

Elementary

723025

Text not  
completed

# Information Security

SECOND  
EDITION

Richard E. Smith



JONES & BARTLETT  
LEARNING



100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

100-101101-1

# CONTENTS

Preface xvii

## Chapter 1 Security From The Ground Up 1

### 1.1 The Security Landscape 1

#### 1.1.1 Making Security Decisions 3

#### 1.1.2 Framework for Risk Management 5

### 1.2 Assessing Risks 8

#### 1.2.1 The Proprietor's Risk Management Framework 11

#### 1.2.2 Goals and Assets 14

#### 1.2.3 Security Boundaries 15

#### 1.2.4 Security Architecture 18

### 1.3 Identifying Risks 19

#### 1.3.1 Threat Agents 20

#### 1.3.2 Potential Attacks 26

#### 1.3.3 Risk Matrix 29

### 1.4 Prioritizing Risks 32

### 1.5 Drafting Security Requirements 35

#### 1.5.1 Analyzing Alice's Risks 37

#### 1.5.2 Monitoring Security Measures 39

### 1.6 Ethical Issues in Security Analysis 41

#### 1.6.1 Searching for Vulnerabilities 42

#### 1.6.2 Sharing and Publishing Cyber Vulnerabilities 43

### 1.7 Resources 45

#### 1.7.1 Review Questions 46

#### 1.7.2 Exercises 47

<b>Chapter 2</b>	<b>Controlling a Computer</b>	<b>49</b>
2.1	Computers and Programs	49
2.1.1	Input/Output	51
2.1.2	Program Execution	54
2.1.3	Procedures	56
2.2	Programs and Processes	57
2.2.1	Switching Between Processes	59
2.2.2	The Operating System	60
2.3	Buffer Overflows and the Morris Worm	62
2.3.1	The “Finger” Overflow	62
2.3.2	Security Alerts	66
2.3.3	Studying Cyberattacks	67
2.4	Access Control Strategies	71
2.4.1	Puzzles and Patterns	72
2.4.2	Chain of Control: Another Basic Principle	75
2.5	Keeping Processes Separate	77
2.5.1	Sharing a Program	79
2.5.2	Sharing Data	81
2.6	Selecting Security Controls	83
2.7	Security Plan: Process Protection	86
2.8	Resources	91
2.8.1	Review Questions	92
2.8.2	Exercises	93
<b>Chapter 3</b>	<b>Controlling Files</b>	<b>95</b>
3.1	The File System	95
3.1.1	File Ownership and Access Rights	97
3.1.2	Directory Access Rights	99
3.2	Executable Files	101
3.2.1	Execution Access Rights	102
3.2.2	Computer Viruses	103
3.2.3	Macro Viruses	106
3.2.4	Modern Malware: A Rogue’s Gallery	107

3.3	Sharing and Protecting Files	110
3.3.1	Security Policies for Sharing and Protection	112
3.4	Security Controls for Files	115
3.4.1	Deny by Default: A Basic Principle	116
3.4.2	Managing Access Rights	117
3.5	File Security Controls	119
3.5.1	File Permission Flags	121
3.5.2	Security Controls to Enforce the Isolation Policy	123
3.5.3	States and State Diagrams	123
3.6	Patching Security Flaws	125
3.7	Resources	129
3.7.1	Review Questions	129
3.7.2	Exercises	130
Chapter 4	Sharing Files	133
4.1	Controlled Sharing	133
4.1.1	Basic File Sharing on Windows	135
4.1.2	User Groups	136
4.1.3	Least Privilege and Administrative Users	139
4.2	File Permission Flags	142
4.2.1	Permission Flags and Ambiguities	143
4.2.2	Permission Flag Examples	144
4.3	Access Control Lists and OS X	146
4.4	Microsoft Windows ACLs	150
4.4.1	Denying Access	151
4.4.2	Default File Protection	154
4.4.3	A Different Trojan Horse	156
4.5	Monitoring Cyber System Security	159
4.5.1	Logging Events	161
4.5.2	External Security Requirements	164
4.6	Resources	167
4.6.1	Review Questions	167
4.6.2	Exercises	168

