Security in Computing

FIFTH EDITION

Charles P. Pfleeger
Shari Lawrence Pfleeger
Jonathan Margulies

PRENTICE HALL

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

Foreword xix

Preface xxv

Acknowledgments xxxi

About the Authors xxxiii

Chapter 1 Introduction 1

1.1 What Is Computer Security? 2

Values of Assets 4

The Vulnerability–Threat–Control Paradigm 5

1.2 Threats 6

Confidentiality 8

Integrity 10

Availability 11

Types of Threats 13

Types of Attackers 16

1.3 Harm 21

Risk and Common Sense 22

Method–Opportunity–Motive 26

1.4 Vulnerabilities 28

1.5 Controls 28

1.6 Conclusion 31

1.7 What's Next? 32

1.8 Exercises 34

Chapter 2 Toolbox: Authentication, Access Control, and Cryptography 36

2.1 Authentication 38
Identification Versus Authentication 38
Authentication Based on Phrases and Facts: Something You Know 40
Authentication Based on Biometrics: Something You Are 53
Authentication Based on Tokens: Something You Have 65
Federated Identity Management 68
Multifactor Authentication 70
Secure Authentication 70
2.2 Access Control 72
Access Policies 72
Implementing Access Control 75
Procedure-Oriented Access Control 85
Role-Based Access Control 85
2.3 Cryptography 86
Problems Addressed by Encryption 87
Terminology 87
DES: The Data Encryption Standard 95
AES: Advanced Encryption System 98
Public Key Cryptography 100
Public Key Cryptography to Exchange Secret Keys 103
Error Detecting Codes 109
Trust 117
Certificates: Trustable Identities and Public Keys 121
Digital Signatures—All the Pieces 124
2.4 Exercises 127

Chapter 3 Programs and Programming 131

3.1 Unintentional (Nonmalicious) Programming Oversights 133
Buffer Overflow 134
Incomplete Mediation 152
Time-of-Check to Time-of-Use 155
Undocumented Access Point 157
Off-by-One Error 159
Integer Overflow 160

Unterminated Null-Terminated String 161
Parameter Length, Type, and Number 162
Unsafe Utility Program 162
Race Condition 163
3.2 Malicious Code—Malware 166
Malware—Viruses, Trojan Horses, and Worms 167
Technical Details: Malicious Code 176
3.3 Countermeasures 196
Countermeasures for Users 197
Countermeasures for Developers 203
Countermeasure Specifically for Security 216
Countermeasures that Don't Work 224
Conclusion 229
Exercises 229

Chapter 4 The Web—User Side 232

4.1 Browser Attacks 234
Browser Attack Types 234
How Browser Attacks Succeed: Failed Identification and Authentication 240
4.2 Web Attacks Targeting Users 245
False or Misleading Content 246
Malicious Web Content 253
Protecting Against Malicious Web Pages 259
4.3 Obtaining User or Website Data 260
Code Within Data 261
Website Data: A User's Problem, Too 265
Foiling Data Attacks 266
4.4 Email Attacks 267
Fake Email 267
Fake Email Messages as Spam 267
Fake (Inaccurate) Email Header Data 273
Phishing 274
Protecting Against Email Attacks 275
4.5 Conclusion 277
4.6 Exercises 278

Chapter 5 Operating Systems 280

5.1 Security in Operating Systems 280
Background: Operating System Structure 281
Security Features of Ordinary Operating Systems 282
A Bit of History 284
Protected Objects 286
Operating System Tools to Implement Security Functions 292
5.2 Security in the Design of Operating Systems 308
Simplicity of Design 309
Layered Design 309
Kernelized Design 312
Reference Monitor 313
Correctness and Completeness 314
Secure Design Principles 315
Trusted Systems 316
Trusted System Functions 319
The Results of Trusted Systems Research 325
5.3 Rootkit 329
Phone Rootkit 329
Rootkit Evades Detection 330
Rootkit Operates Unchecked 334
Sony XCP Rootkit 335
TDSS Rootkits 336
Other Rootkits 338
5.4 Conclusion 338
5.5 Exercises 339

Chapter 6 Networks 341

6.1 Network Concepts 342
Background: Network Transmission Media 343
Background: Protocol Layers 349
Background: Addressing and Routing 350

Part I—War on Networks: Network Security Attacks 353

6.2 Threats to Network Communications 354
Interception: Eavesdropping and Wiretapping 354
Modification, Fabrication: Data Corruption 361
Interruption: Loss of Service 366
Port Scanning 369
Vulnerability Summary 374

