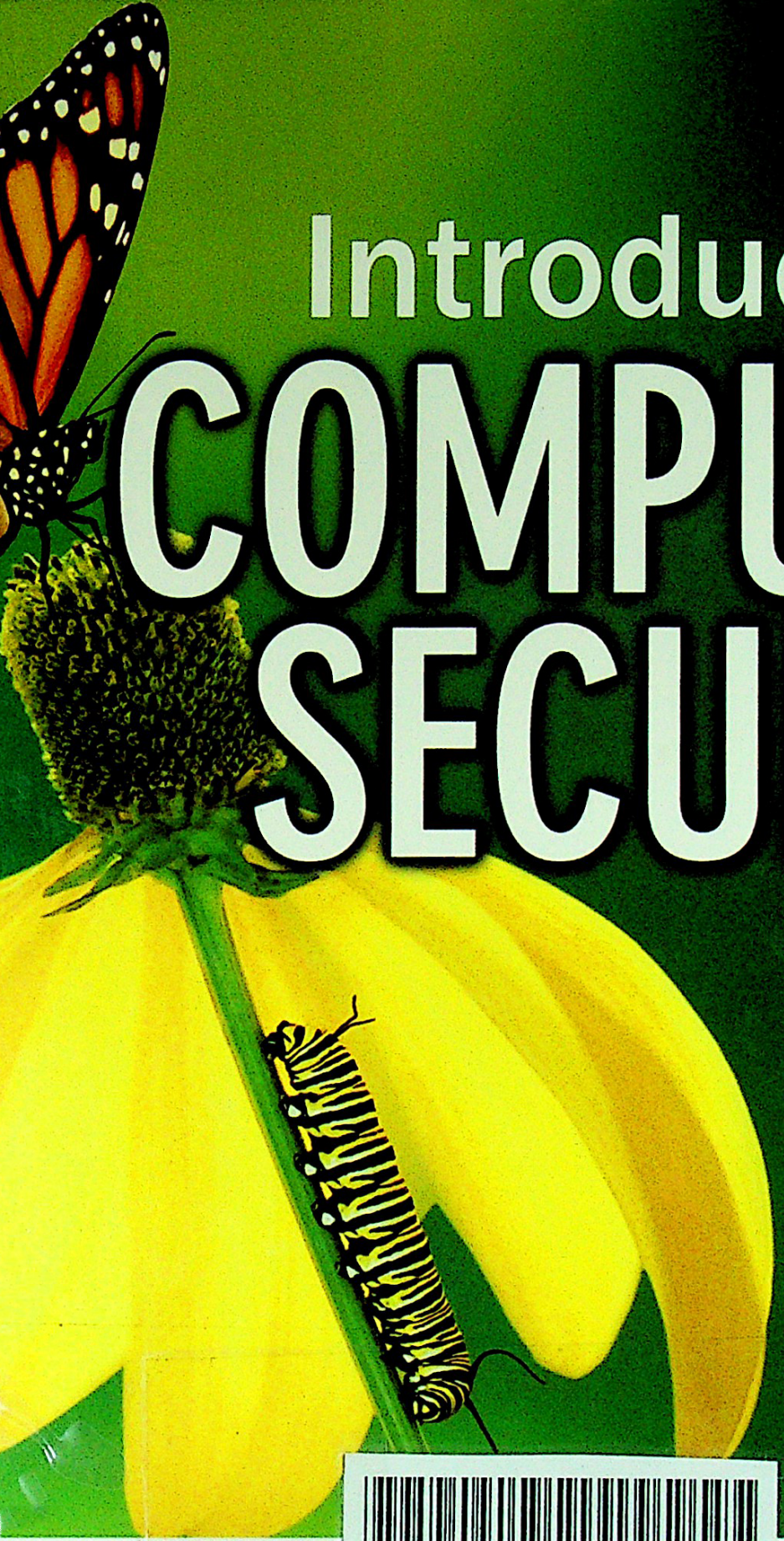
Introduction to COMPUTER SECURITY



SKN008804

Matt Bishop

005.8
B622

Introduction to Computer Security

Matt Bishop

THƯ VIỆN TRƯỜNG ĐHSPKT
SKN 008804

Addison-Wesley

Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

Preface ..... **xxv**
Goals xxvi
Philosophy xxvii
Organization xxix
Differences Between this Book and *Computer Security: Art and Science* xxx
Special Acknowledgment xxxi
Acknowledgments xxxi

