软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.005142]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

网络安全态势感知综述

龚 俭[1,2,3], 臧小东[1,2,3], 苏 琪[1,2,3], 胡晓艳[1,2,3], 徐 杰[1,2,3]

[1](东南大学 计算机科学与工程学院,江苏 南京 211189)

[2](江苏省计算机网络重点实验室,江苏 南京 211189)

[3](计算机网络和信息集成教育部重点实验室,江苏 南京 211189)

通讯作者: 龚俭,E-mail: jgong@njnet.edu.cn

通讯作者: 臧小东,E-mail: xdzang@njnet.edu.cn

摘 要: 随着网络空间安全的重要性不断提高,网络安全态势感知(Network Security Situation Awareness,简称NSSA)的研究与应用正在得到更多地关注.NSSA 实现对网络中各种活动的行为辨识、意图理解和影响评估，以支持合理的安全响应决策.它是对网络的安全性进行定量分析的一种手段,网络安全管理系统可以借助其宏观把握整个网络的安全状况,分析攻击者的意图,为管理决策提供重要的依据.本文讨论了 NSSA 的任务范围,并据此对网络安全态势感知的概念进行了重新定义.然后本文分别从网络安全态势觉察、网络安全态势理解、网络安全态势投射三个层面综述了网络安全态势感知的研究现状和存在的问题.

关键词: 网络安全态势感知;数据融合;模型;关联性分析;综述

中图法分类号: TP311

Survey of Network Security Situation Awareness

GONG Jian[1,2,3], ZANG Xiao-Dong[1,2,3] ,SU Qi[1,2,3], HU Xiao-Yan[1,2,3],XU Jie[1,2,3]

1(School of Computer Science and Technology, Southeast University, Nanjing 210023, China)

2(Jiangsu Provincial Key Laboratory of Compmer Network Technology, Nanjing 9211189, China)

3(Key Laboratory of Computer Network and Information Integration Ministry of Education, Nanjing 211189, China)

Abstract: As the priority of cyber-security is raising world-widely, Network Security Situation Awareness (NSSA) and its application is getting more concerns by reseachers. NSSA is able to identify network activities, understand their intentions and evaluate the impact of these activities on the managed network, so as to support an optimal security response to the security threats. It is a means of quantitative analysis for network security, with which network security management system can have a global view of security states of the managed network, find the intention of attackers, make a management decision based on these findings. In the paper, the coverage of NSSA is discussed to redefine the concept of NSSA. Then this paper gives a suvey to the state-of-art of NSSA's research in the aspects of network security situation perception, comprehension and projection. Finally the features and challenges of network security situation awareness are summarized.

Key words: network security situation awareness;data fusion;models;correlation analysis;survey

0 引言

互联网基础设施的不断发展和新应用的不断涌现使得网络规模逐渐增大,拓扑结构日益复杂,网络安全管理的难度不断增加.为了应对日益复杂、隐蔽的网络威胁,各种检测技术相继出现,如:脆弱性检测技术,恶意代码检测技术入侵检测技术等.这些技术试图从不同的角度发现网络中可能存在的安全问题,但在适时全面地寻找出网络系统中存在的真实威胁方面不够理想和有效,限制了网络安全管理员做出最佳响应决策的能力.近年来,网络安全态势感知的概念逐渐引起研究人员的兴趣,希望利用其从大量、存在噪声的数据中辨识出网络中的攻击活动,宏观地把握整个网络的安全状况,并合理有效地进行响应,以尽可能降低因攻击造成的损失.这对于提

基金项目:基于网络编码的信息中心网络研究(61602114)
收稿时间: 2016-05-11; 修改时间: 2016-08-09, 2016-10-2; 采用时间: 2016-11-11; jos在线出版时间: 2016-11-24
CNKI网络优先出版: 2016-11-24 13:41:13, http://www.cnki.net/kcms/detail/11.2560.TP.20161124.1341.003.html

高网络系统的监控能力和应急响应能力具有积极的作用.然而目前人们对网络安全态势感知的研究仍处于探索阶段,还未形成一致的认识.

鉴于网络安全态势感知对网络安全管理的积极作用,且目前该领域的研究尚在起步阶段,本文试图对网络安全态势感知的基本概念、研究内容与难点、意见及目前的研究热点进行综述,具体贡献如下:

⑴对网络安全态势感知的概念进行了重新表述,进一步明确了它的研究目标.⑵依据本文给出的网络安全态势感知定义,对已有的概念模型进行分析,并在此基础上给出了一个更为准确合理的概念模型.⑶对相关的研究内容进行了分类讨论,分析存在的问题.⑷探讨了网络安态势感知目前的热点问题,进一步指出网络安全态势感知下一步的研究重点.

本文第一节中主要阐述了态势感知的概念及起源,重新表述了网络安全态势感知的概念.第二、三、四节分别从网络安全态势觉察、网络安全态势理解、网络安全态势觉察投射三层面阐述网络安全态势感知的研究内容和存在的问题.第五节基于网络安全态势感知的目标探讨了这个领域的研究重点.最后是全文总结.

1 网络安全态势感知的基本概念

本节主要阐述了态势感知的概念,重新表述了网络安全态势感知的概念,并分析了态势感知与网络安全态势感知之间的关系.

1.1 态势感知

状态是指一个物质系统中各个对象所处的状况,由一组测度来表征.顾名思义,态势是系统中各个对象状态的综合,是一个整体和全局的概念.任何单一的情况和状态均不能成为态势,它强调系统及系统中的对象之间的关系[1].微观而言,表征状态的测度取值依赖于对应系统的要素内容,这些要素之间的关系如图 1 所示,其中:

原始数据是指传感器产生的未经处理的数据,它反映的是原始数据的观测结果.

信息是指对原始数据进行有效性处理后得到的数据记录.

知识是指采用相关技术所识别出的系统中的活动内容.

理解是指针对各个活动,分析得到的其意图和特征.

状态评估是指预测这些活动对系统中各个对象所产生的作用.

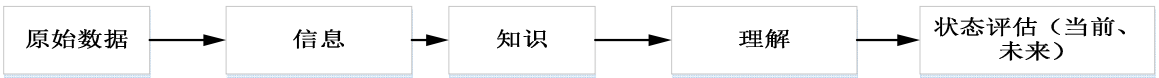

Fig.1 Situation awareness cognitive mapping process

图 1 态势感知的认知映射[2]

从图 1 可以看到,感知是一种 “认知映射”.所谓认知映射是指决策者采用数据融合、风险评估及可视化等相关技术对不同地点获得的不同格式的信息去噪、整合,从而得到更准确、更全面的信息,然后不断的对这些信息进行语义提取,识别出需要关注的重要要素及其意图,决策者可以实时有效地评估其对系统产生的影响.

态势感知是指在一定的时间和空间范围内,提取系统中的要素,理解这些要素的含义,并且预测其可能的效果[3].Endsley 将其概括为三个层面:态势觉察(Situation Perception)、态势理解(Situation Comprehension)及态势投射(Situation Projection).根据这个定义,态势感知可以理解为一个认知过程[4],通过使用过去的经验和知识,识别、分析和理解当前的系统状况.分析人员对当前的态势进行感知,更新”状态知识”,然后再进行感知以致构成一个循环的映射过程.这个映射过程不是简单的数据变换而是一种语义提取[5].因此感知的过程表现为不断地作认知映射以获取更多更详细的语义.态势感知是一个动态变化的过程,不同的人由于经验、知识等不同,得到的态势感知不尽相同.

态势感知最早来源于美国军方在军事对抗中的研究.在军事术语中,态势感知的目标是使指挥官了解双方的情况,包括敌我的所在位置、当前状态和作战能力,以便能做出快速而正确的决策,达到知己知彼,百战不殆的目的[5].态势感知方法在人机交互系统[7,8],战场指挥[5]、和医疗应急调度[9]等领域均有应用.Tim Bass 于 1999 年

提出网络态势感知这个概念[10],次年将该技术应用于多个 NIDS 检测结果的数据融合分析[2],主要是解决单一入侵检测系统无法有效识别出当前系统中存在的所有攻击活动及整个网络系统的安全态势的问题.随后学术界开始致力于网络安全态势感知的研究,并提出了多种相关的模型和技术.

目前人们对网络安全态势感知的研究存在三种观点,一种认为 NSSA 是网络安全事件应用大数据处理和可视化技术的汇总结果,如传统的安全服务提供商(McAfee,Symantec)及新出现的重点关心 APT 攻击的企业(FireEye, Mandiant)等,通过公开一些技术报告记录 APT 的攻击实例[11,12];一种认为 NSSA 是基于网络安全事件融合计算的网络安全状态量化表达[13,14];还有认为 NSSA 作为一种网络安全管理工具,是网络安全监测的一种实现形式,并提出了诸多模型[3,15-18].