6.3 Wireless Network Security 374
WiFi Background 374
Vulnerabilities in Wireless Networks 381
Failed Countermeasure: WEP (Wired Equivalent Privacy) 388
Stronger Protocol Suite: WPA (WiFi Protected Access) 390
6.4 Denial of Service 396
Example: Massive Estonian Web Failure 396
How Service Is Denied 398
Flooding Attacks in Detail 402
Network Flooding Caused by Malicious Code 403
Network Flooding by Resource Exhaustion 407
Denial of Service by Addressing Failures 408
Traffic Redirection 413
DNS Attacks 414
Exploiting Known Vulnerabilities 419
Physical Disconnection 420
6.5 Distributed Denial-of-Service 421
Scripted Denial-of-Service Attacks 423
Bots 426
Botnets 426
Malicious Autonomous Mobile Agents 430
Autonomous Mobile Protective Agents 430

Part II—Strategic Defenses: Security Countermeasures 432

6.6 Cryptography in Network Security 432
Network Encryption 433
Browser Encryption 437
Onion Routing 443
IP Security Protocol Suite (IPsec) 444
Virtual Private Networks 447
System Architecture 450
6.7 Firewalls 451
What Is a Firewall? 452
Design of Firewalls 453
Types of Firewalls 454
Personal Firewalls 465
Comparison of Firewall Types 467
Example Firewall Configurations 467
Network Address Translation (NAT) 472
Data Loss Prevention 473

6.8 Intrusion Detection and Prevention Systems 474
Types of IDSs *476*
Other Intrusion Detection Technology *481*
Intrusion Prevention Systems *482*
Intrusion Response *483*
Goals for Intrusion Detection Systems *486*
IDS Strengths and Limitations *488*
6.9 Network Management 489
Management to Ensure Service *489*
Security Information and Event Management (SIEM) *492*
6.10 Conclusion 496
6.11 Exercises 496

Chapter 7 Databases 501

7.1 Introduction to Databases 502
Concept of a Database *502*
Components of Databases *502*
Advantages of Using Databases *506*
7.2 Security Requirements of Databases 507
Integrity of the Database *507*
Element Integrity *508*
Auditability *510*
Access Control *511*
User Authentication *512*
Availability *512*
Integrity/Confidentiality/Availability *512*
7.3 Reliability and Integrity 513
Protection Features from the Operating System *513*
Two-Phase Update *514*
Redundancy/Internal Consistency *516*
Recovery *516*
Concurrency/Consistency *517*
7.4 Database Disclosure 518
Sensitive Data *518*
Types of Disclosures *519*
Preventing Disclosure: Data Suppression and Modification *529*
Security Versus Precision *530*

7.5 Data Mining and Big Data 535
Data Mining *536*
Big Data *540*
7.6 Conclusion 549
Exercises 549

Chapter 8 Cloud Computing 551

8.1 Cloud Computing Concepts 551
Service Models *552*
Deployment Models *552*
8.2 Moving to the Cloud 553
Risk Analysis *553*
Cloud Provider Assessment *554*
Switching Cloud Providers *556*
Cloud as a Security Control *557*
8.3 Cloud Security Tools and Techniques 560
Data Protection in the Cloud *561*
Cloud Application Security *566*
Logging and Incident Response *567*
8.4 Cloud Identity Management 568
Security Assertion Markup Language *570*
OAuth *573*
OAuth for Authentication *577*
8.5 Securing IaaS 579
Public IaaS Versus Private Network Security *580*
8.6 Conclusion 583
Where the Field Is Headed *584*
To Learn More *584*
8.7 Exercises 584

Chapter 9 Privacy 586

9.1 Privacy Concepts 587
Aspects of Information Privacy *587*
Computer-Related Privacy Problems *590*
9.2 Privacy Principles and Policies 596
Fair Information Practices *596*
U.S. Privacy Laws *597*

Controls on U.S. Government Websites 599
Controls on Commercial Websites 600
Non-U.S. Privacy Principles 603
Individual Actions to Protect Privacy 605
Governments and Privacy 607
Identity Theft 609
9.3 Authentication and Privacy 610
What Authentication Means 611
Conclusions 615
9.4 Data Mining 616
Government Data Mining 617
Privacy-Preserving Data Mining 617
9.5 Privacy on the Web 619
Understanding the Online Environment 620
Payments on the Web 621
Site and Portal Registrations 622
Whose Page Is This? 622
Precautions for Web Surfing 624
Spyware 628
Shopping on the Internet 630
9.6 Email Security 632
Where Does Email Go, and Who Can Access It? 632
Interception of Email 633
Monitoring Email 633
Anonymous, Pseudonymous, and Disappearing Email 634
Spoofing and Spamming 635
Summary 636
9.7 Privacy Impacts of Emerging Technologies 636
Radio Frequency Identification 636
Electronic Voting 640
VoIP and Skype 642
Privacy in the Cloud 642
Conclusions on Emerging Technologies 643
9.8 Where the Field Is Headed 644
9.9 Conclusion 645
9.10 Exercises 645

