21世纪 高等学校信息安全专业规划教材

信息安全原理与技术

（第2版）

郭亚军 宋建华
李 莉 董慧慧 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

信息安全原理与技术(第2版)

郭亚军　宋建华　李　莉　董慧慧　编著

清华大学出版社
北京

内 容 简 介

本书系统地介绍了信息安全的基本原理和基本技术。全书共分为12章，包括信息安全的数学基础、对称密码技术、公钥密码技术、消息认证与数字签名、身份认证与访问控制、网络安全协议、公钥基础设施、防火墙、入侵检测、恶意代码和无线网络安全。

本书体现了以读者为中心的思想。为了让读者充分理解每一章节内容以及它们之间的联系，每一章都附有“本章导读”，并用大量的实例帮助读者理解重点知识和难点知识。

本书可作为计算机、信息安全、通信等专业的本科生以及低年级的研究生的教材，也可供从事信息安全相关专业的教学人员、科研人员和工程技术人员参考。

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。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

信息安全原理与技术/郭亚军等编著. --2版. --北京：清华大学出版社，2013.4
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-31300-7

Ⅰ. ①信… Ⅱ. ①郭… Ⅲ. ①信息系统－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第012239号

责任编辑：魏江江　王冰飞
封面设计：杨　兮
责任校对：焦丽丽
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.25　　**字　　数**：467千字
版　　次：2008年9月第1版　2013年5月第2版　　**印　　次**：2013年5月第1次印刷
印　　数：1～3000
定　　价：33.00元

产品编号：048501-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人次。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21世纪高等学校信息安全专业规划教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

试读结束:需要全本请在线购买: www.ertongbook.com

第 2 版前言

随着计算机技术与网络技术的飞速发展，信息成为了社会发展的重要资源。信息安全的新技术、新标准也在不断涌现，我国已经把信息安全技术与产业列为今后一段时期的优先发展领域。信息安全是一门跨学科、跨专业的综合性学科，涉及的知识面很广，本书的目标是力图向读者系统地介绍信息安全的基本原理与技术。

本书的第 2 版仍然遵循第 1 版的思路，从深入浅出、通俗易懂的角度让读者“看透”信息安全基本技术。首先，从整体上先让读者了解其外貌，从全局的角度向读者揭示信息安全研究的基本内容和基本技术；其次，在每一章节都向读者展示应该学些什么以及它们的作用等（如导读部分）；最后，每一章后面都列出了关键术语和精心编排的习题，让读者能够加强对每章所学基本概念和理论的理解，从而巩固所学的知识。

本书的第 2 版对第 1 版中的部分内容进行了修正，并增补了近年来密码学和网络安全领域出现的新理论和新技术。在本书第 3 章中增加了我国商用密码算法 SMS4 的内容；第 6 章在身份认证方面增加了 OpenID 和 OAuth 协议的内容；第 10 章增加了入侵防御系统技术的内容。另外，还增加了两个章节的内容：恶意代码（第 11 章）和无线网络安全（第 12 章）。

本书作者多年从事信息安全课程的教学和研究，了解学生的需要，因此本书始终是从读者的角度进行编写的。此外，为了方便教师授课，我们还专门整理了本书的课件以及本书习题的全部答案，可在清华大学出版社网站（http://www.tup.com.cn）下载。

本书由郭亚军整体规划和统稿，郭亚军编写了第 1 章、第 2 章、第 3 章、第 4 章，宋建华编写了第 6 章、第 7 章、第 9 章、第 10 章，李莉编写了第 5 章和第 8 章，董慧慧编写了第 11 章和第 12 章。在本书的编写过程中查阅和参考了大量国内外文献和书籍，限于篇幅未能在书后参考文献中一一列出，在此，编者对原作者表示真诚的感谢！

