

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。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

### 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于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,包含网络与信息安全管理(MINT)、网络与信息安全管理(NISE)、数据库管理(NDAT)、网络游戏技术(NGCT)、数据分析(CFDA)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养及认证体系。

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](http://www.ntc.org.cn)

电子邮件: [ntc@ntc.org.cn](mailto: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

主 编：胡 铮

副主编：马忠林      林 鹏

编 委：洪京一      刘占山      盘冠员

孙蔚敏      徐亚国      苏 红

王连宝      何志平      梁铭会

罗耀春      温安顺      张宏阳

刘 旻      陈红岩      刘兴池

张忠杰      李转琴      金湘宇

刘 岗      蔡晶晶

# 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](http://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的。

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

<b>第 1 章 安全体系框架</b> .....	1
1.1 安全概述 .....	1
1.1.1 安全的产生背景 .....	1
1.1.2 网络信息安全的现状 .....	2
1.1.3 国内外安全形势 .....	4
1.1.4 信息安全意识与教育 .....	10
1.2 安全分类 .....	11
1.2.1 计算机网络安全 .....	11
1.2.2 信息安全 .....	12
1.2.3 安全的原则 .....	13
1.3 信息安全的基本要求 .....	14
1.4 信息安全面临的威胁 .....	16
1.4.1 人为的无意失误 .....	16
1.4.2 黑客的恶意攻击 .....	17
1.4.3 偶然的破坏者 .....	18
1.4.4 坚定的破坏者 .....	18
1.4.5 间谍 .....	18
1.4.6 攻击动机 .....	19
1.5 行业面临的威胁 .....	19
1.5.1 银行系统面临的风险 .....	20
1.5.2 政府面临的威胁 .....	20
1.5.3 运营商面临的威胁 .....	21
1.6 信息安全防御体系 .....	21
1.6.1 动态防御模型 .....	21
1.6.2 身份认证技术 .....	23
1.6.3 访问控制技术 .....	25
1.6.4 加密技术 .....	28
1.6.5 防火墙技术 .....	29
1.6.6 安全审计技术 .....	31
1.6.7 入侵检测技术 .....	32
<b>第 2 章 互联网应用安全基础</b> .....	35
2.1 计算机网络基础 .....	35

2.1.1 计算机网络的定义 .....	35
2.1.2 网络的分类 .....	36
2.1.3 网络的拓扑结构 .....	37
2.1.4 TCP/IP 协议 .....	38
2.1.5 TCP/IP 协议的脆弱性 .....	40
2.2 Internet 概述 .....	41
2.2.1 Internet 的发展历史 .....	41
2.2.2 Internet 的组织管理 .....	42
2.2.3 Internet 在企业内部网中 的应用——Intranet .....	46
2.2.4 Internet 在我国的发展 .....	47
2.3 互联网应用 .....	49
2.3.1 万维网 .....	49
2.3.2 电子邮件 E-mail .....	54
2.3.3 FTP .....	55
2.3.4 BBS .....	61
2.3.5 DNS .....	65
<b>第 3 章 桌面安全</b> .....	71
3.1 桌面系统漏洞检测 .....	71
3.2 账号安全 .....	73
3.3 文件系统的安全 .....	77
3.4 停止多余的服务 .....	79
3.5 注册表的安全配置 .....	79
3.6 异常检测 .....	80
3.6.1 异常端口检测 .....	80
3.6.2 异常进程检测 .....	82
3.6.3 Windows 内存保护 .....	85
3.7 IE 浏览器的安全 .....	85
3.7.1 常规属性的设置 .....	85
3.7.2 安全属性的设置 .....	87
3.7.3 高级属性的设置 .....	92
3.8 Windows 日志 .....	93