态势感知常被应用在由观察(Observe)、导向(Orient)、决策(Decision)和行动(Act)等四阶段构成的一个控制过程环中(图 2).这类控制模型过去有很多研究成果,如:Boyd 控制循环模型[15]、JDL 数据融合模型[15]、Endsley 在 1995 提出的模型[3]、龚正虎等提出的网络态势感知模型[16]、Tadda 提出的将 JDL 与 Endsley 的三层模型相结合的模型[17]及刘效武提出的认知融合感控模型[18]等.

OODA 环的概念直接来自 Boyd 控制循环模型,它描述了目的与活动的感知过程,并将感知循环过程分为观察、判断、决策、行动这 4 个阶段.其中观察实现了从物理域跨越到信息域,判断和决策属于认知域;而行动实现信息域到物理域的闭合,完成循环.前 3 个阶段类似于 JDL 数据融合模型,而行动阶段考虑了决策对真实世界中的影响来闭合循环,更适用于需要进行主动干预的环境中.Lenders等将 OODA 应用到企业网中,解决了之前 OODA 模型中将判断、决策的任务留给人进行手动处理的问题[5].

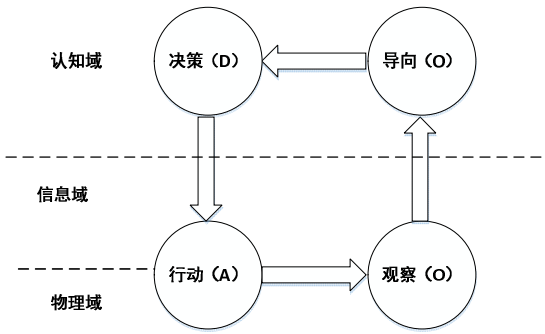

Fig.2 OODA Decision Making Model

图 2 OODA 决策模型[15]

需要强调的是,这些研究得到的并不是态势感知模型,而是态势感知应用模型,态势感知的工作只涉及图 2 中认知域的活动,不涉及信息域和物理域的活动.因此基于这些模型来直接代表态势感知的概念是不合适的.

1.2 网络安全态势感知

美国空军通信与信息中心的 Tim Bass 在 1999 年首次提出将态势感知技术应用于多个 NIDS 检测结果的数据融合分析,认为"多传感器数据融合技术为下一代入侵检测系统和网络态势感知系统提供了一个重要的功能框架,它可以融合多源异构 IDS 的数据,识别出入侵者身份、攻击频率及威胁程度等"[2].该文没有给出网络安全态势感知概念的明确定义,只是强调了数据融合是态势感知的核心手段.之后的研究中也很少有人直接对网络安全态势感知的概念进行直接的定义,而是使用意会的方式,这是导致这个领域研究中概念不统一的重要原因.

文献[1]探讨了网络安全态势感知的概念,认为它是指"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".这个定义基本上属于 Endsley 定义[3]的翻译,并且缺乏对网络安全态势感知中网络安全态势投射层面的内容,对网络安全态势感知目标的理解是不完整的.

文献[4]将"网络安全态势感知视为态势感知的一个子集,其主要关注的是网络安全领域,数据源主要是 IDS 的警报、脆弱性信息等".这个定义过于模糊,没有明确子集的含义是针对功能,还是针对数据,也没有明确网络安

全态势感知是态势感知结果的一部分还是功能的一部分.网络安全态势感知与态势感知实质是类型和实例的关系而不是子集的问题,态势感知既包括安全态势感知也包括工业控制态势感知等,是使用同一种方法应用在不同的领域.

我们认为网络安全态势感知的目的应当是将态势感知的理论和方法应用到网络安全领域中,能够使网络安全人员在动态变化的网络环境中,宏观把握整个网络的安全状态,为高层管理人员提供决策支持.鉴于态势感知是一种认知过程,且网络安全态势感知是态势感知方法在网络安全领域的应用,因此我们可以将网络安全态势感知的概念定义如下.

定义 1: **网络安全态势感知 NSSA 是对网络系统安全状态的认知过程,包括对从系统中测量到的原始数据逐步进行融合处理和实现对系统的背景状态及活动语义的提取,识别出存在的各类网络活动以及其中异常活动的意图,从而获得据此表征的网络安全态势和该态势对网络系统正常行为影响的了解.**

定义中需要解释的是,网络系统是对各种形态网络的抽象,包括计算机互联网、物联网、以及其它采用不同通信方式和终端类型的网络.这意味着不同类型的网络在网络安全态势感知的概念和方法上是具有共性的.测量是对各种网络检测功能的抽象,包括网络管理数据和网络安全监测数据.其中,测量数据的生成不是 NSSA 的任务,而这些数据的获取则是 NSSA 的任务.这意味着网络安全态势感知的研究目标与研究内容与网络管理和网络入侵检测等这些传统的研究领域之间有着区分和不同的侧重点.背景状态是系统当前所处的运行状态,这是动态变化的,与系统之前的部署和定义可能是不一致的."安全"只有在动态的系统中才有意义,因此攻击活动及安全缺陷对系统的影响效果应当基于系统当前的状态进行判定.活动语义是系统中的主体作用于客体的动作所构成的序列,要进行安全态势察觉,管理人员应当了解系统中存在的所有活动,不能仅止于辨识攻击活动,即要辨清敌我.响应决策本身不是NSSA的任务,因为态势感知只是OODA的支撑技术.这意味着安全响应技术和安全策略管理技术等传统上属于网络安全管理领域的内容不属于网络安全态势感知的研究范畴.

根据上述定义,NSSA 的任务包括网络安全态势觉察（Perception）、网络安全态势理解（Comprehension）、网络安全态势投射（Projection）三个层面.其中,态势觉察完成原始测量数据的融合与语义提取任务,以及活动辨识任务;态势理解完成这些辨识出的活动的意图理解任务;态势投射完成这些活动意图所产生的威胁判断任务.层与层之间存在依赖关系[19,20],即如果网络安全态势觉察和网络安全态势理解没有合理的结果,得到网络安全态势投射很可能也是不正确的或不完整的.但另一方面,每层的结果均可以独立呈现并直接使用,以满足不同的网络安全管理需要.这意味着网络安全态势感知的结果及其表达方式具有多样性,蕴含的语义粒度也可以随需求的视角而不同.但是无论如何,网络安全态势感知的结果应当是可响应的(Reactionable),否则缺乏实际意义.另外,网络安全态势感知是一个测量数据驱动的认知过程,测量数据的数量与质量影响感知的结果.

基于上述理解,我们给出网络安全态势感知的一般功能模型,如图 3 所示.该模型包含网络安全态势觉察、网络安全态势理解、网络安全态势投射及可视化等模块,如下简要概括各模块的功能.

网络安全态势觉察主要目的是辨识出系统中的活动,即对网络中相关的检测设备与管理系统产生的 Raw Data 进行降噪、规范化处理得到有效信息,然后对这些信息进行关联性分析,识别出系统中有"谁" (系统中的主体、客体) 存在,进一步分辨出异常的活动.

网络安全态势理解的主要任务是在网络安全态势觉察的基础上,发现攻击活动,理解并关联攻击活动的语义,然后在此基础之上理解其意图.

网络安全态投射的主要任务是在前两步的基础上,分析并评估攻击活动对当前系统中各个对象的威胁情况.这种投射包括发现这些攻击活动在对象上已经产生和可能产生（即预测）的效果.通过将态势感知的结果投射到确定的系统对象上,可以获得该对象在当前态势下的状态.尽管要感知的是系统中的活动,而感知的最终结果则应表达为这些活动对系统对象的影响,不能仅止于活动的识别,因为系统因之而产生的反应是施加于对象的,而不是直接施加于活动本身.这是一个再认识的过程,即融合从系统中观察到的各个对象的状态以构成态势,再看这个态势对系统各个对象的意义.

