普通高等教育“十一五”国家级规划教材
计算机类核心课程教改项目成果系列教材

计算机网络安全

（第三版）

顾巧论　主编

科学出版社

免费提供电子课件

普通高等教育“十一五”国家级规划教材

计算机类核心课程教改项目成果系列教材

计算机网络安全

（第三版）

顾巧论　主编

科学出版社

北　京

内 容 简 介

网络安全是一门涉及计算机科学、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综合性科学。网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

本书利用通俗易懂的语言阐述了网络所涉及的安全问题，主要内容包括上篇（事前预防）、中篇（事中监测与治理）和下篇（事后恢复）三个部分。上篇内容包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术介绍和网络安全法律法规；中篇内容包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和 Web 的安全；下篇内容包括数据备份技术和安全恢复技术。

本书不仅适合高职高专学生使用，同时也适合于任何对网络安全感兴趣的读者。

图书在版编目(CIP)数据

计算机网络安全/顾巧论主编. —3 版. —北京：科学出版社，2011

ISBN 978-7-03-030368-4

Ⅰ.①计… Ⅱ.①顾… Ⅲ.①计算机网络-安全技术-高等学校-教材

Ⅳ.①TP 393.08

中国版本图书馆 CIP 数据核字（2011）第 028168 号

责任编辑：陈晓萍 / 责任校对：王万红

责任印制：吕春珉 / 封面设计：东方人华平面设计部

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

铭浩彩色印装有限公司 印刷

科学出版社发行　　各地新华书店经销

*

2011 年 3 月第 三 版　　开本：787×1092　1/16

2011 年 3 月第十一次印刷　　印张：15 3/4

印数：34 001—37 000　　字数：380 000

定价：28.00 元

（如有印装质量问题，我社负责调换〈骏杰〉）

销售部电话 010-62144126　　编辑部电话 010-62135517-8003

第三版前言

由于计算机技术发展迅速，网络安全的相关技术在不断推陈出新，第一版《计算机网络安全》教材中的部分内容已经过时。为此，本书将从网络安全的事前预防（上篇）、事中监测与治理（中篇）和事后恢复（下篇）三个层面，在对原版中过时的内容进行修订的基础上，采用通俗易懂的语言，对计算机网络安全的各个方面进行阐述。

上篇内容主要是对网络安全相关知识的介绍，包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术介绍和网络安全法律法规；中篇内容主要是关于网络运行过程中的相关安全技术，包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和 Web 的安全；下篇内容主要是关于在网络安全事故发生后如何恢复的技术，包括数据备份技术和安全恢复技术。具体内容如下：

第 1 章是网络安全概述，包括网络安全简介、网络安全面临的威胁、网络出现安全威胁的原因、网络安全机制。

第 2 章是操作系统安全常识，包括安全等级标准、漏洞、Windows NT 系统安全、UNIX 系统安全、Linux 系统安全、Windows XP 系统安全及 Windows 7 系统安全。

第 3 章是病毒知识介绍，包括计算机病毒简介、网络病毒及其防治、典型病毒介绍及常用杀毒软件介绍。

第 4 章是数据安全技术介绍，包括数据加密及数据压缩。

第 5 章是网络安全法律法规，包括与网络有关的法律法规、网络安全管理的有关法律和其他法律规范。

第 6 章是防火墙技术，包括防火墙简介、防火墙的类型、防火墙配置、防火墙系统、防火墙的选购和使用及防火墙产品介绍。

第 7 章是黑客攻击与入侵检测，包括黑客常用的攻击方法和防范措施、入侵检测响应与追踪。

第 8 章是虚拟专用网，包括 VPN 概述和 VPN 的配置实现。

第 9 章是网络通信安全，包括网络通信的安全性、网络通信存在的安全威胁、调制解调器的安全及 IP 安全。

第 10 章是 Web 的安全，包括 Web 技术简介、Web 的安全需求、Web 服务器安全策略、Web 浏览器安全策略及 Web 站点安全八要素。

第 11 章是数据备份技术，包括数据完整性、容错与网络冗余及网络备份系统。

第 12 章是安全恢复技术，包括网络灾难、安全恢复的条件、安全恢复的实现及安全恢复案例。

本书第 1 章由顾巧论修订；第 2 章、第 4 章、第 6 章、第 9 章由彭英慧修订；第 3 章、第 10 章、第 11 章、第 12 章由申莉莉修订；第 5 章、第 7 章、第 8 章由蔡振山修订。本书由顾巧论统稿。

