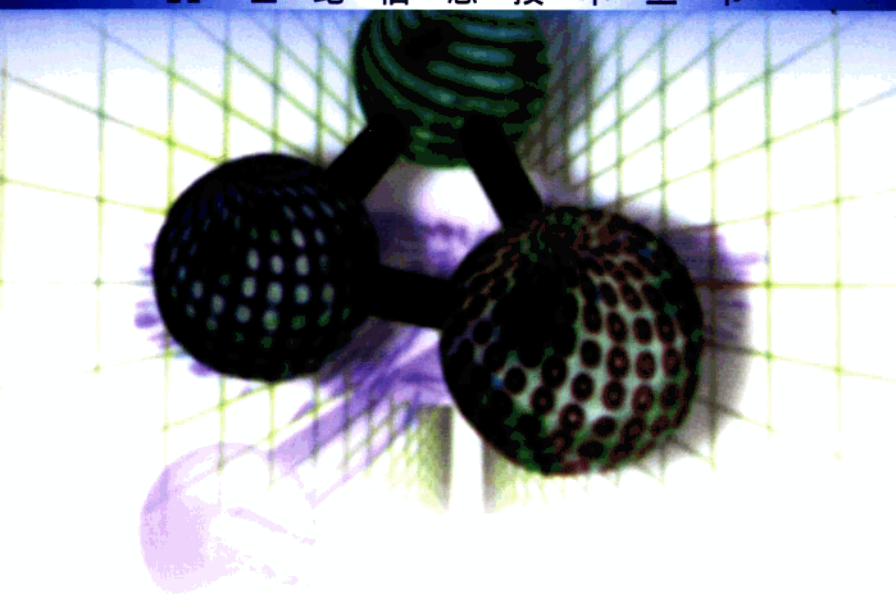
21 世纪信息技术丛书



网络信息安全与保密

WANGLUO XINXI ANQUAN YU BAOMI

（修订版）

杨义先 钮心忻 李名选 编著

北京邮电大学出版社
www.buptpress.com

前言

20世纪90年代是信息网络化大发展的时期。到2000年底，因特网已遍及世界180多个国家，连接100多万个各类网络，接入1亿多台主机，为5亿多用户提供多样化的网络与信息服务。当前（2001年），我国上网计算机数约892万台，其中专线上网计算机141万台，拨号上网计算机751万台。我国上网用户人数约2 250万人，其中专线上网的用户人数约为364万，拨号上网的用户人数约为1 543万，同时使用专线与拨号的用户人数为343万，除计算机外同时使用其他设备（移动终端、信息家电等）上网的用户人数为92万。cn下注册的域名总数为122 099个，WWW站点数（包括.cn，.com，.net，.org下的网站）约265 405个，我国国际线路的总容量为2 799 MB。

在因特网上，除了原来的电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、静态及视频等通信技术都在不断地发展与完善。在信息化社会中，网络信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络信息系统的依赖也日益增强。各种各样完备的网络信息系统，使得机密信息和财富高度集中于计算机中。另一方面，这些网络信息系统都依靠计算机网络接受和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个

主题。

随着网络的开放性、共享性及互联程度的扩大，特别是因特网的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，比如，电子商务、电子现金、数字货币、网络银行等，以及各种专用网的建设，比如金融网等，使得网络与信息系统的安全与保密问题显得越来越重要，成了关键之所在。

现在，国内外几乎每天都有各种各样的“黑客”故事：1994年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国CITYBANK银行发动了一连串攻击，通过电子转账方式，从CITYBANK银行在纽约的计算机主机里窃取1 100万美元。1996年8月17日，美国司法部的网络服务器遭到“黑客”入侵，并将“美国司法部”的主页改为“美国不公正部”，将司法部部长的照片换成了阿道夫·希特勒，将司法部徽章换成了纳粹党徽，并加上一幅色情女郎的图片作为所谓司法部部长的助手。1988年11月，美国康乃尔大学的学生Morris编制的名为“蠕虫”的计算机病毒通过因特网传播，致使网络中约7 000台计算机被传染，造成经济损失约1亿美元。1997年12月19日～1999年8月18日，黑客先后19次入侵某证券公司上海分公司电脑数据库，非法操作股票价格，累计挪用金额1290万元。1998年2月25日，黑客入侵中国公众多媒体通信网广州蓝天BBS系统并得到系统的最高权限，系统失控长达15小时（国内首例网上黑客案件）。1998年9月22日，黑客入侵扬州中国工商银行电脑系统，将72万元注入其户头，提出26万元（国内首例利用计算机盗窃银行巨款案件）。2000年3月8日，山西日报国际互联网站遭到黑客数次攻击，被迫关机（国内首例黑客攻击省级党报网站事件）。2000年6月11和12日，中国香港特区政府互联网服务指南主页遭到黑客入侵，服务被迫暂停。

