

基于攻击图的网络安全度量研究综述

胡浩^{1,2}, 刘玉岭³, 张玉臣^{1,2}, 张红旗^{1,2}

(1. 信息工程大学三院, 河南 郑州 450001;

2. 河南省信息安全重点实验室, 河南 郑州 450001;

3. 中国科学院软件研究所可信计算与信息保障实验室, 北京 100190)

摘要: 网络安全度量面临的主要挑战之一, 即如何准确地识别目标网络系统中入侵者利用脆弱性之间的依赖关系进行威胁传播, 量化对网络系统的潜在影响。攻击图由于具备优越的可视化展示能力, 是解决该问题的有效途径之一。首先, 介绍了安全度量的概念、发展历程和通用测度模型; 然后, 阐述攻击图构建、分类和应用的相关研究; 其次, 提出一种基于攻击图的层次化安全度量框架, 从关键“点”、攻击“线”和态势“面”3个层次总结归纳了现有网络安全度量方法; 最后, 阐述了目前研究面临的难点问题与发展趋势。

关键词: 网络安全度量; 攻击图; 安全漏洞; 告警分析; 量化评估

中图分类号: TP393.8

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018072

Survey of attack graph based network security metric

HU Hao^{1,2}, LIU Yuling³, ZHANGYuchen^{1,2}, ZHANG Hongqi^{1,2}

1. The Third Institute, Information Engineering University, Zhengzhou 450001, China

2. Henan Key Laboratory of Information Security, Zhengzhou 450001, China

3. Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Abstract: One of the main challenges of network security metrics is how to accurately identify the intrusion of the intruders exploiting the dependence between the vulnerabilities for threat propagation in the target network system as well as to quantify the potential impact on the network system. Because of its superior performance of visual display, the attack graph becomes one of the effective ways to solve the problem. Firstly, the concept, development and general metric models of security metrics were introduced. Secondly, the related researches with respect to attack graph construction, classification and application were discussed. Thirdly, a hierarchical framework for security metric using attack graph was proposed, and then existing methods of network security metric were summarized from three levels (key “point”, attack “line” and situation “plane”). Finally, the difficult issues and development trends for the current research were discussed.

Key words: network security metric, attack graph, security vulnerability, alert analysis, quantitative assessment

收稿日期: 2018-06-15; 修回日期: 2018-08-10

通信作者: 胡浩, wjjhh_908@163.com

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA016006); 国家重点研发计划基金资助项目(No.2016YFF0204002, No.2016YFF0204003); 郑州市科技领军人才基金资助项目(No.131PLJRC644); “十三五”装备预研领域基金资助项目(No.6140002020115); CCF-启明星辰“鸿雁”科研计划基金资助项目(No.2017003)

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016006), The National Key Research and Development Program of China (No.2016YFF0204002, No.2016YFF0204003), The Science and Technology Leading Talent Project of Zhengzhou (No.131PLJRC644), The Equipment Pre-research Foundation During the 13th Five-Year Plan Period (No.6140002020115), The CCF-Venus Hongyan Research Plan (No.2017003)

1 引言

近年来,随着物联网、云计算、大数据等新兴技术的不断发展,计算机网络已经成为信息化建设的支撑性基础设施,深入渗透到政治、经济、军事、民生等各个方面,许多网络协议并不安全,软件应用多数存在安全漏洞,网络攻击事件频发,给政府、企业和个人带来潜在的安全威胁。

在全球范围内,互联网频繁地遭到攻击。赛门铁克公司近期公布了第22期《互联网安全威胁报告》,报告指出,大型企业在2017年内被作为攻击目标的平均次数超过3次,造成1.91亿条记录泄露。 ^{$\frac{3}{4}$} 的常用网站存在重大安全漏洞,用户

隐私面临严重窃取风险。2016年,僵尸网络Mirai通过入侵摄像头等物联网设备,发动了大范围DDoS攻击,造成法国网络服务提供商OVH和Brian Krebs个人网站大规模瘫痪;2016年8月,比特币交易平台Bitfinex被黑客盗走约6580万美元的比特币;2017年5月,勒索攻击“WannaCry”在全球范围内肆意传播,短短数小时内席卷数十个国家,发动的攻击次数达到上万次,政府、企业、医疗、高校等各行业均有IT设备中招,再次敲响了网络安全的警钟。

在我国,网络攻击的种类与数量也在持续增长,网络安全面临严峻挑战。2017年4月,国家互联网应急中心(CNCERT)公布的《国家互联网网络安全态势报告》,通过对Gafgyt僵尸网络抽样检测,在第一季度,42.5万台物联网智能设备被恶意服务器操控,总计发起DDoS攻击超过1.8万次,其中有72次DDoS攻击的峰值流量在5Gbit/s以上。国家信息安全漏洞共享平台(CNVD)发布的全年安全漏洞累积超过1万个,较上年度增幅为33.9%,包括4000多个高危漏洞,其中“零日”漏洞为2203个,增长率高达82.5%,漏洞主要涵盖Google、Oracle、Adobe、Microsoft、IBM、Apple、Cisco、Wordpress、Linux、Mozilla、Huawei等诸多知名软件厂商,由于我国工业控制系统规模庞大,恶意探测和基于漏洞利用的定向攻击,大量的安全漏洞带来了严重安全隐患。漏洞发现不及时,漏洞风险监控不准确,使用户持续遭受攻击威胁,因此我国互联网安全状况不容乐观。

网络攻击由以往的孤立事件,演变为大规模、多阶段、协调攻击,实施多步攻击已成为当前的主流攻击行为。例如,Zeus僵尸网络^[1],防御网络多步攻击已刻不容缓。因此亟需研究面向多步攻击的网络安全度量及防御策略选取方法,以提高对多步攻击的识别与防护能力,增强对网络攻击行为的认知、理解和度量。

网络安全事件层出不穷,攻击渗透日益猖獗,亟需科学全面地度量网络安全状况。2002年,ACSA与MITRE Corporation联合开展了关于信息系统安全度量的研讨,指出信息系统的安全度量通过一系列评估过程,从一个偏序集中选取与系统安全质量相关的值,用于表征、描述或预言系统安全的信任程度。一般而言,信息安全相关的质量涉及信息的机密性(confidentiality)、可用性(availability)和完整性(integrity)这3方面,安全度量是通过收集、分析与信息安全管理相关的数据,并给出报告以协助信息安全决策、改善信息安全状况的过程。

目前,越来越多的国内外学者从事面向多步攻击的网络安全度量研究,其研究机构主要包括麻省理工学院林肯实验室、堪萨斯州大学、科罗拉多州大学、乔治梅森大学、加利福尼亚州立大学、卡内基梅隆大学、中国科学院信息安全国家重点实验室、清华大学、北京大学、哈尔滨工业大学、北京邮电大学、国防科学技术大学、上海交通大学等国内外知名科研院所。其研究成果频现于《IEEE Transactions on Information Forensics and Security》《IEEE Transactions on Dependable and Secure Computing》《ACM Transactions on Information and System Security》和《ACM Conference on Computer and Communications Security》等国际高水平期刊会议上,取得了显著的研究成果,但仍存在一些问题,表现在管理人员缺乏对网络攻击行为刻画及风险状况进行科学定量分析的方法,同时,攻击行为分析及安全度量的科学性、准确性、规范性、全面性有待进一步提高。

攻击图通过枚举所有可能的攻击路径,直观地描述多步攻击过程,具备优越的可视化展示能力,是解决该问题的有效途径之一。基于攻击图的网络安全度量指从攻击图中提取与攻击行为相

关的安全信息。目前研究者已开发多种攻击图自动生成工具，兴起了基于攻击图的安全度量研究的新一轮热潮。综上，开展面向多步攻击的网络安全度量研究具有重要的理论意义和广阔的应用前景。

2 安全度量

安全度量模型和方法的研究主要分为两大类：一是基于标准体系的安全度量模型和方法研究，该类研究的优点是范围更广；二是学者归纳提炼的安全度量模型和方法研究，该类研究的优点是针对性更强。基于攻击图的网络安全度量则属于第二类，它从攻击者视角出发，可视化地展示了所有可能的入侵路径，对于测度攻击行为，重构攻击场景，分析安全威胁具有重要意义。

本节首先介绍安全度量的概念，然后分析了信息安全度量发展历程，并给出基于标准体系的信息安全度量的和模型。

2.1 安全度量概述

度量一词源于自然科学，也被称为测量，有较长的发展历史，常用于描述度量的词有 measure、metric、score、rating、estimate、evaluate、assessment 等。Roberts^[2]指出：事物可被度量的程度，决定了发展不完备和完备的科学差距，正如管理学常言，不能被度量就不能被管理，这一说法来源于管理学之父 Lord Kelvin 的 “If you can't measure it, you can't improve it”。经典的度量研究领域包含质量管理、软件度量、工程能力成熟度量等。对于信息安全也同样成立，“没有规矩，不成方圆”，安全度量为信息系统的安全性提供了

量化准则。

2.2 信息安全度量的发展

在信息安全管理领域，信息安全度量是指“一个行为或一组行为，利用测量形式对一个实体的属性进行测度，获取量化值”。针对信息安全度量，Sademies^[3]认为，如果没有度量，信息安全保障水平就只能靠猜测和估计。近些年，信息安全量化模型、方法和指标体系引起了学者的广泛关注。通用的信息安全度量方面的研究包括：美国国家标准和技术学会（NIST）的 SP800-55《信息技术系统安全度量指南》，国际标准化组织 ISO 的 SC27 分委会的 IS027004《信息安全管理测量》等。

