

Contents

PREFACE	xv
1 IS THERE A SECURITY PROBLEM IN COMPUTING?	1
1.1 Characteristics of Computer Intrusion	3
1.2 Kinds of Security Breaches	3
1.3 Security Goals and Vulnerabilities	4
<i>Security Goals, 4</i>	
<i>Vulnerabilities, 6</i>	
<i>Summary of Exposures, 11</i>	
1.4 The People Involved	11
<i>Amateurs, 12</i>	
<i>Crackers, 12</i>	
<i>Career Criminals, 13</i>	
1.5 Methods of Defense	13
<i>Controls, 13</i>	
<i>Effectiveness of Controls, 15</i>	
1.6 Plan of Attack	15
<i>Encryption, 16</i>	
<i>Hardware and Software Security, 16</i>	
<i>Human Controls in Security, 17</i>	
1.7 Summary	17
1.8 Bibliographic Notes	18
1.9 Terms and Concepts	18
1.10 Exercises	19

2	BASIC ENCRYPTION AND DECRYPTION	21
2.1	Terminology and Background	21
	<i>Terminology</i> , 22	
	<i>Representation of Characters</i> , 24	
2.2	Monoalphabetic Ciphers (Substitutions)	25
	<i>The Caesar Cipher</i> , 25	
	<i>Other Monoalphabetic Substitutions</i> , 27	
	<i>Cryptanalysis of Monoalphabetic Ciphers</i> , 28	
2.3	Polyalphabetic Substitution Ciphers	31
	<i>Vigenère Tableaux</i> , 33	
	<i>Cryptanalysis of Polyalphabetic Substitutions</i> , 35	
	<i>Concluding Remarks on Polyalphabetic Ciphers</i> , 40	
	<i>The “Perfect” Substitution Cipher</i> , 40	
	<i>Summary of Substitutions</i> , 46	
2.4	Transpositions (Permutations)	47
	<i>Columnar Transpositions</i> , 47	
	<i>Generalized Transpositions</i> , 53	
2.5	Fractionated Morse	53
	<i>Morse Code</i> , 53	
	<i>Morse Code for Encryption</i> , 54	
	<i>Cryptanalysis of Fractionated Morse</i> , 55	
2.6	Stream and Block Ciphers	55
2.7	Characteristics of “Good” Ciphers	58
	<i>Shannon Characteristics</i> , 58	
	<i>Confusion and Diffusion</i> , 59	
	<i>Information Theoretic Tests</i> , 59	
	<i>Unicity Distance</i> , 62	
2.8	What the Cryptanalyst Has to Work With	63
	<i>Ciphertext Only</i> , 63	
	<i>Full or Partial Plaintext</i> , 63	
	<i>Ciphertext of Any Plaintext</i> , 64	
	<i>Algorithm and Ciphertext</i> , 64	
2.9	Summary of Basic Encryption	64
2.10	Bibliographic Notes	65
2.11	Terms and Concepts	65
2.12	Exercises	66

3 SECURE ENCRYPTION SYSTEMS**69**

- 3.1 “Hard” Problems: Complexity 70
 - NP-Complete Problems, 71*
 - Characteristics of NP-Complete Problems, 72*
 - The Meaning of NP-Completeness, 75*
 - NP-Completeness and Cryptography, 76*
- 3.2 Properties of Arithmetic 77
 - Inverses, 77*
- 3.3 Public Key Encryption Systems 82
 - Motivation, 82*
- 3.4 Merkle–Hellman Knapsacks 83
 - Introduction to Merkle–Hellman Knapsacks, 83*
 - Detailed Explanation of the Merkle–Hellman Technique, 84*
 - The Encryption Technique, 85*
- 3.5 Rivest–Shamir–Adelman (RSA) Encryption 91
 - Introduction to the RSA Algorithm, 91*
 - Detailed Description of the Encryption Algorithm, 93*
- 3.6 El Gamal and Digital Signature Algorithms 96
 - El Gamal Algorithm, 96*
 - Digital Signature Algorithm, 96*
- 3.7 Hash Algorithms 97
 - Description of Hash Algorithms, 97*
 - Secure Hash Algorithm, 98*
- 3.8 Secure Secret Key (Symmetric) Systems 99
 - Advantages and Disadvantages, 100*
 - Problems of Symmetric Key Systems, 100*
- 3.9 The Data Encryption Standard (DES) 100
 - Background and History, 101*
 - Overview of the DES Algorithm, 103*
 - Details of the Encryption Algorithm, 103*
 - Decryption of the DES, 110*
 - Questions About the Security of the DES, 112*
 - Weaknesses of the DES, 114*
 - Security of the DES, 116*
- 3.10 Key Escrow and Clipper 118
 - The Clipper Program, 118*
 - Conclusions, 121*

