

Contents

	Foreword	xix
	Preface	xxv
	Acknowledgments	xxxix
	About the Authors	xxxiii
Chapter 1	Introduction	1
	1.1 What Is Computer Security?	3
	<i>Values of Assets</i>	4
	<i>The Vulnerability–Threat–Control Paradigm</i>	5
	1.2 Threats	6
	<i>Confidentiality</i>	8
	<i>Integrity</i>	10
	<i>Availability</i>	11
	<i>Types of Threats</i>	13
	<i>Types of Attackers</i>	17
	1.3 Harm	24
	<i>Risk and Common Sense</i>	25
	<i>Method–Opportunity–Motive</i>	28
	1.4 Vulnerabilities	30
	1.5 Controls	30
	1.6 Conclusion	33
	1.7 What’s Next?	34
	1.8 Exercises	36

Chapter 2	Toolbox: Authentication, Access Control, and Cryptography	38
2.1	Authentication	40
	<i>Identification vs. Authentication</i>	40
	<i>Authentication Based on Phrases and Facts:</i>	
	<i>Something You Know</i>	42
	<i>Authentication Based on Biometrics: Something You Are</i>	57
	<i>Authentication Based on Tokens: Something You Have</i>	69
	<i>Federated Identity Management</i>	72
	<i>Multifactor Authentication</i>	74
	<i>Fitting Authentication to the Situation</i>	76
2.2	Access Control	78
	<i>Access Policies</i>	78
	<i>Implementing Access Control</i>	82
	<i>Procedure-Oriented Access Control</i>	92
	<i>Role-Based Access Control</i>	92
2.3	Cryptography	93
	<i>Problems Addressed by Encryption</i>	94
	<i>Terms and Concepts</i>	94
	<i>DES: The Data Encryption Standard</i>	104
	<i>AES: Advanced Encryption System</i>	106
	<i>Public Key Cryptography</i>	108
	<i>Using Public Key Cryptography to Exchange Secret Keys</i>	112
	<i>Error Detecting Codes</i>	117
	<i>Signatures</i>	122
	<i>Trust</i>	126
	<i>Certificates: Trustable Identities and Public Keys</i>	130
	<i>Digital Signatures—All the Pieces</i>	134
2.4	Conclusion	137
2.5	Exercises	138
Chapter 3	Programs and Programming	141
3.1	Unintentional (Nonmalicious) Programming Oversights	143
	<i>Buffer Overflow</i>	144
	<i>Incomplete Mediation</i>	163
	<i>Time-of-Check to Time-of-Use</i>	166
	<i>Undocumented Access Point</i>	168
	<i>Off-by-One Error</i>	171
	<i>Integer Overflow</i>	172

	<i>Unterminated Null-Terminated String</i>	173
	<i>Parameter Length, Type, and Number</i>	174
	<i>Unsafe Utility Program</i>	174
	<i>Race Condition</i>	175
	<i>Unsynchronized Activity</i>	175
3.2	Malicious Code—Malware	178
	<i>Malware—Viruses, Worms, and Trojan Horses</i>	179
	<i>Technical Details: Malicious Code</i>	188
3.3	Countermeasures	211
	<i>Countermeasures for Users</i>	212
	<i>Countermeasures for Developers</i>	217
	<i>Countermeasure Specifically for Security</i>	232
	<i>Countermeasures That Don't Work</i>	241
3.4	Conclusion	245
3.5	Exercises	245

Chapter 4 The Internet—User Side 248

4.1	Browser Attacks	251
	<i>Browser Attack Types</i>	251
	<i>How Browser Attacks Succeed: Failed Identification and Authentication</i>	258
4.2	Attacks Targeting Users	265
	<i>False or Misleading Content</i>	265
	<i>Malicious Web Content</i>	273
	<i>Protecting Against Malicious Webpages</i>	279
4.3	Obtaining User or Website Data	280
	<i>Code Within Data</i>	281
	<i>Website Data: A User's Problem Too</i>	285
	<i>Ransomware</i>	287
	<i>Foiling Data Attacks</i>	288
4.4	Mobile Apps	289
	<i>Apps and Security</i>	289
	<i>Threats to Mobile Computing</i>	293
	<i>Vulnerabilities from Using Apps</i>	294
	<i>Why Apps Have Flaws</i>	300
	<i>Finding Secure Apps</i>	303
	<i>Protecting Yourself After Installing an App</i>	305
	<i>Developing Secure Apps</i>	307

