SECOND EDITION

# COMPUTER SECURITY

## [ ART and SCIENCE ]

MATT BISHOP

*With contributions from* ELISABETH SULLIVAN *and* MICHELLE RUPPEL

# Computer Security

## Second Edition

# Computer Security: Art and Science

## Table of Contents

Cover

Title Page

Copyright Page

Contents

Preface

Acknowledgments

About the Author

PART I: INTRODUCTION

Chapter 1 An Overview of Computer Security

1.1 The Basic Components

1.2 Threats

1.3 Policy and Mechanism

1.4 Assumptions and Trust

1.5 Assurance

1.6 Operational Issues

1.7 Human Issues

1.8 Tying It All Together

1.9 Summary

1.10 Research Issues

1.11 Further Reading

1.12 Exercises

PART II: FOUNDATIONS

Chapter 2 Access Control Matrix

2.1 Protection State

# Table of Contents

2.2 Access Control Matrix Model

2.3 Protection State Transitions

2.4 Copying, Owning, and the Attenuation of Privilege

2.5 Summary

2.6 Research Issues

2.7 Further Reading

2.8 Exercises

Chapter 3 Foundational Results

3.1 The General Question

3.2 Basic Results

3.3 The Take-Grant Protection Model

3.4 Closing the Gap: The Schematic Protection Model

3.5 Expressive Power and the Models

3.6 Comparing Security Properties of Models

3.7 Summary

3.8 Research Issues

3.9 Further Reading

3.10 Exercises

PART III: POLICY

Chapter 4 Security Policies

4.1 The Nature of Security Policies

4.2 Types of Security Policies

4.3 The Role of Trust

4.4 Types of Access Control

4.5 Policy Languages

4.6 Example: Academic Computer Security Policy

4.7 Security and Precision

4.8 Summary

4.9 Research Issues

4.10 Further Reading

# Table of Contents

4.11 Exercises

Chapter 5 Confidentiality Policies

5.1 Goals of Confidentiality Policies

5.2 The Bell-LaPadula Model

5.3 Tranquility

5.4 The Controversy over the Bell-LaPadula Model

5.5 Summary

5.6 Research Issues

5.7 Further Reading

5.8 Exercises

Chapter 6 Integrity Policies

6.1 Goals

6.2 The Biba Model

6.3 Lipner's Integrity Matrix Model

6.4 Clark-Wilson Integrity Model

6.5 Trust Models

6.6 Summary

6.7 Research Issues

6.8 Further Reading

6.9 Exercises

Chapter 7 Availability Policies

7.1 Goals of Availability Policies

7.2 Deadlock

7.3 Denial of Service Models

7.4 Example: Availability and Network Flooding

7.5 Summary

7.6 Research Issues

7.7 Further Reading

7.8 Exercises

Chapter 8 Hybrid Policies

# Table of Contents

8.1 Chinese Wall Model

8.2 Clinical Information Systems Security Policy

8.3 Originator Controlled Access Control

8.4 Role-Based Access Control

8.5 Break-the-Glass Policies

8.6 Summary

8.7 Research Issues

8.8 Further Reading

8.9 Exercises

Chapter 9 Noninterference and Policy Composition

9.1 The Problem

9.2 Deterministic Noninterference

9.3 Nondeducibility

9.4 Generalized Noninterference

9.5 Restrictiveness

9.6 Side Channels and Deducibility

9.7 Summary

9.8 Research Issues

9.9 Further Reading

9.10 Exercises

PART IV: IMPLEMENTATION I: CRYPTOGRAPHY

Chapter 10 Basic Cryptography

10.1 Cryptography

10.2 Symmetric Cryptosystems

10.3 Public Key Cryptography

10.4 Cryptographic Checksums

10.5 Digital Signatures

10.6 Summary

10.7 Research Issues

10.8 Further Reading

# Table of Contents

10.9 Exercises

Chapter 11 Key Management

11.1 Session and Interchange Keys

11.2 Key Exchange

11.3 Key Generation