国际上，信息安全标准化工作起源于 20 世纪 70 年代中期，其发展历程如图 1 所示，作为计算机系统安全度量的首个正式标准，美国国防部于 1985 年颁布可信计算机系统评价标准（TCSEC，Trusted Computer System Evaluation Criteria）意义重大，TCSEC 标准定性地将安全程度划分为 D、C1、C2、B1、B2、B3、A1 这 7 个安全级别。1991 年，欧洲共同体发布了信息安全技术安全度量准则（ITSEC，Information Technology Security Evaluation Criteria）。1991 年，美国对 TCSEC 进行修改，并在补充吸收 ITSEC 优点的基础上，发布了美国信息技术安全度量联系标准 FC，在美国政府、民间和商业领域得到广泛应用。1993 年 6 月，美国、加拿大、英国、法国 4 国共同起草了信息技术安全度量公共标准（CCITSE，Common Criteria of Information Technical Security Evaluation），简称 CC，是目前国际上最通行的信息安

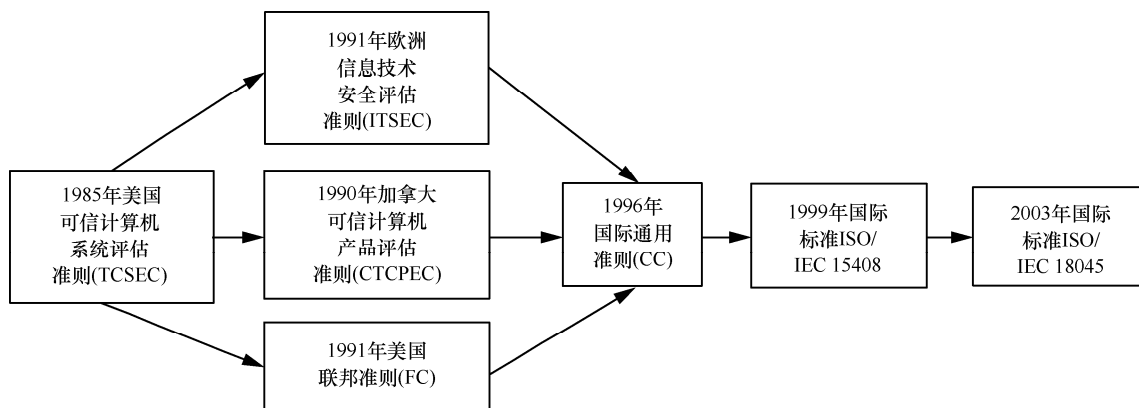


图 1 信息安全测评认证的发展历程

全技术产品及系统安全性评估标准，也是信息安全度量结果国际互认的基础。

我国在信息安全度量领域的研究开展较晚，当前仍处于起步发展阶段，国内信息安全标准化工作多借鉴国际标准。1998年10月，由国家质检总局牵头成立了中国国家信息安全测评认证中心，是我国专门从事信息技术安全度和风险评估的权威职能机构。公安部主持制定、国家质量技术监督局颁布的国家标准 GB17895-1999《计算机信息系统安全等级划分准则》已正式颁布并实施，定性地将信息系统安全划分为5个等级。随后，2002年4月，国家信息安全标准化技术委员会正式成立，同年颁布了 GB18336《信息技术安全技术评估准则》，作为度量信息技术产品与信息安全特征的基础准则。2009年，开始正式实施《信息安全风险评估规范 GB20984》。近些年，伴随着信息化驱动引领经济社会发展作用的凸显，国家逐步重视和支持网络安全工作，网络安全已上升到国家战略层面，2014年2月，着眼国家安全和长远发展，中央网络安全和信息化领导小组成立，负责统筹协调国家网络安全和信息化重大问题，显著提高了国家的信息安全保障能力。

2.3 信息安全度量模型

信息安全度量模型是一个将信息需求与相关属性关联起来的结构，描述了如何量化有关安全属性，并转变能为决策提供基础的指标，参照国

际标准 ISO/IEC27004:2009，文献[4]给出的一种信息安全测量模型，如图2所示。

模型包括以下要素：度量方法、基本度量、度量函数、导出函数、分析模型、指标、决策准则和度量结果。对度量对象的多种安全属性实施度量方法，得到基本度量，单个度量目标可能包含多个安全属性，需要提取对基本度量有用的属性作为模型输入。度量方法是以规定标准量化属性的逻辑操作集合。度量函数是为输出度量结果而组合基本测试执行的计算，度量函数包括多种，如对基本度量计算平均值，或者对基本度量取方差和标准差，抑或加权后求和，度量函数是一个或多个基本度量的组合。指标是对模型输出度量结果进行评估的测量标准，并将它们与决策准则相结合。分析模型是将多个导出度量与决策进行结合的算法。决策准则衡量度量结果置信度的阈值，决定下一步的行动方案。

3 攻击图技术

网络安全度量作为信息安全度量中的一个研究分支，受到学术界和工业界的广泛关注，而实施网络系统安全度量的一个重要工具是攻击图，目前研究者已开发多种攻击图自动生成工具，兴起了基于攻击图的安全度量研究的新一轮热潮。攻击图借鉴图论的相关知识分析网络中的脆弱性利用关系，是当前研究多步攻击

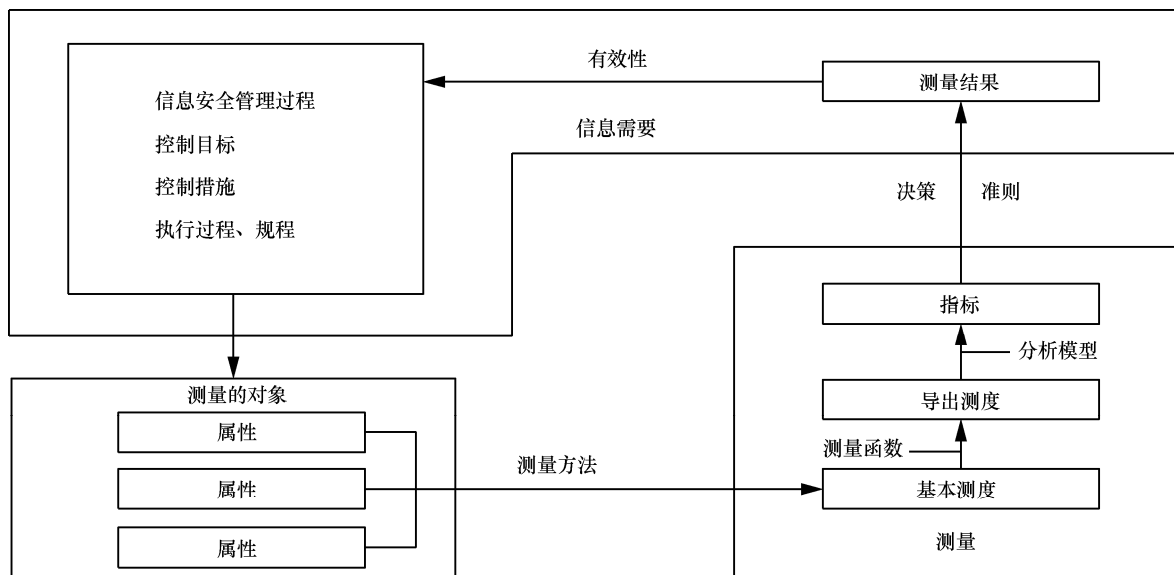


图2 信息安全度量标准模型

的重要工具，它从入侵者视角出发，通过分析网络环境和漏洞信息，在图中枚举全部入侵路径，直观地展示不同攻击步骤间的因果关系，以及漏洞利用造成的潜在威胁。下面分别从攻击图构建、攻击图分类和攻击图应用 3 个方面进行介绍。

3.1 攻击图构建

在攻击图技术的发展过程中，攻击图的构造是基础和核心，经过不断的发展和改进，攻击图构造方法由手工向自动构建逐步推进，由仅适用于小型网络向大规模网络不断发展。

1) 手工构建

表 1 给出典型攻击图手工构建方法的分析与比较。

利用模型检测手段生成攻击图时，包括基于网络状态和主机状态 2 种方式。基本原理是首先对网络或主机中的关联要素进行编码，利用有限状态机模型刻画状态变迁过程，并通过检测工具搜索反例，每个反例对应一条攻击路径，将全部反例对应的路径进行整合生成攻击图。

基于逻辑推理的攻击图生成方法中，通过形式化描述网络配置信息、主机信息和安全策略等要素信息，建立规则刻画原子攻击，并应用逻辑推理工具还原攻击场景，如 Ou 等^[5]利用形式化描述语言 Prolog 设计攻击图生成方法。

