高等院校密码信息安全类专业系列教材

中国密码学会教育工作委员会推荐教材

网络安全

陈 兵　钱红燕　胡 杰　编著
王 箭　主 审

WANGLUO ANQUAN

国防工业出版社
National Defense Industry Press

高等院校密码信息安全[illegible]教材
中国密码学会教育工作委员会推荐教材

网络安全

陈 兵　钱红燕　胡 杰　编著
王 箭　主审

国防工业出版社
·北京·

内 容 简 介

本书围绕网络安全进行展开，首先介绍网络安全的基本概念，对网络安全问题进行综述；其次介绍常见的网络攻击技术，重点了解各种攻击的原理和方法；再次，针对各种网络安全威胁及攻击手段，提出多种安全防护技术，如通过防火墙进行内外网的隔离，通过身份认证技术进行识别，通过 VPN 实现跨越公网的数据传输，通过 IDS 将攻击扼杀在摇篮之中；最后，介绍各种安全管理的措施，以弥补技术上可能带来的不足。

本书适合作为高等院校信息安全专业的本科生和研究生的教材；也适合企业 IT 管理人员、信息技术人员使用。

图书在版编目(CIP)数据

网络安全 / 陈兵，钱红燕，胡杰编著. —北京：
国防工业出版社，2012.7
高等院校密码信息安全类专业系列教材
ISBN 978-7-118-08131-2

Ⅰ. ①网… Ⅱ. ①陈… ②钱… ③胡… 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(2012)第 124976 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号 邮政编码 100048）
三河市鑫马印刷厂
新华书店经售
*
开本 787×1092 1/16 印张 14 字数 311 千字
2012 年 7 月第 1 版第 1 次印刷 印数 1—3000 册 定价 30.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)88540777 发行邮购：(010)88540776
发行传真：(010)88540755 发行业务：(010)88540717

总　序

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。我国政府对网络与信息安全问题高度重视，国办印发的文件《关于网络信任体系建设的若干意见》明确指出了要特别重视网络安全的6方面内容；中办、国办印发的《国家2006年至2020年长期科学发展规划》中也突出了对各种网络安全问题的关注，将建设国家信息安全保障体系列为我国信息化发展的战略重点；国家“十一五”计划中也包含了提升国家信息安全保障服务能力的战略要求。西方发达国家纷纷制订了本国的网络与信息安全战略。比如，美国奥巴马政府正在采取措施加强美国网络战的备战能力，其中一项措施是创建网络战司令部，这表明美国的网络与信息安全战略已经由克林顿时代的“全面防御”、布什时代的“攻防结合”，转到奥巴马时代的“攻击为主，网络威慑”。

当前，制约我国网络与信息安全事业发展的瓶颈之一就是人才极度匮乏，为此，教育部从2001年起，陆续批准了包括北京邮电大学在内的近百所各类高校开设信息安全本科专业。但是，毕竟与其他经典的本科专业相比，信息安全本科专业的建设问题还面临许多挑战，需要全国同行共同努力，早日探索出一条办好信息安全专业的捷径。可喜的是，现在国内若干高校的教授团队都纷纷行动起来，各尽所能在信息安全本科专业建设方面取得了不少业绩。比如，灵创团队（http://www.cleader.net）就是众多热心于信息安全本科专业建设的创新团队，该团队中的“信息安全教学团队”被教育部和财政部批准为“2009年度国家级教学团队”；其完成的成果“信息安全专业规范研究与专业体系建设”获得了国家级教学成果奖二等奖；其带头人也被评为“国家级教学名师”并受到了胡锦涛等党和国家领导人的接见。希望国内能够有更多的类似教学团队投身于信息安全本科专业建设。

由于教材建设是信息安全专业建设的重点和难点之一，中国密码学会教育工作委员会自成立以来就一直致力于推进密码学与信息安全方面的教学和教材建设，比如，与国防工业出版社联合主办了“密码学与信息安全教学研讨会”等一系列研讨活动，并成立“普通高等教育本科密码信息安全类系列教材”编审委员会来组织策划相关系列教材。编审委员会在充分研究信息安全本科专业规范的基础上，经过细致研究，多次反复讨论，规划了与信息安全本科专业规范相配套的本系列教材。