<b>Chapter 5</b>	<b>Storing Files</b>	<b>171</b>
5.1	Incident Response and Attack	171
5.1.1	The Aftermath of an Incident	173
5.1.2	Legal Disputes	174
5.2	Digital Evidence	175
5.2.1	Collecting Legal Evidence	177
5.2.2	Digital Evidence Procedures	178
5.3	Storing Data on a Hard Drive	179
5.3.1	Hard Drive Controller	183
5.3.2	Hard Drive Formatting	184
5.4	Common Drive Concepts	186
5.4.1	Error Detection and Correction	187
5.4.2	Drive Partitions	189
5.4.3	Memory Sizes and Address Variables	192
5.5	FAT: An Example File System	195
5.5.1	Boot Blocks	196
5.5.2	Building Files from Clusters	197
5.5.3	FAT Directories	200
5.6	Modern File Systems	201
5.6.1	Unix File System	203
5.6.2	Apple's HFS Plus	205
5.6.3	Microsoft's NTFS	206
5.7	Input/Output and File System Software	207
5.7.1	Software Layering	210
5.7.2	A Typical I/O Operation	213
5.7.3	Security and I/O	215
5.8	Resources	216
5.8.1	Review Questions	217
5.8.2	Exercises	218

**Chapter 6 Authenticating People 221****6.1 Unlocking a Door 221**

6.1.1 Authentication Factors 223

6.1.2 Threat Agents and Risks 225

6.1.3 Database Thefts 229

**6.2 Evolution of Password Systems 231**

6.2.1 One-Way Hash Functions 234

6.2.2 Sniffing Credentials 236

**6.3 Password Guessing 238**

6.3.1 Password Search Space 240

6.3.2 Truly Random Password Selection 242

6.3.3 Cracking Speeds 244

**6.4 Attacks on Password Bias 245**

6.4.1 Biased Choices and Average Attack Space 246

6.4.2 Estimating Language-Based Password Bias 250

**6.5 Authentication Tokens 251**

6.5.1 Challenge-Response Authentication 253

6.5.2 One-Time Password Tokens 257

6.5.3 Token Vulnerabilities 260

**6.6 Biometric Authentication 261**

6.6.1 Biometric Accuracy 262

6.6.2 Biometric Vulnerabilities 264

**6.7 Authentication Policy 265**

6.7.1 Weak and Strong Threats 265

6.7.2 Policies for Weak Threat Environments 267

6.7.3 Policies for Strong and Extreme Threats 268

6.7.4 Password Selection and Handling 271

**6.8 Resources 274**

6.8.1 Review Questions 274

6.8.2 Exercises 275

<b>Chapter 7</b>	<b>Encrypting Files</b>	<b>279</b>
7.1	Protecting the Accessible	279
7.1.1	The Encrypted Diary	280
7.1.2	Encryption Basics	281
7.1.3	Encryption and Information States	284
7.2	Encryption and Cryptanalysis	286
7.2.1	The Vigenère Cipher	287
7.2.2	Electromechanical Encryption	289
7.3	Computer-Based Encryption	291
7.3.1	Exclusive Or: A Crypto Building Block	293
7.3.2	Stream Ciphers: Another Building Block	295
7.3.3	Key Stream Security	298
7.3.4	The One-Time Pad	299
7.4	File Encryption Software	302
7.4.1	Built-In File Encryption	302
7.4.2	Encryption Application Programs	304
7.4.3	Erasing a Plaintext File	306
7.4.4	Choosing a File Encryption Program	308
7.5	Digital Rights Management	310
7.6	Resources	313
7.6.1	Review Questions	314
7.6.2	Exercises	314
<b>Chapter 8</b>	<b>Secret and Public Keys</b>	<b>317</b>
8.1	The Key Management Challenge	317
8.1.1	Rekeying	319
8.1.2	Using Text for Encryption Keys	321
8.1.3	Key Strength	323
8.2	The Reused Key Stream Problem	325
8.2.1	Avoiding Reused Keys	327
8.2.2	Key Wrapping: Another Building Block	330
8.2.3	Separation of Duty: A Basic Principle	333
8.2.4	DVD Key Handling	335



8.3	Public-Key Cryptography	336
8.3.1	Sharing a Secret: Diffie-Hellman	340
8.3.2	Diffie-Hellman: The Basics of the Math	341
8.3.3	Elliptic Curve Cryptography	343
8.4	RSA: Rivest-Shamir-Adleman	344
8.4.1	Encapsulating Keys with RSA	345
8.4.2	An Overview of RSA Mathematics	347
8.5	Data Integrity and Digital Signatures	351
8.5.1	Detecting Malicious Changes	352
8.5.2	Detecting a Changed Hash Value	355
8.5.3	Digital Signatures	356
8.6	Publishing Public Keys	359
8.6.1	Public-Key Certificates	360
8.6.2	Chains of Certificates	362
8.6.3	Authenticated Software Updates	367
8.7	Resources	369
8.7.1	Review Questions	370
8.7.2	Exercises	370
Chapter 9	Encrypting Volumes	373
9.1	Securing a Volume	373
9.1.1	Risks to Volumes	374
9.1.2	Risks and Policy Trade-Offs	376
9.2	Block Ciphers	379
9.2.1	Evolution of DES and AES	382
9.2.2	The RC4 Story	385
9.2.3	Qualities of Good Encryption Algorithms	387
9.3	Block Cipher Modes	389
9.3.1	Stream Cipher Modes	392
9.3.2	Cipher Feedback Mode	396
9.3.3	Cipher Block Chaining	397

