普通高等学校“十一五”国家级规划教材

普通高校计算机专业精品教材系列

（第2版）

计算机网络安全导论

编　著／龚俭　吴桦　杨望

Introduction to Network Security

PUTONG GAOXIAO JISUANJI ZHUANYE JINGPIN JIAOCAI XILIE

東南大學出版社
Southeast University Press

普通高等学校“十一五”国家级规划教材
普通高校计算机专业精品教材系列

计算机网络安全导论

（第2版）

龚俭　吴桦　杨望　编著

东南大学出版社
·南京·

内容提要

本书从数据安全和网络安全两方面介绍了计算机网络安全的基本知识和常用的安全技术。在数据安全方面介绍了目前主流的数据加密技术和密钥管理技术，支持数据完整性保护的信息摘录技术和多种数字签名技术，支持身份认证的各种数据鉴别技术，包括无否认、匿名通信等支持数据安全所需的一些基本公平服务。在网络安全方面介绍了几种典型的访问控制技术和信任管理的基本内容，目前一些主要的网络威胁，网络安全监测技术以及包括防火墙技术在内的安全响应技术。本书还介绍了计算机网络安全管理方面的基本内容和互联网网络基础设施安全的一些重点发展领域的现状，包括 DNSSEC、IPsec 和 TLS。通过这些内容，可使读者掌握计算机网络（特别是计算机互联网络）安全的基本概念，了解设计和维护安全的网络及其应用系统的基本手段和常用方法。本书可用作计算机专业本科生或研究生的教材，也可作为相关领域技术人员的参考书。

图书在版编目(CIP)数据

计算机网络安全导论/龚俭，吴桦，杨望编著. —2 版.
南京：东南大学出版社，2007.9
ISBN 978-7-5641-0793-2

Ⅰ.计... Ⅱ.①龚…②吴…③杨… Ⅲ.计算机网络-安全技术-高等学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2007)第 082045 号

计算机网络安全导论(第 2 版)

编　　著：龚俭　吴桦　杨望
责任编辑：张　煦
责编邮址：amberzhang@stu.edu.cn
装帧设计：王　玥
出版发行：东南大学出版社
出 版 人：江　汉
社　　址：江苏省南京市四牌楼 2 号(210096)
经　　销：江苏省新华书店
制　　版：南京水晶山制版有限公司
印　　刷：南京玉河印刷厂
版　　次：2007 年 9 月第 2 版　2007 年 9 月第 1 次印刷
开　　本：787mm×1 092mm　1/16
ISBN　978－7－5641－0793－2/TP・131
印　　张：24.50
字　　数：627 千
印　　数：6 001—10 000 册
定　　价：38.00 元

编 者 的 话

期待了七年的新版终于要付锌，激动的心情难以抑制，有些话不得不说！

本书的第一作者龚俭，现任东南大学计算机科学与工程学院教授，博士生导师，中国教育和科研计算机网 CERNET 专家委员会委员；CERNET 华东（北）地区网络中心主任，江苏省计算机网络技术重点实验室主任；IEEE 会员，中国电子学会和中国计算机学会高级会员，江苏省互联网协会副理事长。龚教授参与了 CERNET 的创建与之后的运行管理，从 1993 年开始从事网络安全方面的科研工作，组建了国内最早的网络安全事件应急响应小组之一（NJCERT），多年来主持承担了多项网络安全方面的国家 863 计划课题、国家自然科学基金课题和教育部“211”工程公共服务体系建设课题，这些网络安全的研究与实践活动对本教材内容的编写与取舍可提供十分有益的经验。

龚教授治学严谨、为人谦和，成果丰硕、学养渊博，深受业界好评和学生的景仰。能有幸成为龚教授仅有的两本著作之一的责任编辑，审读堪称国内第一本全面介绍网络安全技术的专著型教材，对我来说责任和压力非同一般。幸好有龚教授的信任和支持，于 2000 年出版的《计算机网络安全导论》先后重印了三次，得到国内同行的高度评价，并于 2002 年获教育部评选的全国普通高校优秀教材二等奖、华东地区大学出版社第五届优秀教材学术专著二等奖，更于 2006 年被教育部列入普通高等教育“十一五”国家级规划教材。

