网络系统安全度量综述

吴晨思[1]，谢卫强[1,2]，姬逸潇[1,2]，杨粟[1]，贾紫艺[1]，赵松[1,2]，张玉清[1,2]

（1. 中国科学院大学国家计算机网络入侵防范中心，北京 101408；
2. 西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：随着人们对网络系统全面和客观认识的不断提高，网络系统安全度量（NSSM）正在得到更多的研究和应用。目前，网络系统安全量化评价正朝着精确化和客观化发展。NSSM 可以为攻防对抗以及应急响应决策提供客观和科学的依据，其中网络系统安全全局度量是安全度量领域的重点。从全局度量的角度，分析总结了全局度量在网络系统安全中的地位和作用，归纳总结了度量的 3 个发展阶段（感知、认识、深化）及其特点，给出了全局度量的工作过程，梳理了度量模型、度量体系、度量工具等方法，并指出了各自的特点及其在安全度量中的作用和相互关系。同时详尽地分析了网络系统全局度量面临的技术挑战，并以表格方式总结了十大机遇与挑战。最后展望了网络系统安全度量研究的下一步方向与发展趋势。分析表明，NSSM 在网络安全中具有良好的应用前景。

关键词：网络系统；安全度量；安全评估；全局度量

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019148

Survey on network system security metrics

WU Chensi[1], XIE Weiqiang[1,2], JI Yixiao[1,2], YANG Su[1], JIA Ziyi[1], ZHAO Song[1,2], ZHANG Yuqing[1,2]

1. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China
2. School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: With the improvement for comprehensive and objective understanding of the network system, the research and application of network system security metrics (NSSM) are noticed more. The quantitative evaluation of network system security is developing towards precision and objectification. NSSM can provide the objective and scientific basis for the confrontation of attack-defense and decision of emergency response. The global metrics of network system security is a crucial point in the field of security metrics. From the perspective of global metrics, the status and role of global metrics in security evaluation were pointed out. Three development stages of metrics (perceiving, cognizing and deepening) and their characteristics were analyzed and summarized. The process of global metrics was described. The metrics models, metrics systems and metrics tools were analyzed, and their functions, interrelations, and features in security metrics were pointed out. Then the technical challenges of global metrics of network systems were explained in detail, and ten opportunities and challenges were summarized in tabular form. Finally, the next direction and development trend of network system security metrics research were forecasted. The survey shows that NSSM has a good application prospect in network security.

Key words: network system, security metrics, security evaluation, global metrics

---

收稿日期：2019−03−22；**修回日期**：2019−06−04

通信作者：张玉清，zhangyq@nipc.org.cn

基金项目：国家重点研发计划基金资助项目（No.2016YFB0800700）；国家自然科学基金资助项目（No.U1836210, No.61572460）；信息安全国家重点实验室开放课题基金资助项目（No.2017-ZD-01）；国家发改委信息安全专项基金资助项目（No.(2012)1424）

Foundation Items: The National Key R & D Program of China (No.2016YFB0800700), The National Natural Science Foundation of China (No.U1836210, No.61572460), The Open Project Program of the State Key Laboratory of Information Security (No.2017-ZD-01), The National Information Security Special Projects of National Development and Reform Commission of China (No.(2012)1424)

1　引言

网络系统安全的重要性日益突出，其安全问题已经被提到战略性高度。提高人们对网络系统整体安全性认知的准确性，可以更好地保障网络系统安全且能够有效应对未知问题[1]。对网络系统安全状况进行客观、全面的认知比以往任何时候都显得更重要、更迫切。

目前，人们对网络系统安全的认知主要有管理安全和技术安全 2 个角度。网络系统管理安全是对人们管理网络系统活动中涉及的安全性因素的分析，如制度建设、流程控制、日常操作等；网络系统技术安全是对网络安全技术及系统安全属性（可用性、完整性和机密性等）进行再认识，以更科学地评价安全性。本文主要讨论技术安全范围内的内容。

网络系统安全性评价分为定性评价与定量评价。安全性定性评价依据知识、经验等资料，通过观察、分析、归纳等方法对网络系统的安全状况做出判断，一般以安全级别等非数值化的形式呈现结论；安全性定量评价依据数学模型和数量指标，通过分析、量化等方法对网络系统安全状况做出判断，一般以数值化的形式呈现结论[2]。相比于定量评价，网络系统安全性定性评价稍侧重主观判断。

随着网络系统复杂性的增加，人们需要更科学、更直观地分析安全性，因此对网络系统安全定量分析也产生了新的要求，即以客观化数值来描述系统的安全性。量化评价朝着更精确化、更客观化发展，从而有效提升了评价结果的严密度和可信度[3]，进而形成了安全度量（security metrics）。因此，为增强评估结果的客观性，一些量化安全评估问题的研究也朝着安全度量转变[4-6]。

目前，安全度量没有标准的定义。IEEE 术语标准辞典给出：度量是对一个系统、构件或过程具有的某个给定属性的度的一个定量测量[7]。所以，人们可以认为安全度量是基于某一尺度衡量安全性和保护数据的一种有效过程[8]。网络系统需要量化与系统安全质量相关的安全要素，如脆弱性、风险、攻击、防御等，用于表征、描述或预测系统安全的信任程度[9]。为了使度量结果具有可比性，将网络系统的最小安全保证设置为安全基线（security baseline），且安全基线随着网络系统规模的变化而变化。将度量结果与安全基线进行比较，可以了解网络系统不同时段的安全状况[10]。安全度量的主要目的是发现安全要素间的相互联系、相互作用，有助于深入理解网络系统安全，其对增强网络系统安全的认知至关重要。安全度量通过量化复杂的安全活动、分析相关数据，能够确定系统优势和劣势，降低部署成本，是客观分析网络系统安全性的关键手段[11]。

与安全度量容易混淆的是安全测量（security measure）、安全测度（security measurement）。安全测量只是获取安全要素的直观原始数据；安全测度则是通过量化安全问题空间，使用以百分数、频率、平均数或其他相似术语对具体定量的安全指标进行数字化的描述[12]。安全度量进一步利用安全测度得到的数据，通过比较或计算等方法来分析安全要素的变化，深入挖掘系统安全情况，准确反映网络系统安全的各个方面。之后利用安全度量得到的安全要素的相关值来确定网络系统的安全程度并制定安全策略。

网络系统安全度量（NSSM, network system security metrics）对网络系统中的安全要素进行客观分析，给出网络系统安全性的综合性或某个方面的描述。根据安全指标维度大小，当把具体网络系统看成一个整体时，维度相对最大，涉及的安全要素也最多，对整体度量表现为全局度量（GM, global metrics）。GM 是 NSSM 的重要组成部分，参照度量基线能跟踪网络系统安全性变化。GM 反映的是网络系统安全程度。针对网络系统中指定对象的度量，如主机脆弱性程度、网络风险大小、业务子系统安全程度等，可以看作对系统局部的度量。局部度量（local metrics）的维度可扩展，其结果在一定维度上能代表全局度量说明网络系统的安全性，但缺少客观性、全局性。

网络系统安全度量是网络系统安全分析工作的重点与难点。目前，人们对网络系统安全度量方法的研究仍处于探索阶段，相关问题还未形成统一的认识。

鉴于网络系统安全度量对网络安全的积极作用，本文将主要围绕全局度量，对网络系统安全全局度量问题的发展历程、现状（度量过程、度量方法）、未来（挑战、展望）进行综述，具体贡献如下。

1) 从客观量化的角度，对网络系统安全度量相关概念进行了梳理。按照人们的理解，总结了度量

的发展历程，首次将其划分为3个阶段。

2) 对网络系统安全全局度量过程进行了总结，分析了全局度量过程中每一步骤的作用，为标准化网络系统安全度量提供参考。

3) 对网络系统安全全局度量方法进行了梳理，包括度量模型、度量体系、度量工具，阐述了各自的特点，指出了它们在全局度量方法中所起到的作用。

4) 探讨了网络系统安全度量目前的机遇与挑战，并在此基础上给出了网络系统安全度量下一步的研究方向。

2 度量发展阶段

安全度量的发展伴随着安全评估的发展，全局度量蕴于度量之中。经过30多年的发展，全局度量开始逐渐显现。本文依据度量方法或过程的复杂性，对全局度量发展过程中具有里程碑性质的节点进行了梳理，得到发展历程如图1所示。以对网络系统安全度量认识程度为主线，将度量主要分为3个阶段：感知度量阶段、认识度量阶段、深化度量阶段。这也是第一次在时间上对度量发展进行分段总结。

2.1 感知度量阶段

感知度量阶段，人们对度量的存在形式有了初步理解与认识，但对网络系统安全度量这一概念的整体反映属于浅显的层次。特点是主观性强，认识不够深刻。这一阶段人们所理解的网络系统安全性度量主要是以安全测量和简单量化的形式，对数据进行单一的统计计算。人们从实际中总结经验，通过制定安全准则来规定系统应达到的安全性。依据安全体系，以度量脆弱性为主来说明系统的安全性。大部分工作都是通过手工进行的，安全性量化分析效率较低。随着网络系统规模的增大，分析工作量越来越大，且很容易出现疏漏。自动化的分析技术及工具应运而生。网络扫描技术是早期用来分析网络安全性的技术，现在依然不断地进行改进与发展[20]，如Satan[21]、Nessus[22]、Nmap[20]等。受限于此阶段网络技术发展的情况，表面上简单的度量安全性即可满足当时的量化分析需求。

2.2 认识度量阶段

认识度量阶段，学者们开始对网络系统安全度量深入理解、赋予意义并做出进一步的解释。表现为研究安全要素的度量，提出了多种度量方法。此阶段以粗略度量为主，如风险度量、攻击度量，并以此代表系统整体度量。度量的实际操作是由安全分析人员基于其自身知识和经验印象而进行的，偏主观因素，网络系统安全性不能得到完全客观的反映[23]。不过人们的观念相较于感知阶段有了重大变化。人们开始对全局度量有所认识，由重视度量过程转为重视全局指标体系建设。Villarrubia 等[14]提出的一系列用于对安全指标进行分类的特性很具有参考价值，指出指标的质量及指标量化的质量好坏对度量结果影响较大。

认识度量阶段主要存在的问题是人们将一部分指标测度研究认为是对系统的度量研究，这是因为对度量理解不够准确。美国国家标准与技术研究院（NIST, National Institute of Standards and Technology）在2008年发布的《信息安全性能测量指南》取代了旧版的度量指南[15]，国际标准信息安全管理测量ISO/IEC 27004于2009年发布[24]。2个文献的更改与发布一方面说明了人们对测度与度量区别的认识有所深入；另一方面也反映了网络系统整体