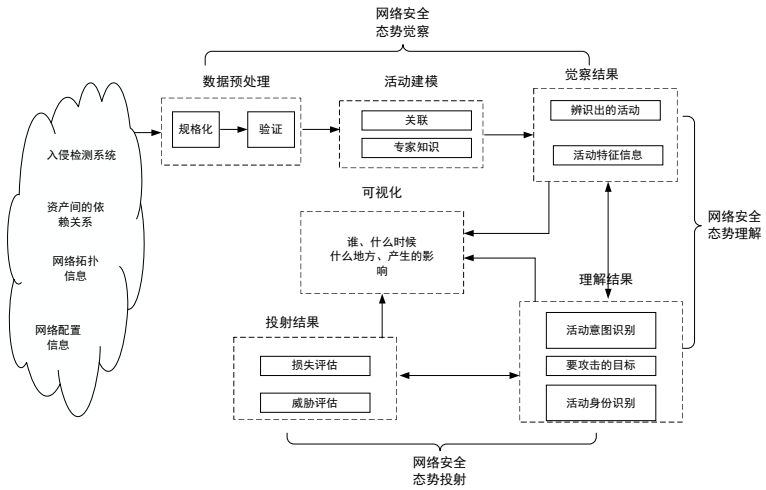

Fig.3 Network situation awareness model

图 3 网络安全态势感知模型

理想情况下,网络安全态势感知将网络安全状况以可视化[21-23]的形式表示成”谁在什么时候什么地方对谁产生什么样的影响”,(即 Who 、When、Where、Impact).研究人员可以观察在特定的时间段系统中某个攻击活动的情况,也可以观察所有活动的分布情况,这取决于具体的研究目标和需求,其中:

Who 是指辨识出的系统中的攻击活动;When 是指攻击活动在时间轴上的演化过程(侦查、隐藏、攻击、后门利用);Where 是指攻击活动的分布(即被管网络中哪些主机和服务器已被攻击);Impact 是指攻击活动对被管网络造成的影响,包括已造成的影响和潜在影响.总之,网络安全态势感知的目标是了解自己,了解敌人(威胁).

本文的定义希望在足够抽象的层面上尽量完整地体现网络安全态势感知的目标和任务,特别强调了网络安全态势投射对网络安全态势感知的意义,我们在后文第 2、3、4 节中分别对各个层面的研究内容与研究现状进行归纳讨论.

2 网络安全态势觉察

2.1 基本任务

网络安全态势觉察的基本任务是辨识出系统中的所有活动(包括攻击活动)以及这些活动的规律和特征(即图 4 中活动建模).本节首先介绍网络安全态势觉察的一般模型,然后阐述在网络安全态势觉察中使用的建模方法.

网络安全态势觉察一般模型包含数据预处理、活动建模和网络安全态势觉察结果等三个功能,如图 4 所示.数据预处理完成测量数据的规范化和验证,有利于后续的融合处理.活动建模借助这些测量数据本身语义完成之间的关联性分析.察觉结果完成活动的辨识和特征提取.态势觉察是一个学习过程,因此活动建模和觉察结果之间存在反馈关系.

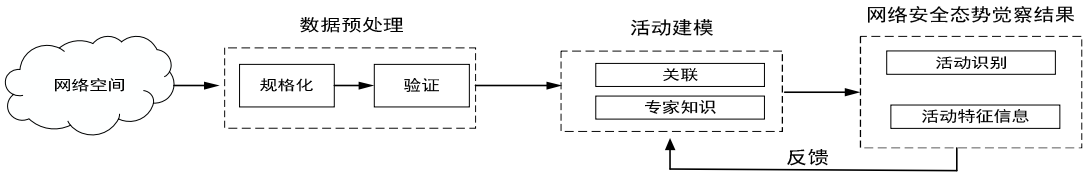

Fig.4 Network security situation perception model

图 4 网络安全态势觉察模型

目前多数的研究集中在攻击活动辨识方面,总体的解决思路如图 5 所示.研究热点有两个,一个是基于先验

知识,将观察到的警报与已知的攻击行为进行匹配(即图 5 中专家知识),相关方法有基于攻击场景的方法.另一个是在缺乏先验知识的情况下分析警报之间的关系,发现攻击步骤之间的相关性,构成攻击行为的描述(即图 5 中关联).

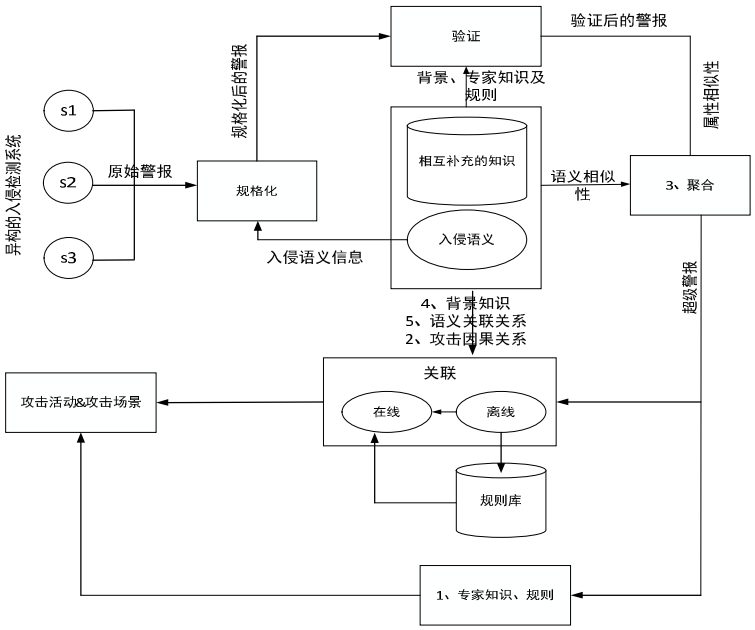

Fig.5 Attack activities reconstruction model

图 5 攻击活动重构模型

2.2 基于先验知识的方法

基于先验知识方法是基于专家经验和知识定义知识库,最常用的建模方法是基于场景的方法.该方法通过专家规则或知识定义一个攻击序列模板(即图 5 中的 1)以描述可能的攻击行为,然后将观察到的警报按模板进行匹配,以还原攻击过程.

Cuppens 等[24]开发了 LAMBDA 语言来支持模板和匹配过程的描述.研究者[25-29]通常将一个攻击行为分为多个阶段,如 IKC Multi-stage Attack Model[30].通过分析每个攻击警报的语义,将经过网络配置信息和脆弱性信息验证后有效警报与已知的攻击阶段进行匹配,以识别整个攻击过程.

基于攻击场景的方法通常以有向图的形式表示攻击序列的模板,图中的节点对应着一个安全事件,边表示事件之间的依赖关系,边中的权重表示事件间转换概率.该方法能够高效地识别出已知的攻击行为,但无法识别未知的攻击行为,且还存在可扩展性较差的问题.

2.3 不基于先验知识的方法

不基于先验知识方法是通过数据挖掘、机器学习等技术分析警报之间的关系,以还原完整的攻击过程.目前常用的建模方法有相似性方法、因果关联方法及交叉关联方法.这类方法由于不依赖预定义的攻击模板,因此可以发现未知的攻击行为.

相似性方法认为相似警报的来源和产生的影响是相同的或相似的,它通过计算警报特征之间的相似程度对警报进行聚类(Clustering)或聚合(Aggregation)以减少警报的数量.目前基于相似性的研究方法主要有两种,属性相似性方法和时序相似性方法,该方法的关键是定义适当的相似度量标准(即图 5 中的 3).文献[31]定义相似函数,比较属性相似程度聚合 IDS 的警报.而文献[32]认为"同种故障产生的警报通常发生在一个较小的时间窗口内,提出了基于时序的相似性方法聚合 IDS 的警报.相似性方法仅对每个警报的属性进行处理,无法识别出

警报间的因果关系,为此该方法需要与其它模型相结合.文献[33,34]分别将聚类算法和隐马尔科夫模型(HMM)相结合,分析最有可能的攻击序列和识别攻击的类型.

Peng Ning 等[35]和 Zhaowen 等[36]认为攻击的状态不是独立存在的,不同的攻击阶段是相互关联的,之前的攻击阶段为后续的攻击提供条件,这是因果关联方法(即图 5 中的 2)的基本思路.但是他们的方法需由专家指定入侵的条件和结果,以构建完整的攻击前因、后果数据库,可扩展性较差,不适用于大型网络.为此文献[37-44]分别提出数据挖掘方法、时间序列分析方法和机器学习方法挖掘警报之间的因果关系.这些方法既无需预定义知识库也无需网络的配置信息,就可以发现攻击行为之间的因果关系和识别未知的攻击行为.因果关联方法的优点是无需知道整个攻击过程就可以构造攻击场景,但是它无法处理 IDS 漏报的攻击行为,因此需要与其它方法相结合才能高效的工作.

为了解决因果关联方法的缺陷,提高关联的准确性,文献提出了交叉关联的方法[45-49],将因果关系与背景知识相结合,实现攻击场景的重建,有效解决了因果关联方法的缺陷.该方法通常使用背景知识(即图 5 中的相互补充的知识及 4、5),如:网络拓扑信息、脆弱性信息和主机配置信息等来融合、验证 IDS 的告警,以提高警报的质量,同时还可以分析告警的成功率和威胁程度,最终达到区分真实威胁和过滤误报的目的.此外,文献[50-54]提出了基于入侵本体知识的方法和将本体知识和背景知识相结合的方法,定义警报信息的语义,使用一系列预定义的语义推断规则得到警报信息间的隐含关系,高效地重建攻击过程.另外还有研究人员提出 multi-agent fuzzy consensus 态势感知框架[55]、蚁群算法[56]筛选信息,并借鉴于大数据的处理能力,利用大数据提供的平台和技术进行觉察分析,尤其是分析 APT 攻击[57],进一步提高了察觉的准确性.