在本书的编写过程中我们得到了许多同行的热情帮助和支持，也得到了清华大学出版社编辑们的关心和帮助，在此一并表示衷心的谢意。

由于作者水平有限，书中难免会有错误和不当之处，敬请读者提出宝贵意见。

作　者

2012 年 10 月

第1版前言

信息安全涉及的知识面很广，本书的目标是力图向读者系统地介绍信息安全的基本原理与技术。全书主要由下面几个部分组成。

第一部分：信息安全的数学基础。这一部分介绍了信息安全所需要的数学知识，包括数论、代数基础、计算复杂性理论和单向函数等。

第二部分：信息安全的基本理论与技术。这一部分包括密码技术、认证、数字签名和访问控制等。

第三部分：信息安全技术在网络安全上的应用。这一部分重点介绍了 PKI 技术、网络安全协议。

第四部分：系统安全技术。这一部分简单介绍了保障系统安全的防火墙技术和入侵检测技术。

信息安全涉及许多复杂的概念和技术。为了处理这种复杂性，本书从两个方面让读者"看透"信息安全基本技术：一是从整体上让读者了解其外貌，从全局的角度向读者揭示信息安全研究的基本内容和基本技术，本书的章节安排体现了这一点；二是在局部方面向读者展示每一章应该学些什么以及它们的作用等(如导读部分)。

本书作者多年从事信息安全课程的教学和研究，了解学生的需要，因此本书始终是从读者的角度进行编写的。每一章的导读部分介绍了本章的知识要点、作用以及它们之间的联系。在正文中用大量的实例来帮助读者理解重点知识和难点知识。

为了方便教师授课，我们还专门整理了本书的课件以及本书习题的全部答案，可在清华大学出版社网站(www. tup. com. cn)下载。

本书由郭亚军整体规划和统稿，郭亚军编写了第 1、2、3、4 章，宋建华编写了第 6、7、9、10 章，李莉编写了第 5、8 章。本书在编写过程中参考了国内外许多文献和书籍，在此，编者对原作者表示真诚的感谢！

在本书的编写过程中得到了许多同行的热情帮助和支持，得到了清华大学出版社编辑们的关心和帮助，在此一并表示衷心的谢意。

由于作者水平有限，书中难免有不足之处，敬请读者提出宝贵意见。

作　者

2008 年 7 月

目　录

第 1 章　引言 …… 1

1.1　安全攻击 …… 2

1.2　安全机制 …… 3

1.3　安全目标与安全需求 …… 4

1.4　安全服务模型 …… 5

1.4.1　支撑服务 …… 5

1.4.2　预防服务 …… 6

1.4.3　检测与恢复服务 …… 6

1.5　安全目标、安全需求、安全服务和安全机制之间的关系 …… 7

1.6　网络安全模型 …… 8

1.7　网络安全协议 …… 9

1.8　关键术语 …… 10

1.9　习题 1 …… 11

第 2 章　数学基础 …… 12

2.1　数论 …… 12

2.1.1　因子 …… 12

2.1.2　素数 …… 14

2.1.3　同余与模运算 …… 15

2.1.4　费马定理和欧拉定理 …… 20

2.1.5　素性测试 …… 21

2.1.6　中国剩余定理 …… 22

2.1.7　离散对数 …… 22

2.1.8　二次剩余 …… 24

2.2　代数基础 …… 24

2.2.1　群和环 …… 25

2.2.2　域和有限域 …… 26

2.3　计算复杂性理论 …… 29

2.3.1 问题的复杂性 …… 29
2.3.2 算法的复杂性 …… 30
2.4 单向函数 …… 31
2.5 关键术语 …… 32
2.6 习题2 …… 33

第3章 对称密码技术 …… 35
3.1 基本概念 …… 36
3.2 对称密码模型 …… 36
3.3 密码攻击 …… 37
3.3.1 穷举攻击 …… 37
3.3.2 密码攻击类型 …… 38
3.3.3 密码分析方法 …… 39
3.4 古典加密技术 …… 40
3.4.1 单表代换密码 …… 40
3.4.2 多表代换密码 …… 45
3.4.3 多字母代换密码 …… 47
3.4.4 置换密码 …… 50
3.5 数据加密标准 …… 51
3.5.1 DES加密过程 …… 51
3.5.2 DES子密钥产生 …… 55
3.5.3 DES解密 …… 57
3.5.4 DES的强度 …… 57
3.5.5 三重DES …… 58
3.6 高级加密标准 …… 59
3.6.1 AES的基本运算 …… 59
3.6.2 AES加密 …… 62
3.6.3 字节代换 …… 64
3.6.4 行移位 …… 66
3.6.5 列混淆 …… 66
3.6.6 轮密钥加 …… 68
3.6.7 AES的密钥扩展 …… 68
3.6.8 AES解密算法 …… 70
3.6.9 等价的解密变换 …… 71
3.6.10 AES的安全性 …… 73
3.7 中国商用密码算法——SMS4 …… 73
3.7.1 SMS4加密 …… 73
3.7.2 密钥扩展算法 …… 75