- 3.11 Summary of Secure Encryption 122
- 3.12 Bibliographic Notes 122
- 3.13 Terms and Concepts 123
- 3.14 Exercises 124

4 USING ENCRYPTION: PROTOCOLS AND PRACTICES

126

- 4.1 Protocols: Orderly Behavior 126
 - Definition of Protocols, 126*
 - Kinds of Protocols, 127*
- 4.2 Protocols to Solve Problems 129
 - Key Distribution, 129*
 - Digital Signatures, 140*
 - Key Escrow, 145*
 - Mental Poker, 148*
 - Voting by Computer, 151*
 - Oblivious Transfer, 153*
 - Contract Signing, 155*
 - Certified Mail, 158*
- 4.3 How to Use Encryption 159
 - Amount of Secrecy, 160*
 - Key Management, 161*
 - Lost (Revealed) Keys, 161*
 - Complexity to Encrypt, 161*
 - Propagation of Errors, 162*
 - Size of Ciphertext, 163*
- 4.4 Enhancing Cryptographic Security 163
 - Error Prevention and Detection, 163*
 - One-Way Encryption, 166*
- 4.5 Modes of Encryption 169
 - Cipher Block Chain, 169*
 - Two Keys Give the Effect of a 112-Bit Key, 171*
- 4.6 Summary of Protocols and Practices 172
- 4.7 Bibliographic Notes 172
- 4.8 Terms and Concepts 173
- 4.9 Exercises 173

5	PROGRAM SECURITY	176
5.1	Viruses and Other Malicious Code	177
	<i>Why Worry About Malicious Code?</i>	177
	<i>Kinds of Malicious Code,</i>	179
	<i>How Viruses Attach,</i>	180
	<i>How Viruses Gain Control,</i>	182
	<i>Homes for Viruses,</i>	183
	<i>Virus Signatures,</i>	186
	<i>The Source of Viruses,</i>	189
	<i>Preventing Virus Infection,</i>	189
	<i>Truths and Misconceptions About Viruses,</i>	190
	<i>Virus Example: Brain Virus,</i>	191
	<i>Other Malicious Code Example: Internet Worm,</i>	192
5.2	Targeted Malicious Code	195
	<i>Trapdoors,</i>	195
	<i>Salami Attack,</i>	198
	<i>Covert Channels: Programs That Leak Information,</i>	199
5.3	Controls Against Program Threats	207
	<i>Programming Controls,</i>	207
	<i>Process Improvement,</i>	214
	<i>Operating System Controls on Use of Programs,</i>	221
	<i>Administrative Controls,</i>	223
5.4	Summary of Program Threats and Controls	224
5.5	Bibliographic Notes	224
5.6	Terms and Concepts	225
5.7	Exercises	226
6	PROTECTION IN GENERAL-PURPOSE OPERATING SYSTEMS	228
6.1	Protected Objects and Methods of Protection	228
	<i>A Bit of History,</i>	228
	<i>Protected Objects,</i>	229
	<i>Security Methods of Operating Systems,</i>	229
6.2	Protecting Memory and Addressing	231
	<i>Fence,</i>	231
	<i>Relocation,</i>	232
	<i>Base/Bounds Registers,</i>	233
	<i>Tagged Architecture,</i>	234
	<i>Segmentation,</i>	236
	<i>Paging,</i>	239
	<i>Combined Paging with Segmentation,</i>	241

6.3	Protecting Access to General Objects	242	
	<i>Directory</i> ,	243	
	<i>Access Control List</i> ,	244	
	<i>Access Control Matrix</i> ,	246	
	<i>Capability</i> ,	247	
	<i>Procedure-Oriented Access Control</i> ,	249	
6.4	File Protection Mechanisms	250	
	<i>Basic Forms of Protection</i> ,	250	
	<i>Single Permissions</i> ,	252	
	<i>Per-Object and Per-User Protection</i> ,	254	
6.5	User Authentication	254	
	<i>Use of Passwords</i> ,	255	
	<i>Attacks on Passwords</i> ,	256	
	<i>Password Selection Criteria</i> ,	260	
	<i>The Authentication Process</i> ,	263	
	<i>Flaws in the Authentication Process</i> ,	263	
	<i>Authentication Other Than Passwords</i> ,	264	
6.6	Summary of Security for Users	264	
6.7	Bibliographic Notes	265	
6.8	Terms and Concepts	265	
6.9	Exercises	266	
7	DESIGNING TRUSTED OPERATING SYSTEMS		269
7.1	What Is a Trusted System?	270	
7.2	Security Policies	271	
	<i>Military Security Policy</i> ,	271	
	<i>Commercial Security Policies</i> ,	273	
7.3	Models of Security	276	
	<i>Multilevel Security</i> ,	277	
	<i>Models Proving Theoretical Limitations of Security Systems</i> ,	280	
	<i>Summary of Models of Protection Systems</i> ,	286	
7.4	Design of Trusted Operating Systems	286	
	<i>Trusted System Design Elements</i> ,	286	
	<i>Security Features of Ordinary Operating Systems</i> ,	287	
	<i>Security Features of Trusted Operating Systems</i> ,	289	
	<i>Kernelized Design</i> ,	292	
	<i>Separation/Isolation</i> ,	297	
	<i>Virtualization</i> ,	298	
	<i>Layered Design</i> ,	302	

