Contents

List of Figures xi

List of Tables xv

Foreword xvii

About the Author xix

Acknowledgments xxi

Preface xxiii

1 Brief History of Computers, Communications, and Security 1
- 1.1 Pre-Renaissance 2
- 1.2 Renaissance to World War I 4
- 1.3 World War I 7
- 1.4 World War II 9
- 1.5 Cold War 14
- 1.6 Organized Crime and Botnets 18
- 1.7 Cyberwar 21
- 1.8 Problems 22
- 1.9 Glossary 23

2 Security and Privacy Overview 25
- 2.1 Introduction 25
- 2.2 Security Attributes 26
- 2.3 Social Engineering 29
  - 2.3.1 Nigerian 419 scams 31
  - 2.3.2 Spam 31
  - 2.3.3 Phishing 32
  - 2.3.4 Pharming 33
  - 2.3.5 Spear-phishing 34
  - 2.3.6 Mules 34
- 2.4 Authentication and Authorization 34
- 2.5 Access Permissions 38
  - 2.5.1 Unix file access permissions 38
  - 2.5.2 OASIS standards 40

2.6 Audit 42
2.7 User Interface Issues 43
2.8 On Trusting Trust 45
2.9 Taxonomy of Attacks 46
2.9.1 Vulnerabilities 47
2.9.2 Attacks 49
2.9.3 Advanced persistent threat 51
2.10 Case Study – Mobile Code 52
2.11 Case Study – Connected Vehicles 56
2.11.1 Anti-theft systems 58
2.11.2 Vehicular Ad Hoc Network (VANet) 60
2.11.3 Electronic control units 62
2.11.4 Integrated business services 63
2.11.5 Connected vehicle summary 67
2.12 Summary 69
2.13 Problems 69
2.14 Glossary 71

3 Cryptography Primer **75**
3.1 Introduction 75
3.2 Substitution Ciphers and Frequency Analysis 78
3.3 Vigenère Cipher and Cryptanalysis 80
3.4 Block Ciphers 82
3.4.1 Operations 83
3.4.2 Data Encryption Standard 84
3.4.3 Advanced Encryption Standard 85
3.4.4 ECB and CBC modes 87
3.4.5 Cryptanalysis 88
3.5 RSA Public Key Cryptography 90
3.6 Hash Functions 91
3.7 One-time Pads 92
3.8 Key Management 93
3.8.1 Notation and Communicating Sequential Processes (CSP) 93
3.8.2 Symmetric key distribution 93
3.8.3 Asymmetric key distribution and public key infrastructure (PKI) 94
3.9 Message Confidentiality 95
3.10 Steganography 96
3.11 Obfuscation and Homomorphic Encryption 96
3.12 Problems 99
3.13 Glossary 100

4 SSL/TLS – Case Study Project 103
4.1 Introduction 104
4.2 Cryptographic Protocol 105
4.3 Verification 107
4.4 DNS and Routing 111
4.5 X.509 and SSL Certificates 116
4.6 Man-in-the-Middle Attacks 120
4.7 Usability 121
4.8 Summary 122
4.9 Assignment 122
4.10 Problems 123
4.11 Glossary 123

5 Securing Networks 125
5.1 Introduction 125
5.2 Firewalls 126
5.3 Virtual Private Networks (VPNs) 127
5.4 Wireless Security 129
5.5 Intrusion Detection Systems (IDS) 131
5.5.1 Statistical IDS 131
5.5.2 Biologically inspired IDS 132
5.5.3 IDS testing 132
5.5.4 IDS products 134
5.6 Denial of Service 137
5.7 Problems 140
5.8 Glossary 140

6 Virtual Private Network – Case Study Project 143
6.1 Laboratory Preparation 143
6.2 Assignment 144
6.3 Virtual Machine (VM) Use 145
6.4 Sniffer Use 150
6.5 VPN Installation 152
6.6 Problems 153
6.7 Glossary 154

7 Insertion Attacks 155
7.1 SQL Injection 155
7.2 Buffer Overflow Attack 157
7.3 Printer Format Vulnerability 158
7.4 SSH Insertion Attacks 161
7.5 IDS Insertion Attacks 162
7.6 Viruses 163
7.7 Worms 164
7.8 Virus and Worm Propagation 166

7.9 Problems . . . 171
7.10 Glossary . . . 171

8 Buffer Overflow – Case Study Project 173
8.1 Stack Smashing . . . 174
8.1.1 Stack exploration . . . 179
8.1.2 Shell code . . . 182
8.2 Heap Smashing . . . 183
8.2.1 Code injection – heap spray . . . 184
8.2.2 Heap corruption . . . 184
8.3 Arc Injection . . . 185
8.4 Pointer Clobbering . . . 185
8.5 Countermeasures . . . 186
8.6 Assignment . . . 187
8.7 Problems . . . 188
8.8 Glossary . . . 189

9 Polymorphic Virus – Advanced Case Study Project 197
9.1 Virus Basics . . . 198
9.2 Anti-virus . . . 199
9.3 Pseudo-virus with Alternate Data Streams . . . 201
9.4 Simple Virus – Timid . . . 202
9.5 Infection Spreading . . . 203
9.6 Self-modifying Code . . . 205
9.7 Simple Polymorphism . . . 206
9.8 Packing and Encryption . . . 207
9.9 Frankenstein Viruses . . . 208
9.10 Assignment . . . 208
9.11 Problems . . . 209
9.12 Glossary . . . 209

10 Web Security 211
10.1 Cross Site Scripting (XSS) . . . 212
10.2 Cross Site Request Forgery (XSRF, CSRF) . . . 213
10.3 Man-in-the-Browser . . . 214
10.4 Penetration Testing . . . 214
10.5 Problems . . . 215
10.6 Glossary . . . 216

11 Privacy and Anonymity 217
11.1 Anonymity Metrics . . . 219
11.2 Anonymity Tools . . . 220
11.3 Computer Forensic Tools . . . 224
11.4 Privacy Laws . . . 226
11.5 Privacy Discussion Assignments – Antonin Scalia . . . 228
11.5.1 Dog poop girl . . . 228

11.5.2 Antonin Scalia 228
11.6 Problems 230
11.7 Glossary 230

12 Side-Channel Attacks 231
12.1 Power Analysis 232
12.2 Traffic Analysis 233
12.3 Time Analysis 234
12.4 Red-black Separation 236
12.5 Side-channel Countermeasures 236
12.6 Problems 238
12.7 Glossary 238

13 Digital Rights Management and Copyright 239
13.1 Copyright History 239
13.2 Fair Use 241
13.3 Creative Commons 241
13.4 Digital Rights Management 242
13.5 Digital Millennium Copyright Act 243
13.6 The Darknet 243
13.7 Patent Trolls 244
13.8 Discussion Assignment – Business Case for DRM 245
13.9 Discussion Assignment – Technical Case for DRM 245
13.10Glossary 245

14 Security Economics 247
14.1 Liability and EULAs 248
14.2 Network Externalities 248
14.3 Code Bloat 249
14.4 Lemon Markets 249
14.5 Software Engineering 249
14.6 Macroeconomics and Game Theory Introduction 250
14.7 Problems 250
14.8 Glossary 250

15 Conclusions 253

Bibliography 255

Index 289