基于图论的攻击图构建，以网络连通性、

网络配置、主机信息以及网络漏洞信息为输入，利用图论的理论知识，通过设计攻击图生成算法，输出由初始状态到目标状态的可能攻击路径信息。

2) 自动构建

为提升攻击图的构造效率，开发人员已研制了多种攻击图的自动生成软件，如 MuVAL、NetSPA、TVA 等^[6]，常见的攻击图自动构建工具比较如表 2 所示。

MuVAL (multi-host, multi-stage vulnerability analysis) 是一种多主机多漏洞分析工具，由 Ou 等^[7]牵头开发的一个开源项目，可用于大规模企业网络的攻击图生成，目前已开放源代码，利用逻辑编程语言 Datalog 表示网络元素间的安全联动关系。MuVAL 的输入是网络连通性信息、网络漏洞、主机/网络配置、访问策略。具体实施时，首先利用 Nessus 或 OVAL 等工具扫描系统漏洞信息，然后将上述网络元素利用 Datalog 语言形式化表述后，作为推理引擎的输入，并输出可能存在的一条攻击路径。MuVAL 的网络数据采集能力强大，能够自动提取 ICAT/NVD 漏洞数据库信息，生成攻击模板，为采集到的漏洞提供利用前提和结果影响的参考。实验数据表明，对于包含 2 000 台主机的模拟网络，生成攻击图的时间在 15 s 左右，当包含 n 个网络节点时，该工具的算法复杂度为 $O(n^2)O(n^3)$ ，符合多项式时间要求。在得到所有可能的攻击路径后，使用 Graphviz

表 1 攻击图手工构建方法比较

采用方法	节点	边	单调性	搜索策略
模型检测	否	网络状态	状态转换	逆向
	是	主机状态	原子攻击	深度优先
逻辑推理	是	逻辑状态、攻击规则	依赖关系	逆向
基于图论	是	状态、条件及漏洞节点	依赖关系	广度优先

表 2 攻击自动构建工具比较

构建工具	是否开源	展示界面	复杂度	特点
MuVAL	是	命令行界面	$O(n^2)$	攻击图生成准确度高
TVA	否	图形界面	$O(n^6)$	实现网络渗透的自动分析，商用软件，收费昂贵
NetSPA	否	图形界面	$O(n \log n)$	环形攻击图，商用软件
Skybox View	否	图形界面	$O(n \log n)$	网络配置信息采集全面，商用软件
AGT	否	图形界面	$O(2^n)$	Linux 平台工具，生成复杂度高

图形生成器自动绘制并输出 pdf 和 jpg 格式的攻击图文件, 由于 MulVAL 生成攻击图准确度高, 并具有较好的可扩展性, 得到了工业界和学术界的一致认可, 已广泛应用于网络可行性验证和性能测评。

TVA (topological vulnerability analysis) 是一种基于拓扑脆弱性分析的攻击图生成工具^[8], 由美国乔治梅森大学的 Noel 等提出, 在分析网络攻击的渗透过程, 结合攻击步骤和攻击条件构建完整的多步攻击图, 并分析网络配置的脆弱性, 但攻击模板仍需要手工录入, 缺乏自动化的模板生成方法, 且算法的空间复杂度高达 $O(n^6)$, 应用到大规模网络时存储空间消耗过高, 此外, TVA 的网络脆弱性信息输入完全依赖漏洞扫描工具 Nessus^[9], 漏洞扫描结果不准确也会影响 TVA 的分析结果, 由于自动化程度低及扩展性不高的限制, 目前应用不是很广泛。

NetSPA (network security planning architecture) 是 MIT 林肯实验室的项目, 该软件在 2008MIT 企业竞赛中胜出, 并基于 NetSPA 组建了 CyberAnalytix 公司, 现已转化为一款商用软件, NetSPA 的网络模型包括主机、端口和漏洞, 由 Nessus 扫描得到上述信息, 并利用自动化工具提取 NVD 和 Bugtraq 漏洞数据库信息。生成的攻击图包含 3 类节点: 状态节点、前提条件节点、漏洞节点。其中, 状态节点代表入侵者获得的主机权限; 前提条件节点表示实现该状态, 攻击者需要具备的前提权限, 状态节点与前提条件节点通过有向边连接; 前提条件节点与漏洞节点相连, 表示具备此前提条件, 可利用该漏洞, NetSPA 算法复杂度是 $O(n \log n)$ 。

Skybox View 也是一款商用软件^[10], 通过对网络建模, 并模拟攻击后生成报告, 与 NetSPA 类似, 通过 Nessus 扫描漏洞, 能够实现攻击图的自动化构建。AGT (attack graph toolkit) 由 Sheyner 等^[11]设计, 基于 Linux 操作平台, 利用该工具可生成状态攻击图, 状态节点表示系统全局状态, 节点连接边表示状态转移, 但构建算法的复杂度为指数级。2009 年, 加利福尼亚州立大学的 Danforth 等^[12]提出了一种改进的基于策略驱动的脆弱性分析工具 EVA (evolutionary vulnerability analysis), 该工具支持多种网络安全分析, 允许

管理人员依据指定的使用规则和需求进行安全分析, 采用渗透类的抽象模型显著降低了攻击模板的匹配速度, 通过对相似主机进行聚类, 构建 meta-machine, 有效减小了攻击图规模, 提高了攻击图的构建效率。

3.2 攻击图分类

1) 状态攻击图

法国国家科学研究中心的 Dacier 等^[13]首先提出了特权图 (privilege graph), 利用特权图描述攻击状态, 故又称为状态攻击图, 描述了入侵者在攻击过程中的权限提升过程, 在特权图中, 节点代表攻击者获取的权限, 边代表网络系统中存在可被攻击利用的漏洞, 其中, 特权指攻击者为实现既定攻击意图, 所需要获取的权限集合。随后, Phillips 等^[14]用节点表示网络状态变量集合, 边表示攻击者的原子攻击动作集合, 通过从目标节点单向回溯搜索路径并生成攻击图, 该方法的时间复杂度呈指数级增长。

卡内基梅隆大学的 Cimatti 等^[15]在分析不同网络组件和脆弱性关联关系的基础上, 提出使用模型检测器 NuSMV 产生入侵反例, 生成违背安全属性的攻击路径, 在此基础上构建状态攻击图, 包括主机描述、网络连通性、入侵起点和攻击方法等要素信息, 在一次运行中可以找出多个违反安全性的反例。

此外, 其他学者提出了多种状态攻击图生成方法, 加州大学的 Templeton 等^[16]提出了需求 (require) 和供给 (provider) 的攻击链设计模型, 需求代表攻击产生的前因, 供给表示攻击导致的后果, 攻击表示攻击者具有的能力集合, 基于利用能力集合构建攻击模板, 满足相应网络组件需求, 攻击形式化描述借用编程语言 JIGSAW。

为了提升大规模目标网络中攻击图的构建效率, 叶云等^[17]采用攻击图建模语言 AGML 形式化描述漏洞知识库和目标环境, 通过对目标环境进行预处理, 并建立安全属性索引, 最后结合攻击模式实例化技术构建攻击图, 提高了攻击图构建方法的可扩展性。

一般而言, 状态攻击图可以用一个二元组 $AG = (E, V)$ 表示, 其中, E 是边的集合, 表示一次漏洞利用 (原子攻击动作), 任意边 $e \in E$ 都表

示攻击者的状态迁移； V 表示状态节点集合，对于任意 $v \in V$ ，用一个四元组 $\langle hos, ser, vul, oth \rangle$ 表示，其中， hos 、 ser 、 vul 、 oth 分别表示此状态对应主机、服务、漏洞和其他信息（IP 地址、端口号等），图中允许出现重复的状态节点。如图 3 所示，其中， $sshd_bof(0, 1)$ 指主机 0 上的攻击者利用主机 1 的 $sshd$ 漏洞发起缓冲区溢出攻击，从而获取主机 1 的 User 权限。

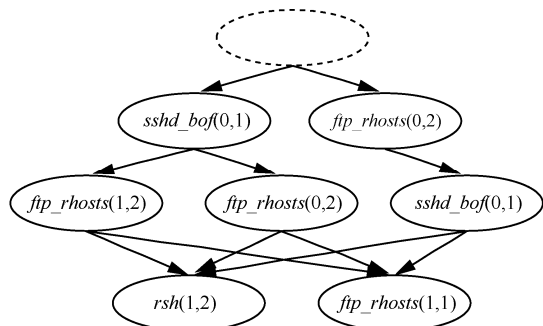


图3 状态攻击图

从状态攻击图的构建过程可知，由于可包含重复的状态节点，随着目标网络中主机和漏洞数量的增加，攻击图规模呈现指数级递增，难以满足实际大规模网络的应用需求。

2) 属性攻击图

为了解决状态攻击图的状态爆炸问题，Ammann 等^[18]提出了攻击单调性假设，即入侵者在渗透过程中不会针对已有权限发起重复攻击，基于该假设，可以将状态攻击图的规模由指数级降低为多级式级别，学者相继提出了多种属性攻击图生成方法，增强了应用的可操作性。

属性攻击图中，存在两类顶点和连接边，两类顶点分别是条件和脆弱性，其中，条件顶点表示攻击者具备的前提权限，脆弱性顶点表示主机配置错误和软件漏洞等，表征通过该脆弱性能获取