<b>第4章 计算机病毒</b> .....	95
4.1 计算机病毒概述.....	95
4.1.1 计算机病毒的定义.....	95
4.1.2 计算机病毒的特征行为.....	96
4.1.3 计算机病毒的传播途径.....	98
4.1.4 计算机病毒的分类.....	100
4.1.5 计算机病毒感染征兆.....	102
4.1.6 病毒的清除.....	107
4.1.7 基本的防病毒方式.....	108
4.2 防病毒系统的部署.....	109
<b>第5章 安全法律法规</b> .....	111
5.1 信息时代对法律提出的挑战.....	111
5.2 国外信息安全立法现状.....	112
5.3 国内信息安全立法现状.....	113
5.4 电子商务的概念和电子商务.....	114
法律范畴.....	114
5.4.1 国际电子商务立法状况.....	115
5.4.2 我国电子商务立法现状.....	116
5.4.3 数字签名法.....	117
5.5 隐私保护.....	118
5.5.1 隐私保护与信息安全的.....	
一致性与对立性.....	119
5.5.2 隐私保护的 legal 与政策趋向.....	120
5.6 密码政策.....	121
5.6.1 世界各国密码政策综述.....	121
5.6.2 我国的《商用密码.....	
管理条例》.....	126
5.7 计算机取证概念及探讨.....	127
5.7.1 Computer Forensics 的.....	
发展历史.....	128
5.7.2 我国 Computer Forensics.....	
的发展现状.....	129
<b>第6章 黑客攻击技术</b> .....	131
6.1 攻防综述.....	131
6.2 攻击一般流程.....	132

6.2.1 隐藏自身.....	132
6.2.2 预攻击探测.....	132
6.2.3 采取攻击行为.....	133
6.2.4 清除痕迹.....	133
<b>6.3 攻击技术方法</b> .....	134
6.3.1 远程信息探测.....	134
6.3.2 远程缓冲区溢出攻击.....	140
6.3.3 CGI 攻击.....	140
6.3.4 拒绝服务攻击.....	140
6.3.5 口令攻击.....	142
6.3.6 木马攻击.....	142
6.3.7 欺骗攻击.....	143
6.3.8 恶意代码.....	143
6.3.9 社会工程.....	144
<b>第7章 密码学技术及其应用</b> .....	145
7.1 密码学概述.....	145
7.1.1 密码学与信息安全的关系.....	145
7.1.2 密码学的历史与发展.....	146
7.1.3 密码学的基本概念.....	148
7.1.4 密码体制的分类.....	149
7.2 常规加密的经典技术.....	149
7.2.1 常规加密模型.....	150
7.2.2 密码分析.....	151
7.2.3 隐写术.....	151
7.2.4 经典加密技术.....	152
7.3 常规加密的现代技术.....	158
7.3.1 流密码.....	159
7.3.2 分组密码.....	159
7.3.3 数据加密标准.....	165
7.3.4 常规加密的算法.....	170
7.4 公开密钥密码.....	181
7.4.1 公开密钥密码概述.....	181
7.4.2 基于大整数分解的公开.....	
密钥密码体制.....	183
7.4.3 基于离散对数的公开.....	
密钥密码体制.....	190