事实上，我们听到的关于通过网络的入侵只是实际所发生的事例中非常微小的一部分。相当多的网络入侵或攻击并没有被发现。即使被发现了，由于这样或那样的原因，人们并不愿意公开它，以免公众作出强烈的惊慌失措的反应。绝大多数涉及数据安全的事件从来就没有被公开报道过。据统计，商业信息被窃取的事件以每月260%的速率在增加。然而，据专家估计，每公开报道一次网络入侵，就有近500例是不被公众所知晓的。

现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互联程度的扩大，这种安全机制对于网络环境来讲形同虚设。另外，目前网络上使用的协议，比如TCP/IP协议，在制订之初也没有把安全考虑在内，所以没有安全可言。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

面对如此严重危害网络信息系统的种种威胁和网络安全与保密的重要性，必须采取有力的措施来保证网络信息的安全与保密。网络的安全措施一般分为三类：逻辑上的、物理上的和政策上的。面对越来越严重的危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来有效防范计算机犯罪显得十分有限和困难，因此必须同时采用逻辑上的措施，即研究开发有效的网络安全技术。

即使是有非常完备的安全与保密政策法规，有非常先进的安全与保密技术，以及天衣无缝的物理安全机制，如果这些知识得不到普及，那么所有的努力都是白费。然而，目前国内几乎没有一本科普性的书籍对网络信息系统的安全与保密进行过全面系统的介绍。本书的主要目的之一便是想填补这一空白。

本书是北京邮电大学信息安全中心和北京市科委保密处的全体成员集体智慧的结晶。林晓东博士、邢育森博士、夏光升博

士、冯运波博士、李子臣博士、张磊学士、陈文杰学士等为本书提供了丰富的参考文献。特别感谢胡正名教授、钮心忻博士、孙伟博士、李中献博士、詹榜华博士。他们同心协力，率领北京邮电大学信息安全中心近 40 位研究人员在网络信息安全与保密研究方面的丰富成果是本书的营养源泉。感谢北京邮电大学出版社将此书选入《跨世纪信息技术丛书》。

由于作者水平有限，书中难免出现各种失误和不当，欢迎大家批评指正。

作　者

1999 年 9 月

修订版前言

非常感谢广大读者的厚爱。本书第一版自1999年出版以后，受到了全社会的热烈欢迎。许多读者发来了热情洋溢的书信、传真和电子邮件，许多专家提出了若干宝贵的意见和建议，许多管理部门已经正式采纳了书中提出的若干安全管理方案和措施，许多安全企业也对书中的若干新技术表现出了高度的兴趣并承让了部分科研成果。读者的肯定是我们的最大安慰，也是我们进一步改进工作的最大动力。应出版社的要求，再加上最近两年来国内外在网络信息安全与保密方面出现了许多新情况，所以我们决定对本书进行一些修订。与第一版相比，本次修订版主要在以下几个方面作了一些改进：

(1) AES（先进加密标准算法）已经于2000年被正式推出。所以，我们增了对AES的详细介绍，同时去掉了第一版中对其他AES备选算法的描述。

(2) 信息化的迅速发展使得以智能卡为代表的移动终端对密码算法的计算资源提出了更苛刻的要求。而新出现的椭圆曲线密码几乎是能够满足此苛刻要求的唯一密码，所以在本书的第二版中我们增加了对椭圆曲线密码的介绍。