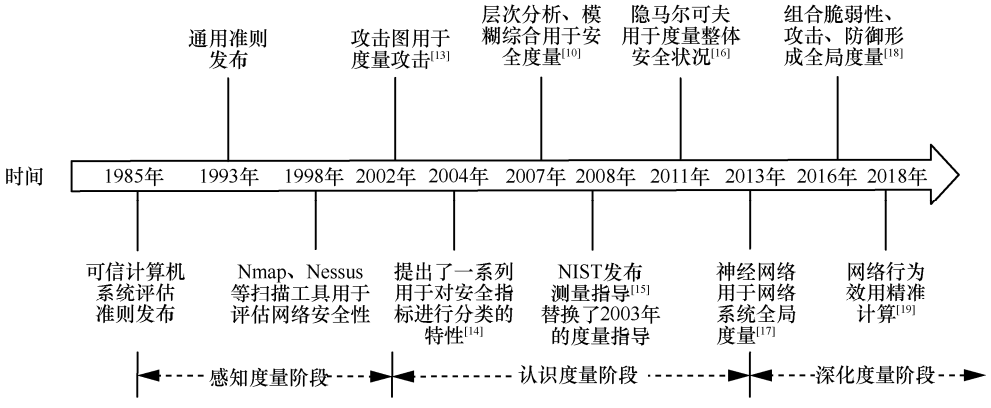

图1 度量发展历程

性安全度量指标建设和指标测量的基础性、重要性。当然，这 2 个文献也可以用来对全局度量指标的建设提供指导。

2.3　深化度量阶段

深化阶段是在人们对局部度量做了大量研究的基础上，对网络系统安全度量概念的发展。主要表现为深入理解度量，不再围绕着某一单方面的度量；提出全局度量，以实现安全程度量化为目标，促进精准度量理论的系统化。其解决的根本问题是由于安全的多维性，如何分解安全性以及如何将局部度量因素组合成整个系统安全性的单一表示形式[25]。

深化度量阶段可分为 2 个分阶段：平稳期和爆发期。在平稳期，人们对度量研究的热度逐渐降低，回归理性，认真思考度量的本质。2016 年，文献[18]站在系统级角度，详细分析了主要安全要素之间的关系及其影响因素的不确定性，如系统安全漏洞、敌方攻击能力及目标等，提出了以时间为参数的动态全局度量函数，但其客观性、准确性依然不足。2018 年后进入爆发期，文献[19]将网络系统发生的所有安全活动看作行为过程并进行了精准度量，奠定了网络系统全局度量的数学基础，具有创新性。度量需要假设和抽象，以数学方法解决全局度量问题会带来度量开创性的研究成果，具体的方法将在第 4 节进行详细介绍。

2.4　小结

本节对度量发展进行了分阶段总结，方便研究人员更清晰地了解度量在每个时期的主要特点，为进一步的研究提供参考。从总体来看，感知度量阶段、认识度量阶段、深化度量阶段是朝着全局度量方向前进的。可以认为，网络系统全局度量的发展是从手动度量到自动度量、由粗略度量向精准度量进行的。当前阶段，全局度量可以用来对网络系统安全进行强有力的定量预测，但全局度量依然有很大的局限性。虽然人们对全局度量没有明确的共识，也无法真正理解它，但努力研究它将是有用的，即使这些研究可能发现对网络系统是不能完全实现全局度量的[26]。

3　全局度量过程

全局度量是加强网络系统技术安全不可缺失的部分。建立通用的度量过程可以提升全局度量的可行性和实用性，并为网络系统安全度量标准化提供技术借鉴。

全局度量的过程是对经典的计划−执行−检查−处理（PDCA, plan-do-check-act）模式的具体实现[27]，采用 PDCA 的循环机制，通过建立指标体系、实施综合度量、分析度量结果、制定优化方案这 4 个主要环节，可以持续改进网络系统安全性。网络系统安全全局度量过程如图 2 所示，以全局度量指标建设为核心，将度量过程分为 3 个模块：模块 1 为度量准备阶段，明确度量目的，确定系统度量目标，制定度量内容与度量活动规划；模块 2 为指标量化阶段，选取网络系统度量指标，对具体指标进行量化与组合，并根据系统安全需求建立度量基线；模块 3 为全局度量实施阶段，选择全局度量模型，将处理好的指标输入模型进行度量，并对度量有效性进行检查，对度量结果进行总结分析。

3.1　度量准备

安全度量需要具有一定的专业背景知识的人员。因此，准备阶段应组建专业的度量小组，负责有序推进度量活动并监督整个度量过程。准备阶段主要提出度量对象的范围，指定度量目标，制定度量方案。为了保证每次度量结果的一致性、权威性，前一次的度量结果应进行过程认证，该认证是一个针对度量结果的独立检查过程，并生成最终的正式

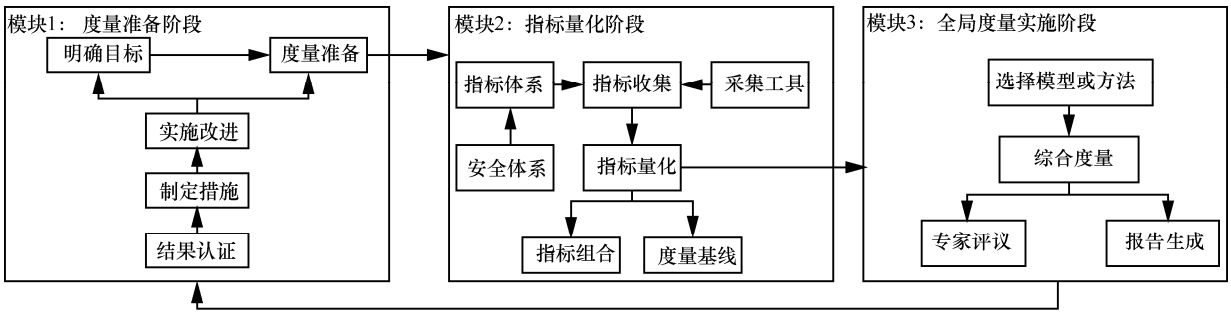

图 2　全局度量过程

结论。依据结论，检查是否达到预定的安全目标，发现存在的问题，制定与落实相应的安全改进措施。结果认证、制定措施、实施改进是为下一次安全度量进行准备，因此将这三部分归入图2中的模块1，使各模块呈周期性出现。

3.2 指标量化

建立科学、客观的网络系统安全度量指标是保证度量过程正常进行的前提。根据安全体系建立指标体系是比较常用的方式，第4节将详细介绍。当然，也可以从其他角度去建立指标体系。例如，Fu等[28]从安全属性的角度对度量指标的选择及指标质量进行了讨论，对建立网络系统全局度量指标有参考价值。为了对已选取指标进行量化，需要获取与指标相关的基础数据。数据获取的准确性、全面性直接关系到整个网络系统安全度量工作的质量。因此，一般使用采集工具获取客观数据。采集工具是部署在网络节点的网络设备，设备既可以基于软件也可以基于硬件。Jing 等[29]按照采集方法将安全数据分为4类：数据分组级、流量级、连接级、主机级，并整理讨论了各类数据采集方法的优缺点。

将采集到的基础数据进行测度实现指标量化。能够采集到的网络系统数据类似于可直接观察到的。来自软件工程领域的目标−问题−度量法（GQM, goal question metric）能为这种直观提供有价值的指标测度[30]。GQM 自上而下适用于各种安全测量并能拓展度量指标，如文献[31]建立脆弱性描述指标，利用 GQM 对这些指标测度，使修复脆弱点更具体化并能大幅降低成本。

安全测度只是指标量化的一部分。为了进一步体现度量指标的客观性，将部分测度的指标进行组合或聚合形成一些高级指标，如安全要素等，从而对网络系统进行更深入的分析。提出度量基准，构建度量基线也是必不可少的一步，其为实现度量比较、反映网络系统安全程度大小做准备。

3.3 全局度量实施

全局度量采用数学等方法对网络安全问题建立全局度量模型。度量模型有多种，选取适合当前指标体系的度量模型，并将所需的指标输入全局度量模型，实施综合度量，从而得到数值化结果。再根据这个结果对网络系统安全性进行分析[32]。全局度量模型的一般形式为

$$m = f_l(x_1, x_2, \cdots, x_i), i \geqslant 1 \tag{1}$$

$$S = f_g(m_1, m_2, \cdots, m_n), n \geqslant 1 \tag{2}$$

其中，f_l为指标组合函数，x_i为测度的指标值，i为指标个数，S为网络系统安全程度，f_g为全局度量函数，m_n为局部度量值或者指标组合值，n为描述网络系统的因素的个数。不同网络系统安全特点不一样，m_n与f_l都可以是不同的。同一个网络系统n越大，S越能客观准确地表达网络系统安全性。

综合度量结果S与人们长期的网络系统安全经验保持一致，能说明结果的有效性。目前没有具有完全客观性的全局度量模型对局部要素或指标进行融合，从不同侧重点考虑对系统进行度量的全局数量模型较多。如文献[33]结合不同的方法，从网络系统结构和可达性信息的角度，研究了基于主机的度量和基于网络的度量。基于主机的度量被划分为“无概率”和“有概率”两类；基于网络的度量被分为“基于路径”和“基于非路径”两类。文献[34]对网络系统能达到的隐私程度进行分析，构建了隐私度量框架，提升了研究人员在隐私保护方面的工作效率。

综合度量之后，对网络系统安全性进行分析，检查防御等安全方案是否合理、指标体系是否完整，最后形成分析报告。经过专家询问和评议，确定报告内容的正确性。报告中应体现出网络系统安全程度以及对其安全的详细说明。

简单的度量案例来自文献[19]，如表1所示。其包含了选取的两类常用指标以及计算情况。建立客观的数学模型，抽象出网络攻防过程，计算形式如式(3)和式(4)所示。其中，$u(t)$为行为路径曲线在某点位处的切向量，行为效用E是系统功能的一种定量描述形式，因此可以进一步构建网络攻防效用的精准计算。

$$E_{[p,q]} = \int_0^1 g_{ij} u^j(t) \mathrm{d}u^i(t) \tag{3}$$

$$E = \sum E_{[c_i, c_{i+1}]} \tag{4}$$

通过式(4)形成指标对应的计算模型。表1中，E_{A_i}为在第i个环节的攻击时，有序攻击行为集合A_i在M_i场景下的攻击能力；E_{D_i}为在第i个环节的防御时，有序防御行为集合D_i在M_i场景下的防御