7.4.4 基于椭圆曲线的公开 密钥密码体制	193	8.2.2 代理技术	303
7.4.5 椭圆曲线的有关数学背景	194	8.2.3 电路级网关技术	307
7.5 报文鉴别与散列函数	199	8.2.4 状态检查技术	309
7.5.1 鉴别的需求	199	8.2.5 地址翻译技术	311
7.5.2 鉴别函数	199	8.2.6 其他防火墙技术	313
7.5.3 散列算法	200	<b>第 9 章 网络安全监控与分析技术</b>	<b>317</b>
7.6 数字签名	213	9.1 网络安全监控与分析技术 的意义	317
7.6.1 数字签名概述	213	9.2 入侵检测系统概述	318
7.6.2 数字签名标准	215	9.2.1 入侵检测相关术语	318
7.7 PKI 系统架构	217	9.2.2 IDS 在网络安全体系中的 角色	319
7.7.1 什么是 PKI	217	9.2.3 IDS 的作用	321
7.7.2 PKI 起因和解决的核心问题	217	9.2.4 IDS 系统的分类	321
7.7.3 PKI 及其构件	219	9.2.5 IDS 的优势和局限	323
7.7.4 PKI 应用	223	9.3 IDS 系统体系结构	327
7.7.5 PKI 体系的互通性 (互操作性)	223	9.3.1 安全数据生成	330
7.8 数字证书与 CA 系统架构	224	9.3.2 安全数据显示	330
7.8.1 CA 是什么	224	9.3.3 数据的存储管理	331
7.8.2 CA 的功能	225	9.3.4 IDS 系统和其他安全 工具集成	332
7.8.3 CA 的常见术语	225	9.4 入侵检测关键技术	333
7.8.4 CA 理论基础	229	9.4.1 包俘获	333
7.9 PKI 体系的应用	235	9.4.2 主机 IDS 检测技术	336
7.9.1 PKI 应用理论	235	9.4.3 异常检测技术	341
7.9.2 PKI 的应用	246	9.4.4 误用检测技术	344
7.10 CA 发展现状和展望	256	9.4.5 其他入侵检测系统技术	351
7.10.1 国外发展现状	256	9.4.6 事件规则	364
7.10.2 国内发展现状	257	9.5 入侵检测系统外围支撑技术	365
<b>第 8 章 防火墙技术</b>	<b>261</b>	9.5.1 响应机制	365
8.1 防火墙概论	261	9.5.2 日志分析	369
8.1.1 防火墙简介	261	9.5.3 接口标准	369
8.1.2 防火墙策略	269	9.6 IDS 应用指南	371
8.1.3 防火墙的安全策略	271	9.6.1 IDS 的部署方式	371
8.1.4 防火墙的体系结构	276	9.6.2 应用部署	373
8.2 防火墙关键技术	289	9.6.3 IDS 的性能指标	374
8.2.1 数据包过滤技术	289		



9.6.4	IDS 的功能指标	374	12.2.2	文件化	567
<b>第 10 章</b>	<b>操作系统安全配置</b>	<b>383</b>	12.2.3	领导重视	567
10.1	Windows 系统	383	12.2.4	全员参与	568
10.1.1	Windows NT/2000 系统安全	383	12.3	信息安全管理体的建立	568
10.1.2	Windows 2000 新增的 安全机制	391	12.3.1	建立信息安全管理体	568
10.1.3	Windows 2000 的安全 配置实例	410	12.3.2	文件要求	570
10.1.4	Windows 2000 的入侵 检测与恢复	437	12.3.3	文件控制	570
10.2	UNIX 系统	446	12.3.4	记录控制	571
10.2.1	UNIX 系统概述	446	12.4	实施和运作信息安全 管理体系	571
10.2.2	UNIX 系统的安全特征	454	12.5	监控和评审信息安全 管理体系	572
10.2.3	UNIX 系统入侵防范	457	12.5.1	监控信息安全管理体	572
10.2.4	UNIX 系统入侵检测	535	12.5.2	维护和改进信息安全 管理体系	572
10.2.5	UNIX 系统安全审计	539	12.5.3	信息安全管理体的 管理评审	573
<b>第 11 章</b>	<b>信息安全管理概述</b>	<b>553</b>	12.6	信息安全管理体的改进	574
11.1	什么是信息	553	12.6.1	持续改进	574
11.1.1	信息的概念	554	12.6.2	纠正措施	574
11.1.2	信息的特征	555	12.6.3	预防措施	574
11.1.3	信息的性质	556	12.7	控制措施的选择	575
11.1.4	信息的功能	557	12.7.1	信息安全方针	575
11.2	什么是信息安全	557	12.7.2	安全组织	576
11.3	什么是信息安全管理 及其重要性	558	12.7.3	资产分类与控制	581
<b>第 12 章</b>	<b>信息安全管理体建立的 通用方法</b>	<b>561</b>	12.7.4	人员安全	582
12.1	信息安全管理体概述	561	12.7.5	物理和环境安全	585
12.1.1	什么是信息安全管理体	561	12.7.6	通信和操作管理	590
12.1.2	信息安全管理体的作用	562	12.7.7	访问控制	602
12.1.3	信息安全管理体的准备	563	12.7.8	系统开发和维护	614
12.2	建立信息安全管理体 的原则	565	12.7.9	应用系统中的安全	615
12.2.1	PDCA 原则	565	12.7.10	持续运营管理	623
			12.7.11	遵从性	625
			<b>第 13 章</b>	<b>安全标准</b>	<b>631</b>
			13.1	标准概述	631
			13.1.1	信息技术标准的发展趋势	632

