个信息源的数据进行自动监测、关联、相关、估计及组合等处理,即对来自多个传感器或多源信息进行综合处理,从而得到更为准确、可靠的结论。数据融合按信息抽象程度可分为三个从低到高的层次:数据级融合、特征级融合和决策级融合[20]。三个层次中,数据级融合的准确性最高,能够提供其他层次上的融合所不具备的细节信息,但因为需要处理的数据量大,对于计算机的运算速度和内存容量要求较高。决策级的融

合在高层次上进行,所需要处理的数据量小,但由于比较抽象和模糊,精度可能较差,特征级融合介于两者之间。

1)贝叶斯网络

a)贝叶斯网络。它是神经网络和贝叶斯推理的结合[21],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。

b)贝叶斯网络推理。采用贝叶斯网络模型解决实际问题时,首先要构造出符合问题要求的贝叶斯网络,然后通过该网络进行问题的求解,而应用贝叶斯网络进行问题求解的过程称为贝叶斯网络推理[22]。贝叶斯网络推理是计算概率分布的过程,也就是"求给定条件下事件发生的概率",因此在给定模型中计算目标变量的后验概率就是贝叶斯网络推理。现有的贝叶斯网络的推理算法可以分为两类:精确推理,即精确地计算假设变量的后验概率;近似推理,即在不影响计算结果正确性的前提下,通过降低推理精度来简化计算复杂性。精确推理适用于结构较简单的小型贝叶斯网络,近似推理主要用于节点数量大、结构复杂的贝叶斯网络。

尽管贝叶斯网络以其坚实的概率理论基础及其有效性而被认为是目前最好的不确定推理算法之一,但任意复杂结构的贝叶斯网络推理计算是 NP 困难的。另外,尽管贝叶斯网络实现相对简单,但是需要较多的先验知识,当先验知识不足的情况下可以采用 D-S 证据理论方法。

2)D-S 证据理论。它是由 Dempster 于 1967 年提出的,他首先提出了上、下界概率的定义,后由 Shafer 于 1976 年加以推广和发展,故人们也把证据理论称为 D-S 理论。证据理论可处理由未知所引起的不确定性,它采用信任函数而不是概率作为度量,通过对一些事件的概率加以约束以建立信任函数而不必说明精确的难以获得的概率,当约束限制为严格的概率时,它就成为概率论。因此,D-S 证据理论也可以看做是贝叶斯推理的一种扩展[23]。

网络安全中,对待入侵、威胁的判定往往存在一定的未知成分。这些未知成分的存在妨碍了入侵的判定,容易造成误警和虚警,而误警和虚警率过高,也是 IDS 等安全设备的痼疾。证据理论最核心的一点也就是其提供了一套合并证据的规则,能够将不同态势感知节点采集的数据进行融合,消除判决中的不确定成分;能够使得各个态势感知节点对安全事件的判别向假设判别的交集转移,具有良好的证据聚焦能力,能够有效地增加判别的准确性,减少误警和虚警。

随着研究的进一步深入,其不足之处也逐渐暴露出来,总结起来主要有:a)D-S 证据理论的组合规则无法处理证据冲突,且无法分辨证据所在子集的大小,从而按不同的权重聚焦。b)证据推理的组合条件十分严格,D-S 组合规则要求证据之间是条件独立的,而且要求鉴别框架能够识别证据的相互作用。c)证据组合会引起焦元"爆炸",焦元以指数计数递增,造成计算量变大。

3.2　态势值计算

网络安全态势值是通过一系列数学方法处理,将海量的网络安全信息归并融合成一组或者几组在一定值域范围内的数值。这些数值具有表现网络运行状况的特性,随着网络安全事件发生的频率、数量以及网络受到威胁程度的不同,该数值的大小也会随之产生特征性的变化。这些数值的获得过程也就是网络安全态势值的计算方法[24]。

网络安全态势值的作用主要是告诉管理员系统当前是否安全,即通过当前态势值和正常情况下的态势值比较可以判断系统是否安全;也可以提供可能收到的威胁程度有多大的信息,即通过当前态势值和正常状况下态势值的差值来判断可能受到威胁的严重程度。

网络安全态势值表示网络安全状况的优点是可以直观、快速、实时地反映系统的安全状况。配合历史数据回放、各种图表显示方法,可以使管理员对系统一段时间的安全状态进行全面的回顾、了解和分析。但是,对于具体发生了什么安全问题、可以采用什么方法解决这些更加细节的问题,态势值并不能给出可供参考的答案。

