21世纪 高等院校计算机系列教材

# 网络与信息安全教程

吴煜煌 汪 军 阚君满 等编著

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校计算机系列教材

# 网络与信息安全教程

吴煜煌　汪　军　阚君满　等编著

中国水利水电出版社

## 内 容 提 要

本书介绍网络与信息安全的基本理论和关键技术，全书共 11 章，主要内容包括：网络安全、密码技术、数字签名与身份认证技术、防火墙技术、入侵检测技术、计算机病毒的防治、黑客常用的攻击技术、网络站点的安全、操作系统的安全、数据库系统的安全和安全电子交易。

通过对本书的学习，读者能够对计算机网络与信息安全知识有一个比较系统的了解，掌握计算机网络特别是计算机互联网安全的基本概念，了解网络与信息安全的各种关键技术及其系统安全的基本手段和常用方法。

本书适合高等学校电子、计算机网络和信息安全专业或相近专业的学生使用，也可作为从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员的参考书。

**本书配有用 PowerPoint 制作的电子教案，可以任意修改，读者可从中国水利水电出版社网站免费下载，网址为：*http//www.waterpub.com.cn/softdown/*。**

**图书在版编目（CIP）数据**

网络与信息安全教程/吴煜煌等编著. —北京：中国水利水电出版社，2006

21 世纪高等院校计算机系列教材

ISBN 7-5084-4051-X

Ⅰ. 网… Ⅱ. 吴… 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（2006）第 106285 号

| | |
|---|---|
| 书　　名 | 网络与信息安全教程 |
| 作　　者 | 吴煜煌　汪　军　阚君满　等编著 |
| 出版发行 | 中国水利水电出版社（北京市三里河路 6 号　100044）<br>网址：www.waterpub.com.cn<br>E-mail：mchannel@263.net（万水）<br>sales@waterpub.com.cn<br>电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水） |
| 经　　售 | 全国各地新华书店和相关出版物销售网点 |
| 排　　版 | 北京万水电子信息有限公司 |
| 印　　刷 | 北京蓝空印刷厂 |
| 规　　格 | 787mm×1092mm　16 开本　18 印张　432 千字 |
| 版　　次 | 2006 年 10 月第 1 版　2006 年 10 月第 1 次印刷 |
| 印　　数 | 0001—4000 册 |
| 定　　价 | 26.00 元 |

# 前　言

随着计算机网络技术的迅猛发展和网络信息系统的深入应用，信息网络的国际化和社会化使人类社会的生活方式发生了重大变化。网络化、数字化应用业务大量涌现，网上购物、网上炒股、视频会议、远程教育、电子政务、网络银行、数字图书馆等走进了我们的生活。而网络与信息系统的开放性和潜藏的商业、经济、军事利益给网络黑客、计算机犯罪人员、国外敌对势力和恐怖分子等创造了大量可乘之机，使网络与信息安全问题受到了前所未有的关注和重视。

本书重点讲述网络与信息安全技术问题，涵盖了网络安全的基本概念、密码技术、数字签名与身份认证技术、防火墙技术、入侵检测技术、病毒防治与黑客攻击技术、网站安全技术、数据库安全技术等方面的知识，力求从简洁、全面、前沿、深刻的视角分析网络与信息应用领域中存在的相关安全的问题、技术和方法。本书共分 11 章，第 1 章介绍网络安全的基本概念，概述了网络安全的目标、缺陷、发展历史和现状。第 2 章讲解密码技术的相关概念、网络加密方式、密码算法、密钥的管理和分发以及密码技术的应用。第 3 章讲述数字签名技术、CA 身份认证技术、数字证书的标准和使用。第 4 章介绍防火墙的概念和功能、防火墙管理的 TCP/IP 基础、防火墙的体系结构、防火墙的主要技术。第 5 章讲述入侵检测系统的基本概念、分类、分析方式、设置部署以及入侵检测系统的优缺点。第 6 章讲解计算机病毒的产生、种类和具体特征，计算机病毒的预防、检测和清除。第 7 章讲述黑客攻击的一些常用技术，包括端口扫描、特洛伊木马、拒绝服务攻击等。第 8 章介绍网络站点的安全基本知识，包括一些针对 Web、E-mail、DNS 站点的攻击手段及预防措施。第 9 章讲述操作系统的安全机制以及几种常见网络操作系统的安全。第 10 章讲述数据库安全系统特性、数据库安全的威胁、数据库的数据保护。第 11 章讲解电子交易的基本流程、SET 的基本原理与安全需求、SET 中的支付处理。