13.1.2	标准化组织	634	14.4.2	使用 SSE-CMM 进行评定	673
13.2	相关信息安全标准目录	637	14.4.3	决定实施安全工程过程的能力	674
13.2.1	国内信息技术标准	638	14.4.4	用 SSE-CMM 改进过程	676
13.2.2	ISO/IEC JTC1/SC27 信息技术的 安全技术标准	639	14.4.5	组织中如何使用 SSE-CMM	678
13.2.3	ISO/TC68/SC2 银行操作和规程	641	14.5	通用实施	680
13.2.4	欧洲计算机制造商协会信息安全标准(ECMA)	642	14.5.1	能力级别 0——未实施	680
13.2.5	美国信息技术安全标准	642	14.5.2	能力级别 1——非正式实施	680
13.3	我国信息安全标准化概况	643	14.5.3	能力级别 2——计划和跟踪	680
13.3.1	基础类标准	645	14.5.4	能力级别 3——充分定义	683
13.3.2	物理安全标准	647	14.5.5	能力级别 4——定量控制	685
13.3.3	系统与网络标准	649	14.5.6	能力级别 5——连续改进	685
13.4	常用信息安全标准	649	<b>第 15 章 风险管理</b>	<b>687</b>	
13.4.1	互操作标准	649	15.1	风险管理概述	687
13.4.2	信息安全管理与控制标准	650	15.1.1	背景	687
13.4.3	技术与工程标准	653	15.1.2	风险管理要求	688
<b>第 14 章 工程管理</b>	<b>661</b>		15.1.3	风险管理概述	690
14.1	什么是安全工程	661	15.1.4	风险评估简介	691
14.1.1	安全工程的定义	661	15.2	风险管理过程	695
14.1.2	安全工程组织	662	15.2.1	建立环境	695
14.1.3	安全工程的生命期	662	15.2.2	风险鉴定	697
14.1.4	安全工程与其他科目	662	15.2.3	风险分析	698
14.1.5	安全工程特点	663	15.2.4	分析步骤	700
14.2	安全工程过程概述	663	15.2.5	风险识别	705
14.2.1	风险	664	15.2.6	风险处理	706
14.2.2	工程	665	15.2.7	风险评估成功的关键因素	712
14.2.3	保证	666	15.3	评估内容和过程	713
14.3	安全工程体系结构描述	667	15.3.1	评估内容和阶段	713
14.3.1	基本模型	667	15.3.2	制定计划与培训	714
14.3.2	过程区	668	15.3.3	收集资料	715
14.3.3	公共特征	669	15.3.4	收集资料的方法	715
14.3.4	能力级别	670			
14.4	使用 SSE-CMM 实施安全工程	672			
14.4.1	SSE-CMM 适用对象	672			

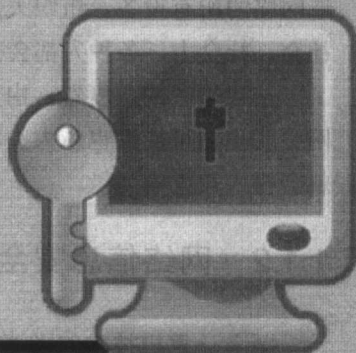


第 16 章 业务连续性管理 .....	717
16.1 概述 .....	717
16.2 应急响应计划 .....	720
16.2.1 应急响应概述 .....	720
16.2.2 安全应急响应管理 系统的建立 .....	726
16.2.3 应急响应流程 .....	735
16.2.4 事件响应通用方法指导 .....	737
16.3 灾难恢复计划 .....	747
16.3.1 概述 .....	747
16.3.2 灾难恢复的相关技术 .....	750
16.3.3 灾难恢复级别 .....	759

16.3.4 灾难恢复计划的制定 .....	760
附录 A 网络安全之攻击和威胁 分析实验 .....	767
附录 B 网络安全之密码学实验 .....	779
附录 C 网络安全之防火墙实验 .....	797
附录 D 网络安全之网络监控实验 .....	805
附录 E 网络安全之审计分析实验 .....	821
附录 F 网络安全之操作系统实验 .....	827



# 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该保密字的存取。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。