2.4 存在的问题

纵观现有的研究工作,我们发现目前网络安全态势觉察在攻击活动的辨识方面仍存在着以下两个问题.

⑴觉察结果的精度.从觉察结果的正确性方面来说,IDS 系统固有的缺陷(存在大量的误报和漏报)对攻击活动的重构仍然有很大的影响.例如 IDS 的漏报会导致警报关联性缺失,将一个攻击活动分裂成两个攻击活动.从觉察结果的分辨率来说,攻击活动产生的痕迹信息量越多,越容易关联.

⑵觉察的效率.从实时性方面来说,现阶段的研究多采用离线的方式进行关联性分析和攻击过程重构,无法满足入侵防御系统的快速响应要求(即时的中断、调整或隔离一些不正常或是具有危害性的网络行为).从体系结构的可扩展性方面来说,警报关联系统存在的体系结构可分为三类:集中式体系结构、分布式体系结构及层次化体系结构[32].目前多数的研究采用在"集中式"体系结构处理 IDS 警报,但随着网络规模不断扩大,异构的程度不断增加,导致"集中式"关联方法日益复杂,难以扩展.

表 1 对上述各关联方法存在的主要问题(如:警报冗余消除、警报聚合、减少误报、识别已知的攻击、识别未知的攻击及漏报的假设推理等)进行比较,其中 √ 表示具备相应的能力,× 表示不具备相应的能力.

Table 1 Comparative analysis of existing techniques

表 1 方法比较

类别 / 方法	冗余消除	警报聚合	减少误报	识别已知的攻击	识别未知的攻击	漏报的假设推理
基于场景的方法	√	√	×	√	×	×
相似性方法	√	√	×	√	×	×
因果关系方法	√	√	√	√	√	×
交叉关联方法	√	√	√	√	√	√

3 网络安全态势理解

3.1 基本任务

网络安全态势理解是基于识别出的攻击活动及其特征,通过进一步分析这些攻击活动的语义以及它们之

间可能的关联关系来推断攻击者的意图,其主要任务包括识别这些攻击活动的源头、类型,并判断攻击者的能力、机会和攻击成功的可能性等.为了有效地推断攻击者的意图,目前多数研究分别从攻击行为本身和攻击目的两个方面进行分析.

3.2 攻击行为预测

所谓攻击行为预测,是要分析攻击行为间的逻辑关系,并以此来推断攻击行为的可能变化,其目的是通过对攻击行为的理解来推断其后续动作.常用的建模方法主要有马尔科夫模型方法、时间序列分析方法、博弈论及机器学习方法等.

马尔科夫模型用马尔科夫链刻画一组状态,用转移概率作为测度来描述状态之间的关系.有研究者采用变长马尔科夫模型(VLMM)和隐马尔科夫模型(HMM)对攻击者的行为建模,将一个攻击阶段视为模型中的一个状态,通过计算状态之间的转移概率来推测最有可能的攻击动作.Yang等[58]从攻击者能力、机会、意图及行为等角度出发,分别考虑了攻击者的能力、脆弱性的可渗透程度及资产重要性等信息,判断攻击行为的变化情况.而文献[59-62]无需考虑上述信息,分别采用 VLMM 和 HMM 方法对 IDS 警报建模,计算转移概率,分析攻击趋势.基于马尔科夫模型的方法存在三方面局限:首先该方法要求安全事件要求满足马尔科夫性的要求,即要求多步攻击的各阶段连续且没有攻击步骤丢失;其次该方法需要较长的观测序列对 HMM 模型的参数进行训练,否则不能保证模型训练结果的正确性;最后随着网络规模不断增大,攻击行为之间的状态转移概率难以计算,可扩展性不理想.

为了减少因使用大量数据集对模型的参数进行训练而产生的开销,Fachkha等和 Kim 等及Pontes等将时间序列分析技术[63-65]结合概率模型、数据挖掘等技术来分析 DDos 攻击特征及行为变化.时间序列分析是一种动态数据处理的统计方法,它的本质特征是相邻观测值的前后具有依赖性,即已知 T 时刻发生的事件,预测 T+1, T+2, …, T+n 时刻的事件.尽管该方法可以减少训练开销,但是它却无法有效处理大量的数据集,而 IDS 每天生产的警报数量巨大导致其性能较低.其次从准确性角度来说,该方法对数据的生成过程需要严格的假设,如滑动平均自回归模型要求攻击行为序列或其某级差分满足平稳性的假设,影响预测的准确性.

为了提高攻击行为识别的准确性,文献[66,67]将先验知识和贝叶斯网络相结合发现攻击者的行为知识,该方法需要一定的先验知识,文献[68-72]进一步提高了方法的适应性,分别提出伪贝叶斯网络方法,自适应的因果矩阵学习方法和决策树学习等机器学习方法,对攻击行为建模,分析其可能变化.尽管机器学习方法具有较好的收敛性和容错能力,即使在网络规模较大的应用环境下也可以较好的性能来处理大量数据,但是该方法仍需要适当的训练,以获得相应的参数,尤其在分类过程中,需要获得标记数据.

研究发现,上述方法均可以有效地分析攻击行为的可能变化,但是在需要主动防御措施的网络环境中,整个网络的安全态势随着攻防双方的交替行动而变化,仅知道攻击行为如何变化远远不够,为了较好的理解攻击者的意图,我们在知道攻击行为如何变化的同时还应采取有效的应对方案,以便降低风险,为此有研究者采用博弈论[73,74]来分析攻击者的战略思维,以便采取更好的防御策略,减少因攻击而造成的损失.

博弈论方法考虑了进攻方和防御方及普通用户三方因素,综合分析三方行为对被管网络产生的影响,同时它还可以根据攻击方的行动空间,给出最佳的加固方案,而上述其它方法仅从攻击行为本身的变化角度分析攻击方的意图,没考虑到后两者的作用.然而,随着网络的规模不断增大,攻击者的行动空间逐步复杂化,需要一定的近似处理,使得结果不一定准确,再加上还要考虑防御方和普通用户的行动空间,使得该方法的处理负担过大,缺乏可扩展性.其次从准确性方面来说,该方法仅讨论在最大最小策略下的应对方案,没考虑混合策略下的纳什均衡,使得其准确性不一定最优.

3.3 攻击目的理解

攻击目的理解基于被管对象中资产的功能及重要性,据此推断攻击者的攻击意图和进行攻击朔源.

Tang 等[75]从被保护对象的角度出发分析攻击者的目的,提出使用动态后向传播神经网络和协方差相结合的方法,基于当前每个主机的服务、攻击活动、服务重要性等分析可能要遭受攻击的服务.Yang等[58]利用虚拟

地形(Virtual Terrain)概念对当前的网络系统建模,结合攻击者的能力、脆弱性的可渗透程度及资产重要性,然后利用VLMM实时地处理IDS的警报,分析攻击行为的变化情况,实现对攻击意图的综合判断.赵文涛等人提出了攻击的分层认知模型[76],可实现对攻击步骤、攻击行为和攻击过程的认知,更好的理解其攻击意图.文献[77,78]通过构建攻击图刻画被管网络内的威胁路径,并计算攻击目标的最大概率攻击路径,这也可视为是对攻击流的建模过程.攻击图从攻击者角度出发,综合分析网络配置信息、漏洞信息等,枚举被管网络内的威胁路径,直观地表示被管网络内漏洞信息的关系.图中的结点表示攻击成功的可能性、攻击目标的重要性及危害的严重性等,边上的权重表示使用的攻击方法及利用的漏洞等,综合上述信息的流入、流出,实现状态转换,可用于刻画攻击的可能途径或攻击的可能进展.

3.4 存在的问题

首先从预测的准确的方面来说,相比博弈论和时间序列方法,马尔科夫模型方法、机器学习方法主要是先从历史数据中得到关联规则,在此基础上再进行分析,这种方案对已知的攻击行为能足够清晰和准确地分析出攻击者下一步要采取的行动,而对于一些新的攻击行为和相似攻击行为的变体需要额外处理,准确性有待提高.

其次从上述预测方法的性能角度来说,攻击活动是动态变化的,攻击活动产生的痕迹等相关信息庞大,传统的基于滑动窗口的批量处理方法不一定可行,无法扩展到实时的大规模的应用场景,为此需要实时的对警报进行优化和聚类.

最后,上述方法基于态势察觉提供的直接观察数据,与相关背景数据和历史数据的融合处理仅仅是初步和简单的,因此在攻击者身份识别与攻击活动溯源等方面比较薄弱.

4 网络安全态势投射

4.1 基本任务

网络安全态势投射的基本任务是基于识别出的攻击活动,评估已经出现的攻击行为对被管网络产生的危害和可能要发生的攻击行为对被管网络造成的潜在威胁.