表 1　　**度量案例**

度量指标	度量模型	测度值	测量依据
攻击能力	$E_{A_i}=\sum_{j=1}^{m}E_{a_{ij}}$	攻击行为、效用微分元（客观标量）	网络系统组成元素、网络系统拓扑结构（多维加权图）、行为路径曲线、平面向量场
防御能力	$E_{D_i}=\sum_{k=1}^{m}E_{d_{ik}}$	防御行为、效用微分元（客观标量）	

能力。$\Delta E_i=E_{A_i}-E_{D_i}$ 为第 i 个环节的网络攻防判定，$y=\sum_{i=1}^{n}\Delta E_i$ 为完整攻防时间内网络安全状况。计算的能力值是一个与流形局部坐标系选择无关的客观量。计算过程始终是客观的，因此，结果具有客观性。根据模块 1 进行结果认证，改进安全措施。

3.4　小结

网络系统安全全局度量需要始终围绕机密性、完整性、可用性进行。全局度量是可重复的、可操作的。本节参考评估过程，详细说明了全局度量过程及主要相关的内容。从度量过程可以看到，全局度量能够促进对网络系统安全的全局、客观描述，帮助网络系统找到更安全的解决方案，提高组织自身的网络安全水平。根据网络系统全局度量的过程对网络系统实施具体的操作，可以将网络系统的安全威胁始终控制在可接受的程度，减少网络系统遭到破坏带来的损失，保证网络系统的可持续运作。

4　全局度量方法

传统的主动防御体系[35]已不能有效应对当今严峻的网络环境。网络系统安全度量可以作为一种主动防御技术，应用全局度量方法对网络系统进行精准防御。

全局度量方法主要依据使用频率和易用性，尽量选取具有代表性的内容进行阐述。本节将从模型、安全体系、工具 3 个方面分别阐述全局度量方法。将部分评估方法应用于全局度量，可使方法目标更明确，更具针对性。度量模型为指标体系和工具的发展提供基础，是精准度量的承载。安全体系主要服务于全局度量指标建设、指标量化及组合。工具增加全局度量的效率，减少人工误差。模型、体系、工具三者关系如图 3 所示。全局化度量方法更容易发现和解决网络系统安全难以实现全局、客观量化的问题。全局方法能清晰刻画网络系统安全，检查系统有效性，即网络系统是否足够安全，是否比以前更安全。

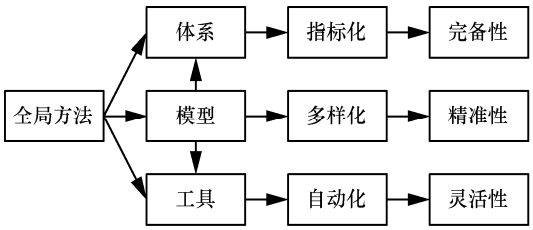

图 3　模型、体系、工具三者关系

4.1　全局度量模型

目前，在网络系统安全领域，全局度量方法具有一定程度的主观性，安全性量化分析只能以粗略比较计算为基础开展。新的网络架构也在不断发展[36]，为增强人们对于网络系统安全更全局且客观的认识，发展全局度量模型至关重要。

目前，已有研究人员对局部度量模型进行了总结。文献[37]详细介绍了基于攻击图和随机模型的量化模型，但对其他模型分析较少。上述文献只是对局部度量模型进行概括，没有对系统全局度量模型进行归纳。本节对局部度量模型进行了补充，并介绍了可用于网络系统全局度量的模型。

4.1.1　基于关联分析的模型

警报关联（alert correlation）技术是检测多步攻击行为的主要技术手段。它是指将属于同一攻击行为的多个步骤前后关联起来，还原最初的攻击场景，全面分析网络系统安全性[38]。

Yi 等[39]提出了警报关联图的基本思想。在攻击图提供的先验知识基础上，根据入侵检测系统（IDS, intrusion detection system）警报信息动态生成警报关联，并基于警报关联的次数计算关联边的权值对网络系统全局量化。不过这种关联图相对简单，并不完善，度量结果粗略。葛海慧等[40]对一定时间间隔内的报警事件进行动态关联分析，考虑防御措施强度与节点漏洞，计算攻击威胁度，利用各节点风险值加权计算风险值代表系统整体的安全性，此方法能够实时度量。陈秀真等[41]基于 IDS 海量报警信息和网络性能指标，采用自下而上、先局部后整体的度量方式，对服务、主机本身的重要性因子进行

加权，进而说明网络系统的安全性。

为了提高度量准确性，有研究人员结合 D-S 证据理论进行分析[42]。D-S 证据理论具有直接表达“不确定”和“不知道”的能力，能够描述网络系统中的不确定性因素。Qu 等[43]基于 D-S 证据理论，结合节点脆弱性、威胁的严重性，全局计算网络系统的安全程度。基于证据理论的关联分析模型具有需要先验知识少、算法性能高等优点，但其在还原攻击场景的能力、识别攻击者的具体攻击动作方面相对较弱。

关联分析通过对网络系统中各类因素进行分析，能更加清晰地掌握网络系统整体的安全状况及防御措施等情况[44]。在大数据飞速发展的背景下，数据挖掘、机器学习中的一些方法应用于全局度量领域是一种研究趋势。以数据驱动的公司常使用关联分析进行安全度量。如 BitSight[45]通过部署在全球各地的传感器，采集海量的威胁情报数据。平台将这些数据依据严重程度、频率、持续时间和信心等指标进行分析，从而对网络系统进行全局度量，并能进行一定的趋势预测。

4.1.2 基于随机模型的模型

随机模型涉及的方法能对网络系统全局进行有效的描述，精确刻画网络系统随机行为以及组件之间的相互关系，有助于量化组合指标，建立全局度量函数。常用的随机模型是隐性马尔可夫模型（HMM, hidden Markov model）[46]。HMM 用来描述一个含有隐含未知参数的马尔可夫过程（Markov process）。HMM 对未知指标的计算有优势。

Zhang 等[16]通过 HMM 对报警检测系统产生的序列进行分析，计算系统中每个主机的危险指数，从而定量分析整个网络的安全状况。Rnes 等[47]把网络系统安全状态的变化过程采用 HMM 来描述，然后实时度量网络整体的安全值。Almasizadeh 等[48]将时间因素考虑进了攻击过程，通过基于状态的随机模型对网络攻击过程进行了建模，进而描述攻击者和系统行为，定量分析了系统的平均安全失效时间、稳态安全等安全指标。相对其他度量，这些指标有助于增强全局度量的客观性。Da 等[49]从整个系统的角度出发将攻防分别抽象并度量，提出了一种 n 维随机模型的全局度量，但其不适用多种攻击同时发生的情况。

网络系统安全存在不确定性，在实践中很难度量不确定性，而且不确定性往往是由观测中的估计误差引起，不一定反映实际的系统状态。

4.1.3 基于数学原理的模型

数学原理是以数学方法为基础，将全局度量进行抽象，能够更准确地度量指标，并进行精准计算。通过数学原理得到的全局度量更客观。

Hu[19]提出了一种网络行为效用计算原理与方法。他认为任何网络行为，都是在由所有可用于提供数字化信息的组件和系统所构成的网络场景上发生的，并给出了网络行为的数学定义。微分流形（differential manifold）是三维欧氏空间中曲线和曲面概念的推广，可以有更高的维数[50]。将网络系统抽象为流形，定量刻画网络行为效用的算法如式(3)和式(4)所示。安全效用计算奠定了网络行为度量的数学基础，为建立全局度量函数提供参考。

文献[51]基于欧氏空间向量投影的思想设计了一个信度向量投影分解算法，将攻击所依赖的漏洞信息和节点本身漏洞信息相关联，对网络系统进行全局度量。Petri 网[52]用来分析离散的并行系统，抽象和描述能力也在不断的发展，在度量领域具有广泛的应用前景。文献[53]将安全要素转化为 Petri 网状态函数，将指标基于 Petri 网的最小可覆盖集进行量化，并对整个系统进行度量。形式化方法用于网络系统安全度量建模有利于度量自动化发展。文献[54]针对系统用户的行为特点，基于访问路径给出了形式化定义和相关的度量规则，提出了一种网络系统全局度量方法。

数学方法有助于发现安全要素的内在联系，找到安全的本质，将复杂度量问题简单化。使用数学方法解决全局度量的研究正在兴起，未来解决度量问题也一定会参考数学方案。

4.1.4 基于攻击图的模型

攻击图[55]是一个抽象概念，它能揭示攻击者利用安全漏洞违反安全策略的方式。攻击图模型采用图论的方法描述网络攻击过程中的细节信息，能够简洁地表示特定网络的不同攻击场景[56]。基于场景解决全局度量问题具有典型性，因此将基于攻击图的模型单独列出。

Jha 等[13]和 Sheyner 等[57]首先使用模型检测的方法生成攻击图模型，利用攻击图将成功概率值赋予攻击中的状态，进而分析攻击者成功实现对网络系统的安全性破坏的概率，实现攻击破坏程度的全局度量。Bhattachary 等[58]根据“利用依赖图”提出了一种通过成本说明网络系统安全性的理论框架。

成功利用网络系统所需的成本越小，说明网络系统安全程度较高；反之，则较低。此过程实际应属于局部度量，但由于攻击图反映的是攻击成功与否，因此也可以代表网络系统全局度量结果。

