Contents

Foreword *xxiii*

Preface *xxvii*

About the Authors *xxxv*

1 SECURITY BLANKET OR SECURITY THEATER? 2

How Dependent Are We on Computers? 6

What Is Computer Security? 8

The Vulnerability–Threat–Control Paradigm 10

Threats 11

Confidentiality 13

Integrity 14

Availability 15

Types of Threats 17

Types of Attackers 19

Harm 23

Risk and Common Sense 24

Method–Opportunity–Motive 27

Vulnerabilities 29

Controls 29

Analyzing Security With Examples 32

Conclusion 33

Exercises 34

2 KNOCK, KNOCK. WHO'S THERE? 38
Attack: Impersonation 39
Attack Details: Failed Authentication 40
Identification versus Authentication 41
Vulnerability: Faulty or Incomplete Authentication 41
Password Use 42
Countermeasure: Strong Authentication 47
Knowledge: Something You Know 48
Biometrics: Something You Are 51
Tokens: Something You Have 59
Multifactor Authentication 61
Secure Authentication 62
Conclusion 63
Recurring Thread: Privacy 65
Anonymity 65
Multiple Identities—Linked or Not 67
Pseudonymity 68
Recurring Thread: Usability 69
Password Guidelines 69
Single Sign-On 70
Exercises 71

3 2 + 2 = 5 72
Attack: Program Flaw in Spacecraft Software 74
Threat: Program Flaw Leads to Security Failing 75
Vulnerability: Incomplete Mediation 77
Definition 77
Security Implication 78
Vulnerability: Race Condition 79
Definition 79
Security Implication 81
Vulnerability: Time-of-Check to Time-of-Use 82
Definition 82
Security Implication 83
Vulnerability: Undocumented Access Point 84
Ineffective Countermeasure: Penetrate-and-Patch 85
Countermeasure: Identifying and Classifying Faults 86
Faults and Failures 86
Types of Flaws 88

Countermeasure: Secure Software Design Elements 89
- Modularity 90
- Encapsulation 91
- Information Hiding 92
- Mutual Suspicion 92
- Confinement 93
- Simplicity 94
- Genetic Diversity 94
- Design Principles for Security 95

Countermeasure: Secure Software Development Process 97
- Peer Reviews 98
- Hazard Analysis 101

Good Design 103
- Prediction 104
- Static Analysis 104
- Configuration Control 105
- Lessons from Mistakes 110
- Standards of Program Development 110
- Design Principles Work 111
- Process Standards 112
- Program Controls in General 113

Countermeasure: Testing 114
- Types of Testing 114
- Effectiveness of Testing 117
- Limitations of Testing 117
- Testing Especially for Security 118

Countermeasure: Defensive Programming 122

Conclusion 123

Recurring Thread: Legal—Redress for Software Failures 125
- Selling Correct Software 126

Exercises 128

4 A HORSE OF A DIFFERENT COLOR 130

Attack: Malicious Code 131

Threat: Malware—Virus, Trojan Horse, and Worm 132
- History of Malicious Code 136

Technical Details: Malicious Code 138
- Harm from Malicious Code 138
- Transmission and Propagation 143

