网络信息系统安全评估理论与应用

林梦泉 著

科学出版社
www.sciencep.com

网络信息系统安全评估理论与应用

林梦泉 著

科学出版社
北京

内 容 简 介

本书从宏观层面系统地研究了网络信息系统的安全评估问题，提出了一整套新的安全评估理论、方法和技术，并通过敏感和教育网络信息系统的实例分析，验证了其可行性和有效性。鉴于网络信息系统本身结构的复杂性、开放性和动态性，本书进行了系统安全评估的总结性研究，对于安全评估的安全五属性模型、基本模型及其约简算法、评估实施方法、流程和保证安全测评可靠性等问题进行了总结和工程化集成，研究评估方法的普遍性和特殊性问题。

本书可供从事网络信息系统安全评估工作的科研人员阅读参考，也可以作为信息安全、计算机软件等相关专业研究生和高年级本科生的教学参考书。

图书在版编目(CIP)数据

网络信息系统安全评估理论与应用/林梦泉著. —北京：科学出版社，2010

ISBN 978-7-03-027217-1

Ⅰ.网… Ⅱ.林… Ⅲ.计算机网络-信息系统-安全评价 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2010)第 065132 号

责任编辑：张艳芬 / 责任校对：朱光光

责任印制：赵 博 / 封面设计：嘉华永盛

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 4 月第 一 版 开本：A5(890×1240)

2010 年 4 月第一次印刷 印张：5 1/8

印数：1—600 字数：126 000

定价：50.00 元

(如有印装质量问题，我社负责调换)

前　言

随着信息科学技术的迅速发展，Internet 已成为全球信息传播的重要平台，它打破了信息交互的地域界线，改变了信息交互的传统模式。由于国际互联网的开放性、普遍性和复杂性，信息传输和存储的安全性、可靠性面临越来越严重的威胁，20 世纪 90 年代中叶已经出现了网络信息安全危机。网络信息系统安全已经成为社会安全的重要组成部分，它直接关系到人们的正常生活、工作和学习，甚至危及到国家军事和经济安全。因此，掌握网络信息安全状况，对其安全态势做到“心中有数”，并进行可预知的安全管理和控制，最大限度地减少因安全问题而导致的信息及服务损失，是目前各国重点关注和加速研究的课题。安全评估是获取信息系统安全状况的重要手段，安全评估结果是制订安全解决方案的重要依据。

在分析了国内外信息系统安全准则、评估模型和评估方法研究现状的基础上，本书瞄准安全评估迫切需要解决的关键问题，从顶层入手，研究构建了网络信息系统安全评估的基本模型，对模型进行了约简优化，讨论了评估方法和评估实施策略等问题；基于以上研究成果并结合部分已有的实用技术和方法，提出了基于安全评估数据仓库、专家知识库和数据挖掘技术的评估决策支持系统的基本框架。

首先，系统地分析和总结了网络信息系统安全特性存在的主要问题，提出了信息系统安全的层次化模型和属性描述模型的概念，给出了这些概念的内涵。通过对两者的比较研究，本书提出了信息系统安全五属性树型模型(CIACM 模型)。该模型能够从全局的角度描述整个信息系统安全属性，其中任意一个属性都能够独立地体现信息系统的一种安全性能，如可管性等。CIACM 模型还具有延续性、相对稳定性和操作简易性，更适用于对信息系统安全性能的有效和快捷评估。CIACM模型强调了信息系统的可控和可管的安全属性，突出了安全管

理在信息系统安全体系中不可替代的重要作用。因而，本书采用CIACM模型研究网络信息系统安全评估问题，并以CIACM模型为基础构建树型结构评估模型(体系)。

树型结构模型的核心问题是模型结构和结构系数，即模型的安全指标项及其结构层次和指标项的权重系数。基于该模型，本书提出了指标安全度的概念，即用各安全指标安全度及其对系统整体安全性能影响的重要程度(权重)来度量系统整体安全度。因此，模型的指标数量和层次及指标的权重决定了系统的整体安全度。树型结构模型指标权重的确定是个难点，本书提出了一种能综合AHP和DELHEI两者优点的混合算法来构造权重集。但在树型结构模型中，一般维数越高(指标多)，得到的权重实用性就越差。此外，网络信息系统树型结构模型中，若体系庞大，指标项过多过细，评估结果的可信度就难以保证，评估成本也较高。为克服这些缺陷，需要简化安全指标项。本书在树型模型的基础上，提出了"最佳节点基本模型"的概念，并给出了建立基本模型的原则和方法。基本模型选择了最科学、最实用的安全测评点，不但提高了评估效率，还适当减低了模型的维数。