将基于攻击图的不同度量元素组合使用，可扩展为网络系统安全全局度量方法。最短路径度量、路径数量度量和路径长度度量是 3 种常用的基于攻击图的安全度量。然而，最短路径度量和路径长度度量的平均值不能充分说明攻击者可能违反安全策略的方式，路径数量度量也不能充分说明与攻击路径相关的攻击工作[59]。使用这些指标可能会有误导性结果，因此有研究结合贝叶斯网络（BN, Bayesian network）进行全局分析。BN 是一种概率图型模型，借由有向无环图中得知一组随机变量及其 n 组条件概率分配的性质。贝叶斯网络作为构造全局度量模型的基础具有以下优点[60]：1) 贝叶斯网络类似神经元网络，能够充分描述人类的推理模式，并且网络的图形方式便于理解和开发；2) 贝叶斯概率的特点使模型能够反映度量的连续性和累积性这 2 个重要特征；3) 模型能够综合最新的证据信息和先验信息，度量结果能动态反映当前信息的同时还综合了历史和先验知识；4) 贝叶斯逻辑在数学上的可靠性使该模型成为一种描述人类思维推理过程的标准模型。文献[61]使用贝叶斯网络模拟网络系统的安全状态，结合攻击图对网络系统进行了全局度量。Poolsappasit 等[62]在攻击图的基础上构建贝叶斯网络，建立警报节点作为证据节点或根据警报将相应的原子攻击节点设为证据节点，形成网络系统整体的安全状态值。基于贝叶斯网络的方法充分利用了贝叶斯网络的量化处理不确定性信息以及因果关联优势和不确定性推理能力，使度量结果比较准确。然而，基于贝叶斯网络的方法由于需要对所有节点都建立条件概率表，因此需要较多的先验知识，不利于区分攻击已经发生的可能性和攻击将要发生的可能性，增大了全局度量的误差。另外，受贝叶斯网络推理算法复杂度的限制，基于贝叶斯网络全局度量的性能不高，难以满足大型网络系统实时度量的性能要求。

攻击图模型包含了网络系统中所有可能的攻击路径。利用攻击图可以对网络攻击等环节有更清楚的认识，可以很直观地展示网络攻击的细节信息，如攻击路径、攻击目标、脆弱性等。在全局度量时，通过攻击图模型可以建立更全面的指标信息，更容易完善全局度量函数。

4.1.5　基于博弈论的模型

博弈论模型对于研究网络系统安全度量问题具有重要的意义，利用博弈论模型可以从攻击和防御 2 个技术方面对网络系统安全性进行全面分析，实现全局度量。

文献[63]模拟真实网络系统的虚拟环境，实现对网络系统各种攻防过程的实验推演。将网络连接关系、脆弱性信息等数据输入网络攻防博弈模型中，实现了全局度量。Li 等[64]通过马尔可夫博弈模型，建立四级数据融合，考虑攻防双方的关系和不确定性，从而度量网络系统整体的安全状态。但模型使用博弈矩阵深度不够，度量粗略。Zhang 等[65]通过分析完全信息静态博弈中的纳什均衡策略，考虑成本参数和效益参数，改进收益计算方法，对系统全局进行度量，该度量结果能够反映攻击者和防御者的均衡策略。

博弈论可以作为全局度量函数的理论基础。攻击和防御是网络系统中的 2 个重要因素，以攻防为核心，向外围扩展，通过演化博弈模型实现全局度量。

4.1.6　基于层次分析法的模型

Fu 等[66]首次提出了层次分析法（AHP, analytic hierarchy process）。AHP 把复杂的网络系统问题分解为各个组成因素，对网络系统全局度量是比较合适的，但过于主观。

层次分析法度量一般分为 4 个步骤[67]：1) 将复杂系统分解为单独因素，根据它们之间的支配关系，建立层次结构；2) 根据上一层中因素的重要性，两两比较本层次中的各个元素，构造出两两比较的判断矩阵；3) 在判断矩阵中，计算被比较元素对于该准则的相对权重；4) 计算各层元素对系统目标的合成权重，并进行排序，最后按层次综合考虑所有影响因素，得出度量结果。Yan 等[68]建立了三层结构（目标层、规则层、标准层），并通过重要程度对指标进行选取，计算系统整体的安全性。由于指标围绕风险进行，此方法用风险值代表了全局度量。Li 等[69]使用 Delphi 法建立度量指标，通过权重使用层次分析对网络系统进行全局度量。

网络系统安全状态随着外部环境的变化和自身价值的变化进行着复杂的演化，描述指标一定是非常多的，而层次分析法在某一层次评价指标很多时，其思维一致性很难保证。因此有学者将模糊层

次分析法（FAHP, fuzzy analytic hierarchy process）引入全局度量中，能较好地解决这一问题。Tuteja 等[70]提出了基于 FAHP 的结构化框架来量化网络系统的安全性，对系统进行分解，确定基本指标，建立模糊关系矩阵全局度量。李景智等[71]在模糊层次分析法的基础上，结合可拓理论，将指标值映射到可拓区间中，计算相对隶属度，对网络系统进行整体度量。信息熵用来描述随机事件不确定性的程度，可以表示不确定性的量。根据指标变异性的大小确定对象的权重，在一定程度上减弱人为主观因素的影响。文献[72-73]利用信息熵确定指标权重，进而应用层次分析实现全局度量，在一定程度上增加了客观性。

层次分析法是全局度量较普遍使用的方法。许多研究人员结合其他方法进行度量，但其人为因素影响较大，受限于专家知识。因此在全局度量对安全性要求很高的大型复杂网络系统时，层次分析显得客观性不足。

4.1.7 基于神经网络的模型

神经网络[74]是由大量处理单元通过广泛互联而构成的，具有大规模并行、分布式处理、自学习等优点。全局度量中，对于大量指标的量化与组合是复杂的。为了提高实时度量，利用神经网络提高度量技术的性能是一个研究方向。

Li[17]采取树型结构构建了三层网络系统安全评价指标以及反向传播（BP, back propagation）神经网络度量模型，通过学习形成一种推理机制，实现了对输入评价指标的非线性反映，最后得到全局度量结果。顾兆军等[75]根据等保测评要求[76]构建全局度量指标体系，利用熵权法确定各指标的权重。将指标加入 BP 神经网络建立度量模型，通过训练给出度量结果。Ma 等[77]提出了一种基于径向基函数（RBF, radial basis function）神经网络的度量模型。根据特定的航空网络系统建立度量模型，将影响任务安全状况的指标作为模型的输入，对模型进行训练，进行全局度量。

基于神经网络的网络系统安全度量的研究多集中于建立全局度量指标体系。指标的选取一方面需要准确反映网络系统情况，另一方面要确保神经网络可以实现指标的输入。模型的主要缺点是训练时的数据量比较小，只能粗略度量系统的安全性。虽然使用神经网络能够提高度量速度，但对指标的提出存在限制，不是任意指标都能加入神经网络中。

表 2 对上述方法进行了对比分析。其中结合方法是度量模型与其他方法常见的搭配。现阶段，对度量模型的研究具有局限性，缺少实时性、准确性以及表征性[78]。度量网络系统的方法虽然较多，但它们的客观分析能力依然不足。度量内容偏重于某一安全要素，如漏洞相关性、风险存在性等，度量效果粗糙、片面。表 2 在度量类别列出了常见的局部度量，局部度量内容不仅限于表 2 中所列，其他的度量有网络弹性度量[79]、信息价值度量[80]、攻击难度度量[81]。本文涉及的模型中专门用于脆弱性度量较少的原因是脆弱性都是作为其他度量的基础。全局度量方法能够适用于风险度量，一方面是人们对风险评估的研究较成熟，对风险的理解比较深入；另一方面，风险评估与全局度量的思路较相似，风险指标容易设计，度量过程容易实施。

全局度量模型不成熟，效果依赖于具体的方法，以局部代替整体的方式较常见。由于 AHP 易

表 2 部分度量模型对比

模型	结合方法	优点	缺点	度量类别		
				攻防度量	脆弱性度量	风险度量
关联分析	数据挖掘、D-S 证据	较客观，方便量化指标	不成熟，需要大量数据	—	文献[39]	文献[40]
随机模型	马尔可夫链、隐马尔可夫	精确刻画系统随机行为，实时性	基于假设，难以验证	文献[48-49]	—	文献[16,47]
数学原理	微分流形、形式化、Petri 网	精准度量	处于发展阶段	文献[19]	文献[51]	文献[53]
攻击图	属性图、状态图、贝叶斯网络	攻击度量成熟，全局度量偏攻击化	客观性弱，受算法效率影响	文献[57]	文献[58,61]	文献[62]
博弈论	马尔可夫	刻画攻防本质，易拓展	全局度量函数难设计	文献[63]	—	文献[65]
层次分析	模糊数学、可拓理论、信息熵	有层次性，灵活简单	有主观性，不适用复杂系统	—	—	文献[68]
神经网络	专家系统、熵权法	度量效率高	训练数据量不足	—	—	文献[77]

操作，因此它是全局度量中常使用的模型，许多研究围绕 AHP 并结合其他技术进行开展。关联分析、神经网络是随着机器学习、人工智能等热门技术兴起的，因此在全局度量方面是有潜力的。随着对度量的深入理解，在度量方面有很好的应用。随机模型和博弈论一般会将脆弱性作为其他安全要素的度量输入，建立全局度量函数应是这 2 个模型未来研究的具体点。度量朝着理论化发展的趋势需要提出或采用新的或抽象的方法来说明度量。采用数学方法研究全局度量会越来越频繁，越来越成熟。当然，对系统全局度量是非常困难的，是一个开放性的问题。在选择具体模型度量时还需根据不同的系统及需求确定，多种方式相互结合的方式可以提高度量效率和全面性。

4.1.8　小结

全局安全度量模型的研究是网络系统安全度量的重要组成。将不同的度量内容进行组合以全局度量的形式表现，能更综合地反映网络系统安全性。将数学理论、人工智能等技术引入网络系统安全程度的度量，有利于促进安全度量研究的全局化、自动化发展。本节通过列举分析，整体阐述了全局度量模型的研究现状，同时指出了现有的研究存在的问题，并给出了一些建议以及解决方法。

4.2　网络系统度量体系

没有指标体系指导的度量是混乱的。依据体系实施全局度量，得到的安全程度证明具有权威性、可比性。目前虽没有成熟的全局度量指标体系，但国内外学者研究安全度量时，主要是借鉴已有的安全标准体系，选取常见的指标。将安全标准体系用于全局度量是可行的，一是安全度量是安全的一部分，二是安全体系经过长期发展，能够满足全局度量指标设计需求。

本文根据指标的使用情况和涉及内容，调研了可用于度量体系的 10 个安全标准体系，并将其分为 3 类，基础性、针对性、全面性。其中，基础性是指体系强调满足网络安全理论的基本指标，有通用性并易于扩展，如可信计算机系统评估准则（TCSEC, trusted computer system evaluation criteria）[82]、通用准则（CC, the common criteria for information technology security evaluation）[83]、PDR 安全防护体系[84]；针对性是指在具体行业、具体系统等一定范围内使用，如 BS7799 安全体系规范[85]、美国联邦信息处理标准系列（FIPS, federal information processing standards）[86]、欧盟网络与信息系统安全指令[87]、NIST 网络安全框架[88]；全面性是指体系涉及的内容丰富，范围广泛，适用性强，如网络安全等级保护基本要求[89]、WPDRRC 信息安全模型[90]、信息保障技术框架（IATF, information assurance technical framework）[91]。下面将举例介绍每类体系中度量指标的应用情况。

