信息产业部IT职业技术培训考试指定教材

胡 铮 主编

网络与信息安全

Wangluo Yu
Xinxi Anquan

清华大学出版社

网络与信息安全

胡　铮　主编

清华大学出版社

北　京

内 容 简 介

本书详细介绍了网络与信息安全方面的知识，内容共分16章，主要包括安全体系框架、互联网应用安全基础、桌面安全、计算机病毒、安全法律法规、黑客攻击技术、密码学技术及其应用、防火墙技术、网络安全监控与分析、操作系统安全配置、信息安全管理概述、安全管理体系建立的方法、安全标准、工程管理、风险管理及业务连续性管理等，书后的附录中则介绍了网络安全防范方面的一些实验。

作为信息产业部IT职业技术培训考试指定教材，本书内容翔实，语言简练，实用性强。主要供信息产业部网络与信息安全技术培训项目认证之用，同时也可作为高等院校、各类职业学校及培训机构的网络与信息安全技术课程的教材。

图书在版编目(CIP)数据核字

网络与信息安全/胡铮 主编. —北京：清华大学出版社，2006.5

ISBN 7-302-12783-2

Ⅰ. 网… Ⅱ. 胡… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2006)第027265号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：胡伟卷

文稿编辑：刘金喜

封面设计：王　永

版式设计：康　博

印 刷 者：北京市世界知识印刷厂

装 订 者：三河市李旗庄少明装订厂

发 行 者：新华书店总店北京发行所

开　　本：185×260　**印张**：53.5　**字数**：1302千字

版　　次：2006年5月第1版　2006年5月第1次印刷

书　　号：ISBN 7-302-12783-2/TP·8142

印　　数：1～4000

定　　价：76.00元

全国网络与信息技术培训认证(NTC)项目简介

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力，对信息化人才的培养与评估不断提出新的要求。建立一个技术领先、既广泛涉及多厂商产品又保持内容中立的政府认证品牌成为我国信息化发展的当务之急。

全国网络与信息技术培训项目(NTC)是信息产业部根据国家对专业技术人员加强培训且须持证上岗等文件精神和国家职业技术标准要求所制定的认证体系，包含网络与信息管理(MINT)、网络与信息安全(NISE)、数据库管理(NDAT)、网络游戏技术(NGCT)、数据分析(CCDA)等认证课程、技能课程、企业战略合作课程、IT 职业资格课程、工程师职称考试在内的五大模块，近 30 种认证课程。主要面向各行政、企事业单位及行业系统的专业技术人员、管理人员进行资格认证。

该认证体系以行业为基础，以技术为核心，积极响应“国务院关于大力发展职业教育的决定”(国发[2005] 35 号)的文件精神，根据信息产业部、劳动和社会保障部相关文件要求，面向实际应用，课程涵盖管理决策层、专业技术层和操作应用层三个层面。以专业化和广泛性的市场调研为基础，在信息产业部职鉴中心等有关部门的指导和大力协助下，旨在培养国家信息化专业技术人才及管理人才，树立 IT 行业的国家标准，并与教育、培训、IT、人力资源等行业的主流机构进行开放性和创新性的合作，逐步建立起了一套具有国际化水准的技术类职业人才培训及认证体系。

为更好地贯彻执行“国家职业资格”从业人员资格证书和“专业技术资格”证书的“双证”制度，落实国家教育科研部门“产学研”相结合的指导精神，结合就业准入制度工作的开展和职业资格证书制度的覆盖面，提升各相关单位的知名度，由全国网络与信息技术培训项目管理中心(NTC-MC)负责面向全国组织 NTC 的授权、考试与管理工作。

NTC-MC 的技术优势

权威的政府资格认证。全国网络与信息技术培训项目(NTC)，由信息产业部职鉴中心根据国家职业技术标准要求颁发相关等级的“资质”证书，可作为国家专业技术资格认证标准与职称评定的依据；相关职业技能考核合格者，由信息产业部与劳动和社会保障部联合颁发“国家职业资格”证书。

国际水准的技术认证。NTC 将成为具有国际水准的网络与信息技术认证，NTC 以厂商中立为基本原则，广泛与国内外知名厂商合作，保持与世界先进水平同步，确保教育技术处于国际领先水平。

关注人才发展的认证。NTC 将在国家政策的指引下，培养足够数量的掌握国际先进信息技术的信息化人才，以不断推动国家信息化进程。同时广泛与跨国企业、国内知名企事业单位、人才交流中心等机构合作，全力推动学员就业。