Chapter 1 An Overview of Computer Security **1**
1.1 The Basic Components 1
1.1.1 Confidentiality 2
1.1.2 Integrity 3
1.1.3 Availability 4
1.2 Threats 4
1.3 Policy and Mechanism 7
1.3.1 Goals of Security 8
1.4 Assumptions and Trust 9
1.5 Assurance 10
1.5.1 Specification 11
1.5.2 Design 12
1.5.3 Implementation 12
1.6 Operational Issues 14
1.6.1 Cost-Benefit Analysis 14
1.6.2 Risk Analysis 15
1.6.3 Laws and Customs 16
1.7 Human Issues 17
1.7.1 Organizational Problems 18
1.7.2 People Problems 19
1.8 Tying It All Together 20
1.9 Summary 21
1.10 Further Reading 22
1.11 Exercises 22

Chapter 2 Access Control Matrix **27**
2.1 Protection State 27
2.2 Access Control Matrix Model 28
2.3 Protection State Transitions 31
2.3.1 Conditional Commands 33
2.4 Summary 34
2.5 Further Reading 35
2.6 Exercises 35

Chapter 3 Foundational Results **37**
3.1 The General Question 37
3.2 Basic Results 38
3.3 Summary 43
3.4 Further Reading 43
3.5 Exercises 44

Chapter 4 Security Policies **45**
4.1 Security Policies 45
4.2 Types of Security Policies 49
4.3 The Role of Trust 51
4.4 Types of Access Control 53
4.5 Example: Academic Computer Security Policy 54
4.5.1 General University Policy 55
4.5.2 Electronic Mail Policy 55
4.5.2.1 The Electronic Mail Policy Summary *56*
4.5.2.2 The Full Policy *56*
4.5.2.3 Implementation at UC Davis *57*
4.6 Summary 58
4.7 Further Reading 58
4.8 Exercises 59

Chapter 5 Confidentiality Policies **61**
5.1 Goals of Confidentiality Policies 61
5.2 The Bell-LaPadula Model 62
5.2.1 Informal Description 62
5.2.2 Example: The Data General B2 UNIX System 66
5.2.2.1 Assigning MAC Labels *66*
5.2.2.2 Using MAC Labels *69*
5.3 Summary 70
5.4 Further Reading 70
5.5 Exercises 71

Chapter 6 Integrity Policies **73**
6.1 Goals 73
6.2 Biba Integrity Model 75
6.3 Clark-Wilson Integrity Model 76
6.3.1 The Model 77
6.3.2 Comparison with the Requirements 79
6.3.3 Comparison with Other Models 80
6.4 Summary 81
6.5 Further Reading 81
6.6 Exercises 82

Chapter 7 Hybrid Policies **83**
7.1 Chinese Wall Model 83
7.1.1 Bell-LaPadula and Chinese Wall Models 86
7.1.2 Clark-Wilson and Chinese Wall Models 87
7.2 Clinical Information Systems Security Policy 88
7.2.1 Bell-LaPadula and Clark-Wilson Models 90
7.3 Originator Controlled Access Control 91
7.4 Role-Based Access Control 92
7.5 Summary 94
7.6 Further Reading 95
7.7 Exercises 95

Chapter 8 Basic Cryptography **97**
8.1 What Is Cryptography? 97
8.2 Classical Cryptosystems 98
8.2.1 Transposition Ciphers 99
8.2.2 Substitution Ciphers 100
8.2.2.1 Vigenère Cipher *101*
8.2.2.2 One-Time Pad *107*
8.2.3 Data Encryption Standard 108
8.2.4 Other Classical Ciphers 112
8.3 Public Key Cryptography 113
8.3.1 RSA 114
8.4 Cryptographic Checksums 116
8.4.1 HMAC 118
8.5 Summary 119
8.6 Further Reading 119
8.7 Exercises 120