其次，探讨了应用粗糙集理论对模型进行进一步约简优化问题。树型模型在评估应用时，其模型的指标是根据安全属性的界定来定义其内涵的，这些安全属性最大的特征是指标之间关联较多，因此基本模型存在进一步简化的可能性。采用一般的相关性分析方法进行化简，需要更多的先验知识，处理难度较大，可信度难以保证。根据数据挖掘理论，在反映客观事实的数据中，蕴涵着客观、内在的知识和规则，采用粗糙集方法恰恰可以方便地发现这些知识和规则。因此，本书在研究粗糙集理论及其在数据挖掘中应用的基础上，首次提出了基于粗糙集理论方法、专家知识和经验的混合启发式约简算法。此约简算法的优化过程可以得到指标重要性权重，同时解决树型模型的结构优化和权重优化两个难点。然后将混合约简得到的模型和基本约简得到的模型进行融合，建立更加优化、更符合实际、能突出核心指标的评估模型。本书以较典型的敏感和教育信息系统为例进行约简实验，约简结果反映了敏感、教育信息系统安全性能特征，说明约简算法能够获取两类系

统评估样本数据中包含的知识和规律。通过两个不同类型信息系统的约简分析，说明基于粗糙集混合启发式约简算法也可以广泛适用于金融、电信等其他类型信息系统安全评估模型的约简优化。因此，本书研究成果对于我国信息系统安全评估具有普遍的实用价值。

再次，研究了模型应用问题。应用约简优化的安全评估模型对网络信息系统进行评估，提高了安全评估效率和准确性。为了采用科学有效的技术和方法快速获得准确、可信的评估结果，针对评估模型和方法的工程实用化问题，提出了安全评估实施过程中影响信息获取可靠性的六个因素及确保可靠性的四个条件，提出了安全评估信息获取的具体方式、方法，提出了关于多渠道信息整合的概念、方法和步骤，给出了安全评估整体性和五属性评估结果的定性、定量安全度分级表及其相互转换的规范，并且定义了定量安全度的物理意义，最后通过实例说明这些技术和方法应用的有效性。

最后，鉴于网络信息系统本身结构的复杂性、开放性、动态性，本书进行了系统安全评估的总结性研究，对于安全评估的安全五属性模型、基本模型及其约简算法、评估实施方法、流程和保证安全测评可靠性等问题进行了总结与工程化集成，研究评估方法的普遍性和特殊性问题。本书还系统性地总结和分析了安全评估的一般过程，在更高层次上提出了安全评估的总体框架，并应用基于专家知识库和数据仓库的数据挖掘方法，研究了评估系统支撑平台的体系结构和构建方法。基于支撑平台可以实现自动化的信息系统评估、安全决策管理。通过教育信息系统安全评估实例，根据决策方法推理分析，结合用户的实际情况，提出了切合实际的安全策略。实例说明，本书提出的评估决策方法具有应用的可行性。

本书从宏观层面系统地研究了网络信息系统的安全评估问题，提出了一整套新的安全评估理论、方法和技术，并通过敏感和教育网络信息系统的实例分析，验证了其可行性和有效性。网络信息系统安全评估是个复杂的系统工程，安全因素是动态变化的，人们对网络信息系统的安全要求也在不断变化和提高。本书只是从网络信息系统安全评估的一个角度，对网络信息系统安全评估问题进行了一些尝试性的探索，

希望对网络信息系统安全评估研究与实践工作有所裨益。

本书在编写过程中，得到了上海交通大学信息安全工程学院常务副院长李建华教授、网络信息安全教育部工程研究中心主任薛质教授的鼓励和支持，另外王强民、陈秀真、李翔和李生红老师也提出了许多有益的建议。同时还要对引用参考文献的作者表示诚挚的谢意。