的权限，两类边分别为：由条件顶点指向脆弱性顶点的边指代脆弱性利用的前提，由脆弱性顶点指向条件顶点的边指代脆弱性利用的后果。

属性攻击图 $AG = (C, V, E)$ ， C 为条件集合， V 为漏洞集合， E 为边集合，对于 $\forall v \in V$ ， $Pre(v)$ 为 v 的父节点集合， $Post(v)$ 为 v 的子节点集合，则当父节点之间存在“与”关系且满足 $(\wedge Pre(v)) \Rightarrow (\wedge Post(v))$ 时，表示利用漏洞 v 的所有前提条件都满足，此次漏洞利用成功，触发其后置结果。对于 $\forall c \in C$ ， $Parent(c)$ 是 c 的父节点集合，若父节点间存在“或”关系，且满足 $(\vee Parent(c)) \Rightarrow c$ ，表示 $Parent(c)$ 中任意一个前提条件被满足，都使后置结果 c 成立。如图 4 所示，椭圆表示原子攻击节点，矩阵表示攻击者的状态节点。例如， $trust(1, 0)$ 表示主机 1 信任主机 0， $ftp_rhosts(0, 1)$ 表示主机 0 上的攻击者利用主机 1 上的 ftp_rhosts 漏洞，建立到主机 1 的信任关系，实现远程登录主机 1。

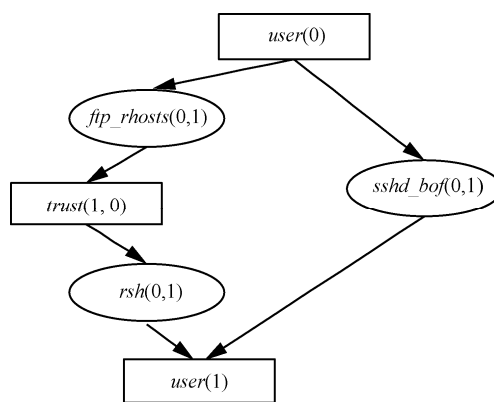


图4 属性攻击图

3.3 攻击图应用

由于攻击图结构灵活，适用于多层面的网络安全分析和评估，给出最小化的网络加固方案，其应用拓展如图 5 所示，包括查找攻击路径、取

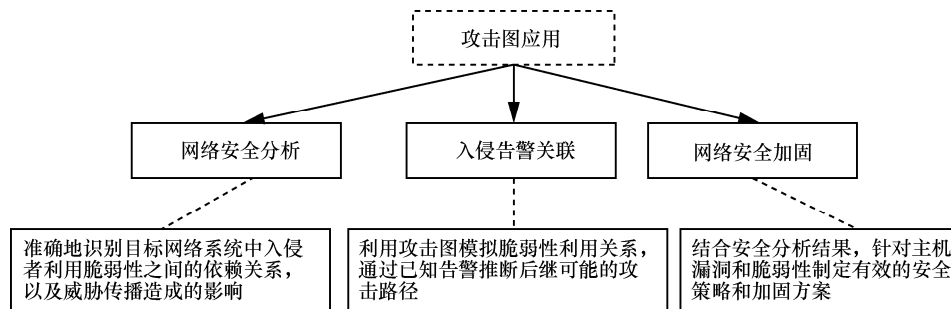


图5 攻击图在安全领域的应用

证分析、安全度量、基于IDS的告警关联、优化防御措施等,尤其在网络安全分析、入侵告警关联、网络安全加固3个方面成果突出。

1) 网络安全分析

对于网络安全度量而言,其研究的困难性在于如何精准地分析、鉴别目标网络系统中,不同脆弱性被攻击者利用的依赖关系,以及威胁传播带来的影响,直观的可视化功能是攻击图的最突出特点,也是解决上述问题的有效方法之一。攻击图枚举了所有可能的脆弱性利用关系,通过在攻击图中模拟攻击步骤,重现攻击场景,能够为安全防御提供更有效的策略指导。

2) 入侵告警关联

告警关联是指攻击过程中,采集入侵检测系统(IDS)的告警数据,利用攻击图模拟脆弱性利用关系,通过已知告警推断后续可能的攻击路径。传统的IDS告警关联仅分析了漏洞利用间的依赖关系,缺少对具体网络环境信息的考虑,导致误报和漏洞较多。由于攻击图描述了系统漏洞利用的因果关系,能够反映威胁的传播过程,因此,结合攻击图对IDS告警数据进行关联,能够提高多步攻击预测的准确性,还原真实的攻击场景,同时减小IDS漏洞和误报。例如,发现某条攻击路径中存在一个原子攻击未产生告警,而攻击者已具备后续攻击状态,则认定此处可能存在漏报,通过提高告警关联的准确性能够有效评估攻击者的可能意图。

3) 网络安全加固

安全加固是在安全度量的基础上,针对度量后的主机漏洞和脆弱性制定有效的安全策略和加固方案,由于攻击图的结构灵活性,既能展示整体又能反映局部安全状态的变迁过程。

考虑安全加固具有相对性,当弥补某个漏洞所要支付的成本高于对网络安全性的提升价值时,此类弥补不具有实际意义,因此脆弱性加固的意义如下。

① 安全威胁排序,网络中需要着重保护的安全目标是什么?辨别需要首先修复的脆弱性节点?哪条路径最有可能被攻击者利用?

② 威胁影响度量,即网络配置更新,防护措施增强能在多大程度上降低安全风险,如何量化

防御效果,进而选择最优防御策略是一个“what if”类型的问题。

不仅如此,随着信息安全形势的日益严峻,软件更新升级加速,恶意软件 and 后门程序泛滥,大量系统脆弱性和软件缺陷暴露,脆弱性修复的重要性日益突显,安全加固涉及网络布局、安全策略调整、配置更新和补丁管理等多个方面。例如,在实施补丁管理时,需要从系统整体安全出发,鉴别关键漏洞,并决定修复的优先次序。特别地,对于大规模网络,孤立地考察单个主机的脆弱性意义不大。需要着重分析漏洞之间被利用次数以及补丁间的依赖关系,如被利用次数最多的漏洞的修复优先权重高,即使与该漏洞所在主机相连的其他主机数量不多,如何在存在多个脆弱性主机的前提下选择最优加固措施,综合考虑加固成本和防御效果成为安全加固的研究重点。

4 基于攻击图的网络安全度量框架

本节首先定义了相关网络安全要素的形式化表示;其次通过分析攻击过程,描述攻击行为,定义攻击图模型;最后从攻击图中的“点”“线”“面”3个不同层面出发,建立层次化的网络安全度量模型。

4.1 网络元素模型化

网络系统上布置了大量的主机和网络组件,运行着复杂多样的应用程序和服务程序,随着网络结构和布局变化,网络拓扑和连通关系动态变化,因此首先需要对网络建模,即形式化描述网络元素,包括主机及服务信息、网络结构、网络配置和脆弱性信息以及网络攻击信息等,通用的描述方法如下。

定义 1 主机信息 H 。主机信息反映了网络中不同主机的特性和特点,可以利用主机标识、服务和端口、运行的程序和软件、系统漏洞、主机权重信息来刻画,具体地,可以用一个五元组 $\langle HostIp, Services, SoftV, Vuls, Weight \rangle$ 表示。

$HostIp$ 表示主机地址信息。

$Services$ 表示主机开放的服务和端口信息,通常用服务名称或者服务开放的端口号表示,如Apache、TCP、Radius、UDP等。

$SoftV$ 是主机上的软件列表,包括操作系统的

类型和版本号, 如 Windows XP SP2、Red Hat Linux 7.2 等。

Vuls 是该主机上的脆弱性与漏洞列表, 可以用统一脆弱性标识符 CVE 表示, 如 CVE-2014-0063 表示一种执行任意代码漏洞。

Weight 是该主机在网络中的重要程度, 当主机包含的资产价值高时, 对应重要性权重越高。

定义 2 脆弱性集 V 。表示网络配置或服务软件存在的漏洞集合, 对于脆弱性 $v \in V$, 使用一个七元组 $\langle id, type, IP, p(v), impact, time, info \rangle$ 表示。

id 表示该脆弱性的唯一标识, 可以用其在 CVE 中对应的编号表示。

type 表示该脆弱性的类型, 包含配置错误和应用程序缺陷, $type \in \{C_Error, Vulner\}$, *C_Error* 表示配置错误类型, *Vulner* 指系统漏洞的类型。

IP 指存在脆弱性的主机网络地址。

$p(v)$ 指脆弱性被入侵者成功利用的概率。

impact 指脆弱性被利用给网络资产带来的危害性, 通用漏洞评分标准 (CVSS) 给出了威胁影响得分, 得分范围为 (0, 10), 得分越高, 表明该漏洞的危害越严重。

time 表示该漏洞首次发布于 SIP (security information providers) 的时间, 若该脆弱性的类型为 *Vulner*, 否则 $time = \emptyset$ 。

info 指脆弱性信息的具体描述。

定义 3 拓扑结构。表示网络中主机间的连接关系, 形式化表示为 $\langle N, E \rangle$ 。

N 是主机节点集合。

E 是节点间连接边的集合。

定义 4 网络连通性。指不同主机间的通信关系。管理者会配置网络安全策略, 保护网络系统的关键资产, 使非授权主机禁止访问隔离区内的主机, 或仅允许经过指定协议和端口实现互通。使用一个四元组 $\langle host_s, host_d, protocol, port \rangle$ 描述网络的通连关系。

