CONTENTS IN DETAIL

ACKNOWLEDGMENTS xvii

INTRODUCTION xix

Who Should Read This Book? xx
About This Book. xx

1
WHAT IS INFORMATION SECURITY? 1

Defining Information Security 2
When Are You Secure? 2
Models for Discussing Security Issues 4
The Confidentiality, Integrity, and Availability Triad 4
The Parkerian Hexad 6
Attacks 8
Types of Attacks 8
Threats, Vulnerabilities, and Risk 10
Risk Management 11
Incident Response 15
Defense in Depth 17
Summary 20
Exercises 21

2
IDENTIFICATION AND AUTHENTICATION 23

Identification 24
Who We Claim to Be 24
Identity Verification 24
Falsifying Identification 25
Authentication 25
Factors 26
Multifactor Authentication 27
Mutual Authentication 27
Common Identification and Authentication Methods 28
Passwords 28
Biometrics 29
Hardware Tokens 32
Summary 33
Exercises 33

3
AUTHORIZATION AND ACCESS CONTROLS 35

What Are Access Controls? . . . 36
Implementing Access Controls . . . 37
    Access Control Lists . . . 38
    Capabilities . . . 42
Access Control Models . . . 43
    Discretionary Access Control . . . 43
    Mandatory Access Control . . . 43
    Rule-Based Access Control . . . 44
    Role-Based Access Control . . . 44
    Attribute-Based Access Control . . . 45
    Multilevel Access Control . . . 45
Physical Access Controls . . . 48
Summary . . . 50
Exercises . . . 50

4
AUDITING AND ACCOUNTABILITY 51

Accountability . . . 52
Security Benefits of Accountability . . . 53
    Nonrepudiation . . . 54
    Deterrence . . . 54
    Intrusion Detection and Prevention . . . 54
    Admissibility of Records . . . 55
Auditing . . . 55
    What Do You Audit? . . . 56
    Logging . . . 56
    Monitoring . . . 57
    Auditing with Assessments . . . 57
Summary . . . 59
Exercises . . . 59

5
CRYPTOGRAPHY 61

The History of Cryptography . . . 62
    The Caesar Cipher . . . 62
    Cryptographic Machines . . . 62
    Kerckhoffs's Principles . . . 66
Modern Cryptographic Tools . . . 66
    Keyword Ciphers and One-Time Pads . . . 67
    Symmetric and Asymmetric Cryptography . . . 68
    Hash Functions . . . 71
    Digital Signatures . . . 72
    Certificates . . . 73
Protecting Data at Rest, in Motion, and in Use . . . 74
    Protecting Data at Rest . . . 74
    Protecting Data in Motion . . . 75
    Protecting Data in Use . . . 76

Summary 77
Exercises 77

6
COMPLIANCE, LAWS, AND REGULATIONS 79

What Is Compliance? 79
Types of Compliance 80
Consequences of Noncompliance 81
Achieving Compliance with Controls 81
Types of Controls 81
Key vs. Compensating Controls 82
Maintaining Compliance 82
Laws and Information Security 83
Government-Related Regulatory Compliance 84
Industry-Specific Regulatory Compliance 85
Laws Outside of the United States 87
Adopting Frameworks for Compliance 87
International Organization for Standardization 88
National Institute of Standards and Technology 88
Custom Frameworks 89
Compliance amid Technological Changes 89
Compliance in the Cloud 89
Compliance with Blockchain 91
Compliance with Cryptocurrencies 92
Summary 92
Exercises 93

7
OPERATIONS SECURITY 95

The Operations Security Process 96
Identification of Critical Information 96
Analysis of Threats 97
Analysis of Vulnerabilities 97
Assessment of Risks 98
Application of Countermeasures 98
Laws of Operations Security 99
First Law: Know the Threats 99
Second Law: Know What to Protect 99
Third Law: Protect the Information 99
Operations Security in Our Personal Lives 100
Origins of Operations Security 101
Sun Tzu 102
George Washington 102
Vietnam War 103
Business 103
Interagency OPSEC Support Staff 103
Summary 104
Exercises 105

8
HUMAN ELEMENT SECURITY 107

Gathering Information for Social Engineering Attacks 108
- Human Intelligence 108
- Open Source Intelligence 108
- Other Kinds of Intelligence 113

Types of Social Engineering Attacks 114
- Pretexting 114
- Phishing 114
- Tailgating 116