最后，感谢那些百忙之中抽出时间对本书进行审阅的老师们。

书中难免出现错误和遗漏之处，恳请有关专家和读者批评指正。

作　者

2010 年 2 月于北京

目　录

第一章　网络信息系统安全及评估概述

本章分析了网络信息系统受到的主要安全威胁及其可能造成的各种危害，总结了网络信息系统的不安全因素，由此说明安全评估和安全管理的重要性；通过梳理国际、国内现有安全标准，分析安全评估标准、思想、方法和工具等研究现状与发展方向，提出了本书研究内容。

1.1　网络信息系统主要威胁及危害

1.1.1　面临的安全威胁

从1969年美国国防部高级研究计划署(DARPA)资助建立世界上第一个分组交换实验网ARPANET开始，到1994年中国互联网的起步，互联网经过高速的发展，如今已经渗透到社会和生活的方方面面，全世界都搭上了互联网的快车。据统计显示，截至2005年年底，全球互联网用户数达到10.8亿，比2004年增长了1.5亿。1995年到2000年期间，全球互联网用户数由4500万增至4.2亿，增长接近10倍。而在随后的五年里，全球互联网用户数也增长了一倍以上。截止2005年年底，我国网民人数达到1.11亿，突破1亿大关，位居世界第二[1]。

如此规模化的互联网已对今天的全球政治、经济以及生活等方面带来了重大的影响，成为当今世界最先进的人际交流和信息沟通平台。然而互联网就像一把双刃剑，在带给人们发展、便利、自由、开放等一切利益的同时，也带来了不可忽视的安全威胁。网络安全威胁主要有主动攻击和被动攻击，其中包括人员的恶意与非恶意攻击、恶意代码、物理临近攻击、网络侦听等。网络安全威胁的现状通过下面的一组统计数据和信息可见一斑：

与2004年相比，2005年国家计算机网络应急技术处理协调中心

(CNCERT/CC)接收的漏洞扫描类和非扫描类事件报告[2]数量增长了一倍左右,如图 1.1 所示。

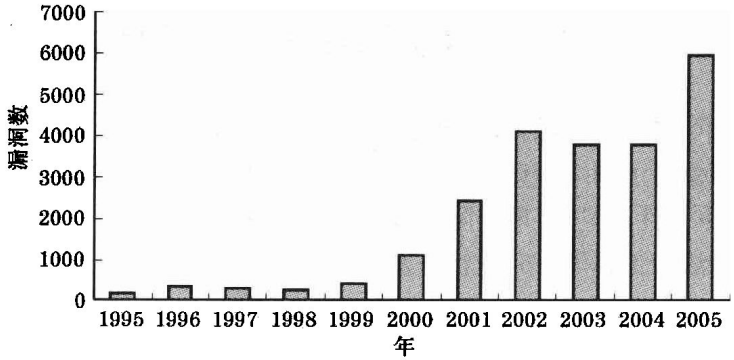

图 1.1 CNCERT/CC 每年的漏洞报告数目统计

利用安全漏洞进行攻击的事件已不再局限于 Windows 平台,其他一些流行商业软件上存在的漏洞也日益得到黑客的青睐[3,4];另据行业预测,今后带有犯罪意图的网络攻击将愈演愈烈,病毒和攻击的形式将更灵活多变、更纷繁复杂,所以网络安全的状况实在不容乐观。网络的不断发展是必然的趋势,因此我们必须面对如今日益严峻的网络安全形势,加强对计算机和网络的安全管理,提高信息系统抵御安全威胁的能力。

1.1.2 电子犯罪对全球经济的影响

纵观近几年的互联网安全态势,安全事件层出不穷,造成的经济损失和社会影响也日益加剧。

(1) 2000 年美国数家顶级互联网网站 Yahoo、Buy、eBay、Amazon、CNN 等遭到大规模拒绝服务攻击,系统瘫痪达数小时之久,经济损失达 12 亿美元以上。