Chapter 9 Key Management **123**
9.1 Session and Interchange Keys 124
9.2 Key Exchange 124
9.2.1 Classical Cryptographic Key Exchange and Authentication. . 125
9.2.2 Kerberos 128
9.2.3 Public Key Cryptographic Key Exchange and Authentication 129
9.3 Cryptographic Key Infrastructures 130
9.3.1 Certificate Signature Chains 131
9.3.1.1 X.509: Certification Signature Chains 132
9.3.1.2 PGP Certificate Signature Chains 134
9.3.2 Summary 136
9.4 Storing and Revoking Keys 136
9.4.1 Key Storage 136
9.4.2 Key Revocation 137
9.5 Digital Signatures 137
9.5.1 Classical Signatures 138
9.5.2 Public Key Signatures 139
9.6 Summary 140
9.7 Further Reading 141
9.8 Exercises 142

Chapter 10 Cipher Techniques **145**
10.1 Problems 145
10.1.1 Precomputing the Possible Messages 145
10.1.2 Misordered Blocks 146
10.1.3 Statistical Regularities 146
10.1.4 Summary 147
10.2 Stream and Block Ciphers 147
10.2.1 Stream Ciphers 148
10.2.1.1 Synchronous Stream Ciphers 148
10.2.1.2 Self-Synchronous Stream Ciphers 150
10.2.2 Block Ciphers 151
10.2.2.1 Multiple Encryption 152
10.3 Networks and Cryptography 153
10.4 Example Protocols 156
10.4.1 Secure Electronic Mail: PEM 156
10.4.1.1 Design Principles 157
10.4.1.2 Basic Design 158
10.4.1.3 Other Considerations 159
10.4.1.4 Conclusion 160

10.4.2 Security at the Network Layer: IPsec 161
10.4.2.1 IPsec Architecture 162
10.4.2.2 Authentication Header Protocol 165
10.4.2.3 Encapsulating Security Payload Protocol 166
10.4.3 Conclusion 167
10.5 Summary 168
10.6 Further Reading 168
10.7 Exercises 169

Chapter 11 Authentication 171
11.1 Authentication Basics 171
11.2 Passwords 172
11.2.1 Attacking a Password System 174
11.2.2 Countering Password Guessing 175
11.2.2.1 Random Selection of Passwords 176
11.2.2.2 Pronounceable and Other Computer-Generated Passwords 177
11.2.2.3 User Selection of Passwords 178
11.2.2.4 Reusable Passwords and Dictionary Attacks 182
11.2.2.5 Guessing Through Authentication Functions 183
11.2.3 Password Aging 184
11.3 Challenge-Response 186
11.3.1 Pass Algorithms 186
11.3.2 One-Time Passwords 187
11.3.3 Hardware-Supported Challenge-Response Procedures 188
11.3.4 Challenge-Response and Dictionary Attacks 189
11.4 Biometrics 190
11.4.1 Fingerprints 190
11.4.2 Voices 191
11.4.3 Eyes 191
11.4.4 Faces 191
11.4.5 Keystrokes 192
11.4.6 Combinations 192
11.4.7 Caution 192
11.5 Location 193
11.6 Multiple Methods 193
11.7 Summary 195
11.8 Further Reading 196
11.9 Exercises 196

Chapter 12 Design Principles **199**
12.1 Overview 199
12.2 Design Principles 201
12.2.1 Principle of Least Privilege 201
12.2.2 Principle of Fail-Safe Defaults 202
12.2.3 Principle of Economy of Mechanism 202
12.2.4 Principle of Complete Mediation 203
12.2.5 Principle of Open Design 204
12.2.6 Principle of Separation of Privilege 205
12.2.7 Principle of Least Common Mechanism 206
12.2.8 Principle of Psychological Acceptability 206
12.3 Summary 207
12.4 Further Reading 208
12.5 Exercises 208