7.5	Assurance in Trusted Operating Systems	306
	<i>Typical Operating System Flaws</i> , 306	
	<i>Assurance Methods</i> , 308	
	<i>Evaluation</i> , 313	
	<i>What Doesn't Lead to Assurance?</i> 324	
7.6	Implementation Examples	325
	<i>General Purpose Operating Systems</i> , 325	
	<i>Operating Systems Designed for Security</i> , 328	
7.7	Summary of Security in Operating Systems	329
7.8	Bibliographic Notes	331
7.9	Terms and Concepts	332
7.10	Exercises	333
8	DATA BASE SECURITY	336
8.1	Introduction to Data Bases	336
	<i>Concept of a Data Base</i> , 337	
	<i>Advantages of Using Data Bases</i> , 339	
8.2	Security Requirements	340
	<i>Integrity of the Data Base</i> , 340	
	<i>Element Integrity</i> , 341	
	<i>Auditability</i> , 342	
	<i>Access Control</i> , 342	
	<i>User Authentication</i> , 343	
	<i>Availability</i> , 343	
	<i>Integrity/Secrecy/Availability</i> , 343	
8.3	Reliability and Integrity	343
	<i>Protection Features from the Operating System</i> , 344	
	<i>Two-Phase Update</i> , 344	
	<i>Redundancy/Internal Consistency</i> , 346	
	<i>Recovery</i> , 347	
	<i>Concurrency/Consistency</i> , 347	
	<i>Monitors</i> , 348	
	<i>Summary of Data Reliability</i> , 349	
8.4	Sensitive Data	349
	<i>Access Decisions</i> , 350	
	<i>Availability of Data</i> , 351	
	<i>Types of Disclosures</i> , 352	
	<i>Security Versus Precision</i> , 353	

8.5	Inference Problem	353	
	<i>Direct Attack</i> ,	355	
	<i>Indirect Attack</i> ,	355	
	<i>Conclusion on the Inference Problem</i> ,	360	
8.6	Multilevel Data Bases	361	
	<i>The Case for Differentiated Security</i> ,	361	
	<i>Granularity</i> ,	362	
	<i>Security Issues</i> ,	363	
8.7	Proposals for Multilevel Security	364	
	<i>Partitioning</i> ,	364	
	<i>Encryption</i> ,	364	
	<i>Integrity Lock</i> ,	365	
	<i>Integrity Lock DBMS</i> ,	367	
	<i>Trusted Front-End</i> ,	368	
	<i>Distributed Data Bases</i> ,	370	
	<i>Window/View</i> ,	370	
	<i>Concluding Remarks</i> ,	372	
8.8	Summary of Data Base Security	372	
8.9	Bibliographic Notes	373	
8.10	Terms and Concepts	374	
8.11	Exercises	375	
9	SECURITY IN NETWORKS AND DISTRIBUTED SYSTEMS		377
9.1	Network Concepts	378	
	<i>Communications</i> ,	379	
	<i>Media</i> ,	379	
	<i>Protocols</i> ,	381	
	<i>Addressing</i> ,	384	
	<i>Types of Networks</i> ,	385	
	<i>Topologies</i> ,	387	
	<i>Distributed Systems</i> ,	387	
	<i>Advantages of Computing Networks</i> ,	389	
9.2	Threats in Networks	390	
	<i>Network Security Issues</i> ,	390	
	<i>Security Threat Analysis</i> ,	391	
	<i>Wiretapping</i> ,	395	
	<i>Impersonation</i> ,	397	
	<i>Message Confidentiality Violations</i> ,	400	
	<i>Message Integrity Violations</i> ,	401	
	<i>Hacking</i> ,	402	
	<i>Code Integrity</i> ,	402	
	<i>Denial of Service</i> ,	404	