(2) 2001 年爆发了 CodeRed 和 Nimda 等蠕虫事件,CodeRed 蠕虫在爆发后的 9 小时内就攻击了 25 万台计算机,造成的损失估计超过 20 亿美元;Nimda 蠕虫造成的损失从 5 亿美元攀升到 26 亿美元后,仍在继续攀升,到现在已无法估计。

(3) 2002 年全球的根域名服务器遭到以 ICMP 洪水方式发动的大规模拒绝服务攻击，险些让互联网陷入全面瘫痪的尴尬境地。

(4) 2005 年 6 月 17 日晚，总部设在纽约的万事达信用卡国际公司宣布，由于一名黑客侵入“信用卡第三方付款处理系统”，包括万事达、维萨(Visa)、美国运通公司和美国发现公司在内的各种信用卡 4000 多万用户的数据资料可能失窃，这是近年来美国发生的最大规模的客户资料泄密事件，也是有史以来最严重的信息安全事件。

随着互联网应用的日益复杂、用户规模的不断扩大，网络上存在的安全漏洞越来越多，可利用的黑客攻击工具也日益增多，对攻击者的技术水平要求不断降低，黑客攻击手法也不断翻新。蠕虫病毒蔓延速度越来越快，周期也越来越短。这些安全事件可能在几分钟内造成大面积的网络灾难，波及范围可涉及国家政府机关、军事单位、金融机构、通信企事业单位等。

事实上，黑客攻击、计算机病毒破坏和网络金融犯罪已构成对世界各国的严重威胁，甚至是头号威胁。进入 21 世纪以来，尽管人们在计算机技术上不断努力，但网络安全形势却是越发令人不安。在各领域的计算机犯罪和网络侵权方面，数量、手段、性质、规模已经到了令人吃惊的地步。

(1) 据统计，目前美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元，德国、英国也都有数十亿美元，法国则有 100 亿法郎，日本、新加坡受到的经济损失也很严重。在国际法律界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首[5]。

(2) 2005 年 CSI/FBI 计算机犯罪和安全调查显示，2004 年计算机信息盗窃造成的金融影响增加了一倍多。

可见，由于电子犯罪导致的全球经济损失在不断地攀升。经济是国家、企事业单位的命脉，网络安全事件导致的巨大经济损失将可能是企事业单位的灭顶之灾，这也是为什么近年来计算机信息系统或者网络安全管理愈来愈得到各国重视的原因。

1.2 网络信息系统的不安全因素

1.2.1 外部的人为因素

影响网络安全的因素很多，既有自然因素，也有人为因素，其中人为因素危害较大。人为因素根据动机本质划分，可分为无意的人为失误和恶意的人为攻击。

（1）无意的人为失误：这主要是由于用户安全意识匮乏和安全技能低下导致的，且通常发生于内部员工身上。通常包括：用户对设备和系统应用等的安全配置不当或疏忽；用户口令选择不慎；用户将自己的账号随意转借他人或与别人共享，以及对网络安全管理不善等。

（2）恶意的人为攻击：人为的恶意攻击主要是来自有明显企图的攻击者。通常攻击者的类型包括：心怀叵测的黑客；企事业单位内部心怀恶意的员工；行业间谍；恐怖分子；对立的情报机关/人员等。

人为恶意攻击对计算机网络造成了极大的危害，并导致了机密数据的泄露，是计算机网络所面临的最大威胁。人是计算机网络最活跃、最不确定、最根本性的不安全因素，因此应将人的教育、培训和管理作为计算机网络安全管理的重中之重。

1.2.2 安全漏洞和计算机病毒

操作系统及网络软件不可能是百分之百无缺陷、无漏洞的，可以说漏洞几乎存在于任何的系统和软件中，包括微软操作系统、各种数据库以及应用系统。另外，编程人员为自便而在软件中留有“后门儿”，一旦漏洞及“后门儿”为外人所知，就会成为整个网络系统受攻击的首选目标和薄弱环节。大部分的黑客入侵网络事件就是由系统的漏洞和“后门儿”所造成的。而且目前漏洞发现的数量迅速增长，周期不断缩短，发现安全漏洞和到发布相关漏洞攻击代码之间的间隔时间也不断缩短，因此由安全漏洞因素导致的危害是不可忽视的。

