



Security in Computing

Sixth Edition

Charles P. Pfleeger
Shari Lawrence Pfleeger
Lizzie Coles-Kemp

Security in Computing

SIXTH EDITION

Security in Computing

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Foreword

Preface

Acknowledgments

About the Authors

Chapter 1 Introduction

1.1 What Is Computer Security?

Values of Assets

The VulnerabilityThreatControl Paradigm

1.2 Threats

Confidentiality

Integrity

Availability

Types of Threats

Types of Attackers

1.3 Harm

Risk and Common Sense

MethodOpportunityMotive

1.4 Vulnerabilities

Table of Contents

1.5 Controls

1.6 Conclusion

1.7 Whats Next?

1.8 Exercises

Chapter 2 Toolbox: Authentication, Access Control, and Cryptography

2.1 Authentication

Identification vs. Authentication

Authentication Based on Phrases and Facts: Something You Know

Authentication Based on Biometrics: Something You Are

Authentication Based on Tokens: Something You Have

Federated Identity Management

Multifactor Authentication

Fitting Authentication to the Situation

2.2 Access Control

Access Policies

Implementing Access Control

Procedure-Oriented Access Control

Role-Based Access Control

2.3 Cryptography

Problems Addressed by Encryption

Terms and Concepts

DES: The Data Encryption Standard

AES: Advanced Encryption System

Public Key Cryptography

Using Public Key Cryptography to Exchange Secret Keys

Error Detecting Codes

Signatures

Trust

Table of Contents

Certificates: Trustable Identities and Public Keys

Digital SignaturesAll the Pieces

2.4 Conclusion

2.5 Exercises

Chapter 3 Programs and Programming

3.1 Unintentional (Nonmalicious) Programming Oversights

Buffer Overflow

Incomplete Mediation

Time-of-Check to Time-of-Use

Undocumented Access Point

Off-by-One Error

Integer Overflow

Unterminated Null-Terminated String

Parameter Length, Type, and Number

Unsafe Utility Program

Race Condition

Unsynchronized Activity

Developing Secure Apps

3.2 Malicious CodeMalware

MalwareViruses, Worms, and Trojan Horses

Technical Details: Malicious Code

3.3 Countermeasures

Countermeasures for Users

Countermeasures for Developers

Countermeasure Specifically for Security

Countermeasures That Dont Work

3.4 Conclusion

3.5 Exercises

Table of Contents

Chapter 4 The InternetUser Side

4.1 Browser Attacks

Browser Attack Types

How Browser Attacks Succeed: Failed Identification and Authentication

4.2 Attacks Targeting Users

False or Misleading Content

Malicious Web Content

Protecting Against Malicious Webpages

4.3 Obtaining User or Website Data

Code Within Data

Website Data: A Users Problem Too

Ransomware

Foiling Data Attacks

4.4 Mobile Apps

Apps and Security

Threats to Mobile Computing

Vulnerabilities from Using Apps

Why Apps Have Flaws

Finding Secure Apps

Protecting Yourself After Installing an App

4.5 Email and Message Attacks

Fake Email

Fake Email Messages as Spam

Fake (Inaccurate) Email Header Data

Phishing

Protecting Against Email Attacks

4.6 Conclusion

4.7 Exercises

Chapter 5 Operating Systems

Table of Contents

5.1 Security in Operating Systems

Background: Operating System Structure

Security Features of Ordinary Operating Systems

A Bit of History

Protected Objects

Operating System Tools to Implement Security Functions

5.2 Security in the Design of Operating Systems

Simplicity of Design

Layered Design

Kernelized Design

Reference Monitor

Correctness and Completeness

Secure Design Principles

Trusted Systems

5.3 Rootkits

Example: Phone Rootkits

Rootkit Characteristics

Rootkit Case Studies

Nonmalicious Rootkits

5.4 Conclusion

5.5 Exercises

Chapter 6 Networks

6.1 Network Concepts

Background: Network Transmission Media

Background: Protocol Layers

Background: Addressing and Routing

Part I War on Networks: Network Security Attacks

6.2 Threats to Network Communications

Interception: Eavesdropping and Wiretapping

Table of Contents

Modification: Data Corruption

Interruption: Loss of Service

Port Scanning

Network Vulnerability Summary

6.3 Wireless Network Security

WiFi Background

Vulnerabilities in Wireless Networks

Failed Countermeasure: WEP (Wired Equivalent Privacy)