Activation 147

Stealth 153

Vulnerability: Voluntary Introduction 155

Vulnerability: Unlimited Privilege 157

Vulnerability: Stealthy Behavior—Hard to Detect and Characterize 157

Countermeasure: Hygiene 158

Countermeasure: Detection Tools 159

Virus Signatures 160

Fake Antivirus Tools 166

Countermeasure: Error Detecting and Error Correcting Codes 166

Error Codes 167

Hash Codes 168

Tripwire 168

Cryptographic Checksum 169

Countermeasure: Memory Separation 170

Countermeasure: Basic Security Principles 171

Least Privilege 171

Complete Mediation 172

Recurring Thread: Legal—Computer Crime 172

Why a Separate Category for Computer Crime Is Needed 172

Why Computer Crime Is Hard to Define 175

Why Computer Crime Is Hard to Prosecute 175

Conclusion 176

Exercises 177

5 THE KEYS TO THE KINGDOM 180

Attack: Keylogging 181

Threat: Illicit Data Access 182

Attack Details 182

Physical Access 184

Method–Opportunity–Motive 184

Harm: Data and Reputation 186

Vulnerability: Physical Access 186

Vulnerability: Misplaced Trust 187

Social Engineering 187

Presumed Innocence 188

Vulnerability: Insiders 188

Vulnerability: System Subversion 191

Recurring Thread: Forensics—Tracing Data Flow 192

Vulnerability: Weak Authentication 193

Failed Countermeasure: Security through Obscurity 193

Countermeasure: Physical Access Control 195

Preventing Access 195

Detecting Access 197

Countermeasure: Strong Authentication 197

One-Time Passwords 197

Continuous Authentication 200

Password Change Frequency 201

Countermeasure: Trust/Least Privilege 201

Conclusion 203

Recurring Thread: Forensics—Plug-and-Play Devices 204

Exercises 206

INTERLUDE A: CLOUD COMPUTING 208

What Is Cloud Computing? 209

Service Models 210

Deployment Models 210

Projected Use and Cost Savings 211

What Are the Risks in the Cloud? 211

What Do Security Characteristics Look Like in the Cloud? 211

Technical Risks 212

Legal Risks 213

6 MY CUP RUNNETH OVER 214

Attack: What Did You Say That Number Was? 215

Harm: Destruction of Code and Data 216

Memory Allocation 217

Code and Data 217

Harm from an Overflow 218

Overwriting Memory 219

Implications of Overwriting Memory 220

The Stack and the Heap 225

Vulnerability: Off-by-One Error 228

Vulnerability: Integer Overflow 229

Vulnerability: Unterminated Null-Terminated String 230

Vulnerability: Parameter Length and Number 231

Vulnerability: Unsafe Utility Programs 232

Attack: Important Overflow Exploitation Examples 232

- Morris Worm 232
- Code Red 235
- SQL Slammer 238
- Conficker 240

Countermeasure: Programmer Bounds Checking 242

Countermeasure: Programming Language Support 242

- Safe Languages 243
- Safe Compilers 244

Countermeasure: Stack Protection/Tamper Detection 245

Countermeasure: Hardware Protection of Executable Space 247

- Fence 248
- Base/Bounds Registers 249
- Tagged Architecture 252
- Paging and Segmentation 254
- Combined Paging with Segmentation 258

Countermeasure: General Access Control 259

- Access Control Directory 261
- Access Control Matrix 264
- Access Control List 265
- Privilege List 267
- Capability 267

Conclusion 270

Exercises 272

7 HE WHO STEALS MY PURSE ... 274

Attack: Veterans' Administration Laptop Stolen 275

Threat: Loss of Data 276

Extended Threat: Disaster 276

Vulnerability: Physical Access 277

Vulnerability: Unprotected Availability of Data 277

Vulnerability: Unprotected Confidentiality of Data 277

Countermeasure: Policy 278

Countermeasure: Physical Security 278

Countermeasure: Data Redundancy (Backup) 280

- Backup 280

Countermeasure: Encryption 284
Terminology and Background 285
Terminology 286
Representing Characters 290
Substitution Ciphers 291
The Caesar Cipher 291
Other Substitutions 294
One-Time Pads 297
Transpositions (Permutations) 302
Combinations of Approaches 306
Making "Good" Encryption Algorithms 307
Symmetric and Asymmetric Encryption Systems 309
Stream and Block Ciphers 310
Confusion and Diffusion 310
Cryptanalysis—Breaking Encryption Schemes 312
The Data Encryption Standard (DES) 315
The AES Encryption Algorithm 320
Countermeasure: Disk Encryption 323
Conclusion 324
Exercises 327

8 THE ROOT OF ALL EVIL 330

Background: Operating System Structure 331
Attack: Phone Rootkit 335
Attack Details: What Is a Rootkit? 336
Rootkit Evades Detection 336
Rootkit Operates Unchecked 339
Sony XCP Rootkit 340
TDSS Rootkits 343
Other Rootkits 344
Vulnerability: Software Complexity 345
Vulnerability: Difficulty of Detection and Eradication 345
Countermeasure: Simplicity of Design 346
Layered Design 346
Kernelized Design 349
Countermeasure: Trusted Systems 351
Trusted Systems 353
Trusted Computing Base (TCB) 355