Chapter 13 Representing Identity **211**
13.1 What Is Identity? 211
13.2 Files and Objects 212
13.3 Users 213
13.4 Groups and Roles 214
13.5 Naming and Certificates 215
13.5.1 The Meaning of the Identity 218
13.5.2 Trust 220
13.6 Identity on the Web 221
13.6.1 Host Identity 221
13.6.1.1 Static and Dynamic Identifiers *222*
13.6.1.2 Security Issues with the Domain Name Service *224*
13.6.2 State and Cookies 225
13.6.3 Anonymity on the Web 226
13.6.3.1 Anonymity for Better or Worse *230*
13.7 Summary 233
13.8 Further Reading 233
13.9 Exercises 234

Chapter 14 Access Control Mechanisms **237**
14.1 Access Control Lists 237
14.1.1 Abbreviations of Access Control Lists 238
14.1.2 Creation and Maintenance of Access Control Lists 240
14.1.2.1 Which Subjects Can Modify an Object's ACL? *241*
14.1.2.2 Do the ACLs Apply to a Privileged User? *241*
14.1.2.3 Does the ACL Support Groups and Wildcards? *242*

14.1.2.4 Conflicts *242*
14.1.2.5 ACLs and Default Permissions *243*
14.1.3 Revocation of Rights 243
14.1.4 Example: Windows NT Access Control Lists 244
14.2 Capabilities 246
14.2.1 Implementation of Capabilities 247
14.2.2 Copying and Amplifying Capabilities 248
14.2.3 Revocation of Rights 249
14.2.4 Limits of Capabilities 250
14.2.5 Comparison with Access Control Lists 251
14.3 Locks and Keys 252
14.3.1 Type Checking 253
14.4 Ring-Based Access Control 255
14.5 Propagated Access Control Lists 257
14.6 Summary 258
14.7 Further Reading 258
14.8 Exercises 259

Chapter 15 Information Flow 261
15.1 Basics and Background 261
15.1.1 Information Flow Models and Mechanisms 263
15.2 Compiler-Based Mechanisms 263
15.2.1 Declarations 264
15.2.2 Program Statements 266
15.2.2.1 Assignment Statements *266*
15.2.2.2 Compound Statements *267*
15.2.2.3 Conditional Statements *267*
15.2.2.4 Iterative Statements *268*
15.2.2.5 Goto Statements *269*
15.2.2.6 Procedure Calls *272*
15.2.3 Exceptions and Infinite Loops 272
15.2.4 Concurrency 274
15.2.5 Soundness 276
15.3 Execution-Based Mechanisms 277
15.3.1 Fenton's Data Mark Machine 278
15.3.2 Variable Classes 280
15.4 Example Information Flow Controls 281
15.4.1 Security Pipeline Interface 282
15.4.2 Secure Network Server Mail Guard 282
15.5 Summary 284
15.6 Further Reading 284
15.7 Exercises 285

Chapter 16 Confinement Problem **287**
16.1 The Confinement Problem 287
16.2 Isolation 290
16.2.1 Virtual Machines 290
16.2.2 Sandboxes 292
16.3 Covert Channels 294
16.3.1 Detection of Covert Channels 296
16.3.2 Mitigation of Covert Channels 303
16.4 Summary 306
16.5 Further Reading 306
16.6 Exercises 307

Chapter 17 Introduction to Assurance **309**
17.1 Assurance and Trust 309
17.1.1 The Need for Assurance 311
17.1.2 The Role of Requirements in Assurance 313
17.1.3 Assurance Throughout the Life Cycle 314
17.2 Building Secure and Trusted Systems 316
17.2.1 Life Cycle 316
17.2.1.1 Conception *317*
17.2.1.2 Manufacture *318*
17.2.1.3 Deployment *319*
17.2.1.4 Fielded Product Life *320*
17.2.2 The Waterfall Life Cycle Model 320
17.2.2.1 Requirements Definition and Analysis *320*
17.2.2.2 System and Software Design *321*
17.2.2.3 Implementation and Unit Testing *321*
17.2.2.4 Integration and System Testing *322*
17.2.2.5 Operation and Maintenance *322*
17.2.2.6 Discussion *322*
17.2.3 Other Models of Software Development 323
17.2.3.1 Exploratory Programming *323*
17.2.3.2 Prototyping *323*
17.2.3.3 Formal Transformation *323*
17.2.3.4 System Assembly from Reusable Components *324*
17.2.3.5 Extreme Programming *324*
17.3 Building Security In or Adding Security Later 324
17.4 Summary 328
17.5 Further Reading 328
17.6 Exercises 329