网络安全态势投射一般模型由投射准备、风险评估技术和网络安全态势投射结果等三方面功能构成,如图 6 所示.投射准备将态势理解的结果映射到实际网络环境,确定被管对象面临的有效威胁.风险评估技术用来判断这些可能的威胁所产生的效果.态势投射结果综合判定系统中被保护对象需要应当的实际威胁.

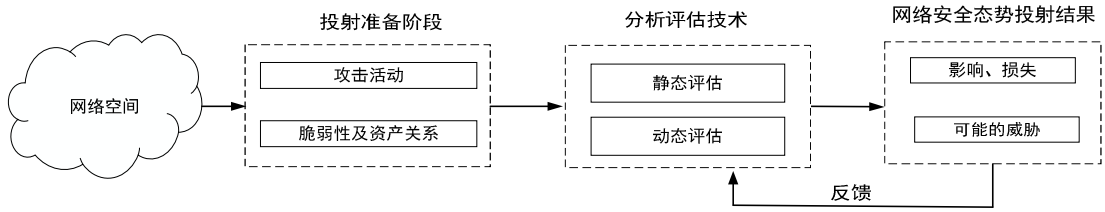

Fig.6 Network security situation projection model

图 6 网络安全态势投射模型

当前研究阶段存在静态评估和动态评估两种风险评估技术.静态评估是指在攻击发生之前,主动地分析和评估被管系统中存在的风险和隐患,支持全面预防性的安全响应决策.动态评估是指在攻击发生之时,基于当前的安全警报进行实时评估和预判型评估,以支持有针对性的动态安全响应决策.目前这方面的研究内容多集中在损失评估方面,即分析相关攻击活动对被管网络已经造成的危害.

损失评估是指网络安全人员根据网络安全态势觉察识别出来的攻击活动和其它检测设备的报告内容,借助数学工具等模型,分析它对网络、系统资源等诸因素已经产生的影响,为了有效的进行评估,研究人员采用了众多评估方法,传统方法包括贝叶斯技术、基于知识的方法、人工神经网络、模糊逻辑技术,引入的新理论有集对分析、 D-S 证据理论、粗集理论、灰度关联分析等.我们将上述研究方法大致分为三类:知识推理方法、

统计方法和灰度理论方法.

4.2 基于知识推理的方法

基于知识推理的方法是凭借专家知识及经验建立评估模型,通过逻辑推理分析整个网络的安全态势,其基本思想是借助概率论、模糊理论、证据理论等来表达和处理安全属性的不确定性,通过推理汇聚多属性信息.相关方法有两类:一类是基于图模型的推理,如贝叶斯网络、模糊认知图(Fuzzy Cognitive Maps,简称 FCM)[79]等;另一类是基于证据理论的推理,如 D-S 证据推理[80].

其中图模型的推理方法是通过有向图的状态转换来分析攻击活动对网络造成的影响.文献[81]使用贝叶斯网络对网络中"不确定因素"建模,计算攻击成功的概率,实时的评估攻击的严重程度.针对多目标优化问题,Poolsappasit等人提出了一个风险评估方法[82],使得管理人员在资源有限的情况下也能做出较好的决策.但因网络中的变量不是相互独立的,导致计算联合概率分布的成本较高,无法适用于大规模的网络环境.为此,Aguilar 等人结合了模糊逻辑与神经网络技术,在认知图[83]的基础上提出了 FCM 的概念,利用它获取网络中重要资产的依赖关系[84],进行危害程度评估.

基于图模型的推理使用有向图表示状态转换,图中隐含了概率、转换及推理相关知识,思路清晰,便于理解,但是在大多数情况下,变量之间不是相互独立的,条件概率及权重矩阵的计算比较困难,加剧了推理的难度,且图的存储开销较大,不适用于大型复杂的网络环境.为此,文献[85,86]设计了一个基于 D-S 证据理论的态势评估架构,融合不确定信息,进行不确定性推理,量化网络的安全态势.尽管评估过程中无需精确了解变量间的概率分布,在先验概率难以获得时,D-S 理论更加有效.但该方法仍具有一些缺陷[87]:(1)需要大量的先验数据来确定基本概率分配函数,同时要求证据间相互独立,目标假设间互斥;(2)计算量比较大,有潜在的组合爆炸问题;(3)其证据组合规则具有组合灵敏性,基本概率分配的微小变化常会导致组合结果的巨大差异.

4.3 统计方法

统计分析的目的是综合考虑影响网络安全的态势要素,构建一个评估函数,实现态势要素和整个网络态势空间的映射.王娟等讨论了态势要素的组成与结构[88].常用的统计方法有权重分析方法和层次分析法(Analytic Hierarchy Process AHP),该方法的关键是求得态势要素的重要性权值.

权重分析法基于资产在网络的重要性,通过为网络中的资源赋值,分析威胁的危害情况[89,90].该方法优点就是将网络安全态势觉察的结果直接作为态势评定函数的参数,拉近了数据融合层次之间的距离[1],但是在评估过程中缺乏合理的量化标准,在权重赋值过程中具有较强的主观性.为了克服这种主观性,Wang等[91]通过统计攻击者需要多少个不同 0-day 漏洞才能对系统造成破坏来评估网络的安全状况.

层次决策分析(Analytic Hierarchy Process)[92]由 Satty 等提出,该方法将定性分析与定量分析相结合,是一种无结构的多准则决策方法,通过思维过程的层次化和数量化,达到分析复杂问题的目的.陈秀真等[13]采用自下而上、先局部后整体的策略建立层次化网络安全威胁态势量化评估模型,在对报警发生频率、警报严重性及其网络带宽耗用率进行统计的基础上,采用逐层汇聚的方式对攻击、服务、主机以及整个网络的重要性权值进行加权,计算威胁指数,据此评估安全威胁态势.

层次分析方法通过两两比较构造判断矩阵,该方法从定性过渡到定量环节,依据经验估计的是相对权重比,而非绝对权重值,这在一定程度上降低了设置权重的难度,但仍无法摆脱人为主观判断,且需检验判断矩阵(反映了评估者的判断思维)的一致性,这往往要反复多次[93,94].

4.4 灰度理论方法

安全态势的趋势变化既有已知信息,也有未知和不确定信息,这种特点决定了安全态势风险值的变化作为一个"灰色系统"而存在.灰色系统理论[95]以"部分信息已知,部分信息未知的小样本、贫信息"的不确定性系统作为研究对象,并在此基础上提取有用信息.灰色系统利用累加生成或逆累加生成的新数据进行建模,有利于找出数据的变化规律,具有弱化原始数据的随机性,所需样本少,短期预测精度高等特点.

Juan L 等[96]提出了将无偏灰度理论(Unbiased Grey Theory)和马尔科夫理论相结合方法,分析网络的风险变化情况.但是 GM(1,1)适用于态势变化为线性的短期线性时间序列分析,不适用于非平稳随机序列.研究发现,

网络安全态势具有随机波动性的特点,且呈"S"曲线形状[97].基于 GM(1,1)的缺陷,Wei Hu 等[98]提出了改进的自适应灰度模型(Improved Adaptive Grey Verhulst Model),对网络安全态势呈"S"曲线的情况进行分析.

在网络安全态势投射研究过程中多数文献没有考虑到成本因素,文献[73,74,99,100]分别从损失成本的角度和响应成本的角度出发分析网络的安全态势投射,以期实现响应成本和预算之间的均衡.

4.5 存在的问题

从评估的准确性角度来说,同一攻击活动在不同的层面具有不同的语义,如:SQL 注入攻击在指令层表示某个内存单元污染,在网络层的语义表示网络会话中存在对受害者主机恶意的查询.这种不同的表现使得我们需要跨层面进行评估[101].单纯的单一层面的评估不能有效的量化产生的危害.

从评估的粒度方面来说,现有的评估结果相对简单.例如可以考虑损失评估在时间和空间维度上的投射.时间维度考虑风险的发生和修复在时间上的约束.空间维度考虑风险的传播范围,即在评估过程中需要考虑系统中资产的重要程度及依赖关系、脆弱性的等级、脆弱性可渗透的复杂程度等多种因素.

由于评估具有很强的主观性,目前缺乏不同评估方法之间的语义互操作性,这不利于网络安全态势感知系统之间的信息共享与协同.

另外我们还发现,现阶段的研究基本都集中在相对简单的静态损失评估方面,而从攻击行为的可能变化角度进行动态评估的研究不足,包括预警分析.