4.2.1　基础性指标体系

TCSEC 的发布具有划时代的意义。后来许多标准都以此为基础发展而来。使用 TCSEC 一般从网络系统设计之初开始。依据系统需求，按照准则中要求的安全级设计安全性。这种专门设计的安全模式是度量复杂系统安全性较为有效的方法。文献[92]说明了 TCSEC 如何为大型、复杂和分布式系统设计安全模式。依照安全模式进行全局度量，增强了可度量性、降低了成本。虽然 TCSEC 目前已经被取代，但其涉及了网络系统全周期的安全要素，因此对建设全局度量指标依然具有指导意义。

CC 综合了早期的安全准则和标准，形成了一个较全面的基础框架，极大地促进了安全体系的发展。CC 基于保护轮廓和安全目标提出安全需求，将保密性、完整性和可用性作为出发点，具有灵活性和可扩充性。由于 CC 的认可度较高，因此依靠其建立网络系统安全全局度量的指标体系可信性较强。将建设的指标结合全局度量模型，如贝叶斯网络，对网络系统进行全局度量具备可靠性[93]。在 CC 体系中，可进行网络系统度量维持，以解决系统在度量后出现变化时度量结果的有效性问题。当然，基于 CC 的全局度量也存在比较大的缺点，即度量复杂性会伴随网络系统所要求的安全级别升高而变得越复杂，其对系统度量的平均周期较长，会导致度量过程的烦琐和高成本。

4.2.2　针对性指标体系

BS7799 是一套完整的网络系统安全管理框架[94]，涵盖了几乎所有的安全议题。其主要为工商业网络系统提供服务，因此基于 BS7799 建立的全局度量的指标体系主要针对于工商业，对于其他方面的应用效果可能不理想。系统全局度量指标对应规范中的控制措施，以改进网络系统安全规划和技术流程为目标[95]，从而保证指标对度量网络系统是有效的。

围绕 BS7799 的学术研究主要集中在安全要素度量问题上，如 Tao 等[96]把 BS7799 与故障树技术结合，对各层安全要素之间的逻辑关系进行分析，

实现网络系统的安全要素定量计算。除了建立指标体系，BS7799 也适合作为大、中、小工商业组织的网络系统在所需的控制范围内的安全基准，并形成全局度量基线。

4.2.3　全面性指标体系

我国发布的计算机信息系统安全保护等级划分准则[97]，用于评价网络系统安全保护能力，从整体上形成多级系统安全保护体系，为安全系统的建设提供了技术指导。为了进一步加强重要领域网络系统安全的规范化建设和管理，全面提高国家网络安全保护的整体水平，形成了新的网络安全等级保护。目前新等级保护虽未正式发布，其整体结构已基本形成，如图 4 所示。新等级保护具有高度灵活性，能够适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用背景下的网络安全全局性、系统性度量工作的开展，提高国家网络系统安全防御能力。

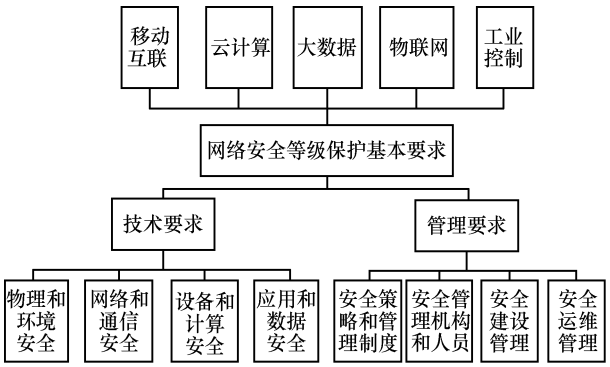

图 4　网络安全等级保护结构

根据新要求，指标体系建设可从多维度、多层面进行，这有利于度量安全要素时灵活地选择模型。新要求中的通用部分可看作网络系统安全的基准，有利于度量基线的统一化建设。国内的安言咨询公司[98]已经开始使用新等级保护，对目标网络系统进行全局量化分析，挖掘业务运营的特定环境中存在的网络系统安全隐患。等级保护体系与全局度量相结合能以数字化的形式展现系统潜在问题、影响范围和发生的可能性，形成动态的、可持续改进的安全度量机制。

4.2.4　体系分析

部分指标体系的对比如表 3 所示。通过对比发现，体系指标的可量化程度还不够客观，存在较多的问题。将体系中提取的指标作为测度的依据，进而对系统实行全局量化。不同的应用场景对网络系统能够提供的安全性程度的要求不同。在选择具体指标时还需根据不同的系统及需求来选择安全体系。通过对体系进行分析形成指标选择的原则有：1) 简洁性，选择各种类型的指标必须简明扼要，且须具有代表性；2) 完整性，选择各种类型的全局度量指标应是互补的，要能够完整描述网络系统要素；3) 可行性，各种指标的选择能够与实际度量相结合，确保其实际操作能力；4) 独立性，各种指标之间具有独立性，减少或者避免它们之间的联系；5) 准确性，指标的选取能够进行论证及提供价值。

在安全基线建设方面，体系的基本要求可确立形成度量基线。虽然同类网络系统之间存在差异以及它们的安全需求是不同的，但其安全基线应是一致的。通过体系能够快速建立安全基准，确保网络系统最低安全性。确定基准后，安全度量指标需是可拓展的，对不同类型网络系统或者对同一系统不同阶段应有所变化，安全体系可被视为安全度量人员的资料库[99]。

安全体系在促进网络系统全局度量的发展中发挥着关键作用，但其不能完全满足度量要求。一方面，网络技术及系统业务模式的发展远远快于安全体系的制定，体系的滞后性影响度量建设。另一

表 3　　**部分指标体系对比**

名称	可量化情况	适用性	优点	缺点
TCSEC	主观量化	为度量指标体系研究提供基础指导方向	技术层面详细，逻辑清晰	强调控制用户，没有关注物理等安全，不再修订
CC	主观量化	适用于一切网络系统，具有普适性	系统刻画了安全的全部内涵，消除重复度量，促进通用性	半形式化语言较难理解，涉及度量体系成本较高，主观性强
BS7799	主客观结合	有法律标准支撑，适用于工商业网络系统	内容详尽，认可度高，度量方法自由选择	每个指标的权重分析不足，测度精度不足
网络安全等级保护基本要求	主客观结合	指标全面细致，实用范围广	范围界定清晰，已上升至法律层面，具有高灵活性	没有衡量攻防过程中的动态变化，缺乏动态指标

方面，从安全体系中选取具有代表性的安全影响因素作为指标时，每类因素可能包含许多不确定的因子，因此会增加全局度量的不准确性。所以，建设科学的安全度量指标体系很重要。我国指标体系建设工作起步较晚。2015 年，发布的信息安全保障指标体系及评价方法[100]提出了安全评价指标体系及其测度过程，阐述了一种实现系统安全性评价的层次结构，可以对网络系统进行粗略全局度量。此标准可以认为是给出了简单的指标指导，但指标体系的构建还存在不足，且这种粗略度量对网络系统整体安全性的刻画还不够客观。

4.2.5　小结

基于安全体系建设网络系统安全度量指标体系有利于全局度量的发展，但仍需进一步地研究与完善。本节介绍了对网络安全产生重要影响的安全体系，指出了体系在全局度量方面的应用（粗略度量、标准建设、安全基线）。通过对比分析，给出了这些体系在度量指标建设方面各自的优劣势，同时总结了网络系统安全度量指标体系构建的原则。

4.3　度量工具

网络安全系统度量工具是全局度量的辅助手段，是保证度量结果可信度的一个重要因素，在一定程度上解决了手动度量的局限性。近年来，不断增多的网络安全事件促进了安全企业迅速发展，同时增加了度量工具的使用频率。由于工具的使用比较灵活，本节简单介绍几款常见的可用于全局度量的工具。

4.3.1　CRAMM（CCTA risk analysis and management method）

CRAMM[101]依据 BS7799 标准建立指标体系，以风险度量为基础，涵盖了安全管理的所有阶段，如资产安全度量、风险计算、控制方案调整等。CRAMM 建有强大的经验数据库，度量时能够参考以往经验，并通过分层对网络系统进行简单的全局定量分析。CRAMM 在实时度量的同时，提供必要的安全解决方案，有效地降低安全实施成本。CRAMM 适用于各种大型的网络系统，但是，其度量主观性较大，部分数据采用人工收集，且主要依靠研究人员的知识和经验，需要经验丰富的从业者使用该工具。

4.3.2　COBRA（consultative, objective and bi-functional risk analysis）

COBRA[102]基于专家知识库对网络系统进行安全分析，它利用动态分析对大量的网络系统数据进行简单的计算，度量所有威胁和漏洞的相对重要性，并以此代表全局度量，从而生成适当的安全建议和解决方案。COBRA 能够控制度量的细节和精度，从而根据实际需要获得更有利于网络系统安全的结果。COBRA 能够提供较大的灵活性，所有功能部分都是可选的，但工具自动化支持相对薄弱，使全局度量时间长，且过程会产生混乱的情况。

4.3.3　工业网络安全工具

绿盟[103]2018 年发布了工业网络系统安全合规工具 ISCAT。ISCAT 集成多个权威合规性安全标准分析模版，能够对网络系统中的设备安全、资产安全等局部度量，也能够通过关联分析进行全局度量。其减弱了专业背景需求，能为用户提供标准、专业的检查指导，并以可视化方法帮助用户快速分析展示网络系统安全状况。ISCAT 的缺点在于度量场景有限，安全指标有待进一步整合与量化。整体来说，ISCAT 有针对性地采取安全防护措施，提升工业控制领域的网络系统安全防护能力，有助于切实保障工业网络系统安全。

4.3.4　小结

本节从自动化的程度出发，介绍了 3 个具有代表性的工具及其优缺点。整体来看，度量工具距离完全实现度量自动化还有一段路需要走。数据的采集有部分依靠人工方式，而且采集方式普遍效率较低；度量指标需要专家确定；数据的整合比较粗略，缺乏模型化。因此，全局度量工具还有很大的改善空间。全局度量工具是网络系统安全发展中必不可少的一环，应当以流程化、自动化为目标。合理使用网络系统安全度量工具，可以降低人力物力的成本，提高安全管理和防护的效率，大幅度减少网络系统的安全问题。