11.4 Cryptographic Key Infrastructures

11.5 Storing and Revoking Keys

11.6 Summary

11.7 Research Issues

11.8 Further Reading

11.9 Exercises

Chapter 12 Cipher Techniques

12.1 Problems

12.2 Stream and Block Ciphers

12.3 Authenticated Encryption

12.4 Networks and Cryptography

12.5 Example Protocols

12.6 Summary

12.7 Research Issues

12.8 Further Reading

12.9 Exercises

Chapter 13 Authentication

13.1 Authentication Basics

13.2 Passwords

13.3 Password Selection

13.4 Attacking Passwords

13.5 Password Aging

13.6 Challenge-Response

13.7 Biometrics

13.8 Location

# Table of Contents

13.9 Multifactor Authentication

13.10 Summary

13.11 Research Issues

13.12 Further Reading

13.13 Exercises

PART V: IMPLEMENTATION II: SYSTEMS

Chapter 14 Design Principles

14.1 Underlying Ideas

14.2 Principles of Secure Design

14.3 Summary

14.4 Research Issues

14.5 Further Reading

14.6 Exercises

Chapter 15 Representing Identity

15.1 What Is Identity?

15.2 Files and Objects

15.3 Users

15.4 Groups and Roles

15.5 Naming and Certificates

15.6 Identity on the Web

15.7 Anonymity on the Web

15.8 Summary

15.9 Research Issues

15.10 Further Reading

15.11 Exercises

Chapter 16 Access Control Mechanisms

16.1 Access Control Lists

16.2 Capabilities

16.3 Locks and Keys

16.4 Ring-Based Access Control

# Table of Contents

16.5 Propagated Access Control Lists

16.6 Summary

16.7 Research Issues

16.8 Further Reading

16.9 Exercises

Chapter 17 Information Flow

17.1 Basics and Background

17.2 Nonlattice Information Flow Policies

17.3 Static Mechanisms

17.4 Dynamic Mechanisms

17.5 Integrity Mechanisms

17.6 Example Information Flow Controls

17.7 Summary

17.8 Research Issues

17.9 Further Reading

17.10 Exercises

Chapter 18 Confinement Problem

18.1 The Confinement Problem

18.2 Isolation

18.3 Covert Channels

18.4 Summary

18.5 Research Issues

18.6 Further Reading

18.7 Exercises

PART VI: ASSURANCE

Chapter 19 Introduction to Assurance

19.1 Assurance and Trust

19.2 Building Secure and Trusted Systems

19.3 Summary

19.4 Research Issues

# Table of Contents

19.5 Further Reading

19.6 Exercises

Chapter 20 Building Systems with Assurance

20.1 Assurance in Requirements Definition and Analysis

20.2 Assurance during System and Software Design

20.3 Assurance in Implementation and Integration

20.4 Assurance during Operation and Maintenance

20.5 Summary

20.6 Research Issues

20.7 Further Reading

20.8 Exercises

Chapter 21 Formal Methods

21.1 Formal Verification Techniques

21.2 Formal Specification

21.3 Early Formal Verification Techniques

21.4 Current Verification Systems

21.5 Functional Programming Languages

21.6 Formally Verified Products

21.7 Summary

21.8 Research Issues

21.9 Further Reading

21.10 Exercises

Chapter 22 Evaluating Systems

22.1 Goals of Formal Evaluation

22.2 TCSEC: 19831999

22.3 International Efforts and the ITSEC: 19912001

22.4 Commercial International Security Requirements: 1991

22.5 Other Commercial Efforts: Early 1990s

22.6 The Federal Criteria: 1992

22.7 FIPS 140: 1994Present

# Table of Contents

22.8 The Common Criteria: 1998Present

22.9 SSE-CMM: 1997Present

22.10 Summary

22.11 Research Issues

22.12 Further Reading

22.13 Exercises

PART VII: SPECIAL TOPICS

Chapter 23 Malware

