LOIS

信息安全国家重点实验室

信息安全丛书

Network Security Principle and Technology（第二版）

网络安全原理与技术

冯登国　徐静　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

（第二版）

冯登国　徐　静　编著

科学出版社

北京

内 容 简 介

本书主要介绍了一系列安全技术和用于保护计算机网络的安全协议、安全策略。主要内容包括：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 IPSec 协议，TLS 协议，IKE 协议，PGP 协议，3G 安全体系，无线局域网安全标准 IEEE 802.11i 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。

本书可作为高等院校计算机、通信、信息安全、密码学等专业的硕士生和本科生的教材，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，徐静编著．—2 版．—北京：科学出版社，2010

(信息安全国家重点实验室信息安全丛书)

ISBN 978-7-03-028839-4

Ⅰ.①网… Ⅱ.①冯… ②徐… Ⅲ.①计算机网络-安全技术-高等学校-教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 170579 号

责任编辑：鞠丽娜 / 责任校对：王万红

责任印制：吕春珉 / 封面设计：三函设计

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

*

2003 年 9 月第 一 版 开本：B5 (720×1000)

2010 年 10 月第 二 版 印张：22

2010 年 10 月第六次印刷 字数：440 000

印数：9 501—12 500

定价：38.00 元

(如有印装质量问题，我社负责调换〈新欣〉)

销售部电话 010-62134988 编辑部电话 010-62138978-8002

《信息安全国家重点实验室信息安全丛书》编委会

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，在人们驾驭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，人们还有许多科学技术问题需要认真的研究。人们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，已经拥有了全面的解决方案；人们也不能因为面对各种麻烦，就灰头土脸、自暴自弃，我们需要的是具有革命的乐观主义精神，坚韧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、技术上得到新的启发和收获,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

第二版前言

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。信息系统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,需要从多方面着手,采取各种措施,比如物理措施、管理措施和技术措施等,夸大任何一方面都是片面的、不正确的。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,系统介绍了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。

本书是在第一作者于 2003 年出版的《网络安全原理与技术》的基础上写作而成,除了对已保留的内容进行了修改、调整和补充外,还增加了部分新章节。为了便于读者自学,每章后面配备了大量习题。与此同时,也吸收了国内外现有相关著作中的许多精华,这些著作已在书后主要参考文献中列出。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多次,这些教学实践对本书的形成具有十分重要的意义。《网络安全原理与技术》(第一版)于 2003 年在科学出版社出版后,受到众多读者的厚爱,我们在第二版的修订过程中充分采纳了读者的修改意见和建议。

本书分为 10 章。第 1 章主要介绍一系列相关概念和定义,包括网络安全需求、网络安全策略、安全威胁与防护措施、网络安全服务、网络体系结构、安全服务的分层配置等。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 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 5 章主要介绍安全电子邮件,包括 PGP 标准、S/MIME 标准等。第 6 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、恶意代码分析与检测等。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 9 章主要介绍无线通信网络安全体系,包括 GSM 安全机制、3G 安全体系结构、无线局域网安全标准 IEEE 802.11i 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、安全风险评估等。

本书的出版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(项目编号为:2007CB311202)的资助,也得到了很多学者的鼓励和帮助,在此深表感意。

冯登国

2010 年 3 月

于北京

第一版前言

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

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、真实性和可控性。这六种性质的具体含义如下：

1）可用性(availability)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。

2）机密性(confidentiality)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。

3）完整性(integrity)是指保障被传输、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。

4）非否认性(non-repudiation)是指保证信息行为人不能事后否认曾经对信息进行的生成、签发、接受等行为。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。

5）真实性(authenticity)是指保证实体(如人、进程或系统)身份或信息、信息来源的真实性。

6）可控性(controllability)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。

信息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。信息网络安全(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，但本书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 网络安全威胁

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。

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。

目前还没有统一的方法来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环境的变化而变化的。

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

如搭线窃听或其他更加错综复杂的信息探测攻击；

2）完整性破坏：数据的完整性通过未授权的创建、修改、删除和重放等操作而受到损坏；

3）拒绝服务：对信息或其他资源的合法访问被无条件地阻止。这可能是由于以下攻击所致：攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的负载，从而导致系统的资源对合法用户也是不可使用的，也可能由于系统在物理上或逻辑上受到破坏而中断服务；

4）未授权访问：某一资源被某个未授权的人或以某一未授权的方式使用。这种威胁的例子有：侵入某个计算机系统的攻击者会利用此系统作为盗用电信服务的基点或者作为侵入其他系统的出发点。