5　挑战与机遇

数据化的快速发展导致度量的方式会有所不同，并且会加快网络系统全局度量的发展。没有全局度量的网络，就不会真正地清楚安全目标。对网络系统的每次全局度量都是为了让网络系统变得更安全。目前的度量发展太过单一，全局度量应用于具体网络系统能更好地驱动全局度量的进步。未来的全局度量将围绕 what（度量的数据有什么）与 how（如何应用度量）展开。当前是全

局度量最好的发展时期，自动化、智能化等新技术的迅速出现为全局度量创新了思维、创造了条件、提供了机会。

5.1 挑战

5.1.1 全局度量可行性

安全度量的现状和实际操作还无法完全满足各方的期望。利益相关方的期望对网络系统全局度量有着很大的影响，这些期望基本都围绕着全局度量的可行性和度量结果的参考价值。理解并进一步满足这些期望有助于准备开展安全度量项目的组织获得成功，提升网络系统整体度量客观性[104]。大部分企业或者组织在对系统进行安全性评价时，评价指标、全局度量方法的选取各不相同，因此得到的度量结果没有可比性。

5.1.2 全局度量方法论

全局度量的方法论在标准化、普适性等方面进展缓慢、存在局限，在以下几点存在较多缺陷。

1) 度量基线

一个标准化的、最小的量度集是安全度量的度量基线。围绕基线扩展全局度量范围，新的测度可以随着时间推移加入，但是核心的测度应保持固定以应对网络系统的变更。

2) 局部度量

机密性、完整性、可用性是网络安全内在的关键基础特性。越来越庞大的网络系统导致了系统自身很难用简单的量化模型来呈现。复杂系统涉及的内容繁多，仅从风险等独立安全要素角度只能比较片面地解释网络系统存在问题。用漏洞度量、攻防度量等局部度量的方式来代表全局度量不能准确说明安全程度，将导致不准确或者错误地衡量系统安全性。

3) 持续性

全局度量的持续性与组织的领导力有很大关系，只要对项目保持强有力的支持，网络系统安全度量就会持续地展开。全局度量对于管理层具有战略目的，停滞的度量无法用于管理决策。

4) 术语和定义

全局度量缺乏被广泛接受的术语和概念框架，相关词汇定义较含糊，存在交叉，对度量范围界定不清晰。需要明确定义和使用量度作为全局度量的特征来表示网络系统的安全状态，从而形成基本的定义和通用的术语集[105]。随着技术的发展，人们对全局度量的术语会逐步趋于一致。然而要提高一致性的程度并在安全度量实践者中取得共识，还有更多的工作要做。

5.1.3 全局度量可操作性

完善已有的方法、探索还没有被识别的特性的数据组合将有助于推进全局度量谜题的解决，促进精准化度量的实施。

1) 指标

零散指标难以聚合。哪些数据需要被测度，度量标准提供的信息具有一定借鉴作用。测度的数据是广泛的，把测度值集合成一个确定的高层次的指标是必要的。整合指标的数量以及将零散的测度数据升华为复合的指标进行全局度量的方式都需要不断地实践。解决具有不同粒度的度量值存在精度丢失的问题还需要研究人员投入大量的精力。

2) 度量方法

全局度量的方法已经有许多，但都不完善，有各自的优势和劣势。不同的度量方法能从不同角度度量网络系统安全要素，多种方法交叉使用能更系统地表示和建模网络系统中涉及的主要元素或组成部分之间的内部依赖关系[106]。结合人工智能等相关技术实现实时的、自动化度量，能够提高全局度量准确性、完善其高效性和促进其广泛性。

3) 数据格式

数据格式通用性有待改进。不同行业、不同渠道采集的数据格式是有区别的，需要耗时进行处理与关联分析。使用标准格式采集和编制数据，将有益于快速实施全局度量、验证已有的度量结论、创建和对比不同网络系统的原始度量、促进数据共享交换、建立全局度量标杆。

5.2 机遇

5.2.1 全局度量的迫切性

全局度量事关网络系统安全的每一个利益相关者，涉及安全生命周期每一个环节、每一个方面。没有准确的全局度量，就无法形成有效的安全认知，安全相关的所有行为都将处于迷茫。目前，在网络系统安全领域，安全度量及标准具有很大程度的主观性，全局度量处于粗略比较状态。为实现对网络系统安全的精准、客观认识，迫切需要发展全局度量科学。

5.2.2 全局度量的必要性

网络空间成为第五空间，社会基础产业全面网络化，客观的网络系统安全性描述源于更强大的全

局度量。全局度量能够挖掘网络系统安全的内在本质，已成为安全度量发展的客观趋势。网络系统安全全局度量所追求的目标是用较少的成本来获得必要的安全信任。以主动提高网络系统安全性为目的，对网络系统全局度量可以及时发现各类隐含的安全问题及潜在风险，并提出相关的解决建议，确保管理可落实、操作可管控、技术可实施等。通过网络系统所涉及的信息流，进一步建立并实施一系列的全局度量手段，持续不断地改进网络系统安全工作。

5.3　小结

本节首先从可行性、普适性、可操作性等角度说明了全局度量的研究存在挑战。接着又从迫切性和必要性两方面说明了全局度量的研究还面临着机遇。挑战和机遇的提出表明了虽然全局度量研究是困难的，但也为研究人员提供了创新机会，同时提升研究人员的研究热情。

6　未来研究展望

网络系统安全度量研究一直是网络空间安全研究的重要方向之一，这对网络空间安全有着非常重要的意义。通过整理第 5 节，得到全局度量总体的研究状况如下：完整的理论体系仍未形成；客观、量化的标准缺乏，目标不一致；还具有很大程度的主观性、处于粗略比较状态；针对某些特定系统组件，已建立一些成功的安全度量方法，但仍难以完全实现全局度量、客观量化及精准描述网络安全。由此可见，实现全局化度量等研究还有很长的路要走。表 4 总结了网络系统全局度量研究的一些难点问题以及可能的解决方法。

6.1　系统化度量方法学

度量方法学尚未形成完整的、系统化的理论方法。需要将网络安全全局度量形成科学的方法，逐步扩大度量范围，建成具体的体系或框架，让体系或框架指导具体的网络系统安全度量工作，降低业务遭受的损失，保证功能正确实施。度量方法学应提供基本说明，以理解什么是度量、为什么度量、什么时候以及如何度量。研究如何使用度量指标来简化管理、合理预算和分析趋势，设计更有效的网络系统全局度量计划[107]。安全问题很多情况下是由管理问题引起的，管理度量是比较重要的。而在度量组织管理上，方法学应提供如人员情况、法律要求、资源分配、权限设置等管理方面的工作方法[108]。

6.2　全局度量与态势感知相结合

态势感知是对网络系统安全性进行定量分析的一种手段，网络安全分析人员可以借助度量，宏观把握整个网络的安全状况[109]。虽然目前还无法描述网络系统具体的安全程度，但通过态势感知平台可以对一些全局度量方法进行可视化验证，使安全分析人员和网络运营商能粗略地衡量其网络的安全状况和运作的成功与否。可视化技术处理安全大数据时能得到有效应用，尤其是针对大型网络系统的安全指标。通过获取网络系统态势数据，对比分析当前数据和历史数据，将度量结果进行可视化，使人们更能直观地认识网络系统安全状态[110]，从而制定更精准的决策响应突发情况或者预防未来可能发生的不利状况。网络安全监控企业 Scorecard[111]为企业用户提供安全基准测试服务，能感知整个网络系统，度量系统

表 4　　**网络系统全局度量研究面临的问题与方法**

问题	方法
全局度量方法学	新的度量体系与流程
指标体系发展	新的指标标准
态势感知与度量	态势感知、行为分析与度量
攻防效用计算	微分流形原理
安全管理度量	新的度量模型对管理进行量化分析
度量高效性	深度学习算法
攻防模拟与可视化度量	利用可视化模拟攻防过程，对系统进行全局度量
度量数据集	建立一个公开、可以作为度量基准的数据集
自动化网络系统度量	利用机器学习确定全局度量模型，自动化度量
网络系统安全度量行业化	结合不同行业网络，使度量落地

的网络健康状况并做出预测，但度量和预测结果偏主观性。

6.3 度量指标体系建设

精准度量网络系统，客观建立度量指标体系、指标标准化、准确度量指标值是关键。指标体系应包含数据采集、数据测度、指标组合等内容。不同场景下的网络系统全局度量的指标一般是不同的，指标体系应给出指导。提出能够客观描述整体网络系统情况的指标体系，并使之形成标准是一项长期工作。网络系统安全全局度量指标的建设与研究初期借鉴 CC、等级保护等安全体系可以快速形成度量指标并实施度量。例如，一些安全公司结合体系和实际经验建立了自己的度量指标。UpGuard[112] 建立了约 2 000 个网络系统安全度量指标，从企业外部和内部对其信息完整性、脆弱性、合规性、安全性等进行全局度量，并能给出一份网络威胁报告（CSTAR, cyber security threat assessment report），使客户对网络系统安全问题直观理解，了解自身的安全水平。

6.4 网络系统全局度量建模

目前，还不清楚在什么条件下，一个系统的安全性是有意义的、可比较的，即安全程度判断尚不明确。网络系统全局度量建模是判断安全程度的依据，是解决客观性的核心内容。许多企业在安全方面投入了大量的工作，但大多数企业依然不能够确定网络系统是否足够安全。网络系统的复杂性使全局度量建模成为一项艰巨的任务。设计良好的度量模型能够客观地认识网络系统安全性。全局度量模型应是可伸缩、可互操作和全面的，应支持静态或动态度量、自动化度量[113]。全局度量模型除了对技术进行量化外，还需要关注技术以外的管理因素，技术度量和管理度量同时出现才能设计出一套完整的由数据驱动的网络安全度量方案。

6.5 小结

网络系统安全精准度量是一项富有挑战性的研究。国内外对网络系统安全度量的理解还存在诸多分歧，相应的技术框架尚未完善，缺乏系统化的量化分析工具和支撑平台。本节对这些问题做进一步的说明，并列出了 10 个主要问题并给出了解决方法。解决方法主要围绕领域交叉融合，将可视化、自适应、机器学习等技术应用于全局度量中，能极大提高全局度量的研究效率。

7 结束语

网络系统安全全局度量是一个复杂的过程。全局度量系统安全的程度取决于度量的广度、深度。由于影响网络系统安全的因素很多，且各因素之间又相互关联，使安全因素与度量结果之间呈现出一种复杂的非线性关系。因此，需要构建完整的全局度量框架，建立安全度量理论与技术体系，开展典型应用，从而快速提升全局度量技术水平。逐步实现精准的度量，成为当前全局度量体系全面性拓展的基础条件。对全局度量各方面的研究，是改变安全度量现状的技术途径。当解决了网络系统安全难以全局、客观量化问题时，对网络系统安全的认识会更客观、更全面、更科学、更合理。本文分析了全局度量的相关概念及其过程框架，度量的发展历程，对现有的度量方法、体系、工具进行了比较总结，以期抛砖引玉。最后阐述了目前研究中存在的问题，并展望了其未来的发展方向。

参考文献：

[1] KRAUTSEVICH L, MARTINELLI F, YAUTSIUKHIN A. Formal analysis of security metrics and risk[C]//IFIP WG 112 International Conference on Information Security Theory & Practice: Security & Privacy of Mobile Devices in Wireless Communication. Springer-Verlag, 2011: 304-319.