4.5	Email and Message Attacks	310
	<i>Fake Email</i>	310
	<i>Fake Email Messages as Spam</i>	311
	<i>Fake (Inaccurate) Email Header Data</i>	316
	<i>Phishing</i>	317
	<i>Protecting Against Email Attacks</i>	319
4.6	Conclusion	320
4.7	Exercises	321
Chapter 5	Operating Systems	323
5.1	Security in Operating Systems	323
	<i>Background: Operating System Structure</i>	324
	<i>Security Features of Ordinary Operating Systems</i>	325
	<i>A Bit of History</i>	327
	<i>Protected Objects</i>	329
	<i>Operating System Tools to Implement Security Functions</i>	334
5.2	Security in the Design of Operating Systems	351
	<i>Simplicity of Design</i>	352
	<i>Layered Design</i>	353
	<i>Kernelized Design</i>	355
	<i>Reference Monitor</i>	356
	<i>Correctness and Completeness</i>	357
	<i>Secure Design Principles</i>	358
	<i>Trusted Systems</i>	359
5.3	Rootkits	371
	<i>Example: Phone Rootkits</i>	371
	<i>Rootkit Characteristics</i>	372
	<i>Rootkit Case Studies</i>	378
	<i>Nonmalicious Rootkits</i>	381
5.4	Conclusion	382
5.5	Exercises	382
Chapter 6	Networks	385
6.1	Network Concepts	386
	<i>Background: Network Transmission Media</i>	387
	<i>Background: Protocol Layers</i>	395
	<i>Background: Addressing and Routing</i>	396
	Part I—War on Networks: Network Security Attacks	399
6.2	Threats to Network Communications	400
	<i>Interception: Eavesdropping and Wiretapping</i>	400

	<i>Modification: Data Corruption</i>	406
	<i>Interruption: Loss of Service</i>	411
	<i>Port Scanning</i>	415
	<i>Network Vulnerability Summary</i>	420
6.3	Wireless Network Security	421
	<i>WiFi Background</i>	421
	<i>Vulnerabilities in Wireless Networks</i>	428
	<i>Failed Countermeasure: WEP (Wired Equivalent Privacy)</i>	434
	<i>Stronger Protocol Suite: WPA (WiFi Protected Access)</i>	438
6.4	Denial of Service	443
	<i>Example: Massive Estonian Web Failure</i>	443
	<i>How Service Is Denied</i>	445
	<i>Flooding (Capacity) Attacks in Detail</i>	449
	<i>Network Flooding Caused by Malicious Code</i>	450
	<i>Network Flooding by Resource Exhaustion</i>	454
	<i>Denial of Service by Addressing Failures</i>	455
	<i>Traffic Redirection</i>	460
	<i>DNS Attacks</i>	460
	<i>Exploiting Known Vulnerabilities</i>	466
	<i>Physical Disconnection</i>	467
6.5	Distributed Denial of Service	468
	<i>Scripted Denial-of-Service Attacks</i>	471
	<i>Bots</i>	472
	<i>Botnets</i>	472
	<i>Malicious Autonomous Mobile Agents</i>	477
	<i>Autonomous Mobile Protective Agents</i>	477
	Part II—Strategic Defenses: Security Countermeasures	479
6.6	Cryptography in Network Security	479
	<i>Network Encryption</i>	479
	<i>Browser Encryption</i>	484
	<i>Onion Routing</i>	489
	<i>IP Security Protocol Suite (IPsec)</i>	491
	<i>Virtual Private Networks</i>	494
6.7	Firewalls	497
	<i>System Architecture</i>	498
	<i>What Is a Firewall?</i>	499
	<i>Design of Firewalls</i>	501
	<i>Types of Firewalls</i>	503
	<i>Personal Firewalls</i>	514
	<i>Comparison of Firewall Types</i>	516

	<i>Examples of Firewall Configurations</i>	516
	<i>Network Address Translation (NAT)</i>	521
6.8	Intrusion Detection and Prevention Systems	522
	<i>Types of IDSs</i>	524
	<i>Goals for Intrusion Detection Systems</i>	530
	<i>IDS Strengths and Limitations</i>	531
	<i>Intrusion Prevention Systems</i>	532
	<i>Intrusion Response</i>	533
6.9	Network Management	536
	<i>Management to Ensure Service</i>	537
	<i>Security Information and Event Management</i>	540
	<i>All-of-the-Above Products or Families</i>	542
6.10	Conclusion	545
6.11	Exercises	545
Chapter 7	Data and Databases	549
7.1	Introduction to Databases	550
	<i>Concept of a Database</i>	550
	<i>Components of Databases</i>	550
	<i>Advantages of Using Databases</i>	554
7.2	Security Requirements of Databases	555
	<i>Integrity of the Database</i>	555
	<i>Element Integrity</i>	556
	<i>Auditability</i>	559
	<i>Access Control</i>	559
	<i>User Authentication</i>	560
	<i>Availability</i>	560
	<i>Integrity/Confidentiality/Availability</i>	561
7.3	Reliability and Integrity	561
	<i>Protection Features from the Operating System</i>	562
	<i>Two-Phase Update</i>	562
	<i>Redundancy/Internal Consistency</i>	565
	<i>Recovery</i>	565
	<i>Concurrency/Consistency</i>	565
7.4	Database Disclosure	566
	<i>Sensitive Data</i>	567
	<i>Types of Disclosures</i>	568
	<i>Preventing Disclosure: Data Suppression and Modification</i>	578
	<i>Security versus Precision</i>	580