23.1 Introduction

23.2 Trojan Horses

23.3 Computer Viruses

23.4 Computer Worms

23.5 Bots and Botnets

23.6 Other Malware

23.7 Combinations

23.8 Theory of Computer Viruses

23.9 Defenses

23.10 Summary

23.11 Research Issues

23.12 Further Reading

23.13 Exercises

Chapter 24 Vulnerability Analysis

24.1 Introduction

24.2 Penetration Studies

24.3 Vulnerability Classification

24.4 Frameworks

24.5 Standards

24.6 Gupta and Gligor's Theory of Penetration Analysis

24.7 Summary

24.8 Research Issues

# Table of Contents

24.9 Further Reading

24.10 Exercises

Chapter 25 Auditing

25.1 Definition

25.2 Anatomy of an Auditing System

25.3 Designing an Auditing System

25.4 A Posteriori Design

25.5 Auditing Mechanisms

25.6 Examples: Auditing File Systems

25.7 Summary

25.8 Research Issues

25.9 Further Reading

25.10 Exercises

Chapter 26 Intrusion Detection

26.1 Principles

26.2 Basic Intrusion Detection

26.3 Models

26.4 Architecture

26.5 Organization of Intrusion Detection Systems

26.6 Summary

26.7 Research Issues

26.8 Further Reading

26.9 Exercises

Chapter 27 Attacks and Responses

27.1 Attacks

27.2 Representing Attacks

27.3 Intrusion Response

27.4 Digital Forensics

27.5 Summary

27.6 Research Issues

# Table of Contents

27.7 Further Reading
27.8 Exercises
PART VIII: PRACTICUM
Chapter 28 Network Security
28.1 Introduction
28.2 Policy Development
28.3 Network Organization
28.4 Availability
28.5 Anticipating Attacks
28.6 Summary
28.7 Research Issues
28.8 Further Reading
28.9 Exercises
Chapter 29 System Security
29.1 Introduction
29.2 Policy
29.3 Networks
29.4 Users
29.5 Authentication
29.6 Processes
29.7 Files
29.8 Retrospective
29.9 Summary
29.10 Research Issues
29.11 Further Reading
29.12 Exercises
Chapter 30 User Security
30.1 Policy
30.2 Access
30.3 Files and Devices

# Table of Contents

30.4 Processes
30.5 Electronic Communications
30.6 Summary
30.7 Research Issues
30.8 Further Reading
30.9 Exercises
Chapter 31 Program Security
31.1 Problem
31.2 Requirements and Policy
31.3 Design
31.4 Refinement and Implementation
31.5 Common Security-Related Programming Problems
31.6 Testing, Maintenance, and Operation
31.7 Distribution
31.8 Summary
31.9 Research Issues
31.10 Further Reading
31.11 Exercises
PART IX: APPENDICES
Appendix A: Lattices
A.1 Basics
A.2 Lattices
A.3 Exercises
Appendix B: The Extended Euclidean Algorithm
B.1 The Euclidean Algorithm
B.2 The Extended Euclidean Algorithm
B.3 Solving ax mod n = 1
B.4 Solving ax mod n = b
B.5 Exercises
Appendix C: Entropy and Uncertainty

# Table of Contents

C.1 Conditional and Joint Probability
C.2 Entropy and Uncertainty
C.3 Joint and Conditional Entropy
C.4 Exercises
Appendix D: Virtual Machines
D.1 Virtual Machine Structure
D.2 Virtual Machine Monitor
D.3 Exercises
Appendix E: Symbolic Logic
E.1 Propositional Logic
E.2 Predicate Logic
E.3 Temporal Logic Systems
E.4 Exercises
Appendix F: The Encryption Standards
F.1 Data Encryption Standard
F.2 Advanced Encryption Standard
F.3 Exercises
Appendix G: Example Academic Security Policy
G.1 Acceptable Use Policy
G.2 University of California Electronic Communications Policy
G.3 User Advisories
G.4 Electronic CommunicationsAllowable Use
Appendix H: Programming Rules
H.1 Implementation Rules
H.2 Management Rules
References
Index

Pearson