本书适合高等学校电子、计算机网络和信息安全专业或相近专业的学生使用，也可作为从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员的参考书。

本书由吴煜煌负责全书的统稿定稿工作，主要由吴煜煌、汪军、阚君满编写，参加本书编写的还有李禹生、刘兵、欧阳峥峥、陈学文、高艳霞、蒋丽华、向云柱、李鸣、严华、李承犁、镇涛等。丰洪才教授审阅了全书，并提出了宝贵意见。另外，本书在编写过程中，得到了网络中心和计算机系领导的关系和支持，在此一并表示衷心的感谢。

由于网络与信息安全技术的发展非常快，本书的选材还有一些不尽如人意的地方，加上作者水平所限，书中难免存在不足之处，敬请读者批评指正。作者的电子邮件地址为：wyh@whpu.edu.cn。

编　者

2006 年 7 月

# 目　　录

# 第 1 章　网络安全

## 本章学习目标

本章主要讲解网络安全的基本知识、网络面临的安全威胁、网络安全防护体系、网络安全的发展等内容。通过对本章的学习，读者应该掌握以下主要内容：

- 网络安全的含义、目标
- 网络安全的研究内容
- 网络存在的安全威胁及存在安全威胁的原因
- 网络安全防护体系
- 网络安全的发展、现状及趋势

## 1.1　网络安全的基本知识

### 1.1.1　网络安全的基本概念

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此，可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的机密性、完整性和可用性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。从广义上来说，凡是涉及到网络上信息的机密性、完整性、可用性、真实性、抗否认性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全从其本质上来讲就是网络上的信息安全。

1. 信息安全

信息安全已经历了漫长的发展过程。从某种意义上说，从人类有信息交流开始就涉及信息的安全问题。从古代烽火传信到今天的通信网，只要存在信息交流，就可能存在信息欺骗。信息安全的概念也是与时俱进的，过去是通信保密（COMSEC），昨天是信息安全（INFOSEC），而今天以至于今后是信息保障（IA-Information Assurance）。

（1）通信保密。信息安全的初级阶段，人们似乎更关注信息通信的机密性。通常采用一些简单的替代或置换来保护信息。这些变换是密码学的雏形。这一阶段发展了很多密码算法，但基本的方法都是将字母编号后进行平移、旋转、置换、扩展等变换。此外，还发展了密码分析和破译方法。

（2）信息安全。随着数学、计算机和通信技术的发展，信息的处理能力和传输能力大大提高，靠传统的密码变换已不能满足信息化的要求。因此，信息安全的发展速度也在加速，出现了现代密码理论、计算机安全和通信安全的新理论和新技术。这一阶段的信息安全包括在信

息系统的物理层、运行层，以及对信息自身的保护（数据层）及攻击（内容层）的层面上，所反映出的对信息自身与信息系统在机密性、可用性与真实性方面的保护与攻击等内容。

（3）信息保障。目前，国际研究前沿已将信息安全上升到信息保障的高度，提出了计算环境安全、通信网安全、边界安全及安全支撑环境和条件的概念，并开始研究信息网络的生存性等课题。美国国家安全局（NSA）在 IATFV3.1 中提出了深度防御（Defense-in-Deepth）的概念，把信息安全上升到信息保障的高度，并提出了人（People）、技术（Technology）、操作（Operation）三方面并举的核心策略，基于这个核心，IATF 定义了各种环境下的安全需求和技术方案的框架，对现有的信息安全技术提出了许多新的挑战。

总之，信息安全还没有形成完整的学科概念，但其发展速度正在加快，信息安全研究人员正在增加，信息安全作为独立产业的形态开始显现，主管部门也在加大管理力度，并加紧制定信息安全法律法规。信息安全学科正应时代需要发展和完善。