$host_s$ 表示发起通信请求的源主机, 用主机的 IP 地址表示。

$host_d$ 表示发起被请求访问的目的主机, 用主机的 IP 地址表示。

protocol 表示源主机 $host_s$ 向目的主机 $host_d$

发起连接请求的通信协议。

port 表示源主机 $host_s$ 连接到目的主机 $host_d$ 的端口号。

4.2 攻击图模型

在网络发展初期, 由于攻击技术和工具的限制, 多以无明显目的的零散攻击为主, 主要包括破解口令和利用操作系统的一些简单漏洞, 攻击的持续性和关联性不强。随着网络结构的复杂化和攻击手段的不断发展, 如今的网络攻击已普遍发展为多步骤的复杂攻击。

由于网络结构日趋复杂, 网络入侵者通常难以直接攻入其感兴趣的目标, 如网络隔离区 (DMZ) 的后台数据库, 因此往往采用“迂回”路径, 如先攻入 DMZ 区域内的文件服务器, 获得其 Root 权限, 再以此为跳板尝试攻击内部主机, 因此, 理论上一次攻击需要通过多个步骤完成。近年来, APT (advanced persistent threat) 攻击已成为当前网络系统遭受最严重的攻击之一, 具有攻击目标性强、漏洞利用潜伏周期长的特点。例如, 一个针对 Soloris 平台的 Sadmind 漏洞的 DDoS 攻击, 攻击者利用 Soloris 平台的 Sadmind 程序的缓冲区溢出缺陷, 经过探测、非法入侵、安装 Mstream DDoS 傀儡软件和实施 DDoS 攻击等多个步骤实现整体攻击。其攻击步骤如图 6 所示, 前一个步骤的成功实施往往是后一个步骤开始的前提条件。

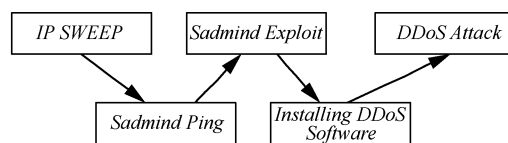


图 6 多步攻击的 5 个步骤流程

定义 5 攻击图 (AG)。图 7 给出一攻击图示例, 可以形式化表示成一个四元组 $AG = (S, A, E, \Delta)$, 其中, S 表示状态节点的集合, A 表示原子攻击节点的集合, E 表示节点间的连接边集合, Δ 表示不同状态节点间转移概率的集合。

$S = \{S_i | i = 1, 2, \dots, n\}$ 表示状态节点集合, 初始状态节点构成集合 O , 攻击意图状态节点构成集合 G 。

$E = S \times A \cup A \times S$, $e \in S \times A$ 表示攻击者拥有该前提条件, 才能发起原子攻击 a , $e \in A \times S$ 表示发起原子攻击 a 后, 使攻击者拥有的后置结果。

$e_{i,j} \in S \times S$, $e_{i,j}$ 表示连接节点 S_i 和 S_j 的有向边 $S_i \rightarrow S_j$, 实现 $e_{i,j}$ 依赖的原子攻击为 $a_{i,j}$, $\Delta(e_{i,j}) \in \Delta$ 表示攻击者由状态 S_i 转移到 S_j 的概率, 即 $\Delta(e_{i,j}) = p(S_i \rightarrow S_j)$, 且 $\Delta(e_{i,j})$ 等于原子攻击 $a_{i,j}$ 的发生概率 $p(a_{i,j})$; 若节点 S_i 到 S_j 不可达, 令 $\Delta(e_{i,j}) = 0$ 。

4.3 层次化的安全度量框架

作为网络安全保障不可缺少的部分, 网络安全度量以网络系统为度量对象, 针对网络可能受到攻击的概率、意图、路径、风险以及策略等进行多角度、全方位的量化测评, 为防御决策提供指导。层次化的安全度量框架如图8所示, 随着网络安全要素的不同拓展、安全数据的不断丰富、攻防手段的不断演进, 研究人员对于网络安全的认知按照“点—线—面”的趋势逐级深入展开, 第5节将以此为脉络介绍各层次典型安全度量方法。

5 基于攻击图的网络安全度量方法

本节以攻击图为依托, 首先围绕安全脆弱性

这一关键“点”; 然后依据攻击“线”程开展纵向的安全建模分析, 从“点”和“线”2个视角都很难看到网络系统整体的安全状况; 最后开展网络系统安全态势“面”评价, 通过总结归纳现有攻击图中的安全度量方法, 对比分析了各方法的特点和不足。

5.1 关键“点”安全度量

网络系统的脆弱性来源于自身设计上的缺陷, 脆弱性被恶意攻击者利用后, 可能导致系统异常甚至瘫痪, 进而导致更严重的后果, 从这一点出发, 网络系统脆弱“点”安全性度量是整个研究的基础, 分析基于脆弱性利用的攻击图中单个节点的转移概率, 特别地, 研究安全脆弱性模型、脆弱性利用规律、脆弱性安全风险, 能够为主动防御提供理论基础和技术支撑, 下面分别进行介绍。

在脆弱性分析模型研究方面, 陈恺等^[19]构建了多周期的软件漏洞发布模型, 从整体出发, 推断安全漏洞的数目与软件程序开发时间上的联系; 相反, 聂楚江等^[20]从微观层面出发, 通过构建安

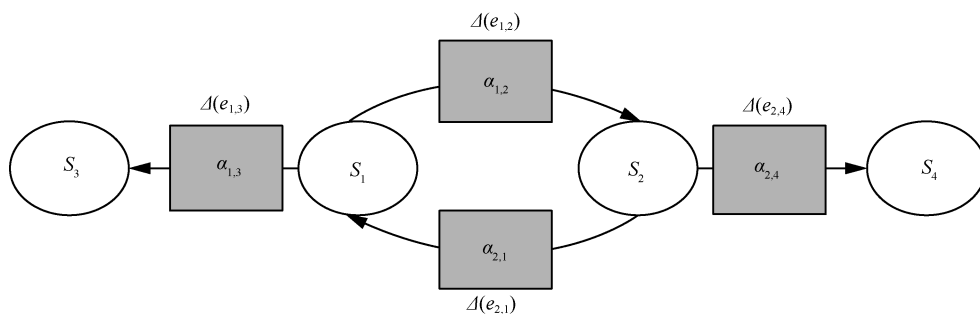


图7 攻击图示例

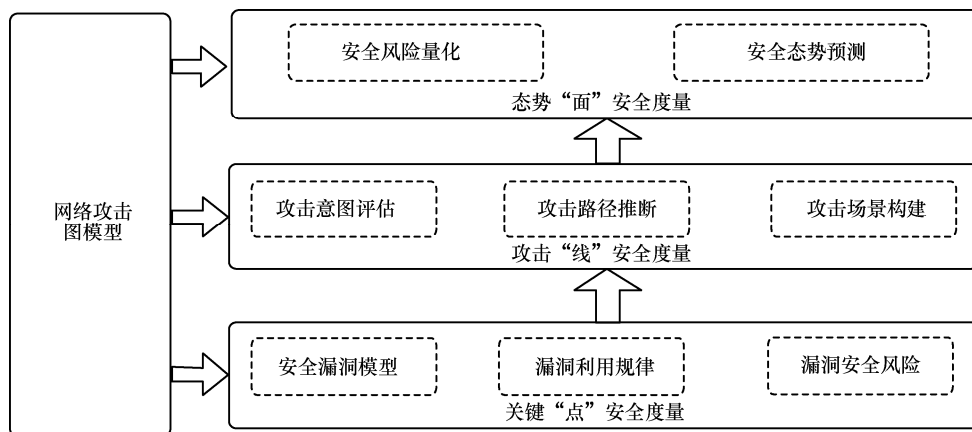


图8 网络系统安全度量框架

全漏洞数量推测模型，研究了程序代码等微观参数的影响，通过关联旧版本软件程序包含的漏洞数量，推断新版本的漏洞数量。类似地，高志伟等^[21]依据漏洞严重程度对漏洞进行分类，设计的预测模型不仅能测度生命周期过程中，软件包含的漏洞数目和漏洞产生时间间隔，而且能分析漏洞的类型及每一种类型漏洞的数目。

美国 CERT 计算机应急响应组织的 Arbaugh 等^[22]首先引入了漏洞生命周期概念，研究了安全漏洞从诞生到消亡过程中所处的不同状态，通过分析美国 CERT/CC 报告，揭示了近年来处于不同生命周期状态的漏洞数量分布。Frej^[23]借鉴系统动力学理论构建了漏洞生命周期模型，然而受实验数据集规模的限制，未深入探讨不同软件厂商的漏洞数量分布情况。法国国家科研中心的 Kaaniche 等^[24]通过研究开源的 OSVDB 漏洞数据库，发现漏洞处于不同生命周期过程的时间长度与其操作系统类型相关，并在 Windows、Unix 和 Mobile OS 操作系统中进行了对比验证。通过引入攻击热度和攻击技术，宋明秋等^[25]在时间维度上对漏洞生命周期进行建模，通过构建 Mamdani 模型量化测度漏洞的时间维度风险。可以看出，现有成果集中于探索漏洞数量在软件开发阶段、部署操作系统和生命周期时间维上的分布情况。如何关联漏洞数量、生命周期、可利用性、威胁影响与风险等多重度量要素，构建全面可靠的漏洞分析模型是后续研究的重点。