2. 主要的可实现威胁

在安全威胁中，主要的可实现威胁是十分重要的，因为任何这类威胁的某一实现会直接导致任何基本威胁的某一实现。因而，这些威胁使基本威胁成为可能。主要的可实现威胁包括渗入威胁和植入威胁。

主要的渗入威胁有：

1）假冒：某个实体（人或系统）假装成另外一个不同的实体。这是渗入某个安全防线的最为通用的方法。某个未授权的实体提示某一防线的守卫者，使其相信它是一个合法的实体，此后便攫取了此合法用户的权利和特权。黑客大多采用假冒攻击；

2）旁路控制：为了获得未授权的权利和特权，某个攻击者会发掘系统的缺陷或安全上的脆弱之处。例如，攻击者通过各种手段发现原本应保密，但是却又暴露出来的一些系统“特征”。利用这些“特征”，攻击者可以绕过防线守卫者渗入系统内部；

3）授权侵犯：被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他未授权的目的，这也称作“内部威胁”。

主要的植入威胁有：

1）特洛伊木马（Torojan horse）：软件中含有一个觉察不出的或无害的程序段，当它被执行时，会破坏用户的安全性。例如，一个外表上具有合法目的的软件应用程序，如文本编辑，它还具有一个暗藏的目的，就是将用户的文件拷贝到一个隐藏的秘密文件中，这种应用程序称为特洛伊木马，此后，植入特洛伊木马的那个人可以阅读到该用户的文件；

2）陷门：在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理一个特定的用户识别号，以绕过通常的口令检查。

3. 潜在威胁

如果在某个给定环境对任何一种基本威胁或主要的可实现威胁进行分析,我们就能够发现某些特定的潜在威胁,而任意一种潜在威胁都可能导致一些更基本的威胁的发生。例如,如果考虑信息泄漏这样一种基本威胁,我们有可能找出以下几种潜在威胁(不考虑主要的可实现威胁):

1) 窃听;

2) 业务流分析;

3) 人员疏忽;

4) 媒体清理。

图 1.1 给出了一些典型的威胁以及它们之间的相互关系。注意,图中的路径可能回旋。例如,假冒威胁可以构成所有基本威胁的基础。然而,假冒威胁本身也有信息泄漏的潜在威胁(因为信息泄漏可能暴露某个口令,而用此口令能够实施假冒)。表 1.2 给出了各种威胁之间的区别。

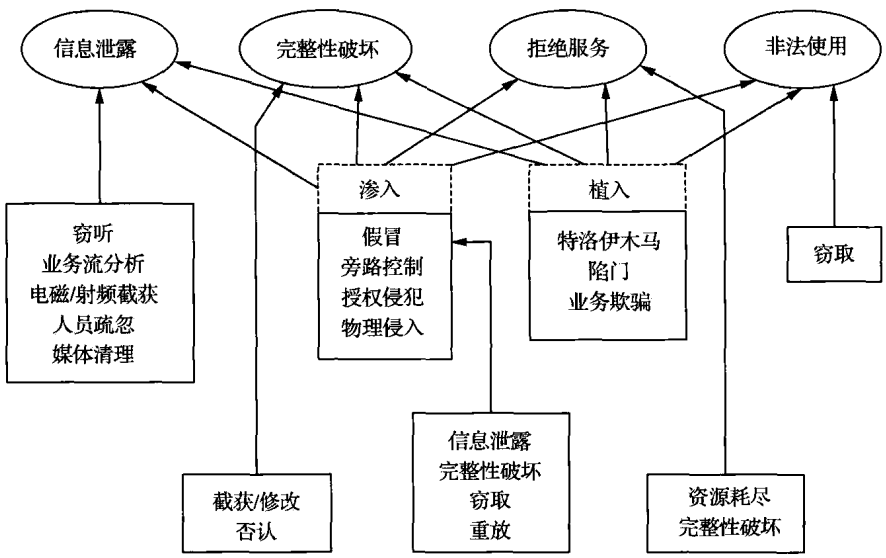

图 1.1 典型的威胁及其他们之间的相互关系

当然,在具体实施攻击时,攻击者往往将几种攻击结合起来使用,Internet 蠕虫(Internet worm)就是将旁路控制与假冒攻击结合起来的一种威胁。在这种威胁中,旁路控制涉及对 Berkeley UNIX 操作系统的已知缺陷的利用,而假冒则涉及对用户口令的破译。