3.2.1　层次分析法

层次分析法(analytic hierarchy process,AHP)是由美国运筹学家、匹兹堡大学 Santy 教授于 20 世纪 70 年代提出的[25,26],他首先于 1971 年在为美国国防部研究应急计划时运用了 AHP,又于 1977 年在国际数学建模会议上发表了"无结构决策问题的建模——层次分析法"一文,此后 AHP 在决策问题的许多领域得到应用,同时 AHP 的理论也得到不断深入和发展。这种将思维过程数据化的方法不仅简化了系统分析和计算,还有助于决策者保持思维过程的一致性。在一般的决策问题中,决策者不能给出精确的比较判断,这种判断的不一致性可以由判断矩阵特征根的变化反映出来。引入判断矩阵最大特征根以外的其余特征根的负平均值作为一致性指标,用于检查和保持决策者判断思维过程的一致性。

AHP 之所以会受到国内外如此众多学者的关注和研究,是因为它具有一些较突出的特点:

a)原理简单。建立在实验心理学和矩阵论基础上的 AHP 原理易被大多数领域的学者所接受,同时由于原理清晰、简明,使研究与应用 AHP 方法的学者无须花大量的时间便会很快进入研究角色。

b)结构化、层次化。它能够将复杂的问题转换为诸多具有结构和层次关系的简单问题来求解。

同时 AHP 法的缺点也非常明显:

a)判断矩阵的一致性指标难以达到,当同一层次上元素很多时,更是如此。此时,容易使决策者作出矛盾和混乱的判断。

b)判断矩阵的一致性与人们决策思维的一致性存在差异。

c)判断矩阵的一致性检验标准 CR <0.1,目前仅是经验数据,缺乏科学有效的证明。

为了解决上述问题,在层次分析法中可以引入模糊数学方法对 AHP 进行改进,从而得到一种实用有效的模糊层次分析法(简称 FAHP)。

3.2.2 模糊层次分析法

FAHP 是将模糊数学的理论运用到层次分析法中,它集模糊数学、层次结构、权衡比较于一体,在决策科学中占有重要的位置。它对于 AHP 的优点在于判断矩阵的模糊性,简化了人们判断目标相对重要性的复杂程度,并借助模糊判断矩阵实现决策由定性向定量方便、快捷地转换,直接由模糊判断矩阵构造模糊一致性判断矩阵,使判断的一致性得到解决[27]。近来国内外研究模糊综合评价项目的成果很多,但在模糊综合评价模型中,当因素较多时,权重的分配极难确定。在现行的综合评价方法中,模糊综合评判法缺乏必要的权重量化值,主观随意性太大。在进行各种评价方法的综合运用过程中,模糊综合评价中的各因素权重是通过其他方法来确定的,因此存在很多不完善的地方,需结合其他评价方法综合使用。

3.2.3 德尔菲专家法

德尔菲法是以古希腊城市德尔菲(Delphi)命名的规定程序专家调查法。它是由组织者就拟定的问题设计调查表,通过函件分别向选定的专家组成员征询调查,按照规定程序,专家组成员之间通过组织者的反馈材料匿名地交流意见,通过几轮征询和反馈,专家们的意见逐渐集中,最后获得具有统计意义的专家集体判断结果。

德尔菲法既可以用于预测,也可以用于评估。国内外经验表明,德尔菲法能够充分利用人类专家的知识、经验和智慧,成为解决非结构化问题的有效手段,对于实现决策科学化、民主化具有重要价值。它是一种有效的直观预测技术,是在广泛征询专家意见的基础上,经过有组织的反复信息交流,使意见逐步趋于一致[28]。

3.2.4 综合分析

权值的衡量和评判对最后的网络安全态势值计算有很大的影响,相应衡量评判应考虑的因素很多。然而,现有的决策评价方法在科学性、合理性方面存在一定欠缺,如在现行的综合评价方法中,模糊综合评价法缺乏必要的权重量化值,主观随意性太大[29,30];层次分析法虽然考虑了权重并给予量化值,但仅仅是以目标计算比重,没有结合多方面的经验数据;德尔菲法通过函询方式获取了专家们富有专业性的意见,提供了经验值,但没有结合网络具体的实际情况,不能充分说明评价结果的合理性。针对现有权值衡量方法中出现的这些问题,模糊层次综合评价法结合模糊综合评价法和层次分析法建立量化模型,把定性指标合理地定量化,很好地解决了现有评价方法中存在的评价指标单一、评价过程不合理的问题,并利用德尔菲专家法中的经验数据对网络安全态势计算各元素的权值进行综合评价,以达到客观、准确评价的目的。