在脆弱性利用规律研究方面，文献[26]分析了零日漏洞的生命周期过程，通过枚举 Linux 和 Microsoft 系统漏洞信息，探讨攻击脚本和脆弱性补丁扩散对脆弱性利用概率的影响。美国科罗拉多州大学 Joh 等^[27]将漏洞生命周期划分为产生、发现、公布、利用和修复 5 个阶段，分析了不同阶段的安全风险程度。作为脆弱性评价行业的公开标准，美国国家基础设施咨询委员会发布的通用脆弱性评分系统准确测度了漏洞的脆弱性利用和威胁影响得分，通过查询美国国家漏洞数据库 (NVD) 得到具体值。国际权威漏洞披露组织 CVE 公布了漏洞字典，实现了对漏洞的统一命名，依据软件厂商、威胁影响及漏洞数目对漏洞进行分类统计。NVD 依据 CVSS 对超过 7.5 万个已知漏

洞进行了评分。OSVDB 提供了开源的漏洞数据集，用于查询包括漏洞生命周期、发布时间、厂商和补丁等信息。密歇根州立大学 Shahzad 等^[28]针对包含 4 万多个漏洞的开源数据集 OSVDB 进行了统计分析，展示了近 20 年不同软件厂商漏洞在生命周期各阶段的数目分布状况，并预测补丁发布周期以及脆弱性利用平均耗时的变化趋势，结果表明，脆弱性利用平均耗时小于补丁开发的平均耗时。该类研究成果侧重于统计学分析，通过大量数据揭示脆弱性利用概率和耗时受软件厂商、补丁发布时间等因素的潜在影响。未来研究可以尝试历史数据分析，提取先验知识，提炼脆弱性利用规律，推测后续发展趋势，对增强研究的实际性具有重要意义。

在脆弱性风险评价方面，Cox 等^[29]考虑漏洞利用产生的威胁影响和利用发生的可能性，依据威胁严重性将漏洞划分多个级别，构建了漏洞风险评估矩阵，利用综合评估法量化信息系统的风险级别。Mkpong 等^[30]通过专家评估法测度漏洞属性对系统的安全影响，构建了基于属性评估的漏洞风险度量模型。上述方法操作方便，但严重依赖领域知识，侧重于已知漏洞评价，评估结果具有一定的主观性。为此，付志耀等^[31]在漏洞属性评估时，借鉴粗糙集理论对关联属性进行约简，提升了评估结果的客观性和准确性，且保证了操作的简便性。Houmb 等^[32]利用已知漏洞数据集训练 Bayesian 信念网络，推断脆弱性被利用的概率及威胁度，并预测未知漏洞的风险等级。在实际应用中，周亮等^[33]借鉴层次分析法，评估了智能电网中调试管理子系统安全漏洞的风险等级，相关研究已广泛应用于安卓移动应用终端、Web 应用程序、电信通用设备以及工业控制系统等相关行业。

综上，现有网络系统脆弱“点”安全度量集中于静态评估，具备算法复杂度低、操作简便的优势，然而，随着网络系统规模的不断增大和复杂异构网络的融合，单个漏洞节点风险在生命周期内动态变化，伴随漏洞信息发布和攻击工具的快速传播，网络风险持续增加，针对单个脆弱“点”，实现在时间维度上动态测度风险，为进一步测度整个网络的宏观风险提供了理论参考。

5.2 攻击“线”安全度量

网络系统单个脆弱“点”的危害有限,通过一系列脆弱点的利用形成攻击“线”渗透,直至完成攻击目标,会产生更为严重的后果,因此实现入侵意图和路径等攻击“线”信息的评估,分析可能的攻击路径,预测潜在的攻击行为,挖掘关键威胁节点,对于安全管理员深入理解攻击者可能的威胁行为具有重要意义。

在攻击意图评价方面,意图推断是网络管理人员实施安全防护的重要手段之一,入侵意图可能性度量为网络安全态势量化提供了数据基础,通过降低攻击发生概率,为进一步实施网络加固和入侵响应提供方法指导,使网络状态向安全方向转移。爱达荷大学的 Yu 等^[34]利用隐彩色 Petri 网对多种攻击行为节点进行区分,通过告警关联预测可能的入侵路径。MIT 林肯实验室的 Sheyner 等^[35]通过马尔可夫决策推理,基于条件转移概率分析非确定性攻击节点。北京理工大学的彭武等^[36]结合时间自动机分析节点状态和节点间的依赖关系,并推算攻击成功概率,精准分析攻击意图的成功概率。

鲍旭华等^[37]利用扩展的有向图描述单步攻击的类别及其逻辑关系,依据攻击链的累计权值计算攻击的可能性,通过对告警信息关联匹配来识别攻击意图。为了提高预测结果的准确性,中科院计算技术研究所的陈小军等^[38]在攻击图模型的基础上构建攻击状态转移概率表,计算多个攻击步骤间的累积成功概率,用累积概率表征攻击意图实现的最大概率,并推断最大概率攻击路径。北京大学的诸葛建伟等^[39]借鉴人工智能领域的规划识别方法,设计基于扩展目标规划图的攻击规划识别算法,挖掘海量告警信息背后蕴藏的攻击意图及规划。上述研究的重点是如何客观衡量攻击状态间的转移概率,在此基础上分析最有可能的攻击意图,但实验攻击场景仅包含一个攻击目标,当攻击场景中包含多个可能的攻击目标时,研究如何量化不同攻击目标的期望成功概率,识别最大可能攻击意图还有待进一步探究。

在攻击路径度量方面,吕慧颖等^[40]构建威胁状态转移图描述威胁事件的时空联系,实时挖掘威胁状态信息,动态测度入侵路径。信息工程大

学的王硕等^[41]和阿根廷国家核心安全研究中心的 Sarraute 等^[42]分别利用改进的 Dijkstra 算法和 Floyd 算法分析最短攻击路径,有效降低了路径搜索的时间复杂度。Ortalo 等^[43]结合攻击图分析入侵路径数量,总数越多表明攻击意图的实现手段越丰富。美国诺瓦东南大学 Li 等^[44]利用路径长度的算术平均值推断最可能的攻击路径长度。为了全面评估路径长度信息,麻省理工学院的 Idika^[45]提出一整套基于攻击图的多维路径度量方法,进一步分析了路径长度的中位值、标准差和模式,通过计算平均值和中位值的差值,发现短攻击路径并及时修复,对长度低于 2 个标准差数量级的路径提前防范,统计不同路径长度模式的出现频率,掌握全网不同攻击路径长度的概率分布。Bopche 等^[46]综合比较上述度量方法,进一步分析了动态网络环境中度量结果随时间的变化规律。北京邮电大学的 Dai 等^[47]利用模糊综合评估法,通过量化路径数量和长度,挖掘风险流路径,但未研究节点的威胁性排序。

IBM 公司的 Abraham 等^[48]引入漏洞生命周期刻画入侵路径长度随漏洞发布时间的变化规律,更贴合实际网络环境。国防科技大学的刘强等^[49]通过构造最佳漏洞利用链,推测最大可能入侵路径。加拿大纽布伦斯威克大学的 Zhu 等^[50]通过告警聚类与关联分析,利用神经网络技术复原攻击场景,分析可能的攻击策略,类似研究还包括路径数量的评估、平均路径长度的度量、最短耗时路径的推测等。Bopche 等^[51]在上述研究的基础上,进一步分析了动态网络环境中度量随时间的变化规律。密苏里科技大学的 Nayot 等^[52]通过量化不同攻击路径的安全风险,优先阻断高威胁路径,但未给出路径不同主机节点的威胁性排序。

5.3 态势“面”安全度量

将复杂的攻击行为信息映射为简单直观的安全威胁态势,于是平“面”化的安全态势度量应运而生,该类方法通过分析系统的资产、脆弱性、威胁得出其安全风险,从而可以迭代性(以评估轮次为代表)地针对网络系统开展全方位体检,进而对其中的高等级安全风险进行预警,提高安全管理员操作的针对性。现有安全态势度量方法主要可以划分以下 3 类。

1) 基于时空序列的方法

该类方法假设网络面临的安全威胁变化遵循一定的周期性和规律,通过分析时空维度上安全态势变化的前因后果,预测后续变化趋势。Qu等^[53]基于多源告警信息融合,分析网络安全态势,并运用D-S证据理论量化测度安全态势,但多证据融合时存在悖论问题。在上述研究中,若攻击图节点的发生概率度量不准确,则可能影响攻击路径预测的准确性。

为此,中科院信息工程研究所的席荣荣等^[54]通过分析告警特征,改进了告警数据源证据的有效性,增强了预测精度,但该方法主要适用于短期预测。杨豪璞等^[55]设计了面向网络多步攻击的安全态势评估方法,通过分析攻击阶段,识别攻击轨迹,重构攻击场景,量化评估攻击场景的威胁影响,但未给出网络安全状态变化趋势的分析。中科院软件研究所刘玉岭等^[56]全面融合网络环境信息、攻击方和防护方态势要素,但未给出态势变化阶段的起止时间节点。自回归移动平均模型(ARIMA)^[57]和指数平滑模型(ES)^[58]是2种常用的时间序列预测模型,能够应用于随时间平稳变化序列的分析,由于实际网络中安全事件突发,应用于网络安全态势预测时难免产生偏差。

