LOIS

信息安全国家重点实验室

信息安全丛书

Network Security
Principle and Technology

网络安全原理与技术

冯登国 编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

网络安全原理与技术

冯登国 编著

国家重点基础研究发展规划项目(项目编号:G1999035800)
国家杰出青年科学基金资助项目(项目编号:60025205)

科学出版社
北京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。书中主要介绍了一系列用于解决计算机网络安全的关键技术和用于保护计算机网络的安全协议、安全策略。本书主要包括两方面的内容：一方面是基本的术语、概念、方法和技术的介绍，包括密码技术，实现安全服务的方法和策略，IDS 技术，网络攻击技术和 PKI 技术；另一方面是一些典型的安全协议标准和技术标准的介绍，包括 OSI 安全体系结构和框架，OSI 层安全协议，IPSec 协议，TLS 协议，IKE 协议，OSI 管理标准，SNMP 协议和安全评估准则。为便于读者掌握和巩固所学知识，书中配备了大量习题。

本书可作为计算机、通信、信息安全、密码学等专业的本科生、研究生的教科书，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

网络安全原理与技术/冯登国编著. —北京：科学出版社，2003
(信息安全国家重点实验室信息安全丛书/冯登国主编)
ISBN 7-03-011986-X

Ⅰ.网… Ⅱ.冯… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2003)第 065817 号

责任编辑：鞠丽娜/责任校对：宋玲玲
责任印制：吕春珉/封面设计：王 浩

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
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 9 月第 一 版 开本：B5 (720×1000)
2003 年 9 月第一次印刷 印张：24 1/2
印数：1—5 000 字数：494 000
定价：38.00 元
(如有印装质量问题，我社负责调换〈路通〉)

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其"暴智"来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头鼠脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人、社会和技术，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系，操作系统安全，数据库安全，网络安全，无线网络安全，网络攻击，密码技术，PKI 技术，信息隐藏，安全协议，安全事件应急响应，量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前　言

信息系统包括信息存储系统(如数据库)、信息处理系统(如操作系统)和信息传输系统(如通信网络)等。它的安全是一个错综复杂的问题,涉及面非常广,威胁它的安全因素也很多,比如自然灾害、各种故障以及各种有意或无意的破坏等。为了确保信息系统的安全,则需要从多方面着手,采取各种措施,例如物理措施、管理措施和技术措施等。计算机网络是一种有着广泛应用的信息传输系统,它是计算机与通信技术相结合的产物,它的安全性至关重要,特别是以 Internet 为代表的计算机网络正在成为未来全球信息系统的最重要的基础设施,如果它的安全性解决不好,将直接影响到社会稳定和国家安全。

从 Internet 国际互联网的发展来看,最初是美国军方出于预防核战争对军事指挥系统的毁灭性打击而提出的研究课题,其后将军事用途分离出去,单纯研究在科研教育的校园环境中解决互联、互通、互操作的技术问题。在校园环境中,理想的技术、信息共享主义使 Internet 的发展忽略了安全问题。20 世纪 90 年代后 Internet 从校园环境走上了社会应用,商业应用的需要使人们意识到了忽视安全的危害,尤其是在网上存在利益的今天,一些不良行为从另一个角度向人们揭示了网络系统的脆弱性,从而引起人们对网络安全的空前重视。本书着重从技术角度出发,针对计算机网络的安全需求,系统地介绍解决计算机网络安全的一些关键技术和实现方法,同时也介绍了一些典型的安全技术标准和协议标准。

本书是在作者于 2001 年出版的著作《计算机通信网络安全》的基础上写作而成,对已保留的内容重新进行了修改、调整和补充,并增加了部分新章节。为了便于读者自学,每章后面都配备了大量习题。与此同时,也吸收了国内外现有相关著作中的许多精华,这些著作已在参考文献中列出。本书也是作者长期从事信息安全研究与开发工作的总结。另外,本书在中国科学院研究生院开设的研究生课程中讲授了三次,这些教学实践对本书的形成具有十分重要的意义。

全书分为 10 章。第 1 章主要介绍一系列相关概念和定义,包括网络安全与开放系统,网络安全策略,安全威胁与防护措施,网络安全服务,入侵检测与安全审计,网络攻击,网络体系结构,安全服务的分层配置与安全服务的管理,安全基础设施等。第 2 章主要介绍密码技术,包括对称密码体制,公钥密码体制,完整性校验值,数字签名技术,密钥管理,秘密密钥的分配,公钥分配和公钥证书等。第 3 章主要介绍实现安全服务的一些方法和策略,包括实现认证、访问控制、机密性、完整性、非否认等服务的方法与策略。第 4 章主要介绍 OSI 安全体系结构与安全标准,