5 网络安全态势感知的研究方向

由于网络安全态势感知对于网络空间安全的重要性,这个领域的研究与应用日益活跃.例如美国国土安全部的先进研究计划署 HSARPA 于 2013 年 9 月发布的的网络空间安全战略研究计划中[102],第三个研究主题为网络安全(Network Security),其中有一个优先发展方向为互联网攻击建模(Modeling of Internet Attacks).这个优先发展方向中有四项任务与网络安全态势感知之间有关,包括开发满足网络安全态势感知需要的数据采集、分类和存储机制;开发新的网络安全态势可视化技术;支持跨域的网络安全态势感知信息共享;实现不同时间粒度的网络安全态势感知以满足从毫秒级攻击自动响应到 APT 检测的不同需要.这四个任务体现了网络安全态势感知的发展方向,特别是第四个任务很典型地反映了网络安全态势感知技术的应用目标.

基于对网络安全态势感知基本概念的理解,以及前面对这个领域相关研究进展的认识,我们认为这个领域目前还面临这样一些需要解决的关键问题.

(1) 海量异构测量数据的融合处理

网络安全态势感知所依赖的原始测量数据可以来自源于不同型号、不同实现技术、不同开发与生产者的网络运行管理系统、网络安全管理系统、主机管理系统和应用管理系统,这些系统产生异构的运行监测数据和日志数据,需要采用流式数据处理方式在不同的时间窗口内完成融合处理任务.目前这方面的研究明显是不够的,现有的大数据分析技术虽然可以提供一定的支持与借鉴,但这些方法对态势觉察的适用性还需要有针对性的研究.

(2) 不完全信息条件下的活动辨识

这个问题是指在测量系统存在漏报、误报、以及信息缺失的前提下,如何尽可能准确地辨识出网络中存在的活动.这类研究可以认为是源自网络入侵检测领域,但在网络安全态势感知的范畴中被赋予了更为广泛的含义.互联网的流量具有重尾的特性,传统的研究往往关注流量行为的典型部分和主要部分,例如像流量分类.但是在态势觉察中,不仅这些部分需要关注,小流量的零星行为也需要专注,例如 APT 检测的需要,而且不完全信息条件下这类活动的辨识更为困难.因此,这个领域需要更为精细的测量数据关联性分析方法.

(3) 网络活动的语义计算

从目前的实践看,网络攻击的意图识别基本上手工完成的,即需要依靠人工经验的判断.鉴于人的能力约束和相关人力资源的不足,这种人工实现方式对于网络安全态势感知的大规模应用带来极大的限制.因此很有必要研究网络活动特征提取和意图识别的机器处理方法,以提高网络安全态势感知系统的自治能力.尽管网络入

侵防范系统IPS领域的工作可以提供一定的基础,但从实现不同时间粒度的网络安全态势感知以满足从毫秒级攻击自动响应到APT检测的不同需要的角度看都是远远不够的.

(4) 网络态势的可视化

网络安全态势感知所处理的海量异构测量数据及其处理结果需要有合适的表示方式来加以表达和应用,可视化技术是一个公认的可行支持.HSARPA 在它的战略研究计划中也提到需要研究可扩展的可视化方法来支持态势感知数据的使用,包括带准确地理定位的可视化方法,支持 Drill-down 的可视化分析方法,以及适合不同用户使用和表达不同内容的可视化技术.

(5) 网络安全态势感知的协同

网络空间安全需要全球合作,至少在国家的层面要求合作的网络安全态势感知系统之间具有协同能力,就像 HSARPA 规划中所要求的那样.如果参照网络入侵检测领域的相关研究,对于合作机制的要求至少包括配置互操作性(即合作各方具有信息交换能力),需要有类似SNMP和IPFIX这样的标准协议;共享信息的语法互操作性,需要有类似 IDMEF 的标准数据结构;以及语义互操作性,例如描述网络安全态势的标准测度及其取值,这在网络入侵检测领域还是空白.此外,由于合作各方可能存在信息访问限制,如何实现信息共享与隐私保护的平衡把握是需要研究的问题.

(6) 更为完善的态势投射方法

目前的态势投射方法基本都是静态的,不能适应网络安全态势感知的过程需要.因此需要研究相应的动态态势投射方法,例如基于非合作不完全信息动态博弈理论设计带预警能力的态势投射方法.

6 结论

网络安全态势感知包括网络安全态势察觉、网络安全态势理解和网络安全态势投射三个层面,是一个完整的认知过程.它不是仅仅将网络中的安全要素进行简单的汇总和叠加,而是根据不同的用户需求,以一系列具有理论支撑的模型为支持,找出这些安全要素之间的内在关系,实时分析网络的安全状况.

网络安全态势感知是网络安全领域的研究热点,尽管已经得到较长时间的关注,但仍未形成完整的体系和明确一致的目标.在现有的网络安全态势感知的研究中,将其视为网络安全事件应用大数据处理和可视化技术的汇总结果的观点和将其视为基于网络安全事件融合计算的网络安全状态量化表达的观点都没有完整地反映其目标和任务;将其视为网络安全监测实现形式的观点则不够准确.为此,本文对网络安全态势感知概念进行重新定义,试图给出一个更为完整清晰的描述,以期抛砖引玉.

目前网络安全态势感知的研究是一个正处于发展中的课题,大部分研究都集中在重构攻击活动方面,基本都是网络入侵检测领域研究的延伸,已有很好的基础但也有很多问题需要研究和解决.另一方面,包括网络测量、网络流量行为学、网络管理技术、大数据处理技术、流式数据处理技术、可视化技术在内的其它相关领域的发展也为网络安全态势感知的研究提供了积极的支持.尽管网络安全态势感知的研究仍处于初级阶段,随着各种相关技术和研究的不断完善,网络安全态势感知技术将走向成熟和实用,为保障网络的安全起到越来越重要的作用.

致谢

本文的匿名评阅者对文章内容,特别是对网络安全态势感知定义的完善提出了许多建设性的意见和建议,作者在此一并表示感谢.

References:

[1] WANG Hui Qiang,LAI Ji Bao,ZHU Liang LIANG Ying.Survey of Network Situation Awareness System,Journal of Computer Science,2006,33(10):5-10(in Chinese with English abstract).

[2] Tim Bass.Intrusion Detection Systems And Multisensor Data Fusion:Creating Cyberspace Situational Awareness.Communications of the ACM,2000,43(4):99-105.

[3] Endsley,M.R.Toward a theory of Situation awareness in dynamic system.Human Factors,1995,37(1):32-64.

[4] Ulrik Franke,Joel Brynielsson.Cyber situational awareness A systematic review of the literature.Computers&Security,2014,46:18-31.

[5] V Lenders,A Tanner,A Blarer.Gaining an Edge in Cyberspace with Advanced Situational Awareness.Security&Privacy IEEE,2015,13(2):65-74.

[6] R.Bearavolu,K.Lakkaraju,W.Yurcik,H.Raje.A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks.Military Communications Conference,MILCOM '03.IEEE 2003,850-855.

[7] Erbacher R,Frincke D,Chung Wong P,Moody S,Fink G.A multiphase network situational awareness cognitive task analysis.Information Visualization,2010,9(3):204-219.

[8] Erbacher R,Frincke D,Wong P,Moody S,Fink G.Cognitive task analysis of network analysts and managers for network situational awareness.In:Proceedings of SPIE The International Society for Optical Engineering,2010,7530(1):423-426.

[9] Government of Canada,Public Safety Canada.Canada's Cyber Security Strategy,2010.http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[10] Bass Tim,GruberD,A glimpse into the future of id.USENIX&SAGE,1999,40-49.

[11] Ping Chen,Lieven Desmet,Christophe Huygens.A Study on Advanced Persistent Threats.IFIP,63-72,2014.

[12] Mandiant.APT1:Exposing One of China’s Cyber Espion age Unit,2013.

[13] Chen XZ,Zheng QH,Guan XH,Lin CG.Quantitative hierarchical threat evaluation model for network security.Journal of Software,2006,17(4):885-897(in Chinese with English abstract).

[14] XI Rong-Rong,XC Yun,YZ Zhang,ZY Hao.An Improved Quantitative Evaluation Method for Network Security.Chinese Journal of Computers,2015,38(4):749-758 (in Chinese with English abstract).

[15] XIN Dan,GAI Weilin,WANG Lu,LIU Xin,HU Jianbin.Survey of cyberspace situation awareness model.Journal of Computer Applications,2013,33(S2):245-250(in Chinese with English abstract).

[16] GONG Zheng-Hu,ZHUO Ying.Research on Cyberspace Situational Awareness.Journal of Software,2010,21(7):1605-1619(in Chinese with English abstract).

[17] George P.Tadda,JS Salerno.Overview of Cyber Situation Awareness.Springer US,2010,13(2):65-74.

[18] LIU XiaoWu,WANG HuiQiang,LÜ HongWu,YU JiGuo,ZHANG ShuWen.Fusion-Based Cognitive Awareness-Control Model for Network Security Situation.Journal of Software,2016,27(8):2099-2114(in Chinese with English abstract).