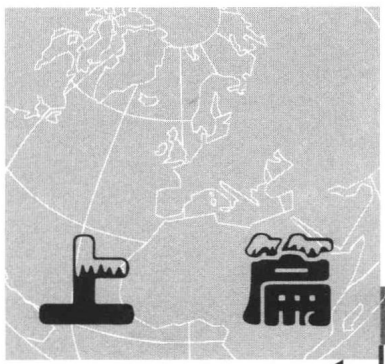
在编写及修订本书过程中，我们参考了大量书籍，在此对这些书的编著者表示感谢。

由于编者水平有限，书中错误和疏漏之处在所难免，希望读者和各位专家批评指正。

目　录

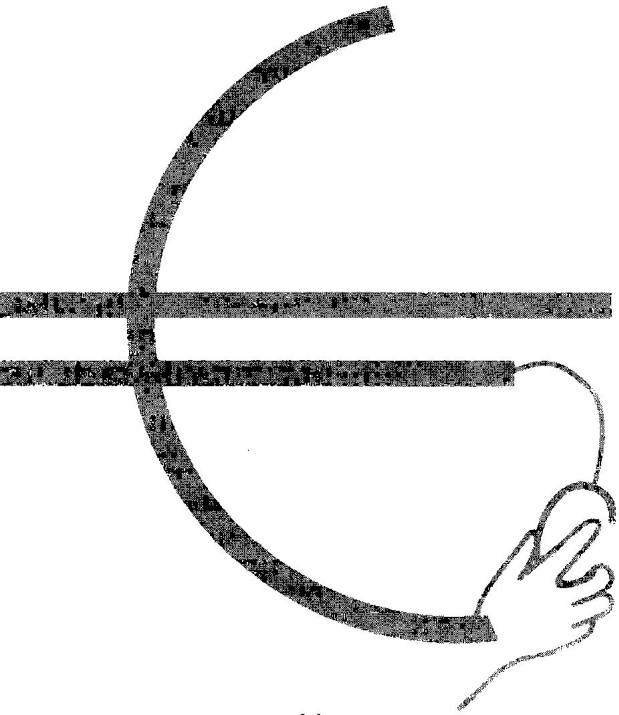
上篇　事前预防

中篇 事中监测与治理



上篇

事前预防



第1章

网络安全概述

知识点

- 网络安全的定义
- 网络面临的安全威胁
- 网络出现安全威胁的原因
- 网络的安全机制

难点

- 网络安全威胁产生的原因

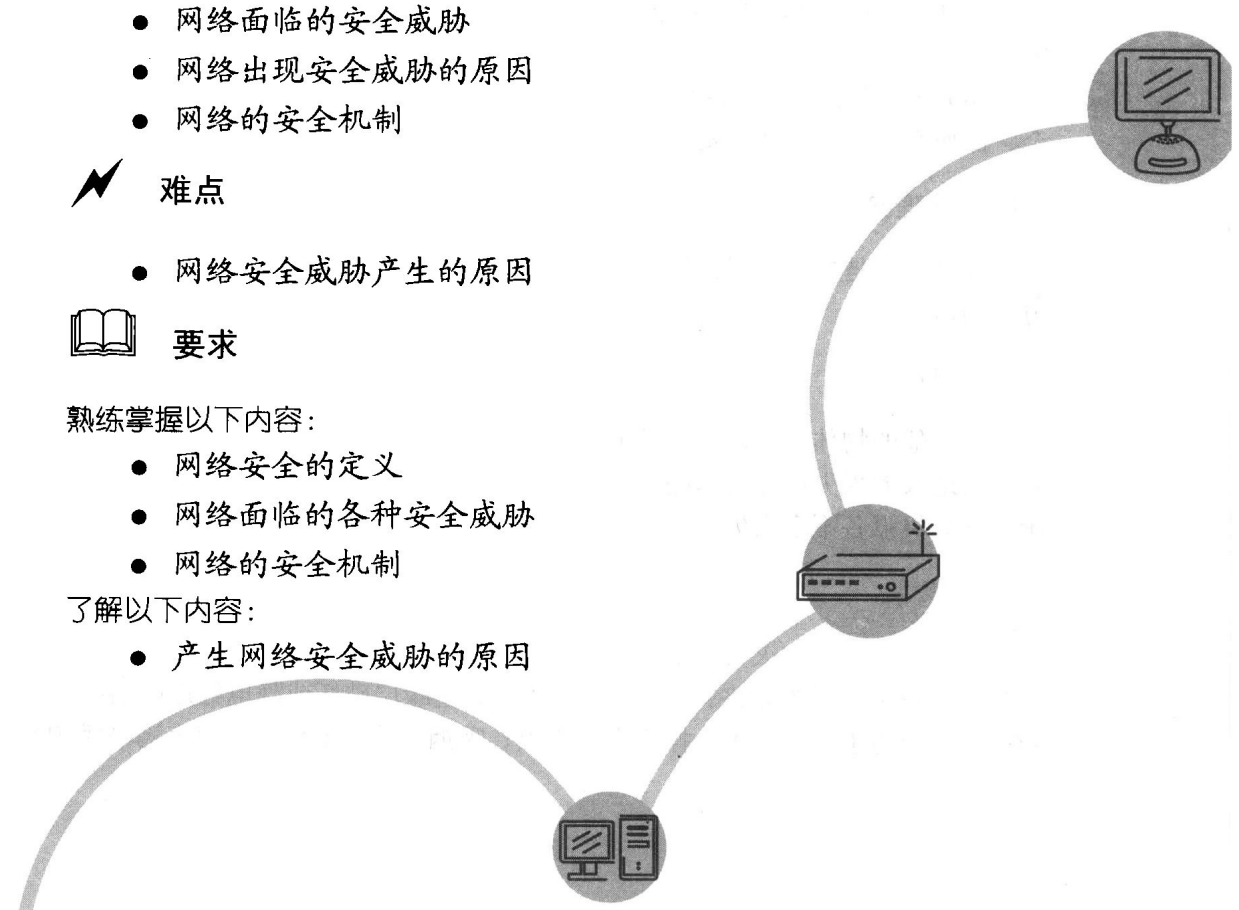
要求

熟练掌握以下内容：

- 网络安全的定义
- 网络面临的各种安全威胁
- 网络的安全机制

了解以下内容：

- 产生网络安全威胁的原因



随着网络技术的不断发展，网络在人们的生活中已经占有一席之地，给人们的生活带来了方便。然而，网络也不是完美无缺的，给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等严重威胁着网络的安全。目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 网络安全简介

网络安全是一门涉及计算机科学、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综合性科学。

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、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

（1）保密性：信息不泄露给非授权用户。

（2）完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）可控性：对信息的传播及内容具有控制能力。网络安全包括物理安全、逻辑安全、操作系统安全、联网安全。

1.1.1 物理安全

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括多方面的内容。

1. 防盗

像其他的物体一样，计算机也是偷窃者的目标，如盗走光驱、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路可能因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎、吸烟、乱扔烟头等，使充满易燃物质（如纸

片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电，放电火花，造成火灾；还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。

4. 防雷击

随着科学技术的发展，电子信息设备的广泛应用，对现代闪电保护技术提出了更高、更新的要求。利用传统的常规避雷针，已不能满足微电子设备的要求，而且带来很多弊端。利用引雷机理的传统避雷针防雷，不但增加雷击概率，而且会产生感应雷。并且感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。

