INFORMATION SECURITY PRINCIPLES AND PRACTICE

Mark Stamp
San Jose State University

WILEY-
INTERSCIENCE
A JOHN WILEY & SONS, INC., PUBLICATION

CONTENTS

Preface xv

About The Author xix

Acknowledgments xxi

1 INTRODUCTION 1

1.1 The Cast of Characters 1
1.2 Alice's Online Bank 1
1.2.1 Confidentiality, Integrity, and Availability 2
1.2.2 Beyond CIA 2
1.3 About This Book 3
1.3.1 Cryptography 4
1.3.2 Access Control 4
1.3.3 Protocols 5
1.3.4 Software 6
1.4 The People Problem 6
1.5 Principles and Practice 7
1.6 Problems 7

I CRYPTO 9

2 CRYPTO BASICS 11

2.1 Introduction 11
2.2 How to Speak Crypto 12
2.3 Classic Crypto 13
2.3.1 Simple Substitution Cipher 13
2.3.2 Cryptanalysis of a Simple Substitution 15
2.3.3 Definition of Secure 16
2.3.4 Double Transposition Cipher 17
2.3.5 One-Time Pad 18
2.3.6 Project VENONA 21

2.3.7 Codebook Cipher 22
2.3.8 Ciphers of the Election of 1876 24
2.4 Modern Crypto History 26
2.5 A Taxonomy of Cryptography 28
2.6 A Taxonomy of Cryptanalysis 29
2.7 Summary 30
2.8 Problems 31

3 SYMMETRIC KEY CRYPTO 33

3.1 Introduction 33
3.2 Stream Ciphers 34
3.2.1 A5/1 34
3.2.2 RC4 36
3.3 Block Ciphers 38
3.3.1 Feistel Cipher 38
3.3.2 DES 39
3.3.3 Triple DES 44
3.3.4 AES 45
3.3.5 Three More Block Ciphers 48
3.3.6 TEA 49
3.3.7 Block Cipher Modes 50
3.4 Integrity 54
3.5 Summary 55
3.6 Problems 56

4 PUBLIC KEY CRYPTO 61

4.1 Introduction 61
4.2 Knapsack 63
4.3 RSA 66
4.3.1 RSA Example 67
4.3.2 Repeated Squaring 68
4.3.3 Speeding Up RSA 69
4.4 Diffie-Hellman 70
4.5 Elliptic Curve Cryptography 72
4.5.1 Elliptic Curve Math 72
4.5.2 ECC Diffie-Hellman 74
4.6 Public Key Notation 75
4.7 Uses for Public Key Crypto 76
4.7.1 Confidentiality in the Real World 76

4.7.2 Signatures and Non-repudiation 76
4.7.3 Confidentiality and Non-repudiation 77
4.8 Public Key Infrastructure 79
4.9 Summary 81
4.10 Problems 81

5 HASH FUNCTIONS AND OTHER TOPICS 85

5.1 What is a Hash Function? 85
5.2 The Birthday Problem 86
5.3 Non-Cryptographic Hashes 88
5.4 Tiger Hash 89
5.5 HMAC 93
5.6 Uses of Hash Functions 95
5.6.1 Online Bids 95
5.6.2 Spam Reduction 95
5.7 Other Crypto-Related Topics 96
5.7.1 Secret Sharing 97
5.7.2 Random Numbers 98
5.7.3 Information Hiding 100
5.8 Summary 104
5.9 Problems 104

6 ADVANCED CRYPTANALYSIS 109

6.1 Introduction 109
6.2 Linear and Differential Cryptanalysis 110
6.2.1 Quick Review of DES 110
6.2.2 Overview of Differential Cryptanalysis 111
6.2.3 Overview of Linear Cryptanalysis 114
6.2.4 Tiny DES 115
6.2.5 Differential Cryptanalysis of TDES 117
6.2.6 Linear Cryptanalysis of TDES 122
6.2.7 Block Cipher Design 124
6.3 Side Channel Attack on RSA 125
6.4 Lattice Reduction and the Knapsack 128
6.5 Hellman's Time-Memory Trade-Off 134
6.5.1 Popcnt 134
6.5.2 Cryptanalytic TMTO 135
6.5.3 Misbehaving Chains 139
6.5.4 Success Probability 143

6.6 Summary 144
6.7 Problems 144

II ACCESS CONTROL 151

7 AUTHENTICATION 153

7.1 Introduction 153
7.2 Authentication Methods 154
7.3 Passwords 154
7.3.1 Keys Versus Passwords 155
7.3.2 Choosing Passwords 156
7.3.3 Attacking Systems via Passwords 158
7.3.4 Password Verification 158
7.3.5 Math of Password Cracking 159
7.3.6 Other Password Issues 162
7.4 Biometrics 163
7.4.1 Types of Errors 164
7.4.2 Biometric Examples 165
7.4.3 Biometric Error Rates 170
7.4.4 Biometric Conclusions 170
7.5 Something You Have 170
7.6 Two-Factor Authentication 172
7.7 Single Sign-On and Web Cookies 172
7.8 Summary 173
7.9 Problems 173

8 AUTHORIZATION 177

8.1 Introduction 177
8.2 Access Control Matrix 178
8.2.1 ACLs and Capabilities 178
8.2.2 Confused Deputy 180
8.3 Multilevel Security Models 181
8.3.1 Bell-LaPadula 182
8.3.2 Biba's Model 184
8.4 Multilateral Security 184
8.5 Covert Channel 186
8.6 Inference Control 188
8.7 CAPTCHA 189
8.8 Firewalls 191
8.8.1 Packet Filter 192
8.8.2 Stateful Packet Filter 193