NTC-MC 发展目标

建立我国 IT 专业技术人才和管理人才的国家标准。

建立国内一流的 IT 专业职业发展体系和课程体系。

建立一个服务于国家信息化建设事业的终身学习、服务机制。

建立一个服务于各企事业单位的 IT 专业技术人才及管理人才的测评标准。

管理中心　网站：www.ntc.org.cn

电子邮件：ntc@ntc.org.cn

电话：010-68200668　68208787

传真：010-68200659

邮编：100846

地址：北京市海淀区万寿路 27 号信息产业部机关大院

全国网络与信息技术培训认证管理中心

编 委 会

作者简介

一、个人资料

胡铮　全国网络与信息技术培训项目管理中心主任、信息产业部 IT 职业技术培训认证指定系列教材主编，曾任国家信息安全教育认证广东省管理中心主任。

特长　国家一级武术师、国家一级武术散手裁判。

社会任职　全国医疗卫生信息技术培训与认证管理中心名誉主任兼专家委员会主任、广东省公安厅计算机信息网络安全协会常务理事、广东省生态学会高新技术技能培训基地主任、广东省景观生态专业委员会副主任、广州医学信息协会常务理事等职务。

二、学术著作

编著及参与编著的著作有：

IT 类　《网络与信息资源管理》、《数据库管理》、《网络与信息安全》、《信息安全基础》、《网络隔离与网闸》、《入侵检测技术》、《数据备份与灾难恢复》、《信息安全法规与标准》、《信息安全团队构建与管理》、《首席信息主管(CIO)》等。

武术类　《中国散打训练教室》、《海外武术集粹》、《菲律宾短棍格斗技术》等；并在《武魂》、《搏击》、《拳击与格斗》等国家级刊物上发表有大量论文及译文。

前　言

互联网的迅猛发展已经深刻地影响到国家的政治、经济、军事、文化等各个领域，与此同时互联网的开放性和安全漏洞所带来的安全风险也对互联网的健康发展带来了不可忽视的影响。网络安全问题不仅给相关单位及网民带来不便，而且已经威胁到国家的信息安全和经济发展。网络与信息安全从1995年开始成为中国信息化发展战略的重要组成部分，在十六届四中全会上通过的《关于加强党的执政能力的决议》中，信息安全与政治、经济、文化安全并列为四大主题，将之提到了前所未有的高度。

随着互联网安全事件发生得越来越频繁，危害越来越大，网络与信息安全技术水平的提高与应急体系的建设、应急能力的提高已成为全球化、网络化竞争中发展的必要条件。为此，信息产业部推出了网络与信息安全技术培训认证项目，包含了网络与信息安全应用、管理技术和计算机网络应急响应体系两个方面。

本教材主要是供信息产业部网络与信息安全技术培训项目认证之用，同时也可作为高等院校、各类职业学校(学院)及培训机构的网络与信息安全技术课程的教材。

信息产业部网络与信息安全技术培训项目是全国网络与信息技术培训(NTC)项目中的安全部分子项目，是信息产业部根据国家职业技术标准要求及国家对专业技术人员加强培训且须持证上岗等文件精神所推出的面向各行政、企事业单位及行业系统的专业技术人员、管理人员进行资格认证的培训项目。培训考核通过者可颁发信息产业部相关等级的“资质”证书及由信息产业部、劳动和社会保障部共同核发的“国家职业资格”证书。由全国网络与信息技术培训项目管理中心(www.ntc.org.cn)负责在全国范围内的推广及相关管理。

本教材囊括了较为系统、全面的安全技术体系和管理体系，包含有理论、技术应用及实验。网络与信息安全技术培训认证，是在进行职业角色分析基础上建立起来的一套科学、系统、实用的考核体系，内容涉及安全技术应用、管理等相关专业领域。

该课程强调实践性和应用性。经过网络与信息安全技术培训与考核，学员将建立起全面、科学的网络与信息安全知识体系及应用、管理技术，能胜任行政、企事业单位与网络信息安全相关的应用与管理工作。

本教材主要强调网络与信息安全技术的应用及管理，在本教材出版后，我们还将和国家计算机网络应急技术处理协调中心联合出版《网络安全应急响应指南》一书，共同列入信息产业部网络与信息安全技术培训认证项目(NISE)的教学体系中。

本书编著过程中得到了信息产业部人事司、信息产业部职鉴中心、全国网络与信息技术培训项目管理中心(NTC-MC)、公安部主管的《信息网络安全》杂志、全国医疗卫生信息技

术培训认证管理中心、国家计算机应急技术处理协调中心及广东分中心的大力支持，特别是国家计算机网络应急技术处理协调中心科技委副主任林鹏教授在本书的编著过程中提供了大量的帮助和支持，在此一并表示感谢。