Building Security Awareness with Security Training Programs 116
- Passwords 116
- Social Engineering Training 117
- Network Usage 117
- Malware 118
- Personal Equipment 118
- Clean Desk Policies 119
- Familiarity with Policy and Regulatory Knowledge 119

Summary 119

Exercises 120

9
PHYSICAL SECURITY 121

Identifying Physical Threats 122

Physical Security Controls 122
- Deterrent Controls 123
- Detective Controls 123
- Preventive Controls 124
- Using Physical Access Controls 124

Protecting People 125
- Physical Concerns for People 125
- Ensuring Safety 126
- Evacuation 126
- Administrative Controls 127

Protecting Data 127
- Physical Concerns for Data 127
- Accessibility of Data 128
- Residual Data 129

Protecting Equipment 129
- Physical Concerns for Equipment 129
- Site Selection 130
- Securing Access 131
- Environmental Conditions 131

Summary 132

Exercises 132

10
NETWORK SECURITY 133

Protecting Networks 134
- Designing Secure Networks 134

Using Firewalls . . . 135
Implementing Network Intrusion Detection Systems . . . 138
Protecting Network Traffic . . . 138
Using Virtual Private Networks . . . 139
Protecting Data over Wireless Networks . . . 139
Using Secure Protocols . . . 140
Network Security Tools . . . 140
Wireless Protection Tools . . . 141
Scanners . . . 141
Packet Sniffers . . . 142
Honeypots . . . 143
Firewall Tools . . . 143
Summary . . . 144
Exercises . . . 144

11
OPERATING SYSTEM SECURITY 145

Operating System Hardening . . . 146
Remove All Unnecessary Software . . . 146
Remove All Unessential Services . . . 147
Alter Default Accounts . . . 148
Apply the Principle of Least Privilege . . . 149
Perform Updates . . . 150
Turn On Logging and Auditing . . . 150
Protecting Against Malware . . . 151
Anti-malware Tools . . . 151
Executable Space Protection . . . 151
Software Firewalls and Host Intrusion Detection . . . 152
Operating System Security Tools . . . 153
Scanners . . . 153
Vulnerability Assessment Tools . . . 155
Exploit Frameworks . . . 156
Summary . . . 157
Exercises . . . 157

12
MOBILE, EMBEDDED, AND INTERNET OF THINGS SECURITY 159

Mobile Security . . . 160
Protecting Mobile Devices . . . 160
Mobile Security Issues . . . 162
Embedded Security . . . 164
Where Embedded Devices Are Used . . . 164
Embedded Device Security Issues . . . 166
Internet of Things Security . . . 167
What Is an IoT Device? . . . 167
IoT Security Issues . . . 169
Summary . . . 171
Exercises . . . 171

13
APPLICATION SECURITY 173
Software Development Vulnerabilities . . . 174
Buffer Overflows . . . 175
Race Conditions . . . 175
Input Validation Attacks . . . 176
Authentication Attacks . . . 177
Authorization Attacks. . . . 177
Cryptographic Attacks . . . 178
Web Security . . . 178
Client-Side Attacks . . . 178
Server-Side Attacks . . . 179
Database Security . . . 181
Protocol Issues . . . 182
Unauthenticated Access . . . 183
Arbitrary Code Execution . . . 183
Privilege Escalation . . . 183
Application Security Tools . . . 184
Sniffers . . . 184
Web Application Analysis Tools . . . 186
Fuzzers . . . 188
Summary . . . 188
Exercises. . . . 189

14
ASSESSING SECURITY 191
Vulnerability Assessment . . . 191
Mapping and Discovery. . . . 192
Scanning . . . 193
Technological Challenges for Vulnerability Assessment . . . 194
Penetration Testing . . . 195
The Penetration Testing Process . . . 196
Classifying Penetration Tests . . . 197
Targets of Penetration Tests . . . 198
Bug Bounty Programs. . . . 200
Technological Challenges for Penetration Testing . . . 201
Does This Really Mean You're Secure? . . . 202
Realistic Testing . . . 202
Can You Detect Your Own Attacks? . . . 203
Secure Today Doesn't Mean Secure Tomorrow . . . 204
Fixing Security Holes Is Expensive . . . 205
Summary . . . 205
Exercises. . . . 206

NOTES 207

INDEX 215