3.3 态势预测

预测是对事物或现象将要发生的或目前不明确的情况进行预先的估计和推测。预测要有一定的科学依据,其建立在对事物历史与现状的调查上,建立在对有关主要因素分析的基础上。态势预测就是根据网络安全威胁发展变化的实际数据和历史资料,运用科学的理论、方法和各种经验、判断、知识去推测、估计、分析其在未来一定时期内可能的变化情况[31]。

由于预测的对象、时间、范围、性质等不同,预测方法可以形成不同的分类,但可根据方法本身的性质特点将预测方法分为三类[32,33]:

a)定性预测方法。根据人们对系统过去和现在的经验、判断和直觉进行预测,其中以人的逻辑判断为主,仅要求提供系统发展的方向、状态、形势等定性结果。它适用于缺乏历史统计数据的系统对象。

b)时间序列分析。根据系统对象随时间变化的历史资料,只考虑系统变量随时间的变化规律,对系统未来的表现时间进行定量预测。它适用于利用简单统计数据预测研究对象随时间变化的趋势。

c)因果关系预测。系统变量之间存在某种前因后果关系,找出影响某种结果的几个因素,建立因与果之间的数学模型。根据因素变量的变化预测结果变量的变化,既预测系统发展的方向又确定具体的数值变化规律。

1)基于灰色理论的预测模型

灰色理论是我国学者邓聚龙于 1982 年提出的,主要以部分信息已知、部分信息未知的小样本、贫信息、不确定性系统为研究对象,通过对部分已知信息的生成、开发、提取,实现对系统运行行为的正确认识和有效控制[34]。与其他不确定性常用研究方法(概率统计和模糊数学)相比,灰色理论具有要求数据信息少,而且对数据无特殊要求等特色。灰色建模要经历五个阶段,依次为语言模型、网络模型、量化模型、动态模型和优化模型,通过灰色生成或序列算子的作用弱化随机性,挖掘潜在的规律。

2)基于灰色支持向量机的预测模型

预测要追求的不是已知样本的拟合情况,而主要是对未知样本的预测能力(即泛化能力)。时间序列预测是由已有的时间序列数据推测下一时刻序列的未来值。对时间序列数据的预测,由于不同的时间序列前后数据关联程度很不同,尤其是复杂的时间序列,选取不同的历史数据长度其预测结果也大不相同,且在不同阶段采用的历史数据长度也不宜相同。

基于灰色支持向量机的预测模型是将灰色预测方法和支持向量机相结合的一种预测模型。首先利用灰色预测方法将原始序列进行一次累加生成,然后利用支持向量机拟合非线性数据能力的优势对新序列建立预测模型,最后将预测结果进行累减还原得预测值[35]。

利用基于灰色支持向量机的模型进行预测,由于其发挥了灰色预测方法中累加生成的优点,削弱了原始数据中的随机性,增强了规律性,同时避免了灰色预测方法及模型存在的理论缺陷,其平均相对误差较低,预测精度得到极大的改善。

3)基于 RBF 神经网络的预测方法

径向基函数(radial basis function,RBF)神经网络是基于人脑的神经元细胞对外界反应的局部性而提出的,是一种新颖而有效的三层前馈式神经网络,其具有最佳逼近性能和全局最优的特性,能够以任意精度逼近任意连续函数。

根据网络攻击的过程化以及安全设备产生告警的非线性时序化,由各类告警加权得到的具有表现网络运行状况特性的网络安全态势值 x 可以抽象为时间序列 t 的函数,即 $x=f(t)$,此态势值具有非线性的特点。

由于 RBF 神经网络是通过非线性基函数的线性组合实现从输入空间 RN 到输出空间 RM 的非线性转换。网络安全态势值是一类非线性较强的时间序列,对它们进行预测,即从前 N 个数据中预测将来的 M 个数据,实质上就是找出 RN 到 RM