[2] 冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7):10-18.
FENG D G, ZHANG Y, ZHANG Y Q.Survey of information security risk assessment[J].Journal of Communications, 2004, 25(7):10-18.

[3] 赵文.基于“风险熵”的信息系统风险评估数量化模型研究[D]. 西安: 陕西师范大学, 2012.
ZHAO W. Research on quantitative model of risk assessment of information system based on risk entropy[D]. Xi’an: Shanxi Normal University, 2012.

[4] MARTIN R A. Making security measurable and manageable[C]// Military Communications Conference. IEEE, 2009: 1-9.

[5] BREIER J, HUDEC L. Towards a security evaluation model based on security metrics[C]// International Conference on Computer Systems & Technologies. ACM, 2012: 87-94.

[6] CHEW E, SWANSON M M, STINE K M. Performance measurement guide for information security[R]. 2008.

[7] STANDARD I. IEEE standard glossary of software engineering terminology[S]. IEEE Std 610.12-1990, 2002: 1-84.

[8] HAYDEN L. IT security metrics: a practical framework for measuring security & protecting data[M]. McGraw-Hill Education Group, 2010.

[9] HENNING R. Information system security attribute quantification or ordering (commonly but improp—erly known as “security metrics”)[R]. 2002.

[10] 吕欣. 信息系统安全度量理论和方法研究[J]. 计算机科学,2008,35(11):42-44.

LYU X. Information system security metrics: theoretics and methodology[J]. Computer Science, 2008, 35(11):42-44.

[11] JAQUITH A. Security metrics[M]. Addison Wesley, 2007.

[12] CHEW E. Performance measurement guide for information security (DRAFT)[J]. National Institute for Standards & Technology, 2008:265.

[13] JHA S, SHEYNER O, WING J. Two formal analyses of attack graphs[C]//15th IEEE Computer Security Foundation Workshop. 2002: 49-63.

[14] VILLARRUBIA C, FERNANDEZ-MEDINA E, PIATTINI M. Towards a classification of security metrics[C]//The International Workshop on Security in Information Systems. 2004:342-350.

[15] CHEW E, SWANSON M, STINE K M. Performance measurement guide for information security[R]. 2008-07-16.

[16] ZHANG B, CHEN Z, WANG S, et al. Network security situation assessment based on HMM[M]// Advanced Intelligent Computing Theories and Applications with Aspects of Artificial Intelligence. Berlin Heidelberg: Springer, 2011:509-516.

[17] LI L. Security evaluation methods of computer networks based on BP neural network[M]//Advances in Intelligent Systems and Computing. Berlin Heidelberg: Springer, 2013: 181.

[18] PENDLETON M, GARCIA R, CHO J, et al. A survey on systems security metrics[J]. ACM Computing Surveys, 2016, 49(4):62.

[19] HU C. Calculation of the behavior utility of a network system: conception and principle[J]. Engineering, 2018, 4(1):78-84.

[20] IM S Y, SHIN S H, RYU K Y, et al. Performance evaluation of network scanning tools with operation of firewall[C]// Eighth International Conference on Ubiquitous & Future Networks. IEEE, 2016: 876-881.

[21] FREISS M. Protecting (telecommunication) networks with SATAN (security analysis tool for analyzing networks)[J]. EDPACS, 1999, 27(1): 16-17.

[22] BEALE J, DERAISON R, MEER H. Nessus network auditing[M]. Syngress, 2004.

[23] BREIER J, HUDEC L. Towards a security evaluation model based on security metrics[C]// International Conference on Computer Systems & Technologies. ACM, 2012: 87-94.

[24] Information technology -security techniques -information security management measurements[S]. ISO/IEC 27004, 2009.

[25] PFLEEGER S, CUNNINGHAM R. Why measuring security is hard[J]. IEEE Security & Privacy, 2010, 8(4):46-54.

[26] STOLFO S, BELLOVIN S M, EVANS D. Measuring security[J]. IEEE Security and Privacy Magazine, 2011, 9(3):60-65.

[27] MENG M. The research and application of the risk evaluation and management of information security based on AHP method and PDCA method[C]// International Conference on Information Management. IEEE, 2014: 379-383.

[28] FU J, HUANG L, YAO Y. Application of BP neural network in wireless network security evaluation[C]//International Conference on Wireless Communications. IEEE, 2010: 592-596.

[29] JING X Y, YAN Z, WITOLD P. Security data collection and data analytics in the Internet: asurvey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1):568-618.

[30] BASILI V R, CALDIERA G, ROMBACH R H. The goal question metric approach[J]. Encyclopedia of Software Engineering. 1994(1): 578-583.

[31] YAHYA F, WALTERS R J, WILLS G B. Using goal-question-metric (GQM) approach to assess security in cloud storage[M]. Enterprise Security. 2017.

[32] 张漪墁,赵小林.网络安全度量与评估的分析与研究[J]. 中国科技论文在线, 2018, 11(4): 328-338.
ZHANG Y M, ZHAO X L. Analysis and research on network security measurement and evaluation[J]. Highlights of Sciencepaper Online, 2018, 11(4): 328-338.

[33] YUSUF S E, HONG J B, GE M, et al. Composite metrics for network security analysis[J]. Journal of Software Networking. 2018, 2017(1): 137-160.

[34] WAGNER I, ECKHOFF D. Technical privacy metrics: a systematic survey[J]. Computer Science, 2015, 51(3).

[35] ZHANG Q,LIU C X,LU G Q. Active defense technology and its developing trend[J]. Computer Modelling &New Technologies, 2014, 18(12B): 383-390.

[36] MAZIKU H, SHETTY S, JIN D, et al. Diversity modeling to evaluate security of multiple SDN controllers[C]// 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE Computer Society, 2018: 344-348.

[37] RAMOS A, LAZAR M, FILHO R H, et al. Model based quantitative network security metrics: asurvey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(4):2704-2734.

[38] KAVOUSI F, AKBARI B. Automatic learning of attack behavior patterns using Bayesian networks[C]//2012 Sixth International Symposium on Telecommunications (IST). IEEE, 2012: 999-1004.

[39] YI Z, KAI Z, LAI B. Alert correlation graph: a novel method for quantitative vulnerability assessment[J]. Journal of National University of Defense Technology, 2012, 34(3):109-112.

[40] 葛海慧,肖达,陈天平,等.基于动态关联分析的网络安全风险评估方法[J]. 电子与信息学报, 2013, 35(11): 2630-2636.
GE H H, XIAO D, CHEN T P, et al.Quantitative evaluation approach for real-time riskbased on attack event correlating[J]. Journal of Electronics & Information Technology,2013,35(11):2630-2636.

[41] 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.
CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4):885-897.

[42] FENG X, WANG D, MA G, et al. Security situation assessment based on the DS theory[C]//International Workshop on Education Technology & Computer Science. IEEE Computer Society, 2010:352-356.

[43] QU Z Y, LI Y, LI P. A network security situation evaluation method based on DS evidence theory[C]//Environmental Science and Information Application Technology (ESIAT). 2010:496-499.

[44] HU H, LIU Y, ZHANG H. Security metric methods for network multistep attacks using AMC and big data correlation analysis[J]. Security and Communication Networks, 2018, 2018:1-14.

[45] GLADSTONE P J S, KIRBY A J, TRUELOVE J M, et al. Security risk management: U. S. Patent 9438615[P]. 2016-09-06.

[46] ÅRNES A, VALEUR F, VIGNA G. Using hidden Markov models to evaluate the risks of intrusions[J]. Lecture Notes in Computer Science, 2006, 4219:145-164.

[47] RNES A, VALEUR F, VIGNA G, et al. Using hidden Markov models to evaluate the risks of intrusions[M]// Recent Advances in Intrusion Detection. Berlin Heidelberg: Springer, 2006:145-164.

[48] ALMASIZADEH J, AZGOMI M A. A stochastic model of attack process for the evaluation of security metrics[J]. Computer Networks,

2013, 57(10):2159-2180.

[49] DA G, XU M, XU S. New approach to modeling and analyzing security of networked systems[C]//The Symposium and Bootcamp on the Science of Security. ACM, 2014: 1-12.

[50] CIARLET P G. An introduction to differential geometry with applications to elasticity[J]. Journal of Elasticity, 2005, 78-79(1-3):1-215.

[51] 刘刚,李千目,张宏.信度向量正交投影分解的网络安全风险评估方法[J]. 电子与信息学报,2012,34(8):1934-1938.
LIU G, LI Q M, ZHANG H. Reliability vector orthogonal projection decomposition method of network security risk assessment[J]. Journal of Electronics & Information Technology, 2012,34(8):1934-1938.

[52] JÖRG D, GABRIEL J. What is a Petri net?[C]// Unifying Petri Nets, Advances in Petri Nets. Springer-Verlag, 2001: 1-25.

[53] HENRY M H, LAYER R M, ZARET D R. Coupled Petri nets for computer network risk analysis[J]. International Journal of Critical Infrastructure Protection, 2010, 3(2):67-75.

[54] YAN Q. A security evaluation approach for information systems in telecommunication enterprises[J]. Enterprise Information Systems, 2008, 2(3):309-324.