Trusted System Functions 359

Trusted Systems Today 360

Conclusion 362

Exercises 363

9 SCANNING THE HORIZON 366

Attack: Investigation, Intrusion, and Compromise 367

Threat: Port Scan 368

Attack Details 369

Harm: Knowledge and Exposure 372

Recurring Thread: Legal—Are Port Scans Legal? 373

Vulnerability: Revealing Too Much 374

Vulnerability: Allowing Internal Access 374

Countermeasure: System Architecture 375

Countermeasure: Firewall 376

What Is a Firewall? 377

Design of Firewalls 378

Types of Firewalls 380

Personal Firewalls 388

Comparison of Firewall Types 391

Example Firewall Configurations 392

Countermeasure: Network Address Translation (NAT) 395

Countermeasure: Security Perimeter 397

Conclusion 398

Exercises 400

10 DO YOU HEAR WHAT I HEAR? 402

Attack: Wireless (WiFi) Network Access 403

Attack Details 404

WiFi Background 405

Harm: Confidentiality–Integrity–Availability 410

Confidentiality 410

Integrity 410

Availability 410

Attack: Unauthorized Access 412

Vulnerability: Protocol Weaknesses 412

Picking Up the Beacon 412

SSID in All Frames 413

Authentication 414

Changeable MAC Addresses 414

Stealing the Association 414

Preferred Associations 414

Failed Countermeasure: WEP 416

WEP Security Weaknesses 416

Bottom Line: WEP Security Is Unacceptable 418

WEP Replacement 419

Stronger but Not Perfect Countermeasure: WPA and WPA2 420

Strengths of WPA over WEP 420

WPA Attacks 422

Conclusion: WPA Is Adequately Secure 424

Conclusion 424

Recurring Thread: Privacy—Privacy-Preserving Design 425

Opt-In versus Opt-Out 425

Exercises 427

11 I HEAR YOU LOUD AND CLEAR 430

Attack: Enemies Watch Predator Video 431

Attack Details 432

Lack of Authentication 432

Lack of Encryption 433

Threat: Interception 435

Cable 435

Microwave 437

Satellite Communication 438

Optical Fiber 439

Vulnerability: Wiretapping 439

What Makes a Network Vulnerable to Interception? 442

Background: Protocol Layers 445

Countermeasure: Encryption 446

Modes of Network Encryption 447

Countermeasure: Virtual Private Networks 450

Countermeasure: Cryptographic Key Management Regime 454

Key Distribution—Not to the Wrong People 454

Key Distribution—To the Right People 455

Key Rescission or Replacement 455

Key Revocation 456
Key Backup 456
Countermeasure: Asymmetric Cryptography 457
Motivation 457
Characteristics 458
Rivest–Shamir–Adelman (RSA) Encryption 459
Uses of Public Key Encryption 460
Countermeasure: Kerberos 462
Conclusion 466
Recurring Thread: Ethics—Monitoring Users 469
Exercises 470

INTERLUDE B: ELECTRONIC VOTING 472

What Is Electronic Voting? 473
Casting Ballots 474
Transmitting and Counting Ballots 474
What Is a Fair Election? 475
What Are the Critical Issues? 475
Secrecy 476
Tampering 477
Assuring Accuracy 478
Usability 478
Cost and Benefit 479

12 DISREGARD THAT MAN BEHIND THE CURTAIN 480

Attack: Radar Sees Only Blue Skies 481
Threat: Man in the Middle 482
Threat: "In-the-Middle" Activity 485
DNS Spoofing 485
Rerouting Routing 486
Router Takes Over a Network 488
Source Routing and Address Spoofing 489
Physical Man in the Middle 489
Man-in-the-Browser Attack 491
Man-in-the-Phone Attack 493
Page-in-the-Middle Attack 493
Program Download Substitution 493
Capturing CAPTCHAs 494
Man-in-the-Middle Attacks in General 496

Vulnerability: Unwarranted Trust 496
Vulnerability: Failed Identification and Authentication 497
Human Authentication 497
Computer Authentication 497
Vulnerability: Unauthorized Access 499
Vulnerability: Inadequate Attention to Program Details 499
Vulnerability: Protocol Weakness 500
Summary 500
Countermeasure: Trust 501
Monitoring 501
Skepticism 501
Countermeasure: Identification and Authentication 501
Shared Secret 502
One-Time Password 502
Out-of-Band Communication 502
Signed Code 503
Continuous Authentication 504
Countermeasure: Cryptography 504
Revised Key Exchange Protocol 504
Summary 505
Related Attack: Covert Channel 506
Covert Channels in Computers 506
Detecting Covert Channels 511
Countermeasures against Covert Channels 513
Related Attack: Steganography 515
Information Hiding 515
Technical Example 516
Conclusion 517
Exercises 518