[19] Mica R. Endsley.Final Reflections: Situation Awareness Models and Measure.Journal of Cognitive Engineering and Decision Making, 2015, 9(1):101-111.

[20] Endsley M.Situation awareness misconceptions and misunderstandings,Journal of Cognitive Engineering&Decision Making,2015, 9(1):4-32.

[21] Goodall JR.Introduction to visualization for computer security.VizSEC 2007,1-17.

[22] Erbacher R.Visualization design for immediate high-levelsituational assessment.ACM International Conference Proceeding Series,2012,9(4):17-24.

[23] Shiravi H, Shiravi A, Ghorbani AA.A survey of visualization systems for network security.IEEE Trans.on Visualization and Computer Graphics,2012,18(8):1313-1329.

[24] F.Cuppens,R.Ortalo.Lambda:A language to model a database for detection of attacks.In RAID '00:Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection,2000,1907:197-216.

[25] P Bhatt,E Toshiro Yano,PM Gustavsson.Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks.IEEE International Symposium on Service Oriented System Engineering,2014,390-395.

[26] Sebastian Roschke,Feng Cheng,Christoph Meinel.A New Alert Correlation Algorithm Based on Attack Graph.CISIS,2011,6694(11):58-67.

[27] MassimilianoAlbanese,AndreaPugliese,V.S.Subrahmanian.Scalable Detection of Cyber Attacks.CISIM,2011,245:9-18.

[28] S Mathew,S Upadhyaya,M Sudit,A Stotz.Situation Awareness of Multistage Cyber Attacks by Semantic Event Fusion.Military Communications Conference,2010,1286-1291.

[29] A Aleroud,G Karabatis,P Sharma,P He.Context and semantics for detection of cyber attacks.International Journal of Information& Computer Security,2014,6(1):63-92.

[30] Hutchins Eric M.,Cloppert Michael J.,Amin Rohan M.Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.ICIW.2011,113-127.

[31] K. Julisch.Clustering intrusion detection alarms to support root cause analysis.ACM Transactions on Information and System Security, 2003,6(4):443-471.

[32] Saeed Salah,Gabriel Maciá-Fernández,Jesús E.Díaz-Verdejo.A model-based survey of alert correlation techniques.Computer Networks,2013,57(5):1289-1317.

[33] D Ourston,S Matzner,W Stump,B Hopkins.Applications of Hidden Markov Models to Detecting Multi-stageNetwork Attacks.Hawaii International Conference on System Sciences,2003,9:73-76.

[34] R Katipally,L Yang,A Liu.Attacker Behavior Analysis in Multi-stage Attack Detection System.Seventh Workshop on Cyber Security &Information Intelligence Research,2011,1-4.

[35] Peng Ning,Yun Cui,Douglas S.Reeves.Constructing Attack Scenarios through Correlation of Intrusion Alerts.In Proceedings of the 9th ACM Conference on Computer&Communications Security,2002,245-254.

[36] L.Zhaowen,L.Shan,M.Yan.Real-time intrusion alert correlation system based on prerequisites and consequence.in:Proc.of the Int.Conf.in Wireless Communications Networking and MobileComputing (WiCOM'10),2010,1-5.

[37] R.Katipally,W.Gasior,X.Cui, L.Yang.Multistage attack detection system for network administrators using data mining.in:Proc.Of the 6th Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10),2010,1-4.

[38] R.Sadoddin,A.A.Ghorbani.Real-time alert correlation using stream data mining techniques.InnovativeApplications of Artificial Intelligence,2008,(3):1731-1737.

[39] R Katipally,W Gasior,X Cui,L Yang.Multistage Attack Detection System for NetworkAdministrators Using Data Mining.Csiirw Proceedings of the Sixth Annual Workshop on Cyber Security&Information Intelligence R,2010.

[40] Bin Zhu,Ali A.Ghorbani.Alert Correlation for Extracting Attack Strategies.International Journal of Network Security,2006,(3):244-258.

[41] Mehdi Bateni,Ahmad Baraani,Ali Akbar Ghorbani.Using Artificial Immune System and Fuzzy Logic for Alert Correlation.International Journal of Network Security,2013(15):160-174.

[42] Chih Hung Wang,Ye Chen Chiou.Alert Correlation System with Automatic Extraction of Attack Strategies by Using Dynamic Feature Weights.International Journal of Computer and Communication Engineering,2016,(5):1-10.

[43] Sean Carlisto de Alvarenga, Bruno Bogaz Zarpel, Rodrigo Sanches Miani.Discovering Attack Strategies Using Process Mining.The Eleventh Advanced International Conference on Telecommunications,2015,119-125.

[44] Xinzhou Qin,Wenke Lee.Statistical Causality Analysis of INFOSEC Alert Data,Recent Advances in Intrusion Detection,International Symposium,RAID,2003,2820:73-93.

[45] Yan Zhai,Peng Ning,Purush Iyer,Douglas S.Reeves.Reasoning about Complementary Intrusion Evidence.Computer Security Applications Conference,2004,39-48.

[46] Sherif Saad,Issa Traore,Marcelo Luiz Brocardo.Context-Aware Intrusion Alert Verfication approach.International Conference on Information Assurance&Security,2015,53-59.

[47] F Alserhani,M Akhlaq,IU Awan,AJ Cullen,P Mirchandani.MARS:Multi-stage Attack Recognition System.IEEE International Conference on Advanced Information Networking&Applications,2010,4(4):753-759.

[48] Peng Ning,Dingbang Xu,Christopher G.Healey,Robert St.Amant.Building Attack Scenarios through Integration of Complementary Alert Correlation Methods.NDSS.2004,97-111.

[49] SJ Yanga,A Stotzb,J Holsoppleb,M Suditc,M Kuhld.High level information fusion for tracking and projection of multistage cyber attacks.Information Fusion,2009,10(1):107-121.

[50] Sherif Saad,Issa Traore.A semantic analysis approach to manage ids alerts flooding.International Conference on Information Assurance&Security,2011,156-161.

[51] Alireza Sadighian,Jos'e M.Fernandez,Antoine Lemay,Saman T.Zargar.ONTIDS A Highly Flexible Context-Aware and Ontology-Based Alert Correlation Framework.Revised Selected Papers of International Symposium on Foundations&Practice of Security-volume,2013,8352:161-177.

[52] Sherif Saad,Issa Traore.Extracting Attack Scenarios Using Intrusion Semantics.Springer Berlin Heidelberg,2013,7743:278-292.

[53] Sherif Saad,Issa Traore.Semantic aware attack scenarios reconstruction.Journal of Information Security&Applications 2013,18(18):53-67.

[54] Alireza Sadighian, Saman Taghavi Zargar, Jose'M. Fernandez, Antoine Lemay.Semantic-based Context-aware Alert Fusion for Distributed Intrusion Detection Systems.2013 International Conference on Risks and Security of Internet and Systems (CRiSIS),2013,1-6.

[55] Giuseppe D'Aniello,Vincenzo Loia,Francesco Orciuoli.A multi-agent fuzzy consensus model in a Situation Awareness framework.Applied Soft Computing,2015,30(c):430-440.

[56] Beaver J,Steed C,Patton R,Cui X,Schultz M.Visualization techniques for computer network defense.In: Proceedings of SPIE The International Society for Optical Engineering,2011,8019(18):6-9.

[57] Paul Giura,Wei Wang.Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats.ASE,2013,1(3):1-13.

[58] SJ Yang,S Byers,J Holsopple,B Argauer,D Fava.Intrusion Activity Projection for Cyber SituationalAwareness.Intelligence and Security Informatics.IEEE International Conference,2008,167-172.

[59] DS Fava,SR Byers,SJ Yang.Projecting Cyberattacks Through Variable-Length Markov Models.IEEE Transactions on Information Forensics&Security,2008,3(3):359-369.

[60] O.De Vel,N.Liu,T.Caelli,T.S.Caetano.An Embedded Bayesian Network Hidden Markov Model for Digital Forensics.In Proceedings of theInternational Conference on Intelligence and Security Informatics,ISI '06,2006,459-465.

[61] D. Lee,D.Kim,J.Jung.Multi-Stage Intrusion Detection System Using Hidden MarkovModel Algorithm.In Proceedings of the Inter-national Conference on Information Science andSecurity, ICISS '08,2008,72-77.

[62] Hamid Farhadi,Maryam AmirHaeri,Mohammad Khansari.Alert Correlation and Prediction Using Data Mining and HMM. ISeCure,2011,3(2):77-101.

[63] C Fachkha,E Bou-Harb,M Debbabi.Towards a Forecasting Model for Distributed Denial of Service Activities.IEEE International Symposium on Network Computing&Applications,2013,110-117.

[64] Kim,S.,Shin,S., Kim,H., Kwon, K.,Hen,Y.Hybrid intrusion forecasting framework for early warning system.In: IEICE transaction on information and systems,ACM,E91-D,2008,1234-1241.