7.5	Data Mining and Big Data	585
	<i>Data Mining</i>	585
	<i>Big Data</i>	591
7.6	Conclusion	599
7.7	Exercises	599
Chapter 8	New Territory	601
8.1	Introduction	601
	<i>Cloud Computing</i>	603
	<i>The Internet of Things</i>	604
	<i>Embedded Systems</i>	605
8.2	Cloud Architectures and Their Security	605
	<i>Essential Characteristics</i>	606
	<i>Service Models</i>	608
	<i>Deployment Models</i>	611
	<i>Security in Cloud Computing</i>	611
	<i>Identity Management in the Cloud</i>	618
8.3	IoT and Embedded Devices	627
	<i>IoT and Security</i>	630
8.4	Cloud, IoT, and Embedded Devices—The Smart Home	638
	<i>Securing Smart Homes</i>	640
	<i>Security Practices and Controls in the Smart Home</i>	642
8.5	Smart Cities, IoT, Embedded Devices, and Cloud	643
	<i>Smart City Digital Architecture</i>	645
	<i>Security and the Smart City</i>	647
8.6	Cloud, IoT, and Critical Services	648
	<i>Healthcare</i>	648
	<i>Security and the Internet of Medical Things</i>	650
	<i>Utilities—Electricity and Water</i>	652
8.7	Conclusion	657
8.8	Exercises	658
Chapter 9	Privacy	659
9.1	Privacy Concepts	660
	<i>Aspects of Information Privacy</i>	660
	<i>Computer-Related Privacy Problems</i>	664
9.2	Privacy Principles and Policies	671
	<i>Fair Information Practices</i>	671
	<i>U.S. Privacy Laws</i>	672

	<i>Controls on U.S. Government Websites</i>	675
	<i>Controls on Commercial Websites</i>	676
	<i>Non-U.S. Privacy Principles</i>	679
	<i>Individual Actions to Protect Privacy</i>	682
	<i>Governments and Privacy</i>	684
	<i>Identity Theft</i>	687
9.3	Authentication and Privacy	688
	<i>What Authentication Means</i>	689
	<i>Conclusions</i>	693
9.4	Data Mining	694
	<i>Government Data Mining</i>	695
	<i>Privacy-Preserving Data Mining</i>	696
9.5	Privacy on the Internet	698
	<i>Understanding the Online Environment</i>	698
	<i>Payments on the Internet</i>	701
	<i>Site and Portal Registrations</i>	703
	<i>Whose Page Is This?</i>	704
	<i>Precautions for Web Surfing</i>	705
	<i>Spyware</i>	709
	<i>Shopping on the Internet</i>	712
9.6	Email and Message Security	713
	<i>Where Does Email Go, and Who Can Access It?</i>	713
	<i>Monitoring Email</i>	714
	<i>Anonymous, Pseudonymous, and Disappearing Email</i>	714
	<i>Spoofing and Spamming</i>	716
	<i>Summary</i>	716
9.7	Privacy Impacts of Newer Technologies	717
	<i>Radio Frequency Identification</i>	717
	<i>Electronic Voting</i>	721
	<i>Privacy in the Cloud</i>	722
	<i>Conclusions on Newer Technologies</i>	723
9.8	Conclusion	724
9.9	Exercises	725
Chapter 10	Management and Incidents	727
10.1	Security Planning	727
	<i>Organizations and Security Plans</i>	729
	<i>Contents of a Security Plan</i>	729

