Contents in Brief

Table of Contents ix
Preface to Second Edition xv
Foreword xix
Preface to First Edition xxiii
Typesetting Conventions xxix

Chapter 1: Security Concepts and Principles 1

Chapter 2: Cryptographic Building Blocks 29

Chapter 3: User Authentication—Passwords, Biometrics and Alternatives 55

Chapter 4: Authentication Protocols and Key Establishment 91

Chapter 5: Operating System Security and Access Control 125

Chapter 6: Software Security—Exploits and Privilege Escalation 155

Chapter 7: Malicious Software 183

Chapter 8: Public-Key Certificate Management and Use Cases 213

Chapter 9: Web and Browser Security 245

Chapter 10: Firewalls and Tunnels 281

Chapter 11: Intrusion Detection and Network-Based Attacks 309

Chapter 12: Wireless LAN Security: 802.11 and Wi-Fi 339

Chapter 13: Bitcoin, Blockchains and Ethereum 375

Epilogue 411

Index 417

Table of Contents

Preface to Second Edition xv
Foreword xix
Preface to First Edition xxiii
Typesetting Conventions xxix

Chapter 1: Security Concepts and Principles ... 1
1.1 Fundamental goals of computer security 2
1.2 Computer security policies and attacks 4
1.3 Risk, risk assessment, and modeling expected losses 6
1.4 Adversary modeling and security analysis 9
1.5 Threat modeling: diagrams, trees, lists and STRIDE 11
1.6 Model-reality gaps and real-world outcomes 16
1.7 ‡Design principles for computer security 20
1.8 ‡Why computer security is hard 25
1.9 ‡End notes and further reading 27
References 28

Chapter 2: Cryptographic Building Blocks ... 29
2.1 Encryption and decryption (generic concepts) 30
2.2 Symmetric-key encryption and decryption 32
2.3 Public-key encryption and decryption 37
2.4 Digital signatures and verification using public keys 39
2.5 Cryptographic hash functions 41
2.6 Message authentication (data origin authentication) 45
2.7 ‡Authenticated encryption and further modes of operation 47
2.8 ‡Certificates, elliptic curves, and equivalent keylengths 49
2.9 ‡End notes and further reading 51
References 52

Chapter 3: User Authentication—Passwords, Biometrics and Alternatives ... 55
3.1 Password authentication 56
3.2 Password-guessing strategies and defenses 59
3.3 Account recovery and secret questions 65
3.4 One-time password generators and hardware tokens 67
3.5 Biometric authentication 71
3.6 ‡Password managers and graphical passwords 76
3.7 ‡CAPTCHAs (humans-in-the-loop) vs. automated attacks 79
3.8 ‡Entropy, passwords, and partial-guessing metrics 81
3.9 ‡End notes and further reading 86
References 88

Chapter 4: Authentication Protocols and Key Establishment ... 91
4.1 Entity authentication and key establishment (context) ... 92
4.2 Authentication protocols: concepts and mistakes ... 97
4.3 Establishing shared keys by public agreement (DH) ... 100
4.4 Key authentication properties and goals ... 104
4.5 Password-authenticated key exchange: EKE and SPEKE ... 105
4.6 ‡Weak secrets and forward search in authentication ... 111
4.7 ‡Single sign-on (SSO) and federated identity systems ... 113
4.8 ‡Cyclic groups and subgroup attacks on Diffie-Hellman ... 115
4.9 ‡End notes and further reading ... 120
References ... 122

Chapter 5: Operating System Security and Access Control ... 125
5.1 Memory protection, supervisor mode, and accountability ... 127
5.2 The reference monitor, access matrix, and security kernel ... 130
5.3 Object permissions and file-based access control ... 133
5.4 Setuid bit and effective userid (eUID) ... 137
5.5 Directory permissions and inode-based example ... 138
5.6 Symbolic links, hard links and deleting files ... 142
5.7 Role-based (RBAC) and mandatory access control ... 144
5.8 ‡Protection rings: isolation meets finer-grained sharing ... 146
5.9 ‡Relating subjects, processes, and protection domains ... 149
5.10 ‡End notes and further reading ... 151
References ... 153