雷击防范的主要措施包括：根据电气、微电子设备的不同功能及不同受保护程度和所属保护层确定防护要点作分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多级层保护。

5. 防电磁泄漏

电子计算机和其他电子设备一样，工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。例如，从20世纪80年代开始，美国市场上出现了一种符合TEMPEST标准的军用通信设备，并逐渐形成商品化、标准化生产。TEMPEST技术是综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及多个学科领域。

屏蔽是防电磁泄漏的有效措施，主要有电屏蔽、磁屏蔽和电磁屏蔽3种类型。

1.1.2 逻辑安全

计算机的逻辑安全需要用口令字、文件许可、查账等方法来实现。防止计算机黑客的入侵主要依赖计算机的逻辑安全。

可以限制登录的次数或对试探操作加上时间限制，还可以用软件来保护存储在计算机文件中的信息，该软件限制了其他人存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止。限制存取的另一种方式是通过硬件完成，在接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如多次登录或请求别人的文件。

1.1.3 操作系统安全

操作系统是计算机中最基本、最重要的软件。同一计算机可以安装几种不同的操作系统。如果计算机系统可提供给许多人使用，则操作系统必须能区分用户，以便于防止他们相互干扰。例如，多数的多用户操作系统不会允许一个用户删除属于另一个用户的文件，除非第二个用户明确地允许。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。通常，一个用户对应一个账户。操作系统不允许一个用户修改由另一个账户产生的数据。

1.1.4 联网安全

联网的安全性只能通过以下两方面的安全服务来达到。

（1）访问控制服务：用来保护计算机和联网资源不被非授权使用。

（2）通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。例如，基于互联网或 WWW 的电子商务就必须依赖并广泛采用通信安全服务。

1.2 网络安全面临的威胁

计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用等。

人为的无意失误，如操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借给他人或与别人共享等都会对网络安全带来威胁。

人为的恶意攻击，是计算机网络面临的最大威胁，如敌人的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动动机，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。

网络软件的漏洞和“后门”：全网络软件不可能是百分之百无缺陷和无漏洞的。然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件大部分都是因为安全措施不完善所导致的苦果。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。

总的来说，网络安全的威胁如图 1-1 所示。