本系列教材参照荣获国家级教学成果奖的信息安全最新专业规范，确定教材题目，组织教材书稿内容。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。由于本系列教材涉及的内容比较多，在教材内容选择时，一

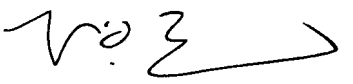
方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；编审委员会多次召开会议，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”。

为便于高校教师选用本套教材，我们将为高校教师提供完善的教学服务，免费为选用本套教材的教师提供所有教材的电子教案和部分教材的习题答案。同时我们还提供信息安全专业本科教学实验室建设方案与实验教学指导咨询和信息安全专业本科生实习、实训与技能认证咨询。

本系列教材尽管通过反复讨论修改，但限于作者水平和其他客观条件限制，难免存在不足和值得商榷之处，敬请批评指正。

教授　博士生导师　国家级教学名师
灾备技术国家工程实验室主任
网络与信息攻防教育部重点实验室主任
北京邮电大学信息安全中心主任



2009 年 9 月 30 日

高等院校密码信息安全类专业系列教材
编委会名单

前　言

在信息社会中，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。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。Internet 一方面给人类带来很多便利，另一方面也打开了潘多拉魔盒，使得新的犯罪行为相伴而来。网络信息系统中的各种犯罪活动已经严重地危害社会的发展和国家的安全。从技术角度看，网络信息安全与保密涉及计算机技术、通信技术、密码技术、应用数学、数论、信息论等多门学科。因此，网络安全的内涵和外延都极其丰富，试图在一本教材中将所有的安全技术都阐述出来是不明智的。

本书将重点聚焦在四个问题，即“为什么要研究网络安全问题?”、“网络威胁有哪些?”、“如何从技术上进行安全防范?”以及“如何进行安全管理?”。

本书共分为 8 章，各章内容安排如下：

第 1 章主要介绍网络安全的基础知识，列举目前常见的计算机网络安全的威胁，以 ISO/OSI 和 TCP/IP 安全体系结构为模型，分析了安全服务和实现机制。第 2 章介绍一些国内外著名的黑客攻击案例、攻击手法和攻击过程，并结合 TCP/IP 协议分析其各层所存在的安全问题。第 3 章～第 7 章详细介绍了网络安全的各种防范技术，通过身份认证决定访问者是否有进入系统的钥匙；访问者进门后通过访问控制来判断其具有哪些访问权限，防火墙如何进行内外网的隔离工作；通过 VPN 实现跨越公网的安全传输；通过 IDS 将攻击扼杀在摇篮之中。第 8 章介绍安全管理方案。

本书在编写过程中参考了大量的国内外优秀的文献，大部分已经列在参考文献中，部分参考文献或因出处不详、或因作者疏忽等原因没有进行标注，敬请原作者谅解。在此，谨向各位为中国的网络安全发展做出贡献的理论研究者和实践探索者致以深深的敬意。没有你们坚持不懈的努力，中国的网络安全肯定无法取得今天令人鼓舞的进展，当然，本书的成稿也是不太可能的。

在本书的编写过程中，我们得到了众多师长、同事和学生的关心、支持与帮助，顾其威教授提出了很多有价值的建议，王立松、冯爱民、杜庆伟、燕雪峰、蔡伟星、王文娟等提供了大量的资料。在此一并向诸位表示最诚挚的谢意。

本书适合于高等院校相关专业师生以及其他对网络安全感兴趣的读者使用。

由于网络安全技术涉及的范围广、内容多、发展更新快，加之编委学识、资料和编写时间所限，书中肯定有不少疏漏和不妥之处，敬请广大读者和专家批评指正。

编者

2012 年 4 月

目　录

第1章　网络安全概念

随着 Internet 的飞速发展，各种安全问题接踵而至：黑客入侵、病毒肆虐、网络瘫痪、主页篡改，各种案例不胜枚举，因此，如何保证网络系统的安全已成为迫在眉睫的问题。