9.4	Encrypting a Volume	399
9.4.1	Volume Encryption in Software	400
9.4.2	Block Modes for Volume Encryption	402
9.4.3	A "Tweakable" Encryption Mode	406
9.4.4	Residual Risks	407
9.5	Encryption in Hardware	409
9.5.1	The Drive Controller	410
9.5.2	Drive Locking and Unlocking	412
9.6	Managing Encryption Keys	413
9.6.1	Key Storage	414
9.6.2	Bootting an Encrypted Drive	416
9.6.3	Residual Risks to Keys	418
9.7	Resources	421
9.7.1	Review Questions	422
9.7.2	Exercises	422
<b>Chapter 10 Connecting Computers 425</b>		
10.1	The Network Security Problem	425
10.1.1	Basic Network Attacks and Defenses	426
10.1.2	Physical Network Protection	428
10.1.3	Host and Network Integrity	429
10.2	Transmitting Data	432
10.2.1	Message Switching	435
10.2.2	Circuit Switching	435
10.2.3	Packet Switching	438
10.3	Putting Bits on a Wire	440
10.3.1	Wireless Transmission	442
10.3.2	Transmitting Packets	444
10.3.3	Recovering a Lost Packe	447
10.4	Ethernet: A Modern LAN	448
10.4.1	Wiring a Small Network	450
10.4.2	Ethernet Frame Format	451
10.4.3	Finding Host Addresses	453
10.4.4	Handling Collisions	455

10.5	The Protocol Stack	457
10.5.1	Relationships Between Layers	459
10.5.2	The OSI Protocol Model	460
10.6	Network Applications	462
10.6.1	Resource Sharing	464
10.6.2	Data and File Sharing	465
10.7	Resources	468
10.7.1	Review Questions	469
10.7.2	Exercises	469
Chapter 11	Networks of Networks	471
11.1	Building Data Networks	471
11.1.1	Point-to-Point Network	473
11.1.2	Star Network	474
11.1.3	Bus Network	476
11.1.4	Tree Network	477
11.1.5	Mesh	480
11.2	Combining Computer Networks	481
11.2.1	Hopping Between Networks	483
11.2.2	Evolution of Internet Security	485
11.2.3	Internet Structure	488
11.3	Talking between Hosts	491
11.3.1	IP Addresses	493
11.3.2	IP Packet Format	494
11.3.3	Address Resolution Protocol	495
11.4	Internet Addresses in Practice	497
11.4.1	Addresses, Scope, and Reachability	498
11.4.2	Private IP Addresses	499
11.5	Network Inspection Tools	502
11.5.1	Wireshark Examples	503
11.5.2	Mapping a LAN with Nmap	505

**11.6 Resources 508**

11.6.1 Review Questions 509

11.6.2 Exercises 510

**Chapter 12 End-to-End Networking 513****12.1 “Smart” Versus “Dumb” Networks 513****12.2 Internet Transport Protocols 514**