的非线性映射关系。

由于 RBF 神经网络算法中的关键参数、隐含层 RBF 的中心数值是根据对评估结果的聚类算法来确定的。在实时在线的网络安全态势感知应用中,聚类算法容易陷入局部最优化问题,同时容易将某些态势的变化作为孤立类,使得数据处理不当,从而导致整个 RBF 神经网络的解结果不稳定[36]。

4　网络安全态势感知当前存在的难题

网络安全态势感知系统一般部署在大规模信息系统中网络骨干节点和地区节点的安全防护中心以及各级网络通信指挥中心,用于建立广域网安全态势体系,实现对各安全管理系统安全态势的监测,形成多级告警、预警体系,进行有效的安全策略管理,构建分级的安全评估体系和应急处置预案库,感知安全态势,并对网络的安全策略和安全态势进行统一管理,构成大规模广域网络安全态势的评估平台。但要达到实用化水平,监控整个网络的态势状况,网络安全态势感知系统还存在如下难点问题[3,18,37~39]:

a)不同组织间的分工协作。很多机构组织采用不同厂商的网络设备,由于没有一套协议机制,不同厂家的安全产品及不同组织之间难以进行协作,难以有效监控整个网络的安全态势状况。

b)应对网络复杂性,缩短响应时间。随着网络结构日益复杂,网络应用日益增多,黑客攻击造成的危害也越来越严重,这就要求 NSSA 系统能够迅速适应网络变化,对全网态势做出准确判断,并对新攻击行为进行自适应响应。

c)多源、多点事件的关联分析。网络攻击行为具有分布性等特点,这就要求 NSSA 系统能够收集并关联多源异构数据,及时发现并判断可疑事件。

d)降低额外网络负荷,提供系统容错性。NSSA 系统要尽量降低探测点带来的额外网络负载,优化探测点数目、探测周期和传输数据量等参数,并提高系统容错能力,当故障发生的情况下仍然能够正常工作。

e)安全态势的可视化。当前数据规模大、攻击复杂性高,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亟待解决的难题。

5　结束语

为保障网络信息安全,开展大规模网络态势感知研究是十分必要的,对于掌控当前的网络状况、发现潜在的恶意攻击、缓解攻击造成的危害、提高系统的应急响应能力等具有十分重要的意义。网络安全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[3~5,18,23,40~42]:

a)实时的态势感知。能对大规模网络进行实时或近实时的态势感知,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。

b)态势预测功能。能利用网络安全属性的历史记录,提供比较准确的网络安全演变趋势,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。

c)未知攻击检测能力。能检测并防御 DoS/DDoS 攻击,并能很好地检测出未知攻击和潜在的恶意网络行为。

d)自适应入侵响应、智能化决策。依靠人工手段对入侵、攻击进行响应的效率极低,并且容易出错,NSSA 系统应该具有自动化、自适应地阻止、反击入侵,甚至智能化决策的能力。

当前,国内对网络安全态势感知的研究才刚刚起步,相关理论和技术还很不成熟,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、态势生成和态势可视化等方面均有许多问题需要研究。

参考文献:

[1] BRUCE P. Software and network security[J]. Network Security, 2004(10):4-5.

[2] MATSUURA K, EBATO K. University-industry collaboration networks in the information security field in Japan: problems and a particular success[C]//Proc of Engineering Management Conference. 2004: 839-844.

[3] 王慧强,赖积保,朱亮,等. 网络态势感知系统研究综述[J]. 计算机科学, 2006, 33(10): 5-10.

[4] 韦勇,连一峰,冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353-362.

[5] 赖积保,王慧强,朱亮. 网络安全态势感知模型研究[J]. 计算机研究与发展, 2006, 43(Z1): 456-460.

[6] BASS T. Intrusion systems and multisensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.

[7] FELTON B. Cyber security breaches threaten, smarter factories and processes emerge, consulting business booms, and engineering talent base shrinks[J]. Civil Engineering/Siviele Ingenieurswese, 2006, 14(1): 26-28.

[8] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885-897.

[9] TIAN Jie, CHEN Jie, DOU Li-hua, *et al*. The research of test and evaluation for multisensor data fusion systems[C]//Proc of the 4th World Congress on Intelligent Control and Automation. 2002: 2104-2108.

[10] SHIFFLET J. A technique independent fusion model for network intrusion detection[C]//Proc of Midstates Conference on Under Graduate Research in Computer Science and Mathematics. 2005: 13-19.