本章主要内容：

★ 网络安全问题的提出

★ 计算机网络安全的威胁

★ 计算机网络安全的定义

★ 网络安全模型结构

1.1　网络安全问题的提出

在信息社会中，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。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，随着网络的快速普及，协同计算、资源共享、开放、远程管理、电子商务、金融电子化等已成为网络时代必然的产物。从技术角度看，网络信息安全与保密涉及计算机技术、通信技术、密码技术、应用数学、数论、信息论等多门学科。

事物总是辨证统一的，网络信息系统的广泛普及，一方面给人类带来很多便利，另一方面也打开了潘多拉魔盒，使得新的犯罪行为相伴而来。网络信息系统中的各种犯罪活动已经严重地危害社会的发展和国家的安全。

为什么网络安全问题如此严重呢？这是因为计算机网络是各种应用系统的数据传输平台。上层的各种应用系统，如电子商务应用、电子政务应用、各种办公系统等，所有的信息都在这个平台上进行传送，应用系统和各种平台的层次关系可以用图 1.1 来表示。

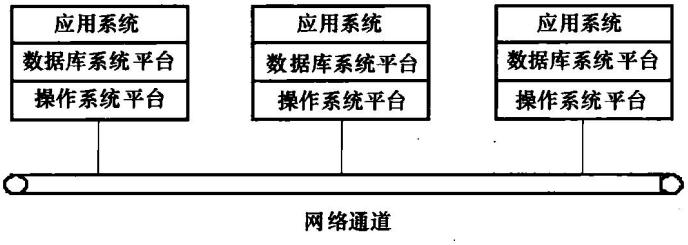


图 1.1　应用系统与网络平台的关系图

我们可以将网络平台看作邮政系统，进行各种信件分拣投递工作的分拣机和邮递员看作网络中的各种节点（如路由器等），而我们自己就是这个系统的上层应用程序。一旦

我们到邮局寄出一封信件，邮局将根据地址进行信件的分拣，并运输到最终客户所在的邮局，通过邮递员送到最终客户。这里，我们寄出一封邮件，相当于发出一个网络分组，信封上的邮寄地址可以看作网络分组中的目的 IP 地址，落款可以看作网络分组中的源 IP 地址。在正常情况下，邮局体系将正确无误地进行传送，并根据信封地址提交给最终客户。但是，如果某个邮递员比较粗心马虎，在投递过程中遗失了信件，那么，采用网络术语而言，就是网络分组在传送过程中丢失了；更有甚者，极个别邮递员对信件内容感兴趣，他可能将信件拆开看一看，这种情况可以称为“被动攻击”。而且还存在这种可能性，这个邮递员是一个写作高手，对语法修辞有着深入的研究，他觉得信件内容有些语法错误，于是，他抑制不住冲动，提笔对信件内容进行了加工修改。这种情况就严重多了，不管他的初衷如何，是否善意，从安全角度而言，这种行为属于“主动攻击”。不管是“被动攻击”还是“主动攻击”，这两种行为对信息进行了窃听、篡改，对网络与信息安全造成威胁。

归纳而言，网络安全的具体内容包括：

（1）运行系统的安全。主要保证信息处理和传输系统的安全。侧重于保证系统正常地运行，避免因为系统崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失。运行系统的安全内容主要包括计算机系统机房环境的保护，计算机网络拓扑结构设计的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全等。运行系统的安全本质上是保护系统的合法操作和正常运行。

（2）网络上系统信息的安全。包括用户身份认证（一般采用口令鉴别），用户存取信息的权限控制，数据库记录访问权限，安全审计（一般系统都有日志记载），计算机病毒防治，数据加密等内容。

（3）信息传播后果的安全。信息传播后果的安全侧重于防止和控制非法的、有害的信息传播，避免信息失控，本质上主要是维护社会的道德、法则和国家利益。

1.2 计算机网络安全的威胁

各种对计算机网络安全形成的威胁可以归结为以下几条：

1. 来自内部和外部的各种攻击

计算机网络极易受到来自外部或内部的各种攻击。攻击的手段包括被动攻击和主动攻击。所谓被动攻击是指侦听、截获、窃取、破译、业务流量分析、电磁信息提取等行为，被动攻击虽然不会对信息进行修改，但会造成信息内容的泄密。而主动攻击是指对网络传输的信息进行修改、伪造、破坏、冒充等操作，或者在网络上进行病毒扩散，这种攻击将对应用系统的安全运行造成极大的危害。典型的例子如冒充领导审批、签发文件等。