3.7.3 SMS4 解密 …… 78
3.7.4 SMS4 的安全性 …… 78
3.8 RC6 …… 78
3.8.1 RC6 的加密和解密 …… 78
3.8.2 密钥扩展 …… 79
3.8.3 RC6 的安全性和灵活性 …… 81
3.9 流密码 …… 81
3.9.1 流密码基本原理 …… 81
3.9.2 密钥流产生器 …… 82
3.9.3 RC4 算法 …… 84
3.10 分组密码工作模式 …… 86
3.10.1 电子密码本模式 …… 86
3.10.2 密码分组链接模式 …… 87
3.10.3 密码反馈模式 …… 88
3.10.4 输出反馈模式 …… 89
3.10.5 计数器模式 …… 90
3.11 随机数的产生 …… 91
3.11.1 真随机数发生器 …… 92
3.11.2 伪随机数发生器 …… 92
3.12 对称密码的密钥分配 …… 96
3.12.1 密钥分配基本方法 …… 96
3.12.2 密钥的分层控制 …… 98
3.12.3 会话密钥的有效期 …… 98
3.12.4 无中心的密钥分配 …… 98
3.13 关键术语 …… 99
3.14 习题 3 …… 100

第 4 章 公钥密码技术 …… 103
4.1 公钥密码体制 …… 103
4.2 公钥密码分析 …… 105
4.3 RSA 密码 …… 106
4.3.1 算法描述 …… 106
4.3.2 RSA 算法的安全性 …… 107
4.4 ElGamal 密码 …… 109
4.5 椭圆曲线密码 …… 110
4.5.1 椭圆曲线的定义 …… 111
4.5.2 椭圆曲线运算规则 …… 112
4.5.3 椭圆曲线密码算法 …… 114

4.5.4 椭圆曲线密码的性能 …… 115
4.6 公钥分配 …… 116
4.7 利用公钥密码分配对称密钥 …… 119
4.8 Diffie-Hellman 密钥交换 …… 120
4.9 关键术语 …… 121
4.10 习题 4 …… 121

第 5 章 消息认证与数字签名 …… 123
5.1 认证 …… 123
5.2 消息认证码 …… 124
5.2.1 MAC 的安全要求 …… 126
5.2.2 基于 DES 的消息认证码 …… 127
5.3 Hash 函数 …… 128
5.3.1 散列函数的安全要求 …… 130
5.3.2 MD5 …… 132
5.3.3 SHA-512 …… 135
5.3.4 HMAC …… 139
5.4 数字签名 …… 141
5.4.1 数字签名的基本概念 …… 141
5.4.2 数字签名方案 …… 142
5.5 关键术语 …… 147
5.6 习题 5 …… 147

第 6 章 身份认证与访问控制 …… 148
6.1 身份认证 …… 149
6.1.1 身份认证的基本方法 …… 150
6.1.2 常用身份认证机制 …… 152
6.1.3 OpenID 和 OAuth 认证协议 …… 157
6.2 访问控制概述 …… 161
6.2.1 访问控制的基本概念 …… 161
6.2.2 访问控制技术 …… 162
6.2.3 访问控制原理 …… 163
6.3 自主访问控制 …… 164
6.4 强制访问控制 …… 165
6.5 基于角色的访问控制 …… 167
6.6 关键术语 …… 171
6.7 习题 6 …… 171