[11] LAU S. The spinning cube of potential doom[J]. Communications of the ACM, 2004, 47(6): 25-26.

[12] WEN Cheng-lin, WEN Chuan-bo. The multiscale sequential filter with multisensor data fusion, systems and control in aerospace and astronautics[C]//Proc of the 1st International Conference on Systems and Control in Aerospace and Astronautics. 2006.

[13] BEARAVOLU R, LAKKARAJU K, YURCIK L. NVisionIP: an animated state analysis tool for visualizing NetFlows[C]//Proc of FIOCON Network Flow Analysis Workshop. 2005.

[14] YIN Xiao-xin, YURCIK W, SLAGELL A. The design of VisFlowConnect IP: a link analysis system for IP security situational awareness[C]//Proc of the 3rd IEEE International Workshop on Information Assurance. Washington DC: IEEE Computer Society, 2005: 141-153.

[15] 冯毅.《中国信息战》我军信息与网络安全的思考[EB/OL]. (2005-06-20)[2009-11-10]. http://www.laocanmou.net/Html/20056194115-1.html.

[16] 韦勇,连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报, 2009, 32(4): 763-772.

[17] LI Zhen-min, TAYLOR J. UCLog: a unified, correlated logging architecture for intrusion detection[C]//Proc of the 12th International Conference on Telecommunication Systems Modeling and Analysis. 2004.

[18] 萧海东. 网络安全态势评估与趋势感知的分析研究[D]. 上海: 上海交通大学, 2008.

[19] 田春岐,邹仕洪,王文东,等. 一种新的基于改进型 D-S 证据理论的 P2P 信任模型[J]. 电子与信息学报, 2008, 30(6): 1480-1484.

[20] 诸葛建伟,王大为,陈昱,等. 基于 D-S 证据理论的网络异常检测方法[J]. 软件学报,2006, 17(3): 463-471.

[21] MOHAMED S, EHAB A S, LATIF K. A novel quantitative approach for measuring network security[C]//Proc of IEEE INFOCOM Mini-Conference. 2008.

[22] NIKLASSON L, RIVEIRO M, HOHANSSON F, *et al*. A unified situation analysis model for human and machine situation awareness[C]// Proc of the 3rd German Workshop on Sensor Data Fusion. Berlin: Springer, 2007: 105-110.

[23] 胡小佳. 态势估计中的不确定性推理方法研究[D]. 长沙:国防科学技术大学, 2007.

[24] BEAUDOIN L, FROH M, GREGOIRE M, *et al*. Computer network defence situational awareness information requirements[C]//Proc of Military Communications Conference. 2006.

[25] SHEN Dan, CHEN Gen-she, HAYNES L, *et al*. Strategies comparison for game theoretic cyber situational awareness and impact assessment[C]//Proc of the 10th International Conference on Information Fusion. 2007.

[26] 文成林,吕冰,葛泉波. 一种基于分步式滤波的数据融合算法[J]. 电子学报, 2004, 32(8): 1264-1267.

[27] 高羽,张建秋. 小波变换域估计观测噪声方差的 Kalman 滤波算法及其在数据融合中的应用[J]. 电子学报, 2007, 35(1): 108-111.

[28] 陆余良,夏阳. 主机安全量化融合模型研究[J]. 计算机学报, 2005, 28(5): 914-920.

[29] LI Tao. Dynamic detection for computer virus based on immune system[J]. Science in China, Series F: Information Science, 2008, 51(2): 1475-1486.

[30] AL-SHAER E, KHAN L, AHMED M S. A comprehensive objective network security metric framework for proactive security configuration [C]//Proc of the 4th Workshop on Cyber Security and Information Intelligence Research. New York: ACM Press, 2008.

[31] MAGNUS A, LINQVIST D, ERLAND J. A multi-sensor model to improve automated attack detection[C]//Proc of the 11th International Symposium on Recent Advances in Intrusion Detection. 2008.

[32] 赵国生,王慧强,王健. 基于灰色 Verhulst 的网络安全态势感知模型[J]. 哈尔滨工业大学学报, 2008, 40(5): 798-801.

[33] YIN Xiao-xin, YURCIK W, TREASTER M. VisFlo connect:netflow visualizations of link relationships for security situational awareness [C]//Proc of ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM Press, 2004:26-34.