包括OSI安全体系结构和框架，安全技术标准，OSI低层安全协议和OSI高层安全协议等。第5章主要介绍Internet安全体系结构，包括IPSec体系结构，认证头协议，封装安全载荷协议，Internet密钥交换(IKE)，TLS协议等。第6章主要介绍网络安全管理协议，包括OSI管理标准，OSI管理安全，SNMPv1的安全特征，SNMPv3的安全特征等。第7章主要介绍入侵检测系统(IDS)与应急响应技术，包括入侵检测方法，入侵检测系统的设计原理和应急响应技术等。第8章主要介绍网络攻击技术，包括网络攻击过程分析，扫描器，缓冲区溢出攻击，口令安全与Crack工具，拒绝服务攻击与防范等。第9章主要介绍公钥基础设施(PKI)，包括PKI的组成部分，PKI的核心服务，PKI的信任模型，实施PKI应考虑的若干因素，WPKI等。第10章主要介绍制定网络安全解决方案的指导准则，包括安全评估准则，整体安全解决方案的规划，BS7799标准等。

本书在写作过程中，得到了科学出版社的大力支持以及国家重点基础研究发展规划项目(项目编号：G1999035800)和国家杰出青年科学基金项目(项目编号：60025205)的资助，也得到了很多学者的鼓励和帮助，在此深表谢意。

冯登国

2003年7月于北京

主要参考文献

戴英侠，连一峰，王航. 2002. 系统安全与入侵检测. 北京：清华大学出版社

冯登国，裴定一. 1999. 密码学导引. 北京：科学出版社

冯登国. 2001. 计算机通信网络安全. 北京：清华大学出版社

王育民，刘建伟. 1999. 通信网的安全——理论与技术. 西安：西安电子科技大学出版社

Andrew S T. 1996. Computer Networks(3rd ed.). Prentice-Hall

Carlisle A, Steve L. 1999. Understanding Publickey Infrastructure: Concepts, Standars and Deployment Considerations, Macmillan Technical Publishing

Carlton R D. 2001. IPSec: Securing VPNs. McGraw-Hill

Ford W. 1994. Computer Communications Security. PTR Prentice Hall

Joel S, Stuart M, George K. 钟向群，杨继张译. 2002. 黑客大暴光. 北京：清华大学出版社

Menezes, A J, Van Oorschor, P and Vanstone S. 1996. Handbook of Applied Cryptography, CRC Press

Stallings W. 1999. Network Security Essentials: Applications and Standards. Prentice-Hall

目　录

第1章 绪 论

1.1 网络安全需求

随着信息技术的发展与应用，信息安全的内涵在不断的延伸，要对信息安全给出一个精确的定义似乎很难，但在当前情况下，信息安全可被理解为在既定的安全密级的条件下，信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据以及经由这些系统所提供的服务的可用性、机密性、完整性、非否认性和可控性。这五性的具体含义如下：

可用性是指尽管存在可能的突发事件如供电中断、自然灾害、事故或攻击等，但用户依然可得到或使用数据，服务也处于正常运转状态。

机密性是指保护数据不受非法截获和未经授权浏览。这一点对于敏感数据的传输尤为重要，同时也是通信网络中处理用户的私人信息所必须的。

完整性是指能够保障被传输、接收或存储的数据是完整的和未被篡改的。这一点对于保证一些重要数据的精确性尤为关键。

非否认性是指能够保证信息行为人不能否认其信息行为。这一点可以防止参与某次通信交换的一方事后否认本次交换曾经发生过。

可控性是指保证信息和信息系统的授权认证和监控管理。这一点可以确保某个实体（人或系统）的身份的真实性，也可以确保执政者对社会的执法管理行为。

计算机通信网络作为一种传输信息系统，由于其广泛的应用，其安全问题日益突出，也成为人们关注的一个焦点。计算机通信网络安全（简称网络安全）问题的解决除了要考虑网络自身的安全因素之外，还必须综合考虑操作系统、数据库、应用系统、人员管理等因素，但本文主要侧重于介绍网络自身的安全因素。