试读结束：需要全本请在线购买： www.ertongbook.com

第 7 章　网络安全协议 …… 173
7.1　简单的安全认证协议 …… 174
7.1.1　Needham-Schroeder 认证协议 …… 174
7.1.2　Otway-Rees 协议 …… 176
7.2　Kerberos 协议 …… 177
7.2.1　Kerberos 概述 …… 177
7.2.2　Kerberos 协议的工作过程 …… 178
7.3　SSL 协议 …… 179
7.3.1　SSL 协议概述 …… 179
7.3.2　SSL 记录协议 …… 180
7.3.3　SSL 修改密文规约协议 …… 181
7.3.4　SSL 告警协议 …… 181
7.3.5　SSL 握手协议 …… 181
7.3.6　TLS 协议 …… 184
7.3.7　SSL 协议应用 …… 184
7.4　IPSec 协议 …… 185
7.4.1　IPSec 安全体系结构 …… 186
7.4.2　AH 协议 …… 188
7.4.3　ESP 协议 …… 190
7.4.4　IKE 协议 …… 192
7.5　PGP …… 195
7.5.1　鉴别 …… 195
7.5.2　机密性 …… 197
7.5.3　鉴别与机密性 …… 197
7.5.4　压缩 …… 197
7.5.5　E-mail 兼容性 …… 198
7.5.6　分段与重组 …… 198
7.5.7　PGP 密钥管理 …… 198
7.6　关键术语 …… 199
7.7　习题 7 …… 199

第 8 章　公钥基础设施 …… 200
8.1　理论基础 …… 200
8.1.1　网络安全服务 …… 201
8.1.2　密码技术 …… 202
8.2　PKI 的组成 …… 204
8.2.1　认证机构 …… 205
8.2.2　证书和证书库 …… 206

8.2.3 证书撤销 …… 207
8.2.4 密钥备份和恢复 …… 208
8.2.5 PKI应用接口 …… 209
8.3 PKI的功能 …… 209
8.3.1 证书的管理 …… 209
8.3.2 密钥的管理 …… 210
8.3.3 交叉认证 …… 211
8.3.4 安全服务 …… 212
8.4 信任模型 …… 214
8.4.1 认证机构的严格层次结构模型 …… 214
8.4.2 分布式信任结构模型 …… 215
8.4.3 Web模型 …… 216
8.4.4 以用户为中心的信任模型 …… 217
8.5 PKI的相关标准 …… 217
8.5.1 X.209 ASN.1基本编码规则 …… 217
8.5.2 X.500 …… 217
8.5.3 X.509 …… 219
8.5.4 PKCS系列标准 …… 223
8.5.5 轻量级目录访问协议 …… 223
8.6 PKI的应用与发展 …… 225
8.6.1 PKI的应用 …… 225
8.6.2 PKI的发展 …… 226
8.7 关键术语 …… 227
8.8 习题8 …… 228

第9章 防火墙 …… 229
9.1 防火墙概述 …… 229
9.1.1 防火墙的基本概念 …… 229
9.1.2 防火墙的作用及局限性 …… 231
9.1.3 防火墙的分类 …… 232
9.2 防火墙技术 …… 235
9.2.1 数据包过滤 …… 235
9.2.2 应用级网关 …… 237
9.2.3 电路级网关 …… 238
9.3 防火墙的体系结构 …… 239
9.3.1 双宿主机防火墙 …… 239
9.3.2 屏蔽主机防火墙 …… 239
9.3.3 屏蔽子网防火墙 …… 240

9.4 关键术语 …… 242
9.5 习题 9 …… 242

第 10 章 入侵检测 …… 243
10.1 入侵检测概述 …… 244
10.1.1 入侵检测基本概念 …… 244
10.1.2 入侵检测系统基本模型 …… 245
10.2 入侵检测系统分类 …… 248
10.2.1 基于主机的入侵检测系统 …… 249
10.2.2 基于网络的入侵检测系统 …… 251
10.2.3 分布式入侵检测系统 …… 252
10.3 入侵检测系统分析技术 …… 253
10.3.1 异常检测技术 …… 253
10.3.2 误用检测技术 …… 255
10.4 入侵防御系统 …… 257
10.4.1 入侵防御系统的基本概念 …… 257
10.4.2 入侵防御系统的分类 …… 258
10.4.3 入侵防御系统的原理 …… 259
10.4.4 入侵防御系统的技术特征 …… 260
10.4.5 入侵防御系统的发展 …… 260
10.5 关键术语 …… 261
10.6 习题 10 …… 261