	<i>Security Planning Team Members</i>	736
	<i>Assuring Commitment to a Security Plan</i>	737
10.2	Business Continuity Planning	738
	<i>Assess Business Impact</i>	740
	<i>Develop Strategy</i>	740
	<i>Develop the Plan</i>	741
10.3	Handling Incidents	742
	<i>Incident Response Plans</i>	742
	<i>Incident Response Teams</i>	745
10.4	Risk Analysis	749
	<i>The Nature of Risk</i>	750
	<i>Steps of a Risk Analysis</i>	751
	<i>Arguments For and Against Risk Analysis</i>	765
10.5	Physical Threats to Systems	767
	<i>Natural Disasters</i>	767
	<i>Human Vandals</i>	769
	<i>Contingency Planning</i>	772
	<i>Physical Security Recap</i>	776
10.6	New Frontiers in Security Management	776
10.7	Conclusion	778
10.8	Exercises	779
Chapter 11	Legal Issues and Ethics	781
11.1	Protecting Programs and Data	783
	<i>Copyrights</i>	783
	<i>Patents</i>	792
	<i>Trade Secrets</i>	796
	<i>Special Cases</i>	798
11.2	Information and the Law	800
	<i>Information as an Object</i>	800
	<i>The Legal System</i>	802
	<i>Summary of Protection for Computer Artifacts</i>	805
11.3	Rights of Employees and Employers	805
	<i>Control of Products</i>	805
	<i>Employment Contracts</i>	808
11.4	Redress for Software Failures	808
	<i>Selling Correct Software</i>	809
	<i>Reporting Software Flaws</i>	811

11.5	Computer Crime	814
	<i>Examples of Statutes</i>	815
	<i>International Dimensions</i>	818
	<i>Why Computer Criminals Are Hard to Catch</i>	820
	<i>What Computer Crime Statutes Do Not Address</i>	821
	<i>Summary of Legal Issues in Computer Security</i>	821
11.6	Ethical Issues in Computer Security	822
	<i>Differences Between the Law and Ethics</i>	822
	<i>Studying Ethics</i>	824
	<i>Ethical Reasoning</i>	825
11.7	An Ethical Dive into Artificial Intelligence	828
	<i>AI's Meaning and Concerns</i>	828
	<i>IBM: A Study in How to Approach Ethical AI</i>	829
11.8	Incident Analyses with Ethics	830
	<i>Situation I: Use of Computer Services</i>	832
	<i>Situation II: Privacy Rights</i>	833
	<i>Situation III: Denial of Service</i>	835
	<i>Situation IV: Ownership of Programs</i>	836
	<i>Situation V: Proprietary Resources</i>	838
	<i>Situation VI: Fraud</i>	838
	<i>Situation VII: Accuracy of Information</i>	840
	<i>Situation VIII: Ethics of Hacking or Cracking</i>	841
	<i>Situation IX: True Representation</i>	844
	<i>Conclusion of Computer Ethics</i>	845
11.9	Conclusion	846
11.10	Exercises	847
Chapter 12	Details of Cryptography	850
12.1	Cryptology	851
	<i>Cryptanalysis</i>	851
	<i>Cryptographic Primitives</i>	856
	<i>One-Time Pads</i>	857
	<i>Statistical Analysis</i>	859
	<i>What Makes a "Secure" Encryption Algorithm?</i>	860
12.2	Symmetric Encryption Algorithms	863
	<i>DES</i>	863
	<i>Attacking Ciphertext</i>	871
	<i>AES</i>	874
	<i>Other Symmetric Algorithms</i>	876

12.3	Asymmetric Encryption	877
	<i>The RSA Algorithm</i>	877
	<i>Strength of the RSA Algorithm</i>	878
	<i>Elliptic Curve Cryptosystems</i>	881
	<i>Digression: Diffie–Hellman Key Exchange</i>	882
12.4	Message Digests	883
	<i>Hash Functions</i>	883
	<i>One-Way Hash Functions</i>	883
	<i>Message Digests</i>	884
	<i>Authenticated Encryption</i>	886
12.5	Digital Signatures	888
12.6	Quantum Key Distribution	889
	<i>Key Distribution</i>	889
	<i>Quantum Physics</i>	890
	<i>Implementation</i>	893
12.7	Conclusion	894

Chapter 13 Emerging Topics 895

13.1	AI and Cybersecurity	896
	<i>AI-Based Decision Making</i>	897
	<i>AI-Driven Security Management</i>	898
	<i>Adversarial AI</i>	903
	<i>Responsible AI</i>	905
	<i>Open Questions</i>	906
13.2	Blockchains and Cryptocurrencies	908
	<i>What Is a Blockchain?</i>	908
	<i>Commerce and Trust</i>	910
	<i>What Is Cryptocurrency?</i>	912
	<i>Cryptocurrency in the World Context</i>	915
	<i>Is the Implementation of Cryptocurrencies Secure?</i>	921
	<i>Open Questions</i>	924
13.3	Offensive Cyber and Cyberwarfare	924
	<i>What Is Cyberwarfare?</i>	924
	<i>Possible Examples of Cyberwarfare</i>	926
	<i>Cyberwar or Offensive Cyber?</i>	929
	<i>Critical Issues</i>	932

13.4	Quantum Computing and Computer Security	936
	<i>Quantum Computers</i>	936
	<i>Quantum-Resistant Cryptography</i>	937
13.5	Conclusion	937
	Bibliography	939
	Index	963