随着近年来对网络安全研究与实践的发展，相关的方法和技术在不断进步，内容越来越丰富，如何对这些内容进行恰当的总结和取舍是对新的教科书的挑战。龚老师的新版教材使读者能够将学习重点放在对网络安全问题本质和对网络安全技术的主要原理的理解，有利于以后对不断涌现的网络安全的新问题和新技术的学习和把握。因此本教材不是一个技术手册型书籍，涵盖网络安全的所有方面，而是侧重在使读者能够具备设计和管理安全的网络与网络应用所需要的基本概念和技能，并为进一步学习网络安全领域的新方法和新技术打下基础。

自从计算机诞生之日起就与国家的重要领域如国防、金融等部门密切相关，安全问题由来已久。网络社会的大背景，呼唤安全、高可用性网络。基于龚俭教授近年科研与教学实践的最新成果面市，是读者的幸事，也是责任编辑的平生快事！祝愿龚老师和他的科研团队在未来路上奔跑地更快更稳！希望我和读者等待下一版的日子不会太漫长。

编者

2007 年 8 月 31 日

第二版前言

时至今日，计算机网络安全问题的重要性已经毋庸置疑。与2000年本书第一版出版时相比，网络安全技术又有了长足的发展，因此有必要对原来的内容进行修订。对于这一版而言，本书的总体思路没有变化。在内容的范围上，本书仍然覆盖信息安全和网络安全两个方面，以适应计算机科学与技术学科本科生和研究生学习的需要。在难度的控制上，本书仍然坚持以介绍概念和基本技术为主，突出了应用的需要，避开了许多原理性的介绍和一些基本数学理论内容，力争反映本领域的最新发展，主要是想满足构造安全的网络应用系统的需要。在内容的选择上，本书避免技术手册式的叙述风格，不罗列所有的相关技术，而是从教学的需要出发，选择介绍基本概念和典型技术。在结构上，这一版取消了原来的第六章，因为从教学的角度看，对PEM和PGP的细致介绍现在看来已经没有必要，其蕴含的技术内容可以在其他章节中反映。另外将原来的第八章分解成了三章，即现在的第七、八、九章。这样设计可以更好地反映网络安全领域这几年的发展变化，从传统的黑客攻防，到现在系统性的网络安全检测与响应体系。对于本书作者而言，对许多问题的认识和技术的理解现在更清楚了，因此是此次修订的重点。坦率地说，网络安全的教学体系结构仍然是一个值得摸索的问题，目前的风格仍然有罗列之嫌。

本书其他章节的内容也有了很多调整。第一章增加了对安全评估内容的介绍，并对与网络安全有关的法律问题进行重新表述。第二章增加了对AES算法和椭圆曲线算法的介绍，以反映加密算法领域的发展，删除了IDEA算法的介绍以控制篇幅。鉴于信息摘录算法方面的最新发展，第四章增加了SHA的新算法的介绍，并增加了一些新的特殊签名方法的介绍。第五章调整了公平服务方面的内容，增加了对匿名通信技术的介绍，以满足应用系统开发的需要。第六章（即原来的第七章）的内容变化较大，基本上属于重写，这章对传统的访问控制技术进行了较为完整的介绍，并增加了信任管理的内容，反映了这一方向的最新发展，更好

地适应基于互联网的应用系统安全的需要。

本书的这一版是在2000年8月第一版的基础上修订成书的，各章还增加了参考文献和习题，使之更加完整。第一版的作者中有两位已经离开了东南大学，因此这一版的作者有所变化。本书的第一、四、五、六章由龚俭编写，第二、三、十章由吴桦和龚俭编写，第七、八、九章由杨望、龚俭、宁卓、魏薇、梅海彬、邢苏霄等编写。网络安全方面的内容有很多出自我的学生们的工作，包括他(她)们撰写的学术论文和学位论文，包括前面提到的几位和已经毕业离校的几位。

由于我的日常教学与科研工作十分繁忙，这本书的修订工作一直拖了下来，念及起来十分愧对读者。尽管我在对东南大学计算机学院和软件学院的硕士生课程中，对本书第一版的内容不断进行着调整，以反映相关技术的发展，但是其他的读者无法分享这些内容。当然，拖延的后果也得自己承担。此番名曰修订，实则大部分内容是重写的。尽管框架没有多少变化，但积累下来的内容变化很多。感谢本书的责任编辑，东南大学出版社的张煦女士，如果不是她的坚持和鼓励，我可能还拖着。因此如果这一版的读者觉着本书还有所裨益，请感谢她！