9.3	Network Security Controls	405
	<i>Encryption</i> ,	406
	<i>Access Control</i> ,	409
	<i>Authentication in Distributed Systems</i> ,	411
	<i>Traffic Control</i> ,	418
	<i>Data Integrity</i> ,	419
	<i>Summary of Network Security Control Techniques</i> ,	422
9.4	Privacy Enhanced Electronic Mail	422
	<i>Requirements and Solutions</i> ,	422
	<i>PEM</i> ,	423
	<i>PGP</i> ,	426
9.5	Firewalls	426
	<i>Design of Firewalls</i> ,	428
	<i>What Is a Firewall?</i>	428
	<i>Types of Firewalls</i> ,	428
	<i>Example Firewall Configurations</i> ,	434
	<i>What Firewalls Can—and Cannot—Block</i> ,	435
9.6	Encrypting Gateway	436
9.7	Multilevel Security on Networks	437
	<i>Trusted Network Interface</i> ,	437
	<i>Secure Communication</i> ,	439
9.8	Summary of Network Security	442
9.9	Bibliographic Notes	443
9.10	Terms and Concepts	443
9.11	Exercises	444
10	ADMINISTERING SECURITY	447
10.1	Personal Computer Security Management	447
	<i>Contributors to Security Problems</i> ,	448
	<i>Security Measures</i> ,	450
	<i>Protection for Files</i> ,	452
	<i>Summary of Personal Computer Security</i> ,	454
10.2	Unix Security Management	454
	<i>Current Software</i> ,	455
	<i>Accounts</i> ,	455
	<i>Privileges</i> ,	456
	<i>Audit</i> ,	457
	<i>Passwords</i> ,	457

10.3	Network Security Management	457
	<i>Wide Area Networks and the Internet, 457</i>	
	<i>Network Architecture, 459</i>	
	<i>Host Security, 460</i>	
	<i>Incidents, 460</i>	
	<i>Tools, 461</i>	
	<i>A Final Word, 462</i>	
10.4	Risk Analysis	462
	<i>Reasons to Perform a Risk Analysis, 463</i>	
	<i>Steps of a Risk Analysis, 463</i>	
	<i>Arguments Against Risk Analysis, 470</i>	
	<i>Summary of Benefits of Risk Analysis, 471</i>	
10.5	Security Planning	471
	<i>Creating a Security Plan, 472</i>	
	<i>Content of a Security Plan, 472</i>	
	<i>Security Planning Team Members, 474</i>	
	<i>Securing Commitment to a Security Plan, 475</i>	
10.6	Organizational Security Policies	475
	<i>Purpose, 475</i>	
	<i>Attributes, 476</i>	
	<i>Examples, 478</i>	
10.7	Disaster Recovery	479
	<i>Perils, 480</i>	
	<i>Natural Disasters, 480</i>	
	<i>Power Loss, 482</i>	
	<i>Heat, 483</i>	
	<i>Contingency Planning, 483</i>	
	<i>Intruders, 485</i>	
	<i>Disposal of Sensitive Media, 487</i>	
10.8	Summary of Administering Security	489
10.9	Bibliographic Notes	489
10.10	Terms and Concepts	489
10.11	Exercises	490
11	LEGAL AND ETHICAL ISSUES IN COMPUTER SECURITY	492
11.1	Protecting Programs and Data	494
	<i>Copyrights, 494</i>	
	<i>Patents, 497</i>	
	<i>Trade Secret, 499</i>	
	<i>Protection for Computer Objects, 501</i>	

- 11.2 Information and the Law 503
 - Information as an Object, 503*
 - Legal Issues Relating to Information, 505*
- 11.3 Rights of Employees and Employers 506
 - Ownership of Products, 506*
- 11.4 Computer Crime 509
 - Why a Separate Category for Computer Crime? 509*
 - Why Computer Crime Is Hard to Define, 511*
 - Why Computer Crime Is Hard to Prosecute, 511*
 - Examples of Statutes, 512*
 - U.S. Federal Statutes Related to Computing, 513*
 - What Computer Crime Does Not Address, 514*
 - Cryptography and the Law, 515*
 - Summary of Legal Issues in Computer Security, 516*
- 11.5 Ethical Issues in Computer Security 517
 - The Law and Ethics Are Not the Same, 517*
 - Studying Ethics, 518*
 - Ethical Reasoning, 520*
- 11.6 Electronic Privacy 522
 - Privacy of Electronic Data, 522*
 - Use of Encryption, 523*
 - Cryptographic Key Escrow, 524*
- 11.7 Case Studies of Ethics 524
 - Case I: Use of Computer Services, 524*
 - Case II: Privacy Rights, 525*
 - Case III: Denial of Service, 526*
 - Case IV: Ownership of Programs, 527*
 - Case V: Proprietary Resources, 529*
 - Case VI: Fraud, 530*
 - Case VII: Accuracy of Information, 531*
- 11.8 Codes of Ethics 532
 - IEEE, 532*
 - ACM, 532*
 - Computer Ethics Institute, 532*
- 11.9 Conclusion 532
- 11.10 Bibliographic Notes 535
- 11.11 Terms and Concepts 536

BIBLIOGRAPHY**537****INDEX****561**