从来源看，攻击有来自外部和内部两种。一些黑客试图穿过边界防火墙进入到内部网络中，当然由于有防火墙，这种来自外部的攻击行为大部分会被阻断，只有少数真正的高手才能穿越防火墙进入到内部系统中。而绝大部分攻击（包括被动攻击和主动攻击）主要来自内部，且大多采用被动攻击方式，即进行网络窃听，了解一些自己感兴趣而又没有权限查看的内容，这也许是人天生的好奇心导致的。更有少数人为达到某种目的，对内部各种服务器进行主动攻击，由于他们身处防火墙内部，而传统的边界防火墙是无法防范内部的各种攻击行为的，因此，内部的主动攻击已经成为网络面临的最大威胁之一。

2. 软件漏洞

主要体现在操作系统的漏洞和各种应用软件的漏洞。这些漏洞可能是软件编制人员为了调试方便预留的,但在软件正式发行时忘记删除了,从而为一些软件高手或者不速之客留下了入侵的后门。当然,也有的漏洞可能是程序员故意预留的,这种情况尤其值得重视。因此,在应用系统最终验收时,尤其要重视安全性方面的测试,防止出现后门。

3. 关键技术失控

目前常用的操作系统、数据库平台以及应用软件绝大部分采用的是国外产品,许多关键技术并没有被我国掌握,更为糟糕的是这些被广泛使用的操作系统大多有"后门",尽管正常情况下,这些后门不会被使用。但一旦出现诸如国家之间的信息战等紧急情况时,黑客攻击可能上升为一种国家间的战争行为,为了各自国家的利益,这些所使用的进口操作系统的厂商可能会被本国政府强行要求公开后门,甚至要求公开源码,到那时,后果将不堪设想。

4. 安全管理水平落后

网上新业务的开展、传统业务的开放式改造、不断变化的网络应用、网上攻击风险的日益增大,都对网络系统的安全管理提出了更高的要求。俗话说"三分技术,七分管理",而恰恰是由于管理跟不上,制度不完善,加上采用的安全技术和产品是零散的,导致许多网络即使在采用先进技术、经过安全配置,甚至在已经使用了一部分专门的安全产品之后,管理人员和技术人员依旧对自己网络的安全性没有很好地把握。如何有效地提高网络的安全性,保障网上业务顺利安全地进行,将网络的安全隐患降低到一个可以接受的程度,让安全管理人员做到心中有数,是网络安全亟待解决的重要问题。

1.3 计算机网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄漏。即通过各种计算机、网络、密码技术和信息安全技术,保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性,并对信息的传播及内容有控制能力。