近几年安全漏洞和计算机病毒已成为主要的网络安全因素[6]，所

以对于安全漏洞和计算机病毒的防护是计算机网络管理不可或缺的一个方面。

1.2.3　自然环境与灾害

计算机系统硬件和通信设施极易遭受自然环境因素(如温度、湿度、灰尘度和电磁场等)以及自然灾害(如洪水、地震等)的影响。自然环境因素容易导致计算机网络硬件、设施的故障和损坏,以及数据的破坏和丢失,而自然灾害对计算机网络导致的损坏和损失是灾难性的、无法估量的。虽然自然环境与灾害因素在一定程度上是不可避免的,但也必须是安全管理的一个环节。

1.2.4　网络安全防护体系中重技术轻管理问题

长期以来,人们对网络安全防护偏重于依靠技术,从早期的加密技术、数据备份、防病毒到近期网络环境下的防火墙、入侵检测、身份认证等。厂商在安全技术和产品的研发上不遗余力,新的技术和产品不断涌现;企事业单位也将网络安全防护理解并实施为安全产品的简单堆砌,把仅有的预算也都投入到安全产品的采购上。

据有关部门统计[7],在所有的计算机安全事件中,约有52%是人为因素造成的,25%由火灾、水灾等自然灾害引起,技术错误占10%,组织内部人员作案占10%,仅有3%左右是由外部不法人员的攻击造成。因此,事实上仅仅依靠技术和产品保障网络安全的愿望往往难尽人意,许多复杂、多变的安全威胁和隐患靠产品是无法消除的。事实上,安全事件中有高达70%以上是属于管理方面的原因,其中绝大多数安全问题是可以运用科学的网络安全管理方法和技术来解决的。在网络信息安全方面,业界目前已开始接受在其他领域总结出来的"三分技术,七分管理"的实践经验和原则,并已意识到管理是网络安全防护的重要基础。

网络安全防护体系是一个复杂的系统工程,涉及人、技术、操作等要素,单靠技术或单靠管理都不可能实现。因此,必须将网络安全技术与管理相结合,包括各种安全技术与运行管理机制、人员思想教育与技

术培训、安全规章制度建设等方面的具体结合，包括防火墙、安全漏洞扫描；入侵检测、网络陷阱、入侵取证、备份恢复和病毒防范、安全评估分析、信息收集、访问控制、蜜罐、内部安全管理等方法、技术和工具，这些都是网络安全体系中十分重要的组成部分，缺少任何一种都会有巨大的危险，必须在安全策略的指导下合理部署，互联互动，形成一个有机的整体，而不仅仅是简单地堆砌。但正如前所说，安全不是简单的技术问题，不落实到管理，再好的技术、设备也是徒劳的，所以在安全技术的基础之上，还应该将正确的安全管理贯彻到整个安全防护体系，实现一个以安全策略为核心，以安全技术为支撑，以安全管理为落实的有效的安全防范体系。

1.3 网络信息系统安全标准

保障信息系统的安全，建立相应的保障体系，采取合适的安全防范和响应措施，所有这些工作的基础就是网络信息系统安全评估。评估基础则是网络安全标准。下面分析目前国际上最为规范、通用和完整的标准及其特点和缺陷，为分析评估现状和问题提供基础。

1.3.1 国外网络信息系统安全标准

随着信息技术的发展、信息社会的形成，对信息系统安全水平的评价受到了世界各国的关注，也形成了一些安全评估标准。

1. 美国 TCSEC(橘皮书)

美国是最早开展计算机系统安全标准研究，并推出第一个操作系统安全评价准则的国家。1985 年，美国国防部所属的国家计算机安全中心(NCSC)出版了《可信计算机评价准则》(TCSEC)，称为“橘皮书”[8]。20 世纪 70 年代，计算机系统安全的基础理论研究出现了部分成果，如 Bell & La Padula 模型，TCSEC 是在该模型基础上提出的，其基本目的是对操作系统的安全性进行评估。随后美国国防部发布了可信数据库解释(TDI)、可信网络解释(TNI)等一系列与安全相关的解