Chapter 6: Software Security—Exploits and Privilege Escalation ... 155
6.1 Race conditions and resolving filenames to resources ... 157
6.2 Integer-based vulnerabilities and C-language issues ... 159
6.3 Stack-based buffer overflows ... 166
6.4 Heap-based buffer overflows and heap spraying ... 168
6.5 ‡Return-to-libc exploits ... 171
6.6 Buffer overflow exploit defenses and adoption barriers ... 172
6.7 Privilege escalation and the bigger picture ... 174
6.8 ‡Background: process creation, syscalls, shells, shellcode ... 176
6.9 ‡End notes and further reading ... 178
References ... 180

Chapter 7: Malicious Software ... 183
7.1 Defining malware ... 184
7.2 Viruses and worms ... 186
7.3 Virus anti-detection and worm-spreading techniques ... 191
7.4 Stealth: Trojan horses, backdoors, keyloggers, rootkits ... 194
7.5 Rootkit detail: installation, object modification, hijacking ... 197
7.6 ‡Drive-by downloads and droppers ... 200
7.7 Ransomware, botnets and other beasts ... 202
7.8 Social engineering and categorizing malware ... 205
7.9 ‡End notes and further reading ... 207
References ... 209

Chapter 8: Public-Key Certificate Management and Use Cases ... 213
8.1 Certificates, certification authorities and PKI ... 214
8.2 Certificate chain validation and certificate extensions ... 217
8.3 ‡Certificate revocation ... 221
8.4 CA/PKI architectures and certificate trust models ... 224
8.5 TLS web site certificates and CA/browser trust model ... 229
8.6 Secure email overview and public-key distribution ... 235
8.7 ‡Secure email: specific technologies ... 238
8.8 ‡End notes and further reading ... 241
References ... 242

Chapter 9: Web and Browser Security ... 245
9.1 Web review: domains, URLs, HTML, HTTP, scripts ... 246
9.2 TLS and HTTPS (HTTP over TLS) ... 252
9.3 HTTP cookies and DOM objects ... 255
9.4 Same-origin policy (DOM SOP) ... 257
9.5 Authentication cookies, malicious scripts and CSRF ... 260
9.6 More malicious scripts: cross-site scripting (XSS) ... 262
9.7 SQL injection ... 266
9.8 ‡Usable security, phishing and web security indicators ... 269
9.9 ‡End notes and further reading ... 274
References ... 276

Chapter 10: Firewalls and Tunnels ... 281
10.1 Packet-filter firewalls ... 282
10.2 Proxy firewalls and firewall architectures ... 288
10.3 SSH: Secure Shell ... 292
10.4 VPNs and encrypted tunnels (general concepts) ... 297
10.5 ‡IPsec: IP security suite (details) ... 300
10.6 ‡Background: networking and TCP/IP ... 303
10.7 ‡End notes and further reading ... 306
References ... 307

Chapter 11: Intrusion Detection and Network-Based Attacks ... 309
11.1 Intrusion detection: introduction ... 310
11.2 Intrusion detection: methodological approaches ... 313
11.3 Sniffers, reconnaissance scanners, vulnerability scanners ... 316
11.4 Denial of service attacks ... 320
11.5 Address resolution attacks (DNS, ARP) ... 325
11.6 ‡TCP session hijacking ... 329
11.7 ‡End notes and further reading ... 332
References ... 335

Chapter 12: Wireless LAN Security: 802.11 and Wi-Fi ... 339
12.1 Background: 802.11 WLAN architecture and overview ... 340
12.2 WLAN threats and mitigations ... 343
12.3 Security architecture: access control, EAP and RADIUS ... 347
12.4 RC4 stream cipher and its use in WEP ... 351
12.5 WEP attacks: authentication, integrity, keystream reuse ... 353
12.6 WEP security summary and full key recovery ... 357
12.7 ‡AES-CCMP frame encryption and key hierarchy ... 361
12.8 Robust authentication, key establishment and WPA3 ... 364
12.9 ‡End notes and further reading ... 369
References ... 371

Chapter 13: Bitcoin, Blockchains and Ethereum ... 375

13.1 Bitcoin overview 376
13.2 Transaction types and fields 379
13.3 ‡Bitcoin script execution (signature validation) 382
13.4 Block structure, Merkle trees and the blockchain 384
13.5 Mining of blocks, block preparation and hashing targets 386
13.6 Building the blockchain, validation, and full nodes 391
13.7 ‡Simple payment verification, user wallets, private keys 395
13.8 ‡Ethereum and smart contracts 399
13.9 ‡End notes and further reading 405
References 407

Epilogue 411

Index 417