在正常情况下,信息在网络中安全地进行传输,如图 1.2 所示,源节点发出的信息通过网络信道传输到目标节点。

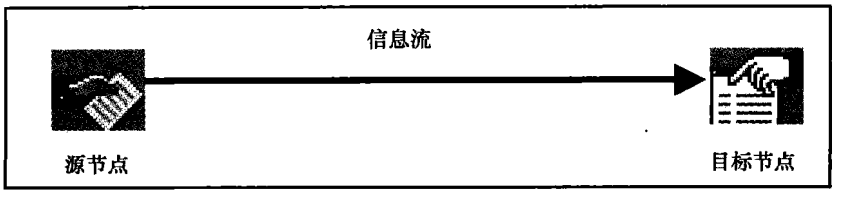


图 1.2 信息在网络中的正常传输

考虑到种种不安全的因素,信息在网络上传递过程中可能会遇到被中断、截取、篡改和伪造等情况,如图 1.3 所示。

因此,考虑到以上这些情况,计算机网络安全的特征主要表现在系统的保密性、真实

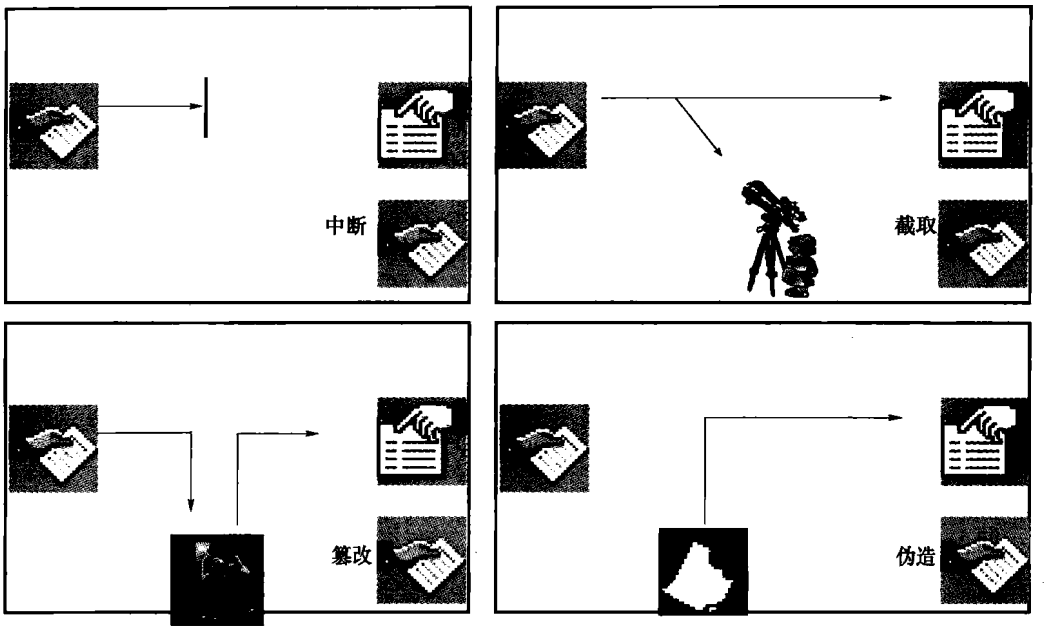


图 1.3　信息在传递过程中被中断、截取、篡改、伪造

性、完整性、可靠性、可用性、不可否认性、可控性等方面，网络上传输的信息被中断、截取、修改或者伪造都会影响信息的可用性、机密性、完整性和真实性，如图 1.4 所示。

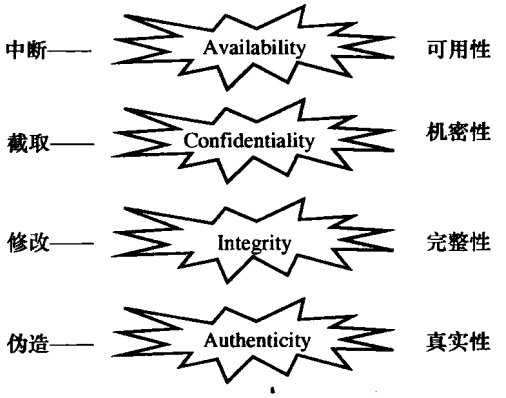


图 1.4　各种行为对网络上传输信息的影响

1. 保密性

保密性是指网络信息不被泄漏给非授权的用户、实体或过程，即信息只为授权用户使用。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属性。

常用的保密技术包括：

（1）物理保密。利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄漏。

（2）防窃听。使对手侦收不到有用的信息。

（3）防辐射。防止有用信息以各种途径辐射出去。

(4) 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获取有效信息。

2. 真实性

真实性是指用户的身份是真实的。例如在一个大型的电子商务网络内,用户张三声明他是张三,但是网络能够相信他吗?会不会是李四冒充张三呢?因此,如何能对通信实体身份的真实性进行鉴别?如何保证用户的身份不会被别人冒充?这是真实性所需要解决的问题。

3. 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添加、删除、修改、伪造、乱序、重放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、正确存储和正确传输。

完整性与保密性不同,保密性要求信息不被泄漏给未授权的人,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以及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) 良好的协议。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) 密码校验和方法。它是抗篡改和传输失败的重要手段。

(3) 数字签名。保障信息的真实性,保证信息的不可否认性。

(4) 公证。请求网络管理或中介机构证明信息来源者身份的真实性。

4. 可靠性

可靠性是指系统能够在规定的条件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础要求之一,是所有网络信息系统的建设和运行的基本目标。

衡量网络信息系统的可靠性主要有三方面: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。例如,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)造成的大面积网络瘫痪事件。

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。例如,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