[65] E Pontes,AE Guelfi,ST Kofuji,AAA Silva.Applying Multi-Correlation for Improving Forecasting in Cyber Security.International Conference on Digital Information Management,2011,179-186.

[66] Thonnard,O., Dacier,M. .Actionable knowledge discovery for threat intelligence support using a multi-dimensional data mining methodology.In:IEEE International Conference on Data Mining Workshops,2008,154-163.

[67] X.Qin ,W.Lee.Attack plan recognition and prediction using causal networks. Computer Security Applications Conf.,2005,370-379.

[68] Hanli Ren,Natalia Stakhanova,Ali A. Ghorbani.An Online Adaptive Approach to AlertCorrelation. DIMVA,2010,153-172.

[69] Mirco Marchetti,Michele Colajanni,Fabio Manganiello.Identification of correlated network intrusion alerts.2011 Third International Workshop on Cyberspace Safety and Security,2011,15-20.

[70] Ali Ahmadian Ramaki,Masoud Khosravi-Farmad,Abbas Ghaemi Bafghi.Real Time Alert Correlation and Prediction using Bayesian Networks.ISCISC,2015,98-103.

[71] Ali Ahmadian Ramaki,Morteza Amini,Reza Ebrahimi Atani.RTECA:Real time episode correlationalgorithm for multi-step attack scenarios detection.Computers&Security,2014,49:206-219.

[72] Mahbobeh Soleimani,Ali A.Ghorbani.Multi-layer episode filtering for the multi-step attack detection.Computer Communications,2012,35(11):1368-1379.

[73] G Yan,R Lee,A Kent,D Wolpert.Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense.Acm Conference on Computer & Communications Security,2012,553-566.

[74] Q Wu,S Shiva,S Roy,C Ellis,V Datla.On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks.Spring Simulation Multiconference,2010,1-8.

[75] Tang,C.,Wan g, X.,Zhang, R.,Xie,Y. .Modeling and Analysis of Network Security Situation Prediction Based on Covariance Likelihood Neural.Springer Berlin Heidelberg,2012,6840:71-78.

[76] Zhao WT,Yin JP,Long J.A cognition model of attack prediction in security situation awareness systems.Computer Engineering and Science,2007,29(11):17-19 (in Chinese with English abstract).

[77] Chen Xiao jun,FANG Bin xing,TAN Qin feng.Inferring Attack Intention Of Malicious Insider Based On Probabilistic Attack Graph Model.Chinese Journal of Computers,2014,37(1):62-72(in Chinese with English abstract).

[78] Ye Yun,Xu Xi shan,Qi Zhi chang.Attack Graph Generation Algorithm For Large-Scale Network System.2013,50(10):2133-2139.(in Chinese with English abstract).

[79] Aguilar Jose.A Survey about Fuzzy Cognitive Maps.International journal of Computational Cognition,2005,3(2):27-33.

[80] Lin Zhigui,Xu Lizhong,Yan Xijun,Huang Fengchen,Liu Yingping.A Decision-Making Method on D-S Evidence Fusion Information Based on Distance Measure.2006,43(1):169-175(in Chinese with English abstract).

[81] P Xie,JH Li,X Ou,P Liu,R Levy.Using Bayesian Networks for Cyber Security Analysis.IEEE/IFIP International Conference on Dependable Systems&Networks,2010,23(3):211-220.

[82] Nayot Poolsappasit,Rinku Dewri,Indrajit Ray.Dynamic Security Risk Management Using Bayesian Attack Graphs.IEEE Transactions on Dependable & Secure Computing,2012,9(1):61-74.

[83] Tolman E. C.Cognitive maps in rats and men.Psychological review.1948,55(4):189-208.

[84] Szwed, P.,P. Skrzynski.A new lightweight method for security risk assessment based on fuzzy cognitive maps.International Journal of Applied Mathematics and Computer Science,2014,24(1):213-225.

[85] ZY Qu,YY Li,P Li.A Network Security Situation Evaluation Method Based on D-S Evidence Theory.Environmental Science& Information Application Technology,International Conference,2010,2:496-499.

[86] S.Boyer,O.Dain, R.Cunningham.Stellar:A fusion system for scenario construction and security risk assessment.Proceedings of 13th IEEE International Workshop on Information Assurance, IEEE,2015,105-116.

[87] Wang li.Research on multiple classifier system based on fusion decision[Master's thesis].Xi'an University of Technology,China,2008,5-20(in Chinese with English abstract).

[88] Wang J,Zhang FL,Fu C,Chen LS.Study on index system in network situation awareness.Computer Applications, 2007,27(8):1907-1909 (in Chinese with English abstract).

[89] Xiangdong Cai, X.C., Y.J. Yang Jingyi, and H.Z. Huanyu Zhang.Network Security Threats Situation Assessment and Analysis Technology Study.International Journal of Security and Its Applications,2012,7(5):217-224.

[90] BJ Argauer,SJ Yang.VTAC:Virtual Terrain Assisted Impact Assessment forCyber Attacks.SPIE Defense&Security Symposium,2008,6973:69730F-69730F-12.

[91] L Wang,S Jajodia,A Singhal,S Noel.k-Zero Day Safety:Measuring the Security Risk of Networks against Unknown Attacks.European Conference on Research in Computer Security,2010,11(1):573-587.

[92] Satty T L.The Analytic Hierarchy Process.Springer New York,1996,4(29):49-68.

[93] Wang Z H,Zeng H W.Study on the risk assessment quantitative method of information security.The 3rd International Conference on Advanced Computer Theory and Engineering,2010,529-533.

[94] Ji X H,Pattinson C.AHP implemented security assessment and security weight verification.IEEE International Conference on Social Computing,2010,1026-1031.

[95] Deng JL.Gray Control System.Wuhan:Publishing House of Center-China University of Technology,1982,10(3)1-10.(in Chinese with English abstract).

[96] L Juan,L Tao,T Gang.A Network Security Dynamic Situation Forecasting Method.In:Internationl Forumon Information Technology and Applications,2009,115-118.

[97] Lai J B,Wang H Q,Zhu L.Study of Network Security Awareness Model Based on Simple Additive Weight and Grey Theory.Proceedings of 2006 International Conference on Computational Intelligence and Security,2006,1545-1548.

[98] Wei Hu,Jian-hua Li,Xiu-zhen Chen,Xing-hao Jiang.Network Security Situation Prediction Based on Improved Adaptive Grey Verhulst Model.Journal of Shanghai Jiaotong University,2010,15(4):408-413.

[99] I Kotenko,E Doynikova.Security Evaluation for Cyber Situational Awareness.High Performance Computing and Communications,2014,1197-1204.

[100] N Ghosh,I Chokshi,M Sarkar,SK Ghosh,AK Kaushik.NetSecuritas:An Integrated Attack Graph-based SecurityAssessment Tool for Enterprise Networks. Proceedings of the 2015 International Conference on Distributed Computing and Networking,2015,1-10.

[101] P Liu,X Jia,S Zhang,X Xiong,YC Jhi.Cross-Layer Damage Assessment for CyberSituational Awareness.Advances in Information Security,2009,46:155-176.

[102] https://www.dhs.gov/publication/fact-sheet-hsarpa.

附中文参考文献:

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

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

[14]席荣荣, 云晓春,张永铮,郝志宇.一种改进的网络安全态势量化评估方法.计算机学报,2015,38(4):749-758.

[15]辛丹,盖伟麟,王璐,刘欣,胡建斌.赛博空间态势感知模型综述.计算机应用,2013,33(S2):245-250.

[16]龚正虎,卓莹.网络态势感知研究.软件学报,2010,21(7):1605-1619.

[18]刘效武,王慧强,吕宏武,禹继国,张淑雯.网络安全态势认知融合感控模型.软件学报,2016,27(8):2099-2114.

[76]赵文涛,殷建平,龙军.安全态势感知系统中攻击预测的认知模型.计算机工程与科学,2007,29(11):17-19.

[77]陈小军,方滨兴,谭庆丰,张浩亮.基于概率攻击图的内部攻击意图推断算法研究.计算机学报,2014,37(1):62-72

[78]叶云,徐锡山,齐治昌,吴雪阳.大规模网络中攻击图自动构建算法研究.计算机研究与发展, 2013, 50(10):2133-2139.

[80]林志贵,徐立中,严锡君,黄凤辰,刘英平.基于距离测度的 D−S 证据融合决策方法.计算机研究与发展. 2006, 43(1): 169-175.

[87]王黎.基于融合决策的多分类器系统研究.西安理工大学硕士学位论文,2008,5-20.

[88]王娟,张凤荔,傅翀,陈丽莎.网络态势感知中的指标体系研究.计算机应用,2007,27(8):1907-1909.

[95]邓聚龙.灰色控制系统.华中理工大学出版社,1982,10(3)1-10.