2) 基于图论的方法

此类方法通过分析网络脆弱性信息,构建攻击状态转移图,从入侵者视角出发,结合当前攻击者状态信息对未来状态迁移进行预测。Liu等^[59]通过挖掘告警序列,结合隐Markov模型,利用Viterbi算法推测最大可能状态迁移序列,识别攻击意图,但该方法未具体量化网络风险值。Fredj等^[60]应用吸收Markov链描述攻击状态转移过程,基于告警关联分析,识别攻击意图,预测攻击行为,但未考虑历史攻击行为信息,其有效性还有待进一步论证。Ghasemigol等^[61]研究了安全事件发生的不确定性,提升了预测精度。上述方法从不同维度度量了攻击行为的特征,但都缺乏对网络整体安全态势的量化评估。

3) 基于博弈论的方法

此类方法着重考虑攻防对抗网络环境,借鉴博弈理论推断攻防双方最可能采取的行为策略,

在此基础上综合分析网络安全的态势变化,其优势在于态势要素选取最为全面。中国科学院计算技术研究所的Wang等^[62]基于网络拓扑和系统漏洞信息,利用随机Pertri网设计攻防博弈模型,实现了对攻击发生概率、平均耗时和可能路径的评估。中国科学技术大学的张勇等^[63]构建了用户、管理员和威胁三方参与的博弈分析模型,通过构建威胁传播网络,总结威胁传播规律,展示安全威胁的演变趋势。Chen等^[64]设计了Markov博弈模型,基于数据融合方法预测威胁,并感知安全态势变化。针对电网系统,上海交通大学的Wu等^[65]基于大数据分析,结合模糊聚类和博弈论,提出的态势感知机制显著提升了预测效果。上述方法未量化态势变化的具体时间,且未对不同类型的攻击者进行区分。

6 结束语

随着攻击图技术应用的逐步成熟,基于攻击图的网络安全度量已取得初步研究成果,但如何借鉴攻击图科学、准确、全面地度量网络安全状态,并为防御决策提供实际指导还有待进一步研究,归纳起来,进一步的研究可以考虑以下几个问题。

1) 系统脆弱性度量,当前针对脆弱性节点的安全性度量未深入讨论脆弱性利用概率随时间的变化规律,以软件漏洞为例,现有研究缺乏对漏洞生命周期整体的考虑,后续可以在以下3方面进行改进:① 安全漏洞模型侧重于漏洞数量预测和漏洞挖掘;② 需考虑存在漏洞的软件厂商,结合该厂商的历史漏洞发布信息,探索漏洞整个生命周期中的利用概率变化,以便更科学、真实地反映时间维度上的漏洞利用规律;③ 精难度量漏洞利用对网络系统造成的威胁影响,结合漏洞生命周期过程,量化评估时间维度上的动态风险,给出更客观精确的漏洞风险度量方法。

2) 攻击行为度量,目前的研究侧重于丰富度量指标层面,随着度量维度的不断细化,度量不准确的问题逐渐显现,原因在于理论模型基于攻击者的“单调性”假设,即攻击者一旦获取某一攻击能力将不会再次获取,因而攻击路径不会被重复利用,本质上是一种理想的攻击场景,事实

上, 由于攻击者对网络结构不熟悉, 攻击者往往选择最有可能实现的攻击目标作为入侵意图, 且实际攻击场景中可能存在重复的状态转移行为, 产生有向有环攻击图, 迫切需要对更能反映现实网络的实际攻击行为进行建模与度量分析。

3) 攻击威胁度量, 通过对攻击方、防护方和网络环境态势要素的动态关联, 实现多角度、全方位的攻击行为度量。具体地, 在以下3方面有待改进: ① 考虑不同入侵者的实际漏洞利用能力不同, 威胁度量过程应对攻击者进行有效区分; ② 现有面向攻击的安全度量侧重于分析攻击意图、成功概率和入侵路径, 缺乏入侵各阶段发生时间的测度; ③ 如何客观地度量攻击对网络系统产生的潜在影响, 设计面向攻击的安全态势量化方法还有待进一步探究。

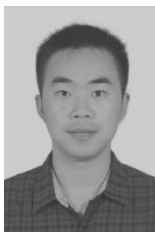
参考文献:

- [1] 江健, 诸葛建伟, 段海新, 等. 僵尸网络机理与防御技术[J]. 软件学报, 2012, 23(1): 82-96.
JIAN J J, ZHUGE J W, DUAN H X, et al. Research on Botnet mechanisms and defenses[J]. Journal of Software, 2012, 23(1): 82-96.
- [2] ROBERTS F S. Measurement theory with applications to decisionmaking, utility, and the social sciences[M]. Addison-Wesley Advanced Book Program, 1979.
- [3] SADEMIES A. Process approach to information security metrics in Finnish industry and state institutions.[C]//Intrinsic Multiscale Structure and Dynamics in Complex Electronic Oxides. 2004.
- [4] 陈长松. 信息安全测量与态势分析关键技术研究[D]. 上海: 上海交通大学, 2012.
CHEN C S. Research on key technologies of information security measurement and situation analysis[D]. Shanghai: Shanghai Jiaotong University, 2012.
- [5] OU X, BOYER W F, MCQUEEN M A. A scalable approach to attack graph generation.[C]//ACM Conference on Computer and Communications Security (CCS 2006). 2006:336-345.
- [6] SHEYNER O, WING J. Tools for generating and analyzing attack graphs[J]. Lecture Notes in Computer Science, 2003, 3188: 344-372.
- [7] OU X, GOVINDAVAJHALA S, APPEL A W. MulVAL: a logic-based network security analyzer[J]. Usenix Security Symposium, 2005: 8.
- [8] JAJODIA S, NOEL S. Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response[J]. Algorithms, Architectures And Information Systems Security, 2005:285-305.
- [9] BEALE J, DERAISON R, MEER H, et al. Nessus network auditing[M]. Elsevier, 2004.
- [10] HUSTON B. Skybox view 3.0[J]. Information Security, 2006.
- [11] SHEYNER, MIKHAIL O. Scenario graphs and attack graphs[J]. Dissertation Abstracts International, 2004: 65-03.
- [12] DANFORTH M. Scalable patch management using evolutionary analysis of attack graphs[C]//Seventh International Conference on Machine Learning and Applications. 2008: 300-307.
- [13] DACIER M, DESWARTE Y. Privilege graph: an extension to the typed access matrix model[C]//Computer Security - ESORICS 94, Third European Symposium on Research in Computer Security. 1994:319-334.
- [14] PHILLIPS C, SWILER L P. A graph-based system for network-vulnerability analysis[C]//The 1998 Workshop on New Security Paradigms. 1998: 71-79.
- [15] CIMATTI A, CLARKE E, GIUNCHIGLIA F, et al. NUSMV: a new symbolic model checker[J]. International Journal on Software Tools for Technology Transfer, 2000, 2(4):410-425.
- [16] TEMPLETON S J, LEVITT K. A requires/provides model for computer attacks[C]//The ACM Workshop on New Security Paradigms. 2001:31-38.
- [17] 叶云, 徐锡山, 齐治昌, 等. 大规模网络中攻击图自动构建算法研究[J]. 计算机研究与发展, 2013, 50(10):2133-2139.
YE Y, XU X S, QI Z C, et al. Attack graph generation algorithm for large-scale network system[J]. Journal of Computer Research and Development, 2013, 50(10): 2133-2139.
- [18] AMMANN P, WIJESEKERA D, KAUSHIK S. Scalable, graph-based network vulnerability analysis[C]//ACM Conference on Computer and Communications Security (CCS 2002). 2002: 217-224.
- [19] 陈恺, 冯登国, 苏璞睿, 等. 一种多周期漏洞发布预测模型[J]. 软件学报, 2010, 21(9):2367-2375.
CHEN K, FENG D G, SU P R, et al. Multi-cycle vulnerability discovery model for prediction[J]. Journal of Software, 2010, 21(9): 2367-2375.
- [20] 聂楚江, 赵险峰, 陈恺, 等. 一种微观漏洞数量预测模型[J]. 计算机研究与发展, 2011, 48(7):1279-1287.
NIE C J, ZHAO X F, CHEN K, et al. An software vulnerability number prediction model based on micro-parameters[J]. Journal of Computer Research and Development, 2011, 48(7):1279-1287.
- [21] 高志伟, 姚尧, 饶飞, 等. 基于漏洞严重程度分类的漏洞预测模型[J]. 电子学报, 2013, 41(9):1784-1787.
GAO Z W, YAO Y, RAO F, et al. Predicting model of vulnerabilities based on the type of vulnerability severity[J]. Acta Electronica Sinica, 2013, 41(9):1784-1787.
- [22] ARBAUGH WA, FITHEN WL, MCHUGH J. Windows of vulnerability: a case study analysis[J]. Computer, 2000,33(12):52-59.
- [23] FREI S. Security econometrics: the dynamics of (in) security[D]. Sissach, Switzerland: ETH Zurich, 2009.
- [24] KAANICHE M, MARCONATO GV, NICOMETTE V. Security-related vulnerability life cycle analysis[C]//The 2013 IEEE International Conference on Risk and Security of Internet and Systems. 2013: 1-8.
- [25] 宋明秋, 王磊磊, 于博. 基于生命周期理论的安全漏洞时间风险研究[J]. 计算机工程, 2011, 37(1):131-133.
SONG M Q, WANG L L, YU B. Research on time risk of security vulnerability based on lifecycle theory[J]. Computer Engineering, 2011, 37(1):131-133.
- [26] JUMRATJAROENVANIT A, TENG-AMNUAY Y. Probability of