由于我们水平所限，加之时间仓促，书中错漏之处在所难免，敬请读者、同行及专家批评指正。

作　者

2006 年 3 月

读者意见反馈卡

亲爱的读者：

感谢您购买了本书，希望它能为您的工作和学习带来帮助。为了今后能为您提供更优秀的图书，请您抽出宝贵的时间填写这份调查表，然后剪下寄到：北京清华大学出版社第五事业部(邮编 100084)；您也可以把意见反馈到 cwkbook@tup.tsinghua.edu.cn。邮购咨询电话：010-62786544，客服电话：010-62786969。我们将充分考虑您的意见和建议，并尽可能地给您满意的答复。谢谢！

本 书 名：_____

个人资料：_____

姓　　名：_____ **性　别：**□男 □女 **出生年月(或年龄)：**_____

文化程度：_____ **职　业：**_____ **通讯地址：**_____

电话(或手机)：_____ **传　真：**_____ **电子信箱(E-mail)：**_____

您是如何得知本书的：_____

□别人推荐 □出版社图书目录 □网上信息 □书店

□杂志、报纸等的介绍(请指明)_____ □其他(请指明)_____

您从何处购得本书：□书店 □电脑商店 □软件销售处 □邮购 □商场 □其他

影响您购买本书的因素(可复选)：

□封面封底 □装帧设计 □价格 □内容提要、前言或目录 □书评广告

□出版社名声 □作者名声 □责任编辑

□其他：_____

您对本书封面设计的满意度：□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书印刷质量的满意度：□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书的总体满意度：

从文字角度：□很满意 □比较满意 □一般 □较不满意 □不满意

从技术角度：□很满意 □比较满意 □一般 □较不满意 □不满意

本书最令您满意的是：

□讲解浅显易懂 □内容充实详尽 □示例丰富到位 □指导明确合理 □其他：_____

您希望本书在哪些方面进行改进？_____

您希望增加什么系列或软件的图书：_____

您最希望学习的其他软件：1._____ 2._____ 3._____ 4._____

您对使用中文版软件或外文版软件介意吗？更喜欢使用哪一种版本？

□介意 □无所谓 □中文版 □外文版

您对图书所用软件版本是否很介意？是否要求用最新版本？

□是，要求是最新版本 □无所谓 □不，因为硬件或软件跟不上要求

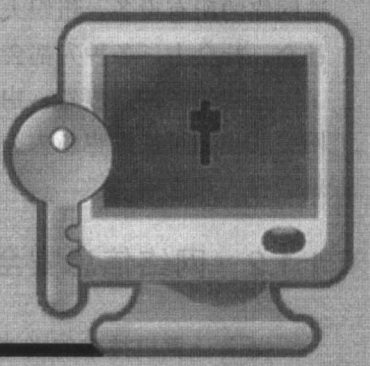
您是如何学习最新软件的？

□看计算机书 □看多媒体教学光盘 □自己摸索或查看软件的帮助信息 □参加培训班 □向其他人请教

□其他：_____

您的其他要求：_____

目　录



第1章 安全体系框架

本章首先介绍安全的基本内容以及安全的分类；然后介绍信息安全的4个基本属性，通过分析了解 TCP/IP 协议的脆弱性以及信息安全所面临的威胁；最后介绍了信息安全防御体系中所应用的一些模型和常用的技术。本章内容适合参加信息安全管理员认证的读者阅读。

1.1 安全概述

1.1.1 安全的产生背景

网络由智能设备构成，而智能设备将按照制造者或设计者的意图实现使用者或拥有者的指令。当制造者与所有者的利益发生冲突时，智能设备会站在哪一边是由制造者在制造时确定的，不能保证制造者的意图全部向使用者或拥有者公开，这包括个别设计人员未经允许偷偷留下的后门和生产测试需要的附件。比如，一个保密的 CPU 使外界无法存储芯片内的某保密字，然而设计者不公开的测试端口保留了对此保密字的存取。网络拥有较为复杂的设备和协议，保证复杂的系统没有缺陷和漏洞是不可能的，如 Windows NT 系统，没有任何个人能全部了解其每一细节，随着用户的增加，其程序错误(BUG)也不断被发现。

Intel 的 MMX 系列芯片经过无数专家审核仍存在设计上的错误；系统设计的后门随着系统的复杂越来越难于发现。系统和软件工程学也告诉我们，大型系统将永远有用户不满意的地方，直到此系统被停止使用，即生命期终止。