信息安全和网络安全所包含的内容非常丰富，无法在有限的篇幅中将它们全部展现出来。一个人和一个团队的视野也是很有限的，作者才疏学浅，无法保证能最恰当地将这个领域中的精华都撷选介绍出来。因此书中的内容肯定有不当之处，甚至是疏漏和谬误，敬请广大读者批评指正。本书介绍的是一个非常重要而又变化很快的领域，我们仍将在适当的时间之后对书中的内容进行修订，以尽力保持其与相关技术发展的同步。

龚 俭

2007年5月于南京

目　录

第一章　计算机系统与网络的安全

1.1　计算机安全

1.1.1　基本概念

(1) 系统安全的相对性

计算机及其网络的安全是一个相对的概念，系统的安全措施可以用统一的术语来描述，但系统的安全程度总是相对于管理员的要求的，而这种要求是可以随系统的任务和系统的环境变化的。图 1－1 大致描述了系统安全各个概念之间的关系。

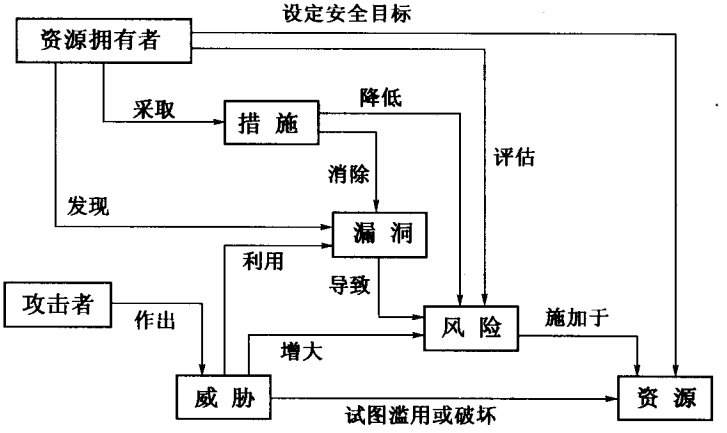

图 1－1　系统安全的相关概念

同一种资源(计算机系统和其中的数据)相对于不同的拥有者具有不同的价值，所以对其的安全要求往往不相同，这要求资源拥有者评估资源可能的风险，以便采取恰当的安全措施。系统的设计、开发、管理和使用的过程中往往存在安全漏洞，导致资源生存期的安全风险，因为攻击者可以利用这些漏洞对资源形成威胁，达到滥用或破坏这些资源的目的。因此资源拥有者必须有能力发现资源中安全漏洞的存在，以便采取对应措施来消除这些漏洞，从而降低资源使用过程中的安全风险。安全措施的运用是有成本的，并非越多越好，需要根据安全目标和系统风险来选择。这是一个动态的过程，系统环境、安全目标和系统的威胁都可以随时间而改变，安全措施也应随之而变化。无论对于系统还是其中的信息，上述的模型在原则上都是适用的。不同的安全目标要求不同的安全措施，具体的细节会在本书的后续章节中逐渐展开。

(2) 系统的脆弱性

自从计算机诞生以来，它一直与国家的重要领域，如国防、金融等部门有着密切的联系，因此计算机系统的安全问题由来已久，已经得到了大量的研究和较充分的认识。在国防安全、经济建设和社会生活的各个方面，计算机正在发挥着日益重要的作用，并越来越多地取代原来需

要手工进行的工作，人类对计算机的依赖越来越强烈。当计算机处理或存储仅供授权者访问的敏感数据时，人们需要保护这些数据不被泄露或破坏，从而需要研究计算机系统中可能导致安全问题的薄弱环节，即系统的脆弱性。在长期的应用过程中，人们发现到目前为止的通用计算机系统仍然是不完善的，还存在着多种安全隐患，使计算机系统有意或无意地受到损害。这些安全隐患包括

● 存储数据的密度极高，因此磁介质的损坏和丢失都会造成大量数据的损失。

● 数据的传送和使用过程中系统的电磁辐射会造成信息泄漏，传输信道可以被窃听。另外储存媒体的许多操作是逻辑的，使得被丢弃的信息往往还实际存在于系统中，若不进行物理清除，就存在被非法访问的可能，如许多系统可以作 Undelete 和内存 dump 操作。