13 NOT ALL IS AS IT SEEMS 520
Attacks: Forgeries 521
Fake Email 521
Fake Web Site 523
Fake Code 524
Threat: Integrity Failure 526
Attack Details 526
Web Site Defacement 526
Substitute Content on a Real Web Site 527

Fake Email Message 528
Fake (Inaccurate) Email Header Data 530
Web Bug 530
Clickjacking 532
Drive-by Download 533
Cross Site Scripting 535
SQL Injection 536
Summary of Threats 538
Vulnerability: Protocol Weaknesses 538
Vulnerability: Code Flaws 539
Vulnerability: Humans 539
Framing 540
Optimism Bias 540
Naïveté 540
Vulnerabilities 541
Countermeasure: Digital Signature 541
Components and Characteristics of Signatures 542
Secure Hash Functions 544
Public Keys for Signing 545
Trust 546
Certificates: Trustable Identities and Public Keys 551
Digital Signatures—All the Pieces 554
Public Key Infrastructure 557
Signed Code 561
Countermeasure: Secure Protocols 562
Countermeasure: Access Control 562
Limited Privilege 563
Procedure-Oriented Access Control 563
Role-Based Access Control 564
Countermeasure: User Education 564
Possible Countermeasure: Analysis 565
Open Source 565
Evaluation 566
Non-Countermeasure: Software Goodness Checker 567
Requirements 567
Complexity 567
Decidability 567
Conclusion 568
Exercises 570

14 PLAY IT [AGAIN] SAM, OR, LET'S LOOK AT THE INSTANT REPLAY 572
Attack: Cloned RFIDs 573
Threat: Replay Attacks 574
Reprocessed Transactions 574
Password Replays 574
Physical Replay 575
Vulnerability: Reuse of Session Data 576
Countermeasure: Unrepeatable Protocol 576
Liveness 576
Liveness Beacon 577
Sequence Number 578
Nonce 578
Similar Attack: DNS Cache Poisoning 578
Countermeasure: Cryptography 579
Asymmetric Cryptography and PKI 579
Cryptographic Key Replacement 580
Conclusion: Replay Attacks 580
Similar Attack: Session Hijack 580
Vulnerability: Electronic Impersonation 584
Vulnerability: Nonsecret Token 584
Countermeasure: Encryption 585
SSH Encryption 585
SSL and TLS Encryption 585
Countermeasure: IPsec 589
IPsec Security Association 590
Headers and Data 590
Key Management 590
Modes of Operation 591
Countermeasure: Design 592
Conclusion 593
Exercises 594

15 I CAN'T GET NO SATISFACTION 596
Attack: Massive Estonian Web Failure 597
Threat: Denial of Service 598
Threat: Flooding 598
Threat: Blocked Access 599
Threat: Access Failure 600

Case: Beth Israel Deaconess Hospital Systems Down 601
Vulnerability: Insufficient Resources 602
- Insufficient Capacity 602
- Network Flooding Attack 602
- Resource Starvation 606

Vulnerability: Addressee Cannot Be Found 607
- Traffic Redirection 607
- DNS Attacks 608

Vulnerability: Exploitation of Known Vulnerability 609
Vulnerability: Physical Disconnection 609
- Transmission Failure 610
- Component Failure 610

Countermeasure: Network Monitoring and Administration 610
- Capacity Planning 611
- Load Balancing 612
- Network Tuning 612
- Network Addressing 612
- Shunning 613
- Blacklisting and Sinkholing 613

Countermeasure: Intrusion Detection and Prevention Systems 614
- Types of IDSs 614
- Other Intrusion Detection Technology 619
- Intrusion Prevention Systems 620
- Intrusion Response 620
- Honeypots 622
- Goals for Intrusion Detection Systems 624
- IDS Strengths and Limitations 625

Countermeasure: Management 626
- Backup 626
- Redundancy and Server Farms 627
- Physical Security 628
- Planning 628

Conclusion: Denial of Service 629
Extended Attack: E Pluribus Contra Unum 631
- Distributed Denial-of-Service Attacks 631
- Scripted Denial-of-Service Attacks 633