第 11 章 恶意代码 …… 263
11.1 计算机病毒 …… 263
11.1.1 计算机病毒的起源与发展 …… 263
11.1.2 计算机病毒的特征 …… 264
11.1.3 计算机病毒的分类 …… 265
11.1.4 计算机病毒的结构和原理 …… 266
11.2 蠕虫病毒 …… 267
11.2.1 蠕虫病毒与一般计算机病毒的异同 …… 267
11.2.2 蠕虫病毒的工作原理 …… 268
11.2.3 典型蠕虫病毒介绍 …… 269
11.2.4 蠕虫病毒的发展与防治 …… 270
11.3 特洛伊木马 …… 271
11.3.1 木马的特征 …… 271
11.3.2 木马的工作原理 …… 272
11.3.3 木马的分类 …… 273

11.4 恶意代码的防治对策 …… 273
11.4.1 计算机病毒的防治 …… 273
11.4.2 其他恶意代码的防治 …… 275
11.5 关键术语 …… 276
11.6 习题11 …… 277

第12章 无线网络安全 …… 278
12.1 无线网络基础 …… 278
12.1.1 无线网络的分类 …… 279
12.1.2 无线局域网常用术语 …… 280
12.1.3 无线局域网常用标准 …… 280
12.2 无线网络面临的安全威胁 …… 280
12.3 无线网络安全解决方案 …… 282
12.3.1 无线局域网的安全性 …… 282
12.3.2 无线局域网的其他安全措施 …… 286
12.3.3 无线城域网的安全性 …… 287
12.3.4 无线广域网的安全性 …… 289
12.4 关键术语 …… 290
12.5 习题12 …… 290

参考文献 …… 291

第1章 引 言

本章导读

- 本章主要介绍安全攻击、安全机制、安全服务、安全需求和安全目标，以及它们之间的关系。最后介绍了信息安全模型以及网络安全协议。
- 安全攻击分为被动攻击和主动攻击。被动攻击的目的是获得传输的信息，不对信息做任何改动；主动攻击则旨在篡改或者伪造信息。
- 安全机制是阻止安全攻击，并对系统进行恢复的机制。
- 安全服务是加强数据处理系统和信息传输的安全性的一种服务，安全服务可利用一种或多种安全机制来阻止安全攻击。
- 实现用户所有的安全要求也就达到了用户的安全目标；不同的安全服务的联合能够实现不同的安全需求。
- 安全问题主要存在于网络传输过程中，以及对信息系统的访问中，本章给出了这两类安全模型。
- TCP/IP 参考模型的安全性是通过在各层增加一些安全协议来实现的。

近十年来，信息技术和信息产业得到了快速发展，与信息技术相关的各个学科和产业（如微电子、通信、计算机科学与工程等）受到各国政府、企业界和学术界的高度重视。现代信息系统的形式多种多样，除了我们日常生活必需的信息以外，还包括一些十分重要的信息，如政府或企业高度机密的信息、机构和个人的产权信息等。如果信息系统受到攻击致使系统瘫痪甚至崩溃，或者某些重要信息被泄露进而被利用，则会造成很大损失。

Internet 的发展使用户之间的信息交换越来越方便，同时也使恶意攻击越来越容易。从国家计算机网络应急技术处理协调中心（CNCERT/CC）2006 年的网络安全工作报告中可以发现，每年出现的安全事件越来越多。2004 年为 4485 件，2005 年为 9112 件，2006 年为 26 476 件。事件类型主要有网络仿冒、网页篡改、网页恶意代码、拒绝服务攻击、病毒、木马、蠕虫等。2006 年我国大陆地区约四万五千个 IP 地址的主机被植入木马；约一千多万个 IP 地址的主机被植入僵尸程序；中国大陆地区被篡改网站总数达到 24 477 个。现在的攻击具有一些更可怕特征，如发动攻击所需要的技能越来越低，检测攻击越来越复杂，攻击的破坏性也越来越大。因此，需要大量的技术和工具来抵抗这些攻击。