● 电子信息可以很容易地被拷贝而不留下任何痕迹；另外由于系统的本地或网络访问控制可能存在漏洞，使数据被非法访问。

● 信息具有聚生性，当信息以分离的小块形式出现时，其价值可能不大，但当大量相关信息聚集在一起时，则可能会产生有意义的结果（如破译）；因此通过对系统的长期观察或零星数据的收集，有可能获取系统的信息。例如翻办公室的垃圾桶就是计算机黑客收集系统信息的常用手法。

● 由于计算机的使用要求一定的知识和技能，不仅非专业人员不容易发现或觉察到围绕计算机的渎职和犯罪行为，就是专业人员进行计算机犯罪的调查取证，也是一件很困难的工作，这方面的技术还远没有成熟。

（3）系统安全的主要威胁

① 无意产生的威胁

系统无意产生的威胁具有很大的偶然性，通常需要采用备份或双重操作等方式进行预防。常见的威胁包括：

● 由硬件故障引起的设备机能失常，例如由于使用寿命或环境因素而引起的硬盘故障往往导致整个系统或数据文件的丢失；

● 由操作失误而引起的人为错误，如按错开关，敲错命令，用错外设或存储介质等；

● 由于系统或应用软件中存在的缺陷而引起的软件故障，导致系统的异常操作甚至破坏；

● 由于电源或空调等环境故障而引起的设备故障。

② 自然灾害的威胁

如火灾、水灾、地震、化学污染、外力破坏（例如滑坡或地陷）等引起的设备损坏。这就要求机房的建设要满足一定的条件，尤其对于大型机系统。

③ 人为攻击

人为攻击对计算机系统产生的威胁分为主动和被动两种类型。被动类型的攻击主要表现为信息的窃取，例如情报机构出于政治、军事、经济等方面的原因，希望获取敌方的信息，采用电磁窃听方式；或者商业领域的竞争对象为竞争的需要而设法窃取对方的商业机密，窃取的方式也有多种。主动攻击主要表现为对数据的篡改，或对资源的非法使用。例如用户冒充他人的名义使用计算机资源；系统内部人员出于报复的目的而对系统进行恶意修改或设置逻辑炸弹；系统内部人员或外部人员利用计算机进行犯罪，经济原因为主，多针对金融系统。

计算机犯罪通常分为以计算机为工具（Computer Related Crime）和以计算机资产为对象

(Computer Aimed Crime)两类,具有隐蔽性强、智能程度高、黑数高和损失大的特点。所谓黑数是指虽已经实际存在,但未被列入官方统计的计算机犯罪总和中的那部分犯罪数字。造成计算机犯罪黑数值高的原因主要有两个:一是由于计算机犯罪往往涉及公民的隐私、公司企业的秘密乃至商业的信誉,受害者为维护自身的信誉并不乐意报案;二是由于目前相关法律体系不够完善以及相关技术手段的滞后而导致问题的难以界定或确认。信息技术及其应用发展非常之快,而相关的法律法规建设和防范技术手段的提高速度却与之很不适应,而且利用计算机网络的计算机犯罪往往跨越司法管辖边界,增加了执行的难度,从而使得对计算机犯罪难以发现,也难以适应计算机犯罪的侦查、起诉和审判等司法活动的需要。

我国的《刑法》中规定了三个与计算机犯罪相关的内容。

● 非法侵入计算机信息系统罪(《刑法》第285条)——违反国家规定,侵入国有事务、国防建设、尖端科学技术领域的计算机信息系统。

● 破坏计算机信息系统罪(《刑法》第286条)——故意对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的行为;故意对计算机信息系统中存储处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的行为;故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的行为。

● 盗窃罪(《刑法》第287条)——利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密。利用计算机实施盗窃的行为纳入盗窃罪定罪处罚的范围。如不法分子利用电子资金过户系统,例如定点销售系统(POSS)、自动存取款机(ATM)、自动化票据交换所(ACHS)、电子身份证系统等提供的便利,使用计算机技术通过网络修改电子资金账目,窃取电子资金。

1.1.2 计算机系统的安全目标

虽然具体计算机系统的安全目标随不同的资源拥有者而变化,但仍然存在一些描述计算机系统安全目标的公共原则。尽管系统管理员在确定自己的安全目标时可以有侧重点不同,这些原则对于各个计算机系统都不同程度地普遍适用。

(1) 安全性

系统的安全性首先表现为系统的真实性,即该系统提供可靠、一致、权威的数据或功能,这意味着系统的实际行为与预期行为是一致的,系统的前后行为是一致的,系统没有被破坏,也没有被劫持。