Technical Details 634
- Bots 634
- Botnets 634

Malicious Autonomous Mobile Agents 638
Autonomous Mobile Protective Agents 638
Recurring Thread: Legal—DDoS Crime Does Not Pay 639
Vulnerability: Previously Described Attacks 639
TFN 640
Trin00 640
Stacheldraht 641
Countermeasures: Preventing Bot Conscription 641
Vulnerability Scan 642
Computer Hygiene 642
Separation and Limited Privilege 642
Outbound Monitoring 642
Countermeasures: Handling an Attack Under Way 643
Firewalls and IPSs 643
Rate Limiting 643
ACLs 643
Filtering and Throttling 644
Conclusion: Distributed Denial of Service 644
Exercises 645

INTERLUDE C: CYBER WARFARE 648

What Is Cyber Warfare? 649
Definition of Cyber Warfare 649
Examples of Cyber Warfare 650
Estonia 650
Iran 650
Israel and Syria 651
Canada 651
Critical Issues 652
When Is It Warfare? 653
How Likely Is It? 653
What Are Appropriate Reactions to Cyber War? 653
Other Policy, Ethical, and Legal Issues 654

16 'TWAS BRILLIG, AND THE SLITHY TOVES ... 658

Attack: Grade Inflation 659
Threat: Data Corruption 660
Sequencing 661
Substitution 661

Insertion 661
Salami 662
Similarity 662
Countermeasure: Codes 663
Error Detection Codes 663
Error Correction Codes 664
Countermeasure: Protocols 664
Countermeasure: Procedures 665
Backup 665
Redundancy 665
Countermeasure: Cryptography 666
Block Chaining 666
Password Salt 668
Conclusion 669
Exercises 670

17 PEERING THROUGH THE WINDOW 672

Attack: Sharing Too Much 673
Attack Details: Characteristics of Peer-to-Peer Networks 673
The P2P Model 674
P2P Network Uses 675
Threat: Inappropriate Data Disclosure 676
Threat: Introduction of Malicious Software 677
Threat: Exposure to Unauthorized Access 678
Vulnerability: User Failure to Employ Access Controls 679
Vulnerability: Unsafe User Interface 679
Vulnerability: Malicious Downloaded Software 680
Countermeasure: User Education 681
Countermeasure: Secure-by-Default Software 681
Countermeasure: Legal Action 682
Countermeasure: Outbound Firewall or Guard 684
Conclusion 685
Recurring Thread: Legal—Protecting Computer Objects 687
Copyrights 687
Patents 692
Trade Secrets 695
Protection for Computer Objects 696
Exercises 700

18 MY 100,000 NEAREST AND DEAREST FRIENDS 702

Attack: I See U 703

Threat: Loss of Confidentiality 704

Threat: Data Leakage 705

Threat: Introduction of Malicious Code 706

Attack Details: Unintended Disclosure 707

Sensitive Data 707

Types of Disclosures 708

Direct Inference 710

Inference by Arithmetic 711

Aggregation 715

Linkage 715

Vulnerability: Exploiting Trust Relationships 717

Vulnerability: Analysis on Data 718

Vulnerability: Hidden Data Attributes 718

Countermeasure: Data Suppression and Modification 720

Statistical Suppression 721

Concealment 723

Query Analysis 725

Countermeasure: User Awareness and Education 725

Understanding the Online Environment 725

Payments on the Web 726

Site and Portal Registrations 727

Whose Page Is This? 727

Shopping on the Internet 728

Countermeasure: Policy 729

Conclusion 730

Exercises 732

AFTERWORD 734

Challenges Facing Us 735

Diverse and Distributed Ownership of the Infrastructure 735

Appeal as a Criminal Tool 736

Difficulty in Quickly Identifying and Reacting to Emergent Behavior 736

Critical Issues 737

Misaligned Incentives 737

The Need for Diversity 738

Compatibility with Organizational Culture and Goals 738

Moving Forward: Suggested Next Steps for Improving Computer Security 738
Address All Unwelcome Behaviors the Same Way 739
Extend Liability Statutes to Cyber Technology 739
Insist on Good Systems Engineering 740
Provide Economic Incentives for Good Security Hygiene 741
Perform Multidisciplinary Research 741
And Now for Something a Little Different 742

Bibliography *745*

Index *769*