Chapter 10 Management and Incidents 647

10.1 Security Planning 647
Organizations and Security Plans 648
Contents of a Security Plan 649
Security Planning Team Members 656
Assuring Commitment to a Security Plan 656
10.2 Business Continuity Planning 658
Assess Business Impact 660
Develop Strategy 660
Develop the Plan 661
10.3 Handling Incidents 662
Incident Response Plans 662
Incident Response Teams 665
10.4 Risk Analysis 668
The Nature of Risk 669
Steps of a Risk Analysis 670
Arguments For and Against Risk Analysis 684
10.5 Dealing with Disaster 686
Natural Disasters 686
Power Loss 688
Human Vandals 689
Interception of Sensitive Information 692
Contingency Planning 694
Physical Security Recap 698
10.6 Conclusion 699
10.7 Exercises 700

Chapter 11 Legal Issues and Ethics 702

11.1 Protecting Programs and Data 704
Copyrights 704
Patents 711
Trade Secrets 714
Special Cases 716
11.2 Information and the Law 717
Information as an Object 717
Legal Issues Relating to Information 720

The Legal System 721
Summary of Protection for Computer Artifacts 724
11.3 Rights of Employees and Employers 725
Ownership of Products 725
Employment Contracts 727
11.4 Redress for Software Failures 728
Selling Correct Software 729
Reporting Software Flaws 731
11.5 Computer Crime 733
Why a Separate Category for Computer Crime Is Needed 734
Why Computer Crime Is Hard to Define 736
Why Computer Crime Is Hard to Prosecute 736
Examples of Statutes 737
International Dimensions 741
Why Computer Criminals Are Hard to Catch 742
What Computer Crime Does Not Address 743
Summary of Legal Issues in Computer Security 743
11.6 Ethical Issues in Computer Security 744
Differences Between the Law and Ethics 744
Studying Ethics 746
Ethical Reasoning 747
11.7 Incident Analysis with Ethics 750
Situation I: Use of Computer Services 750
Situation II: Privacy Rights 752
Situation III: Denial of Service 753
Situation IV: Ownership of Programs 754
Situation V: Proprietary Resources 756
Situation VI: Fraud 757
Situation VII: Accuracy of Information 758
Situation VIII: Ethics of Hacking or Cracking 759
Situation IX: True Representation 762
Conclusion of Computer Ethics 764
Conclusion 765
Exercises 765

Chapter 12 Details of Cryptography 768

12.1 Cryptology 769
Cryptanalysis 769
Cryptographic Primitives 773

One-Time Pads 775
Statistical Analysis 776
What Makes a "Secure" Encryption Algorithm? 777
12.2 Symmetric Encryption Algorithms 779
DES 779
AES 789
RC2, RC4, RC5, and RC6 792
12.3 Asymmetric Encryption with RSA 795
The RSA Algorithm 795
Strength of the RSA Algorithm 797
12.4 Message Digests 799
Hash Functions 799
One-Way Hash Functions 799
Message Digests 800
12.5 Digital Signatures 802
Elliptic Curve Cryptosystems 802
El Gamal and Digital Signature Algorithms 803
The NSA–Cryptography Controversy of 2012 804
12.6 Quantum Cryptography 807
Quantum Physics 807
Photon Reception 808
Cryptography with Photons 808
Implementation 811
12.7 Conclusion 811

Chapter 13 Emerging Topics 813

13.1 The Internet of Things 814
Medical Devices 815
Mobile Phones 818
Security in the Internet of Things 820
13.2 Economics 821
Making a Business Case 821
Quantifying Security 825
Current Research and Future Directions 832
13.3 Electronic Voting 834
What Is Electronic Voting? 835
What Is a Fair Election? 836
What Are the Critical Issues? 837

13.4 Cyber Warfare 841
What Is Cyber Warfare? *842*
Possible Examples of Cyber Warfare *843*
Critical Issues *846*
13.5 Conclusion 850

Bibliography **851**

Index **877**