Chapter 18 Evaluating Systems **331**
18.1 Goals of Formal Evaluation 331
18.1.1 Deciding to Evaluate 332
18.1.2 Historical Perspective of Evaluation Methodologies 333
18.2 TCSEC: 1983–1999 334
18.2.1 TCSEC Requirements 335
18.2.1.1 TCSEC Functional Requirements *335*
18.2.1.2 TCSEC Assurance Requirements *336*
18.2.2 The TCSEC Evaluation Classes 337
18.2.3 The TCSEC Evaluation Process 338
18.2.4 Impacts 338
18.2.4.1 Scope Limitations *339*
18.2.4.2 Process Limitations *339*
18.2.4.3 Contributions *340*
18.3 FIPS 140: 1994–Present 341
18.3.1 FIPS 140 Requirements 341
18.3.2 FIPS 140-2 Security Levels 342
18.3.3 Impact 342
18.4 The Common Criteria: 1998–Present 343
18.4.1 Overview of the Methodology 344
18.4.2 CC Requirements 348
18.4.3 CC Security Functional Requirements 349
18.4.4 Assurance Requirements 351
18.4.5 Evaluation Assurance Levels 351
18.4.6 Evaluation Process 353
18.4.7 Impacts 354
18.4.8 Future of the Common Criteria 354
18.4.8.1 Interpretations *355*
18.4.8.2 Assurance Class AMA and Family ALC_FLR *355*
18.4.8.3 Products Versus Systems *355*
18.4.8.4 Protection Profiles and Security Targets *355*
18.4.8.5 Assurance Class AVA *356*
18.4.8.6 EAL5 ..... *356*
18.5 SSE-CMM: 1997–Present 356
18.5.1 The SSE-CMM Model 357
18.5.2 Using the SSE-CMM 358
18.6 Summary 359
18.7 Further Reading 360
18.8 Exercises 361

Security

Introduction to COMPUTER SECURITY

In this authoritative book, widely respected practitioner and teacher Matt Bishop presents a clear and useful introduction to the art and science of information security. Bishop's insights and realistic examples will help any practitioner or student understand the crucial links between security theory and the day-to-day security challenges of IT environments.

Bishop explains the fundamentals of security: the different types of widely used policies, the mechanisms that implement these policies, the principles underlying both policies and mechanisms, and how attackers can subvert these tools—as well as how to defend against attackers. A practicum demonstrates how to apply these ideas and mechanisms to a realistic company.

Coverage includes

- Confidentiality, integrity, and availability
- Operational issues, cost-benefit and risk analyses, legal and human factors
- Planning and implementing effective access control
- Defining security, confidentiality, and integrity policies
- Using cryptography and public-key systems, and recognizing their limits
- Understanding and using authentication: from passwords to biometrics
- Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more
- Controlling information flow through systems and networks
- Assuring security throughout the system lifecycle
- Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs—and defenses against them
- Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention
- Applying security principles to networks, systems, users, and programs

Introduction to Computer Security is adapted from Bishop's comprehensive and widely praised book, *Computer Security: Art and Science*. This shorter version of the original work omits much mathematical formalism, making it more accessible for professionals and students who have a less formal mathematical background, or for readers with a more practical than theoretical interest.

Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis. A recognized expert in vulnerability analysis, secure systems/software design, network security, access control, authentication, and UNIX security, Bishop also works to improve computer security instruction. He is the author of *Computer Security: Art and Science* (Addison-Wesley, 2003).

nformit.com/aw
http://nob.cs.ucdavis.edu/book

Text printed on recycled paper

Addison-Wesley
Pearson Education

ISBN-13: 978-0-321-24744-5
ISBN-10: 0-321-24744-2

9 780321 247445 58499

$84.99 US
$88.99 CANADA