[55] SWILER L D, PHILLIPS C, GAYLOR T. A graph based network vulnerability analysis system[R]. Albuquerque, USA: Sandia National Laboratories, 1998.

[56] KUNDU A, GHOSH N, CHOKSHI I. Analysis of attack graph-based metrics for quantification of network security[C]// India Conference. IEEE, 2012: 530-535.

[57] SHEYNER O, HAINE S, JHA S, et al. Automated generation and analysis of attack graphs[C]//Symposium on Security and Privacy. IEEE, 2002: 273-284.

[58] BHATTACHARYA P, GHOSH S K. Analytical framework for measuring network security using exploit dependency graph[J]. IET Information Security, 2012, 6(4):264-270.

[59] IDIKA N, BHARGAVA B. Extending attack graph-based security metrics and aggregating their application[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1):0-85.

[60] 张鸣天.基于贝叶斯网络的信息安全风险评估研究[D].北京：北京化工大学,2016.
ZHANG M T. Research on information security risk assessment based on Bayesian network[D].Beijing: Beijing University of Chemical Technology, 2016.

[61] FRIGAULT M, WANG L. Measuring network security using Bayesian network-based attack graphs[C]//IEEE International Computer Software and Applications. IEEE, 2008:698-703.

[62] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 61-74.

[63] 王元卓, 林闯, 程学旗, 等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报,2010,33(9):1748-1762.
WANG Y Z, LIN C, CHENG X Q, et al. Analysis for network attack-defense based on stochastic game model[J]. Chinese Journal of Computers,2010, 33(9):1748-1762.

[64] LI X, LU Y, LIU S. Network security situation assessment method based on Markov game model[J]. Ksii Transactions on Internet & Information Systems, 2018, 12(5):2414-2428.

[65] ZHANG H, HAN J, ZHANG J. Security risk evaluation of information systems based on game theory[C]// International Conference on Intelligent Human-machine Systems & Cybernetics. IEEE, 2013: 46-49.

[66] FU S, ZHOU H. The information security risk assessment based on AHP and fuzzy comprehensive evaluation[C]// IEEE International Conference on Communication Software & Networks. IEEE, 2011: 124-128.

[67] GENG W, HU Y. Information security management model based on AHP[C]// International Conference on Measurement. 2012: 352-355.

[68] YAN C, QIAO B. Study and application of risk evaluation on network security based on AHP[J]. Journal of Huangshi Institute of Technology, 2012, 289:198-205.

[69] LI J H, LI G Z. Study on the evaluation model for network security[J]. Advanced Materials Research, 2011, 317-319:1745-1748.

[70] TUTEJA A, THALIA S. Towards quantification of information system security[M]// Computational Intelligence and Information Technology. Springer Berlin Heidelberg, 2011.

[71] 李景智,殷肖川,胡图.基于可拓理论的网络安全评估研究[J].计算机工程与应用,2012,48(21):79-82.
LI J Z, YIN X C, HU T, et a1. Network security evaluation algorithm based on extension theory[J]. Computer Engineering and Applications, 2012, 48(21):79-82.

[72] FU Y, WU X P, YE Q, et al. An approach for information systems security risk assessment on fuzzy set and entropy weight[J]. Acta Electronica Sinica, 2010, 38(7):1489-1494.

[73] KONG L. Risk evaluation scheme for accounting information system based on Analytic Hierarchy Process[C]// 2017 International Conference on Smart Grid and Electrical Automation (ICSGEA). IEEE Computer Society, 2017.

[74] TEMAM O. The rebirth of neural networks[C]// International Symposium on Computer Architecture. 2010: 349.

[75] 顾兆军,辛倩.熵权神经网络的信息系统安全评估[J].计算机工程与设计,2018,39(7):1856-1860.
GU Z J, XIN Q. Information system security evaluation based in entropy weight method and neural network[J]. Computer Engineering and Design, 2018,39(7):1856-1860.

[76] Standards Press of China. Information security technology system security level protection evaluation requirements[S]. GB/T 28448-2012. 2012.

[77] MA L, PAN D, WU Z. ANN RBF approach of risk assessment for aviation ATM network[J]. Sensors & Transducers Journal, 2013, 159(11): 132-137.

[78] JIANG Y P, CAO C, MEI X, et al. A quantitative risk evaluation model for network security based on body temperature[J]. Journal of Computer Networks & Communications, 2016(4):3.

[79] ZHANG M, WANG L, JAJODIA S. Network diversity: asecurity metric for evaluating the resilience of networks against zero-day attacks[J]. IEEE Transactions on Information Forensics and Security, 2016:1.

[80] CARLO B, MARCO C, GIANLUIGI V. Digital information asset evaluation[J]. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2018, 49(3):19-33.

[81] LEWIS M J. Characterizing risk[C]// Eighth Cyber Security & Information Intelligence Research Workshop. 2013: 1-4.

[82] CHEN C X. Innovation and development of China's information security level protection system[J]. Cyberspace Security, 2016, 7(2): 5-6.

[83] Common criteria for information technology security evaluation V3.1[R]. 2017.

[84] ALCARAZ C, MELTEM SÖNMEZ TURAN. PDR: A Prevention, Detection and Response mechanism for anomalies in energy control systems[J]. American Geophysical Union, 2012, 90(17):22-33.

[85] LIU G C. BS7799 criterion and its application in meso-information systems audit[J]. Journal of Audit & Economics, 2012(3):1-2.

[86] WEIK M H. Federal information processing standard publication[R]. 2002.

[87] NIKOLOPOULOU A. The directive on security of network and information systems (NIS directive)from a practional view [R]. 2019.

[88] National Institute of Standards and Technology. Framework for improving critical infrastructure cyber security[R]. 2014.

[89] Standards Press of China. Information security technology-baseline for classified protection of cyber security[S]. GB/T 22239-2019, 2019.

[90] 姚传军.WPDRRC 信息安全模型在安全等级保护中的应用[J].光通信研究,2010(5):27-29.
YAO C J. Application of WPDRRC information security model in multi-level security protection[J]. Study on Optical Communications, 2010(5): 27-29.

[91] KOROTKA M S, ROGER YIN L, BASU S C. Information assurance technical framework and end user information ownership: a critical analysis[J]. Journal of Information Privacy and Security, 2005, 1(1): 10-26.

[92] HECKMAN M, SCHELL R. Using proven reference monitor patterns for security evaluation[J]. Information, 2016, 7(2):23.

[93] HOUMB S H, RAY I. Trust-based security level evaluation using Bayesian belief networks[C]// Transactions on Computational Science X. 2010: 154-186.

[94] CHEN Y J, LIAO G Y, CHENG T C. Risk assessment on instrumentation and control network security management system for nuclear power plants[C]//International Carnahan Conference on Security Technology. IEEE, 2009: 216-264.

[95] GUAN B C, LO C, WANG P. Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method[C]// IEEE International Carnahan Conference on Security Technology. IEEE, 2003: 168-175.

[96] TAO H, LIANG C, CHI W. The research of information security risk assessment method based on fault tree[C]// Sixth International Conference on Networked Computing & Advanced Information Management. IEEE, 2010: 370-375.

[97] Standards Press of China. Classified criteria for security protection of computer information system[S]. GB17859-1999, 1999.

[98] Aryasec. Measurement of information security effectiveness[EB/OL]. 2019.

[99] SIPONEN M, WILLISON R. Information security management standards: Problems and solutions[J]. Information & Management, 2009, 46(5):267-270.

[100] GB/T 31495. Information security technology—Indicator system of information security assurance and evaluation methods[S].2015.

[101] FRAY I E. A comparative study of risk assessment methods, mehari & cramm with a new formal model of risk assessment (fomra) in information systems[M]// Computer Information Systems and Industrial Management. Berlin Heidelberg: Springer, 2012.

[102] SARKHEYLI A , ITHNIN N B. Improving the current risk analysis technologies by study of their process and using the human body's immune system[C]//The 5th International Symposium on Telecommunications. IEEE, 2010: 651-656.

[103] NSFOCUS. Industrial control system information security assurance framework[R]. 2019.

[104] 王卫东. 安全度量及其面临的挑战[J]. 保密科学技术, 2011(3): 54-58.
WANG W D. Security metrics and challenges[J]. Secrecy Science and Technology, 2011(3):54-58.

[105] KOTT A, WANG C, ERBACHER R F. Cyber defense and situational awareness[M]. Berlin Heidelberg: Springer, 2014.

[106] CHENG Y, DENG J, LI J, et al. Metrics of security[J]. Advances in Information Security, 2014, 62:263-295.

[107] KOVACICH G. Information systems security metrics management[J]. Computers & Security, 1997, 16(7):610-618.

[108] HERRERA S O S. Information security management metrics development[C]// International Carnahan Conference on Security Technology. IEEE, 2005.

[109] 龚俭, 臧小东, 苏琪. 网络安全态势感知综述[J]. 软件学报, 2017, 28(4): 1010-1026.
GONG J, ZANG X D, SU Q. Network security situation awareness[J]. Journal of Software,2017,28(4):1010-1026.

[110] KOTENKO I, NOVIKOVA E. Visualization of security metrics for cyber situation awareness[C]//2014 Ninth International Conference on Availability, Reliability and Security (ARES). 2014: 506-513.

[111] Security Score Card. Analysis of cyber risk exposure for US and European political parties report[R]. 2019-03-14.

[112] UPGUAR D. A beginner's guide to cyber security insurance[M]. Gov.uk Press, 2017.

[113] LUNA J, GHANI H, GERMANUS D, et al. A security metrics framework for the cloud[C]//The International Conference on Security and Cryptography. IEEE, 2011: 245-250.

[作者简介]

吴晨思（1990− ），男，黑龙江大庆人，中国科学院大学博士生，主要研究方向为网络攻防与安全度量。

谢卫强（1992− ），男，河南周口人，西安电子科技大学硕士生，主要研究方向为网络攻防与安全度量。

姬逸潇（1994− ），男，河北衡水人，西安电子科技大学硕士生，主要研究方向为信息安全。

杨粟（1993− ），男，山东临沂人，中国科学院大学博士生，主要研究方向为信息安全与深度学习。

贾紫艺（1994− ），男，河北石家庄人，中国科学院大学硕士生，主要研究方向为网络攻防。

赵松（1994− ），男，陕西西安人，西安电子科技大学硕士生，主要研究方向为信息安全与网络攻防。

张玉清（1966− ），男，陕西宝鸡人，博士，中国科学院大学教授、博士生导师，主要研究方向为网络与信息系统安全。