Stronger Protocol Suite: WPA (WiFi Protected Access)

6.4 Denial of Service

Example: Massive Estonian Web Failure

How Service Is Denied

Flooding (Capacity) Attacks in Detail

Network Flooding Caused by Malicious Code

Network Flooding by Resource Exhaustion

Denial of Service by Addressing Failures

Traffic Redirection

DNS Attacks

Exploiting Known Vulnerabilities

Physical Disconnection

6.5 Distributed Denial of Service

Scripted Denial-of-Service Attacks

Bots

Botnets

Malicious Autonomous Mobile Agents

Autonomous Mobile Protective Agents

Part II Strategic Defenses: Security Countermeasures

6.6 Cryptography in Network Security

Network Encryption

Table of Contents

Browser Encryption

Onion Routing

IP Security Protocol Suite (IPsec)

Virtual Private Networks

6.7 Firewalls

System Architecture

What Is a Firewall?

Design of Firewalls

Types of Firewalls

Personal Firewalls

Comparison of Firewall Types

Examples of Firewall Configurations

Network Address Translation (NAT)

6.8 Intrusion Detection and Prevention Systems

Types of IDSs

Goals for Intrusion Detection Systems

IDS Strengths and Limitations

Intrusion Prevention Systems

Intrusion Response

6.10 Conclusion

6.9 Network Management

Management to Ensure Service

Security Information and Event Management

All-of-the-Above Products or Families

6.11 Exercises

Chapter 7 Data and Databases

7.1 Introduction to Databases

Concept of a Database

Components of Databases

Table of Contents

Advantages of Using Databases

7.2 Security Requirements of Databases

Integrity of the Database

Element Integrity

Auditability

Access Control

User Authentication

Availability

Integrity/Confidentiality/Availability

7.3 Reliability and Integrity

Protection Features from the Operating System

Two-Phase Update

Redundancy/Internal Consistency

Recovery

Concurrency/Consistency

7.4 Database Disclosure

Sensitive Data

Types of Disclosures

Preventing Disclosure: Data Suppression and Modification

Security versus Precision

7.5 Data Mining and Big Data

Data Mining

Big Data

Controls on U.S. Government Websites

7.6 Conclusion

7.7 Exercises

Chapter 8 New Territory

8.1 Introduction

Table of Contents

Cloud Computing

The Internet of Things

Embedded Systems

8.2 Cloud Architectures and Their Security

Essential Characteristics

Service Models

Deployment Models

Security in Cloud Computing

Identity Management in the Cloud

8.3 IoT and Embedded Devices

IoT and Security

8.4 Cloud, IoT, and Embedded DevicesThe Smart Home

Securing Smart Homes

Security Practices and Controls in the Smart Home

8.5 Smart Cities, IoT, Embedded Devices, and Cloud

Smart City Digital Architecture

Security and the Smart City

8.6 Cloud, IoT, and Critical Services

Healthcare

Security and the Internet of Medical Things

UtilitiesElectricity and Water

8.7 Conclusion

8.8 Exercises

Chapter 9 Privacy

9.1 Privacy Concepts

Aspects of Information Privacy

Computer-Related Privacy Problems

9.2 Privacy Principles and Policies

Table of Contents

Fair Information Practices

U.S. Privacy Laws

Controls on U.S. Government Websites

Controls on Commercial Websites

Non-U.S. Privacy Principles

Individual Actions to Protect Privacy

Governments and Privacy

Identity Theft

9.3 Authentication and Privacy

What Authentication Means

Conclusions

9.4 Data Mining

Government Data Mining

Privacy-Preserving Data Mining

9.5 Privacy on the Internet

Understanding the Online Environment

Payments on the Internet

Site and Portal Registrations

Whose Page Is This?