2. 网络安全

过去的信息安全主要是通信保密，通信发展到今天，在以分布系统网络化的前提下，互联网的触角延伸到人们生产、生活的每个角落，由此引出了网络安全这一新课题。

网络安全在不同的环境和应用中会得到不同的解释。对于用户（个人、企业等）而言，网络安全意味着涉及个人隐私和商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的隐私和利益造成侵犯和损害；对于网络运行和管理者而言，网络安全意味着对本地网络信息的访问、读写等操作进行保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击；对安全保密部门而言，网络安全更侧重于对非法的、有害的或涉密的信息进行过滤和防堵，避免其通过网络泄漏，同时避免由于这类信息的泄密而对社会产生危害，对国家造成重大损失。

一般可以认为网络安全包括物理安全、运行安全和数据安全三个层次，它们涵盖的范围如图 1-1 所示。

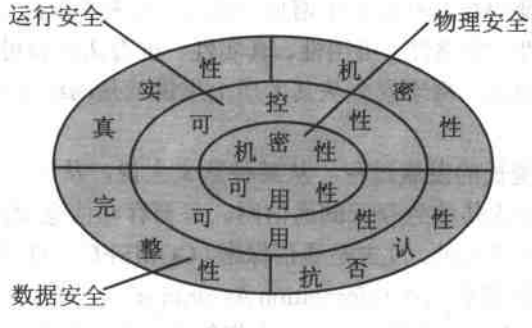


图 1-1 网络安全涵盖的范围

网络安全与其所保护的信息对象相关，本质是在信息的安全期内保证其在网络上流动时或静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密联系的。

网络安全的含义是指通过各种计算机、网络、密码技术和信息安全技术、网络控制技术，保护网络中传输、交换、处理和存储的信息的机密性、完整性、可用性、真实性、抗否认性和

可控性。

3. 网络安全观

网络安全的特征决定了网络安全本身是一个不断变化、快速更新的领域，也意味着人们对于网络安全领域的投资是长期的行为。但现在的问题是，到底该如何利用技术来保护计算机和网络不受安全的威胁。许多用户在应用计算机接入网络时，往往存在侥幸心理，不会将安全作为首要问题考虑，希望其安全措施能永保安全。

首先，网络安全是网络动态发展的问题。从发展趋势来看，信息网络的安全日益显示出了其重要性。不同国家、地区之间的政治、军事、文化等冲突也动辄引发一轮又一轮的网络攻击战争，如中美、中日、大陆与台湾之间都曾多次爆发大规模的有组织的网络攻击。这些有组织、有目的的网络攻击行为一方面提醒了网络建设者要始终把安全问题放在首位，另一方面也将大大促进网络攻击技术的发展。

其次，网络安全实施是一个系统工程。安全问题涉及身份鉴别、访问控制、数据机密、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务，涉及 ISO/OSI 所有的七个协议层次（网络层、链路层、网络层、传输层、会话层、表示层和应用层）覆盖了信息网络中物理环境、通信平台、网络平台、主机平台和应用平台等多个系统单元。因此，这是一个立体的、多方位、多层次的系统问题，在规划、设计、实施信息网络的安全系统时也必须用系统工程的方法论来考虑。

最后，网络安全实施是一个社会工程。在信息网络中，用户接口是至关重要的。在采取了各种复杂的安全技术之后，如果系统的最终用户没有足够的安全意识和安全常识，不能正确应用各项安全措施，那么其后果要么是安全系统不能工作，影响信息网络的正常运转，要么是安全系统演出空城计，不能起实际的作用（如在一个安全系统中使用简单的用户密码）。因此，在安全系统建设工程中，必须充分重视用户的安全，加强对用户安全意识的培训，加强安全常识的教育，加强安全系统的使用培训。

所以说，网络安全是一个动态发展的系统工程和社会工程，需要长期、持久的巨大财力、物力、人力的投入，需要从组织、管理等方面采取强有力的措施，才能确保网络在信息的大洋中永远坚固、安全、可靠。