目前网络安全已不再是军方和政府要害部门的一种特殊需求。实际上，所有的网络应用环境包括银行、电子交易、政府（无密级的）、公共电信载体和互联/专用网络都有网络安全的需求。关于这些典型应用环境的安全需求参见表1.1。

表 1.1 典型应用环境的安全需求

应用环境	安全需求
所有网络	阻止外部的入侵
银行	避免欺诈或交易的意外修改 识别零售的交易顾客 保护个人识别号(PIN)以免泄漏 确保顾客的秘密
电子交易	确保交易的起源和完整性 保护共同的秘密 为交易提供合法的电子签名
政府	避免无密级而敏感的信息的未授权泄漏或修改 为政府文件提供电子签名
公共电信载体	对授权的个人限制访问管理功能 避免服务中断 保护用户的秘密
互联/专用网络	保护团体/个人的秘密 确保消息的真实性

1.2 网络安全与开放系统

从词义上看,网络安全与开放系统似乎是矛盾的,但事实并非如此。开放系统的概念代表了购买者多年来对封闭的、独立的计算机系统以及通信硬件和软件的经销商们所寄予的厚望。人们期望可以自由地选择经销商来购买不同的系统部件,而这些部件可以有机地组合起来以满足购买者的需要。因此,开放系统的发展与应用和许多标准的制定密切相关。

计算机联网是与开放系统并肩发展起来的。开放系统的标志是开放系统互联(Open System Interconnection,OSI)模型的提出。自从 20 世纪 70 年代以来,这个模型得到了不断的发展和完善,从而成为全球公认的计算机通信协议标准。除了 OSI 标准之外,另外还有一些标准化组织也建立了开放系统网络协议。最为有名的当属 Internet 协会,它提出了著名的 TCP/IP 协议。通过围绕开放系统互联所开展的标准化活动,使得不同的厂家所提供的设备进行互联成为可能。

将安全保护措施渗透到开放系统网络中是一项十分复杂的任务。之所以说它复杂，主要是因为它代表了两种技术的完美结合——安全技术的应用与通信协议的设计。为了给开放系统网络提供安全保证，就必须将安全技术与安全协议相结合，而安全协议则是一般的网络协议的重要组成部分。

人们已经在下列三个较宽的领域内设计或建立了一些兼容的或作为补充的标准：1）安全技术；2）一般用途的安全协议；3）特殊用途的安全协议，如银行、电子邮件等的应用。

与以上领域有关的标准主要来自以下四个方面：

1）有关信息技术的国际标准。这些标准是由以下组织建立的：国际标准化组织（International Organization for Standardization，ISO），国际电子技术协会（International Electrotechnical Commission，IEC），国际电信联合会（International Telecommunication Union，ITU，原称 CCITT）和电气与电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）；

2）银行工业标准。这些标准是由 ISO 面向国际社会应用开发的或者是由美国国家标准协会（American National Standards Institute，ANSI）面向美国国内的应用而开发的；

3）国家政府标准。这些标准是由各国政府制定的；

4）Internet 标准。这些标准是由 Internet 协会开发的。

1.3 网络安全策略

在介绍安全策略这个概念之前，我们先介绍安全区域这一概念。所谓一个安全区域通常是指属于某个组织的处理和通信资源之集。安全策略是指在某个安全区域内，用于所有与安全活动相关的一套规则。这些规则是由此安全区域中所设立的一个权威机构来建立的。

安全策略是一个很广泛的概念，这一术语以许多不同的方式用于各种文献和标准之中。OSI 安全体系结构中将安全策略定义为安全服务应达到的各种准则。一些近年来的分析表明，安全策略有以下几个不同的等级：

1）目标安全策略：是某个机构对所要保护的特定资源要达到的目的所进行的描述；

2）机构安全策略：是一套法律、规则和实际操作方法，用于规范某个机构如何来管理、保护和分配资源以达到安全策略的既定目标；

3）系统安全策略：所描述的是如何将某个特定的信息系统付诸工程实现，以支持此机构的安全策略要求。

在本书中，术语“安全策略”通常是指系统安全策略，但是我们必须明白它仅仅

是较广的安全策略概念的一个组成部分。

下面我们对影响网络系统和部件设计的安全策略的三个主要方面做一简要介绍。

1.3.1 授权

授权(authorization)是一个安全策略的基本组成部分。所谓授权是指赋予主体(用户、终端、程序等)对客体(数据、程序等)的支配权力,它等于规定了谁可以对什么做些什么。下面给出在机构安全策略等级意义上的一些授权描述的例子:

1) 文件 PKI-Project 只能由张三修改,并由张三、李四和 PKI-Project 项目组中的成员阅读;

2) 一个人事纪录只能由人事部门的职员进行新增和修改,并且只能由人事部门的职员、执行经理和该纪录所属于的那个人阅读;

3) 在一个有机密、秘密和绝密等密级的多级安全系统中,只有所持许可证级别等于或高于此密级的人员,才有权访问此密级中的信息。

这些安全策略的描述也对各类防护措施提出了要求。例如,采用人事防护措施来决定人们的许可证级别。在计算机和通信系统中,这种要求是通过一种被称作"访问控制策略"的系统安全策略反映出来。

1.3.2 访问控制策略

访问控制策略(access control policies)隶属于系统安全策略,它迫使在计算机系统和网络中自动地执行授权。以上有关授权描述的 1),2) 和 3) 分别对应于以下不同的访问控制策略:

1) 基于身份的策略:该策略允许或拒绝对明确区分的个体或团体进行访问;

2) 基于角色的策略:该策略是基于身份的策略的一种变形,它给每个个体分配角色,并基于这些角色来使用授权机制;

3) 多级策略:该策略是基于信息敏感性的等级以及工作人员许可证等级而制定的一般规则。

访问控制策略有时也被分成强制访问控制策略和自主访问控制策略两类。强制访问控制策略是由安全区域的权威机构强制实施的,任何用户都不能回避它。强制访问控制策略在军事上和其它政府机密环境最为常用,上述的策略 3) 就是一个例子。自主访问控制策略为一些特殊的用户提供了对资源(例如信息)的访问权,这些用户可以利用此权限控制对资源进行访问。上述的策略 1)和 2)就是自主访问控制策略的两个例子。在机密环境中,自主访问控制策略用于强制执行"须知(need to know)"最小特权策略(least privilege policy)或最小泄漏策略(least exposure policy),前者只授予主体为执行任务所必需的信息或处理能力;后者按原则向主

体提供机密信息，并且主体承担保护信息的责任。

1.3.3 责任

支撑所有安全策略的一个根本原则是责任(accountability)。受到安全策略制约的任何个体在执行任务时，都需要对它们的行为负责任。这与人事安全有着十分密切的关联。某些网络防护措施，包括认证工作人员的身份以及与这种身份相关的活动，都直接地支持这一原则。

1.4 安全威胁与防护措施

所谓安全威胁是指某个人、物、事件或概念对某一资源的可用性、机密性、完整性、真实性或可控性所造成的危害。某种攻击就是某种威胁的具体实现。

所谓防护措施是指保护资源免受威胁的一些物理控制、机制、策略和过程。脆弱性是指在防护措施中和在缺少防护措施时系统所具有的弱点。

所谓风险是关于某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。当某个脆弱的资源的价值高，以及成功攻击的概率高时，风险也就高；反之，当某个脆弱的资源的价值低，以及成功攻击的概率低时，风险也就低。风险分析能够提供定量的方法来确定防护措施的支出是否应予以保证。

安全威胁有时可以被分成故意的(如黑客渗透)和偶然的(如信息被发往错误的地址)两类。故意的威胁又可以进一步被分成被动的和主动的两类。被动威胁包括只对信息进行监听(如搭线窃听)，而不对其进行修改。主动威胁包括对信息进行故意的修改(如改动某次金融会话过程中货币的数量)。总的来说，被动攻击比主动攻击更容易以更少的花费付诸工程实现。

1.4.1 安全威胁

目前还没有统一的方法对各种威胁加以区别和进行分类，也难以搞清各种威胁之间的相互联系。不同威胁的存在及其重要性是随着环境的变化而变化的。然而，为了解释网络安全服务的作用，人们将现代计算机网络以及通信过程中常遇到的一些威胁进行了分类，并汇编成一张图表。

1. 基本威胁

要实现信息的机密性、完整性、可用性以及资源的合法使用这四个基本安全目标，必须采取措施对抗下面四个基本安全威胁：

1) 信息泄漏：信息被泄漏或透露给某个未授权的实体。这种威胁主要来自诸如窃听、搭线或其它更加错综复杂的信息探测攻击；