Precautions for Web Surfing

Spyware

Shopping on the Internet

9.6 Email and Message Security

Where Does Email Go, and Who Can Access It?

Monitoring Email

Anonymous, Pseudonymous, and Disappearing Email

Spoofing and Spamming

Summary

9.7 Privacy Impacts of Newer Technologies

Table of Contents

Radio Frequency Identification

Electronic Voting

Privacy in the Cloud

Conclusions on Newer Technologies

9.8 Conclusion

9.9 Exercises

Chapter 10 Management and Incidents

10.1 Security Planning

Organizations and Security Plans

Contents of a Security Plan

Security Planning Team Members

Assuring Commitment to a Security Plan

10.2 Business Continuity Planning

Assess Business Impact

Develop Strategy

Develop the Plan

10.3 Handling Incidents

Incident Response Plans

Incident Response Teams

10.4 Risk Analysis

The Nature of Risk

Steps of a Risk Analysis

Arguments For and Against Risk Analysis

10.5 Physical Threats to Systems

Natural Disasters

Human Vandals

Contingency Planning

Physical Security Recap

10.6 New Frontiers in Security Management

Table of Contents

10.7 Conclusion

10.8 Exercises

Chapter 11 Legal Issues and Ethics

11.1 Protecting Programs and Data

Copyrights

Patents

Trade Secrets

Special Cases

11.2 Information and the Law

Information as an Object

The Legal System

Summary of Protection for Computer Artifacts

11.3 Rights of Employees and Employers

Control of Products

Employment Contracts

11.4 Redress for Software Failures

Selling Correct Software

Reporting Software Flaws

11.5 Computer Crime

Examples of Statutes

International Dimensions

Why Computer Criminals Are Hard to Catch

What Computer Crime Statutes Do Not Address

Summary of Legal Issues in Computer Security

11.6 Ethical Issues in Computer Security

Differences Between the Law and Ethics

Studying Ethics

Ethical Reasoning

11.7 An Ethical Dive into Artificial Intelligence

Table of Contents

AI's Meaning and Concerns

IBM: A Study in How to Approach Ethical AI

11.8 Incident Analyses with Ethics

Situation I: Use of Computer Services

Situation II: Privacy Rights

Situation III: Denial of Service

Situation IV: Ownership of Programs

Situation V: Proprietary Resources

Situation VI: Fraud

Situation VII: Accuracy of Information

Situation VIII: Ethics of Hacking or Cracking

Situation IX: True Representation

Conclusion of Computer Ethics

11.9 Conclusion

11.10 Exercises

Chapter 12 Details of Cryptography

12.1 Cryptology

Cryptanalysis

Cryptographic Primitives

One-Time Pads

Statistical Analysis

What Makes a Secure Encryption Algorithm?

12.2 Symmetric Encryption Algorithms

DES

Attacking Ciphertext

AES

Other Symmetric Algorithms

12.3 Asymmetric Encryption

The RSA Algorithm

Table of Contents

Strength of the RSA Algorithm

Elliptic Curve Cryptosystems

Digression: DiffieHellman Key Exchange

12.4 Message Digests

Hash Functions

One-Way Hash Functions

Message Digests

Authenticated Encryption

12.5 Digital Signatures

12.6 Quantum Key Distribution

Key Distribution

Quantum Physics

Implementation

12.7 Conclusion

Chapter 13 Emerging Topics

13.1 AI and Cybersecurity

AI-Based Decision Making

AI-Driven Security Management

Adversarial AI

Responsible AI

Open Questions

13.2 Blockchains and Cryptocurrencies

What Is a Blockchain?

Commerce and Trust

What Is Cryptocurrency?

Cryptocurrency in the World Context

Is the Implementation of Cryptocurrencies Secure?

Open Questions

13.3 Offensive Cyber and Cyberwarfare

Table of Contents

What Is Cyberwarfare?

Possible Examples of Cyberwarfare

Cyberwar or Offensive Cyber?

Critical Issues

13.4 Quantum Computing and Computer Security

Quantum Computers

Quantum-Resistant Cryptography

13.5 Conclusion

Bibliography

Index