8.8.3 Application Proxy . . . 194
8.8.4 Personal Firewall . . . 195
8.8.5 Defense in Depth . . . 195
8.9 Intrusion Detection . . . 196
8.9.1 Signature-Based IDS . . . 198
8.9.2 Anomaly-Based IDS . . . 199
8.10 Summary . . . 203
8.11 Problems . . . 203

III PROTOCOLS 207

9 SIMPLE AUTHENTICATION PROTOCOLS . . . 209

9.1 Introduction . . . 209
9.2 Simple Security Protocols . . . 210
9.3 Authentication Protocols . . . 212
9.3.1 Authentication Using Symmetric Keys . . . 215
9.3.2 Authentication Using Public Keys . . . 217
9.3.3 Session Keys . . . 218
9.3.4 Perfect Forward Secrecy . . . 220
9.3.5 Mutual Authentication, Session Key, and PFS . . . 222
9.3.6 Timestamps . . . 222
9.4 Authentication and TCP . . . 224
9.5 Zero Knowledge Proofs . . . 226
9.6 The Best Authentication Protocol? . . . 230
9.7 Summary . . . 230
9.8 Problems . . . 230

10 REAL-WORLD SECURITY PROTOCOLS . . . 235

10.1 Introduction . . . 235
10.2 Secure Socket Layer . . . 236
10.2.1 SSL and the Man-in-the-Middle . . . 238
10.2.2 SSL Connections . . . 238
10.2.3 SSL Versus IPSec . . . 239
10.3 IPSec . . . 240
10.3.1 IKE Phase 1: Digital Signature . . . 241
10.3.2 IKE Phase 1: Symmetric Key . . . 243
10.3.3 IKE Phase 1: Public Key Encryption . . . 243
10.3.4 IPSec Cookies . . . 245
10.3.5 IKE Phase 1 Summary . . . 246
10.3.6 IKE Phase 2 . . . 246

10.3.7 IPSec and IP Datagrams 247
10.3.8 Transport and Tunnel Modes 247
10.3.9 ESP and AH 248
10.4 Kerberos 250
10.4.1 Kerberized Login 251
10.4.2 Kerberos Ticket 251
10.4.3 Kerberos Security 252
10.5 GSM 253
10.5.1 GSM Architecture 254
10.5.2 GSM Security Architecture 255
10.5.3 GSM Authentication Protocol 257
10.5.4 GSM Security Flaws 257
10.5.5 GSM Conclusions 259
10.5.6 3GPP 260
10.6 Summary 260
10.7 Problems 261

IV SOFTWARE 265

11 SOFTWARE FLAWS AND MALWARE 267

11.1 Introduction 267
11.2 Software Flaws 268
11.2.1 Buffer Overflow 270
11.2.2 Incomplete Mediation 279
11.2.3 Race Conditions 279
11.3 Malware 281
11.3.1 Brain 282
11.3.2 Morris Worm 282
11.3.3 Code Red 283
11.3.4 SQL Slammer 284
11.3.5 Trojan Example 284
11.3.6 Malware Detection 285
11.3.7 The Future of Malware 287
11.3.8 Cyber Diseases Versus Biological Diseases 289
11.4 Miscellaneous Software-Based Attacks 289
11.4.1 Salami Attacks 289
11.4.2 Linearization Attacks 290
11.4.3 Time Bombs 291
11.4.4 Trusting Software 292
11.5 Summary 292
11.6 Problems 292

12 INSECURITY IN SOFTWARE 295

12.1 Introduction 295
12.2 Software Reverse Engineering 296
12.2.1 Anti-Disassembly Techniques 300
12.2.2 Anti-Debugging Techniques 301
12.3 Software Tamper Resistance 302
12.3.1 Guards 302
12.3.2 Obfuscation 302
12.3.3 Metamorphism Revisited 303
12.4 Digital Rights Management 304
12.4.1 What is DRM? 305
12.4.2 A Real-World DRM System 308
12.4.3 DRM for Streaming Media 310
12.4.4 DRM for a P2P Application 312
12.4.5 DRM in the Enterprise 313
12.4.6 DRM Failures 314
12.4.7 DRM Conclusions 314
12.5 Software Development 315
12.5.1 Open Versus Closed Source Software 316
12.5.2 Finding Flaws 318
12.5.3 Other Software Development Issues 318
12.6 Summary 321
12.7 Problems 322

13 OPERATING SYSTEMS AND SECURITY 325

13.1 Introduction 325
13.2 Operating System Security Functions 326
13.2.1 Separation 326
13.2.2 Memory Protection 326
13.2.3 Access Control 328
13.3 Trusted Operating System 328
13.3.1 MAC, DAC, and More 329
13.3.2 Trusted Path 330
13.3.3 Trusted Computing Base 331
13.4 Next Generation Secure Computing Base 333
13.4.1 NGSCB Feature Groups 334
13.4.2 NGSCB Compelling Applications 336
13.4.3 Criticisms of NGSCB 336

13.5 Summary 338
13.6 Problems 338

APPENDIX 341

A-1 Network Security Basics 341
A-1.1 Introduction 341
A-1.2 The Protocol Stack 342
A-1.3 Application Layer 343
A-1.4 Transport Layer 345
A-1.5 Network Layer 347
A-1.6 Link Layer 349
A-1.7 Conclusions 350
A-2 Math Essentials 351
A-2.1 Modular Arithmetic 351
A-2.2 Permutations 352
A-2.3 Probability 353
A-2.4 Linear Algebra 353
A-3 DES S-Boxes 355

ANNOTATED BIBLIOGRAPHY 359

INDEX 381