(3) CA（认证中心）、PKI（公钥基础设施）和电子商务安全平台都是最近国内信息产业界非常热门的话题，所以本书修订版也对它们作了介绍。

(4) 信息伪装和数字水印技术是当前网络信息安全领域的最新课题，本书修订版尽力用通俗的语言对这些有代表性的高新技

术进行了适当介绍。

(5) 最近大量的各类入侵检测系统几乎是在一夜之间被国内外众多的网络安全公司推向了市场。因此，在本书修订版中，我们宏观地介绍了所有主要的入侵检测系统。

(6) 最近我国自己的“计算机信息系统安全保护等级划分准则（GB 17859－1999）”终于被公布并开始实施了。本书修订版也及时对此作出了反应。

(7) 本书的修订版在增加了一些新内容的同时，也根据具体情况精减了第一版中的若干内容。从而使得修订版的篇幅基本保持不变。

在本书的修订过程中曾志峰博士、夏光升博士、冯运波博士、李新博士、张振涛博士、徐国爱博士、李子臣博士、宋荣功博士、陈明奇博士、钟鸣博士、丘天豪硕士、李琛硕士、庄严硕士、韩炜硕士等为本书提供了丰富的参考文献。特别感谢胡正名教授、李中献博士、古利泽硕士、温巧燕教授、罗守山教授、牛少彰教授、卓新建博士，他们同心协力，率领北京邮电大学信息安全中心百余位研究人员在网络信息安全与保密研究方面的丰富成果是本书的营养源泉。本书也是国家重点基础研究发展规划项目、国家杰出青年基金项目、国家自然科学基金项目资助和高校骨干教师资助计划项目的成果。

作　者

2001 年 10 月于北京

目　录

1

网络信息安全与保密综论

2

密码技术简介

3

防火墙技术简介

4

虚拟专用网技术简介

5

病毒与反病毒技术简介

6

其他安全与保密技术简介

1 网络信息安全与保密综论

1.1 网络信息安全与保密的内涵是什么?

网络信息安全与保密是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。从技术角度看，网络信息安全与保密是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。网络信息安全与保密的重要性有目共睹。特别是随着全球信息基础设施和各国信息基础设施的逐渐形成，国与国之间变得“近在咫尺”。网络化、信息化已成为现代社会的一个重要特征。网络信息本身就是时间，就是财富，就是生命，就是生产力。实际上，网络的快速普及、客户端软件多媒体化、协同计算、资源共享和开放、远程管理化，以及电子商务、金融电子化等已成为网络时代必不可少的产物。

事物总是辨证统一的。科技进步在造福人类的同时，也带来了新的危害。从某种意义上讲，网络信息系统的广泛普及，就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。网络信息系统中的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。网络信息安全与保密便是这些众多新课题中最具代表性的例子。

根据《汉语大词典》(罗竹风主编)的解释，“安全”有两层含义：其一是指“平安，无危险”；其二是指“保护，保全”。

“保密”，则指“保守事物的秘密，不使泄漏”。仅仅根据词典的解释，“网络信息安全与保密”的含义是比较明确的。但是，在具体的工程应用和社会实践中，情况就相当复杂了。

1.1.1 网络信息安全与保密的技术特征

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的技术特征主要表现在系统的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性可以用公式描述为 $R = \mathrm{MTBF}/(\mathrm{MTBF} + \mathrm{MTTR})$，其中 R 表示可靠性，MTBF 表示平均故障间隔时间，MTTR 表示平均故障修复时间。因此，增大可靠性的有效思路是增大平均故障间隔时间或者减少平均故障修复时间。增加可靠性的具体措施包括：提高设备质量，严格质量管理，配备必要的冗余和备份，采用容错、纠错和自愈等措施，选择合理的拓扑结构和路由分配，强化灾害恢复机制，分散配置和负荷等。

网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。

生存性是在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏

是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认，访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制），业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞），路由选择控制（选择那些稳定可靠的子网，中继线

或链路等），审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。

3. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即，防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括：防侦收（使对手侦收不到有用的信息），防辐射（防止有用信息以各种途径辐射出去），信息加密（在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息），物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障，误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码），人为攻击，计算机病毒等。

保障网络信息完整性的主要方法有：

(1) 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段；

(2) 纠错编码方法：由此完成检错和纠错功能，最简单和常用的纠错编码方法是奇偶校验法；

(3) 密码校验和方法：它是抗窜改和传输失败的重要手段；

(4) 数字签名：保障信息的真实性；

(5) 公证：请求网络管理或中介机构证明信息的真实性。

5. 不可抵赖性

不可抵赖性也称作不可否认性。在网络信息系统的信息交互过程中，确信参与者的真实同一性。即，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送的信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等。

1.1.2 网络信息安全与保密的层次结构

网络信息安全与保密的结构层次主要包括：物理安全、安全控制和安全服务。

1. 物理安全

物理安全是指在物理介质层次上对存贮和传输的网络信息的安全保护。物理安全是网络信息安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。一方面，在各种软件和硬件系统中要充分考虑到系统所受的物理安全威胁和相应的防护措施；