[34] AMBROSIO D, TAKIKAWA M, UPPER D, *et al*. Security situation assessment and response evaluation(SSARE)[C]//Proc of the DARPA Information Survivability Conference & Exposition. 2001:387-394.

[35] YEGNESWARAN V, BARFORD P, PAXSON V. Using honey nets for Internet situational awareness[C]//Proc of the 4th Workshop on Hot Topics in Networks. 2005.

[36] 马千里,郑启伦,彭宏,等. 基于模糊边界模块化神经网络的混沌时间序列预测[J]. 物理学报, 2009, 58(3): 1410-1419.

[37] 李军,赵峰. 基于支持向量回归神经网络的时间序列预测[J]. 系统仿真学报, 2008, 20(15): 4025-4030.

[38] RITCHEY R, AMMANN P. Using model checking to analyze network vulnerabilities[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2000: 156-165.

[39] MONTIGNY D, LEBOEUF A, MASSICOTTE F. Passive network discovery for real time situation awareness[C]//Proc of NATO/RTO Symposium on Adaptive Defence in Unclassified Networks. 2004.

[40] 李目,何怡刚,周少武. 混沌时间序列的混合遗传神经网络预测方法[J]. 系统仿真学报, 2008, 20(21): 5825-5828.

[41] 石宇静,柴天佑. 基于神经网络与多模型的非线性自适应广义预测控制[J]. 自动化学报, 2007, 33(5): 540-545.

[42] 刘欣,王小强,朱培栋. 互联网域间路由系统安全态势评估[J]. 计算机研究与发展, 2009, 46(10): 1677-1699.

(上接第 3209 页)

[20] RAJESH S, NICHOLSON C Y. Structural and contextual correlates of charged behavior in product development teams [J]. Jonrnal of Product Innovation Management, 2001, 18(3): 154-168.

[21] 董昊,严洪森. 产品开发团队组织模式的自适应决策模型[J]. 系统工程理论方法应用, 2005, 14(2):33-39.

[22] 秦吉波, 曾德明, 陈立勇. 团队治理:关于提高高新技术企业 R&D 绩效的思考[J]. 数量经济技术经济研究, 2003, 20(3): 43-47.

[23] 张体勤. 知识团队的绩效管理[M]. 北京:科学出版社, 2002.

[24] 张体勤,丁荣贵. 关于知识团队特性的研究[J]. 人类工效学, 2002, 8(3): 41-44.

[25] 蒋蓉华, 周永生. 先进制造环境下知识团队的智力资本及创新[J]. 技术经济, 2003(1): 9-11.

[26] 王蔷,任庆涛. 扁平化组织的组织模式架构[J]. 经济管理, 2004 (6): 14-17.

[27] 孙锐, 李海刚. 基于知识创新的知识团队研究[J]. 科研管理, 2006, 27(6):92-96.

[28] 廖冰,纪晓丽. 浅析知识团队的管理[J]. 现代管理科学, 2003 (6):57-58.

[29] 张伟. 团队复杂系统分析[J]. 复杂系统与复杂性科学, 2005, 2 (2): 77-85.

[30] 汪维扬. 以系统动力学探讨自组织团队的认知机制[D]. 高雄:国立中山大学资讯管理学系, 2001: 23-33.

[31] 刘杰,陆君安. 一个小型科研合作复杂网络及其分析[J]. 复杂系统与复杂性科学, 2004, 1(3): 56-61.

[32] 何阅,张培培,许田,等. 一个科研合作网的双粒子图自适应演化模型[J]. 物理学报, 2004, 53(6): 1710-1715.

[33] 张体勤,伊振中,丁荣贵. 论知识团队的知识循环过程[J]. 自然辩证法研究, 2009, 25(5):109-112.

[34] 伊振中,丁荣贵,张体勤. 基于复杂网络理论的知识团队成长机制研究[J]. 山东经济,2008, 24(6):109-114.

[35] 邹波,张庆普,田金信. 企业知识团队的生成及知识创新的模型与机制[J]. 科研管理,2008, 29(2):81-88.

[36] 邹波,田金信,张庆普. 基于知识类型分野的企业知识团队创新不确定性研究[J]. 哈尔滨工业大学学报:社会科学版, 2008, 10 (1):117-120.

[37] 李焕荣,张晓芹. 基于系统动力学的知识团队绩效管理研究[J]. 科技进步与对策, 2007, 24(5):177-179.