12.2.1 Transmission Control Protocol 516

12.2.2 Attacks on Protocols 520

**12.3 Names on the Internet 523**

12.3.1 Domain Names in Practice 525

12.3.2 Looking Up Names 526

12.3.3 DNS Protocol 528

12.3.4 Investigating Domain Names 531

12.3.5 Attacking DNS 531

**12.4 Internet Gateways and Firewalls 535**

12.4.1 Network Address Translation 536

12.4.2 Filtering and Connectivity 540

12.4.3 Software-Based Firewalls 541

**12.5 Long-Distance Networking 542**

12.5.1 Older Technologies 544

12.5.2 Mature Technologies 548

12.5.3 Evolving Technologies 549

**12.6 Resources 549**

12.6.1 Review Questions 550

12.6.2 Exercises 551

**Chapter 13 Enterprise Computing 555****13.1 The Challenge of Community 555**

13.1.1 Companies and Information Control 556

13.1.2 Enterprise Risks 559

13.1.3 Social Engineering 562



<b>13.2</b>	<b>Management Processes</b>	<b>563</b>
13.2.1	Security Management Standards	564
13.2.2	Deployment Policy Directives	566
13.2.3	Management Hierarchies and Delegation	567
13.2.4	Managing Information Resources	569
13.2.5	Security Audits	570
13.2.6	Information Security Professionals	572
<b>13.3</b>	<b>Enterprise Issues</b>	<b>575</b>
13.3.1	Personnel Security	576
13.3.2	Physical Security	579
13.3.3	Software Security	582
<b>13.4</b>	<b>Enterprise Network Authentication</b>	<b>585</b>
13.4.1	Direct Authentication	588
13.4.2	Indirect Authentication	590
13.4.3	Off-Line Authentication	593
<b>13.5</b>	<b>Contingency Planning</b>	<b>595</b>
13.5.1	Data Backup and Restoration	595
13.5.2	Handling Serious Incidents	598
13.5.3	Disaster Preparation and Recovery	600
<b>13.6</b>	<b>Resources</b>	<b>602</b>
13.6.1	Review Questions	603
13.6.2	Exercises	604
<b>Chapter 14</b>	<b>Network Encryption</b>	<b>605</b>
<b>14.1</b>	<b>Communications Security</b>	<b>605</b>
14.1.1	Crypto by Layers	608
14.1.2	Administrative and Policy Issues	613
<b>14.2</b>	<b>Crypto Keys on a Network</b>	<b>615</b>
14.2.1	Manual Keying: A Building Block	618
14.2.2	Simple Rekeying	619
14.2.3	Secret-Key Building Blocks	621
14.2.4	Public-Key Building Blocks	624
14.2.5	Public-Key Versus Secret-Key Exchanges	626

14.3	Crypto Atop the Protocol Stack	628
14.3.1	Transport Layer Security—SSL and TLS	630
14.3.2	SSL Handshake Protocol	632
14.3.3	SSL Record Transmission	634
14.4	Network Layer Cryptography	636
14.4.1	The Encapsulating Security Payload	639
14.4.2	Implementing a VPN	641
14.4.3	Internet Key Exchange Protocol	642
14.5	Link Encryption on 802.11 Wireless	643
14.5.1	Wireless Packet Protection	645
14.5.2	Security Associations	648
14.6	Cryptographic Security Requirements	649
14.7	Resources	652
14.7.1	Review Questions	653
14.7.2	Exercises	654
<hr/>		
Chapter 15	Internet Services and Email	657
15.1	Internet Services	657
15.2	Internet Email	658
15.2.1	Email Protocol Standards	663
15.2.2	Tracking an Email	665
15.2.3	Forging an Email Message	668
15.3	Email Security Problems	671
15.3.1	Spam	672
15.3.2	Phishing	675
15.3.3	Email Viruses and Hoaxes	677
15.4	Enterprise Firewalls	680
15.4.1	Controlling Internet Traffic	681
15.4.2	Traffic-Filtering Mechanisms	683
15.4.3	Implementing Firewall Rules	685
15.5	Enterprise Point of Presence	689
15.5.1	POP Topology	690
15.5.2	Attacking an Enterprise Site	693
15.5.3	The Challenge of Real-Time Media	695

**15.6 Resources 696**

15.6.1 Review Questions 696

15.6.2 Exercises 697

**Chapter 16 The World Wide Web 699****16.1 Hypertext Fundamentals 699**

16.1.1 Addressing Web Pages 703

16.1.2 Retrieving a Static Web Page 706

**16.2 Basic Web Security 709**

16.2.1 Static Website Security 712

16.2.2 Server Authentication 714

16.2.3 Server Masquerades 719

**16.3 Dynamic Websites 723**

16.3.1 Scripts on the Web 724

16.3.2 States and HTTP 728

**16.4 Content Management Systems 730**

16.4.1 Database Management Systems 732

16.4.2 Password Checking: A CMS Example 734

16.4.3 Command Injection Attacks 736

**16.5 Ensuring Web Security Properties 740**

16.5.1 Web Availability 741

16.5.2 Web Privacy 743

**16.6 Resources 745**

16.6.1 Review Questions 746

16.6.2 Exercises 747

**Chapter 17 Governments and Secrecy 749****17.1 Secrecy in Government 749**

17.1.1 The Challenge of Secrecy 751

17.1.2 Cybersecurity and Operations 754

**17.2 Classifications and Clearances 756**

17.2.1 Security Labeling 759

17.2.2 Security Clearances 761

17.2.3	Classification Levels in Practice	763
17.2.4	Compartments and Other Special Controls	764
17.3	National Policy Issues	770
17.3.1	Facets of National System Security	772
17.3.2	Security Planning	774
17.4	Communications Security	775
17.4.1	Cryptographic Technology	777
17.4.2	Crypto Security Procedures	779
17.4.3	Transmission Security	782
17.5	Data Protection	784
17.5.1	Protected Wiring	786
17.5.2	TEMPEST	787
17.6	Trustworthy Systems	789
17.6.1	Integrity of Operations	792
17.6.2	Multilevel Security	795
17.6.3	Computer Modes of Operation	797
17.7	Resources	799
17.7.1	Review Questions	801
17.7.2	Exercises	801
Appendix A Acronyms		805
Appendix B Alternative Security Terms and Concepts		815
Index		823