### 1.1.2　网络安全目标

在 ISO7498-2 开放系统安全架构中提出，要解决网络安全问题，主要是在四方面提供服务，而 IATF 则近一步演化为安全的六性。

1. 机密性

防止信息被非法获得，即防止信息泄漏给非授权的用户、实体或过程，或供其利用。机密性可以保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

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）。

2. 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。

完整性与机密性不同，机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：

- 协议。通过各种安全协议可以有效地检测出被复制的信息、被删除的字段和被修改的字段。
- 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。
- 密码校验和方法。它是抗撰改和传输失败的重要手段。
- 数字签名。保障信息的真实性。
- 公证。请求网络管理或中介机构证明信息的真实性。

3. 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。可用性是信息资源服务功能和性能可靠性的度量，涉及的是网络信息系统面向用户的安全性能，以及到物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的总体要求。可用性可以保障信息服务能正常提供而不会被攻击，确保网络可被授权实体访问并按需求使用，即当需要时能否存取所需的信息。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）。

4. 抗否认性

防止信息的使用被否认，即保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，是针对通信各方信息真实同一性的安全要求。一般通过数字签名来提供抗否认服务。抗否认性也称作不可抵赖性或不可否认性，在网络信息系统的信息交互过程中，利用信息源证据可以防止发信方不真实地否认已发送信息，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。

5. 可控性

可控性是指对信息的传播及内容具有控制能力。

可控性的概念源于控制理论，是 R.E.Kalman（卡尔曼）首先提出的，是实现各种控制和状态估计的基础，但它只限定讨论控制作用（即输入量）对输出量的控制，这两个量之间的关系惟一地由系统传递函数所确定，只要传递函数不为零，系统的输出量就是可控的。

在状态空间描述中，除了输入量和输出量外，还引入了描述系统内部运动的状态向量。把状态向量看做系统的被控制量，就产生了状态能否被输入控制的问题：能不能控制一个处于某个给定状态下的系统，即加上控制输入能不能使它在有限时间间隔内达到它的零状态？如果能做到，则称该给定状态为可控态。

对于网络系统来说，可以根据需要或者实际情况为网络划分不同的安全等级，可控则是指能否通过某些手段，即控制输入，来达到某个安全等级。如果通过一定的手段或控制能够达到某个安全等级，则该状态（或安全等级）是可控态；否则称为不可控态，在实际中，当然能够达到的安全等级越高越好。

根据控制理论可控态的概念和离散事件动态系统的状态可控性含义，结合研究网络可控性的目的——提高网络安全性，设网络的安全状态分为五级，如表 1-1 所示。对介于各个安全等级之间的安全程度，用相邻的两个安全等级之间的数字表示，比如处于安全和较高安全之间的安全程度用 8 表示。

**表 1-1　网络安全状态等级表**

| 安全等级 | 数字表示 |
|---|---|
| 安全 | 9 |
| 较高安全 | 7 |
| 较安全 | 5 |
| 较低安全 | 3 |
| 不安全 | 1 |

因此，如果通过现有的技术能够达到某个网络要求的安全等级，对于该网络则称网络状态是完全可控的；如果通过现有技术不能达到某个网络要求的安全等级，但是可以实现部分要求，对于该网络则称网络状态是部分可控的；如果通过现有技术不能满足某个网络要求的最低安全等级，对于该网络则称网络状态是不可控的。

计算机网络建立的初衷是为了实现信息共享，而网络安全问题也主要是计算机网络中的关键或重要信息的安全问题，对于网络战来说也是为了提高己方对战场信息的及时获取、迅速传输和有效利用，抑制敌方的信息获取、传输和利用，来达到己方的信息优势，获取“制信息权”。

所以，综合目前的研究成果，计算机网络的可控性定义就是指对网络上的信息及信息系统实施安全监控，做到能够控制授权范围内的信息流向、传播及行为方式，控制网络资源的使用及使用资源的人或实体的使用方式。

6. 真实性

网络中的信息，组成网络的各种软硬件设备，及其使用网络的人员的身份，都要经过权威部门或人员的鉴定，保证信息的来源、信息的内容、实体的身份和用户的身份是真实、可信的。

实现真实性可以采用内容鉴别、实体鉴别和身份鉴别等各种鉴别手段，它是以密码学和