计算机系统的安全性分内部安全和外部安全两方面。系统的内部安全是系统的固有特性,在系统的软、硬件和外设中体现,包括系统中的安全设备,如加密部件、防止电磁辐射的屏蔽罩等;软件中设置的安全功能,如访问控制功能、口令鉴别功能等。

系统外部安全涉及系统的维护和使用,包括

① 物理安全 指对环境的保护,按照系统所担负的处理任务,可包括电源、空调、防尘、防止鼠害、防震、防污染以及安全警卫等方面的内容。

② 人事安全 指有关人员的可靠性,包括操作人员、维护人员、管理人员、勤杂人员、警卫人员等。

③ 过程安全 指操作过程的可靠性,包括有关人员的职责划分,操作规程制定和执行的监管等方面。

可信系统是指那些确认没有安全漏洞的计算机系统,这些系统的安全依赖于对它们的正

确操作。系统的可信程度是相对的，如果对系统的某些方面特别设置安全措施，负责系统安全，则对于这些方面来说系统是可信的。非可信的一般计算机系统称为良性系统，它们存在安全缺陷，可能会对系统造成无意的破坏。例如，如果系统没有自动的硬盘镜像备份功能，则突然发生的硬盘故障就会导致数据丢失，即使有定期的备份也不行。对于像处理信用卡交易的银行计算机系统来说，这样的良性系统就不能满足要求。主动出现不良行为的计算机系统称为恶性系统，例如扩散计算机病毒，或通过网络向其他系统发起攻击。在网络环境中，一个管理员自己控制的系统可以视为可信系统，因为管理员会有意识地不断消除系统中可能出现的安全漏洞，使之处于安全可靠的状态中。网络中的其他系统大多是良性系统，因为它们不受这个管理员的控制，他无法确信这些系统不存在安全漏洞，但是除非被作为跳板，这些系统不会主动向这个管理员的系统发起攻击或展现敌意行为。

为了方便讨论，将系统抽象为有关的计算机及其通信环境的总和，因此系统边界定义了需要安全保护的范围。由内部安全措施构成的安全边界称为安全防线。

系统的安全性的目的是为了防止对系统和其中的信息被误用（Abuse）和滥用（misuse）；前者指对系统和/或信息的构成的破坏，而后者指对系统和/或信息的非授权使用。

简略地说，系统安全性的维护可从用户的进入、使用和事后检查这三个方面来进行。

① 对用户进入系统的控制是通过标识与鉴别来实施的。标识是识别和区分用户的手段，而把用户与他的标识符相结合的过程则称为鉴别（或称为身份认证，本书对这两个术语不加区分地使用）。为了实现可靠的鉴别，鉴别信息必须通过一种系统与用户都不能伪造（或冒充）的途径来交换。

② 对用户使用系统的控制是通过访问控制来实施的，分为三方面的内容

- 授权：决定哪个主体有资格访问哪个客体；
- 确定访问权限：限定这个主体对指定客体的访问方式；
- 实施访问控制：具体实现访问控制。

本书的第六章将专门介绍各种访问控制技术。

③ 审计跟踪实现对用户使用系统情况的追踪了解。它要求在一个计算机系统中对使用了何种系统资源、使用时间、如何使用以及由哪个用户使用等信息提供一个完备的记录，以备非法事件发生后能够进行有效地追查。本书的第九章将讨论这方面的技术问题。

(2) 可用性

系统的可用性是指系统能够按照预期方式工作，完成预定任务，给出正确结果，因此系统的可用性强调的是系统的鲁棒性（Robustness）或可生存性（Survivability）。从安全的角度说，系统的可用性指的是系统在因遭受攻击等原因受到损害时继续完成所担负的工作的能力和从损害中恢复的能力，具体包括系统抵抗攻击的能力；系统检测攻击和评估损失的能力；系统控制损失，维持和及时恢复服务的能力；以及系统依据已获取的攻击信息增强自身抵抗力的能力。提高系统的可用性需要综合运用网络安全、系统容错、系统可依赖性和系统可靠性等方面的技术。

(3) 完整性

完整性体现了系统的可信度，分为软件完整性和数据完整性两方面，本书的第四章将专门介绍这方面的相关技术。

软件的完整性是指软件的标称功能与实际功能的一致性。系统硬件由于采用了标准的单