信息安全主要研究能够抵抗各种攻击的技术。在过去的几十年里，信息安全经历了几个阶段，每个阶段的侧重点不同，但本质一致。在计算机出现之前，主要靠物理安全和管理政策保护信息的安全性。在这个阶段，信息安全的主要目标是研究如何对信息保密。在计算机出现后，信息安全的主要目标则是研究计算机安全，即研究如何用一些工具来保护计算机系统自身的安全，保护计算机中的数据并阻止黑客攻击。国际标准化组织 ISO 将计算机安全定义为数据处理系统建立和采用的技术上和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。在计算机网络出现以后，信息在传

输、处理、存储时都存在安全问题,这个阶段的一个主要研究重点是网络安全,即如何保护数据在传输过程中的安全。在这个阶段,对信息安全的研究涉及传输网络、计算机系统、数据的安全保护。实际上,信息安全、网络安全以及计算机安全这些概念之间的区别已经越来越模糊。本书侧重讨论阻止、防止、检测和纠正信息传输中出现安全问题的措施。在讨论之前,先要了解"安全"的真正含义。"安全"的基本含义为"远离有危害的状态或特性"或"主观上不存在威胁、主观上不存在恐惧"。Bruce Schneier 的一段话形象地说明了安全的本质,"如果把一封信锁在保险柜中,把保险柜藏在纽约的某个地方,然后告诉你去看这封信,这并不是安全,而是隐藏;相反,如果把一封信锁在保险柜中,然后把保险柜及其设计规范和许多同样的保险柜给你,以便你和世界上最好的开保险柜的专家能够研究锁的装置,而你还是无法打开保险柜去读这封信,这才是安全……"中国的《孙子兵法》同样给出了安全的最本质含义。"用兵之法:无恃其不来,恃吾有以待也;无恃其不攻,恃吾有所不可攻也。"信息安全研究的最终目标是保证信息系统具有这样的安全性。

为了更好地理解信息安全的原理与技术,本章首先介绍一些重要概念,它们是安全攻击、安全机制、安全目标与安全需求、安全服务模型,然后给出它们之间的关系。最后介绍网络安全模型以及安全体系结构。

1.1 安全攻击

信息在存储、共享和传输中,可能会被非法窃听、截取、篡改和破坏,这些危及信息系统安全的活动称为安全攻击。安全攻击分为被动攻击和主动攻击。被动攻击的特征是对传输进行窃听和监测。被动攻击的目的是获得传输的信息,不对信息做任何改动,如消息内容的泄露和流量分析等。在受到被动攻击时,系统的操作和状态不会改变,因此被动攻击主要威胁信息的保密性。主动攻击则旨在篡改或者伪造信息,也可以是改变系统的状态和操作,因此主动攻击主要威胁信息的完整性、可用性和真实性。常见的主动攻击包括伪装、篡改、重放和拒绝服务。

下面是一些常见的安全攻击。

- 消息内容的泄露:消息的内容被泄露或透露给某个非授权的实体。攻击者用各种可能的合法的或非法的手段窃取系统中的信息资源和敏感信息。例如,对通信线路中传输的信号搭线监听,或者利用通信设备在工作过程中产生的电磁泄露截取有价值的信息或者利用网络嗅探器窃听网络数据包。
- 流量分析(Traffic Analysis):通过对系统进行长期监听,利用统计分析方法对诸如通信双方的标识、通信频度、消息格式、通信的信息流向、通信总量的变化等参数进行研究。从中发现有价值的信息和规律。在流量分析过程中,攻击者虽然不能获得消息的内容,但攻击者通过分析数据从哪里来到哪里去、传送多长时间、什么时候发送、发送频繁程度以及是否与其他事件有关联等信息可以判断通信的性质。
- 篡改:指对合法用户之间的通信消息进行修改或者改变消息的顺序。
- 伪装:指一个实体冒充另一个实体,通常攻击者通过欺骗通信系统(或用户)冒充成为合法用户,或者特权小的攻击者冒充成为特权大的用户。黑客大多采用的是伪装攻击。

试读结束:需要全本请在线购买: www.ertongbook.com