- attack based on system vulnerability life cycle[C]//The 2008 IEEE International Symposium on Electronic Commerce & Security, 2008: 531-535.
- [27] JOH H, MALAIYA YK. A framework for software security risk evaluation using the vulnerability lifecycle and CVSS metrics[C]//The 2010 International Workshop on Risk & Trust in Extended Enterprises.2010: 430-434.
- [28] SHAHZAD M, SHAFIQ MZ, LIU AX. A large scale exploratory analysis of software vulnerability life cycles[C]//The 2012 IEEE International Conference on Software Engineering. 2012: 771-781.
- [29] COX JLAT. Some limitations of “risk= threat× vulnerability× consequence” for risk analysis of terrorist attacks[J]. Risk Analysis, 2008, 28(6):1749-1761.
- [30] MKPONG-Ruffin I, UMPHRESS D, HAMILTON J, et al. Quantitative software security risk assessment model[C]//The ACM Workshop on Quality of Protection. 2007: 31-33.
- [31] 付志耀, 高岭, 孙骞, 等. 基于粗糙集的漏洞属性约简及严重性评估[J]. 计算机研究与发展, 2016, 53(5):1009-1017.
- FU ZY, GAO L, SUN Q, et al. Evaluation of vulnerability severity based on rough sets and attributes reduction[J]. Journal of Computer Research and Development, 2016,53(5):1009-1017.
- [32] HOUMB SH, FRANQUEIRA VNL, ENGUM EA. Quantifying security risk level from CVSS estimates of frequency and impact[J]. Journal of Systems & Software, 2010,83(9):1622-1634.
- [33] 周亮, 李俊娥, 陆天波, 等. 信息系统漏洞风险定量评估模型研究[J]. 通信学报, 2009, 30(2):71-76.
- ZAO L, LI J E, LU T B, et al. Research on quantitative assessment model on vulnerability risk for information system[J]. Journal on Communication, 2009,30(2): 71-76
- [34] YU D, FRINCKE D. Improving the quality of alerts and predicting intruder's next goal with hidden colored Petri-net[J]. Computer Networks, 2007, 51(3): 632-654.
- [35] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]//The 2002 IEEE Symposium on Security and Privacy. 2002: 273-284.
- [36] 彭武, 胡昌振, 姚淑萍, 等. 基于时间自动机的入侵意图动态识别方法[J]. 计算机研究与发展, 2011, 48(7): 1288-1297.
- PENG W, HU C Z, YAO S P, et al. A dynamic intrusive intention recognition method based on timed automata[J]. Journal of Computer Research and Development, 2011, 48(7): 1288-1297.
- [37] 鲍旭华, 戴英侠, 冯萍慧, 等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报, 2005, 16(12): 2132-2138.
- BAO X H, DAI Y X, FENG P H, et al. A detection and forecast algorithm for multi-step attack based on intrusion intention[J]. Journal of Software, 2005, 16(12): 2132-2138.
- [38] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62-72.
- CHEN X J, FANG B X, TAN Q F, et al. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. Chinese Journal of Computers, 2014, 37(1): 62-72.
- [39] 诸葛建伟, 韩心慧, 叶志远, 等. 基于扩展目标规划图的网络攻击规划识别算法[J]. 计算机学报, 2006, 29(8): 1356-1366.
- ZHUGE J W, HAN X H, YE Z Y, et al. A network attack plan recognition algorithm based on the extended goal graph[J]. Journal of Computers, 2006, 29(8): 1356-1366.
- [40] 吕慧颖, 彭武, 王瑞梅, 等. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5): 1039-1049.
- LV H Y, PENG W, WANG R M, et al. A real-time network threat recognition and assessment method based on association analysis of time and space[J]. Journal of Computer Research and Development, 2014, 51(5): 1039-1049.
- [41] 王硕, 汤光明, 寇广, 等. 基于因果知识网络的攻击路径预测方法[J]. 通信学报, 2016, 37(10): 188-198.
- WANG S, TANG G, KOU G, et al. Attack route prediction method based on causal knowledge[J]. Journal on Communications, 2016, 37(10): 188-198.
- [42] SARRAUTE C, RICHARTE G, LUCÁNGELI OBES J. An algorithm to find optimal attack routes in nondeterministic scenarios[C]//The 4th ACM Workshop on Security and Artificial Intelligence. 2011: 71-80.
- [43] ORTALO R, DESWARTE Y, KAANICHE M. Experimenting with quantitative evaluation tools for monitoring operational security[J]. IEEE Transactions on Software Engineering, 1999, 25(5):633-50.
- [44] LI W, VAUGHN R B. Cluster security research involving the modeling of network exploitations using exploitation graphs[C]//IEEE International Symposium on CLUSTER Computing and the Grid. 2006:26.
- [45] IDIKA N, BHARGAVA B. Extending attack graph-based security metrics and aggregating their application[J]. IEEE Transactions on Dependable & Secure Computing, 2012, 9(1):75-85.
- [46] BOPCHE G S, MEHTRE B M. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks[J]. Computers & Security, 2016, 64:16-43.
- [47] DAI F, HU Y, ZHENG K, et al. Exploring risk flow attack graph for security risk assessment[J]. IET Information Security, 2015, 9(6):344-353.
- [48] ABRAHAM S, NAIR S. a predictive framework for cyber security analytics using attack graphs[J]. International Journal of Computer Networks & Communications, 2015, 7(1).
- [49] 刘强, 殷建平, 蔡志平, 等. 基于不确定图的网络漏洞分析方法[J]. 软件学报. 2011, 22(6): 1398-1412.
- LIU Q, YIN J P, CAI Z P, et al. Uncertain-graph based method for network vulnerability analysis [J]. Journal of Software, 2011, 22(6): 1398-1412.
- [50] ZHU B, GHORBANI A A. Alert correlation for extracting attack strategies[J]. International Journal of Network Security, 2006, 3(3): 244-258.
- [51] BOPCHE G S, MEHTRE B M. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks[J]. Computers & Security, 2016, 64:16-43.
- [52] NAYOT P, RINKU D, INDRAJIT R. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Trans on Dependable &Secure Computing, 2012, 9(1): 61-74
- [53] QU Z Y, LI Y Y, LI P. A network security situation evaluation method based on D-S evidence theory[C]//2010 International Conference on Environmental science and information application technology (ESIAT). 2010: 496-499.
- [54] 席荣荣, 云晓春, 张永铮, 等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报. 2015, 38(4): 749-758.
- XI R R, YUN X C, ZHANG Y Z, et al. An improved quantitative evaluation method for network security[J]. Journal of Computers, 2015, 38(4): 749-758.

- [55] 杨豪璞, 邱辉, 王坤. 面向多步攻击的网络安全态势评估方法[J]. 通信学报, 2017, 38(1): 187-198.
YANG H P, QIU H, WANG K. Network security situation evaluation method for multi-step attack[J]. Journal on Communications, 2017, 38(1): 187-198.
- [56] 刘玉岭, 冯登国, 连一峰, 等. 基于时空维度分析的网络安全态势预测方法[J]. 计算机研究与发展, 2014, 51(8): 1681-1694.
LIU Y L, FENG D G, LIAN Y F, et al. Network situation prediction method based on spatial-time dimension analysis[J]. Journal of Computer Research and Development, 2014, 51(8): 1681-1694.
- [57] LINGL J, SUL, WANG H F, et al. An ARIMA-ANN hybrid model for time series forecasting[J]. Systems Research and Behavioral Science, 2013, 30(3): 1092-7026.
- [58] GE P, WANG J, REN P, et al. A new improved forecasting method integrated fuzzy time series with the exponential smoothing method[J]. International Journal of Environment and Pollution, 2013, 51(3/4): 206-221.
- [59] LIU S, LIU Y. Network security risk assessment method based on HMM and attack graph model[C]//IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. 2016:517-522.
- [60] FREDJ O B. A realistic graph based alert correlation system[J]. Security & Communication Networks, 2015, 8(15):2477-2493.
- [61] GHASEMIGOL M, GHAEEMI B A, TAKABI H. A comprehensive approach for network attack forecasting[J]. Computers & Security, 2016, 58:83-105.
- [62] WANG Y, LI J, MENG K, et al. Modeling and security analysis of enterprise network using attack-defense stochastic game Petri nets[J]. Security & Communication Networks, 2013, 6(1):89-99.
- [63] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495-508.
ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3): 495-508.
- [64] CHEN G, SHEN D, KWAN C, et al. Game theoretic approach to threat prediction and situation awareness[C]//IEEE International Conference on Information Fusion. 2006:1-8.
- [65] WU J, OTA K, DONG M, et al. Big data analysis based security situational awareness for smart grid[J]. IEEE Transactions on Big Data, 2016.

[作者简介]



胡浩 (1989-), 男, 安徽池州人, 信息工程大学博士生, 主要研究方向为网络安全态势感知和图像秘密共享。

刘玉岭 (1982-), 男, 山东济阳人, 博士, 中国科学院软件研究所副研究员, 主要研究方向为网络安全态势感知。

张玉臣 (1977-), 男, 河南郑州人, 博士, 信息工程大学副教授、硕士生导师, 主要研究方向为风险评估、态势感知和密码管理。

张红旗 (1962-), 男, 河北遵化人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为网络安全、风险评估、等级保护和信息安全管理。