Computer Communications and Networks

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers and nonspecialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach so that even the most complex of topics is presented in a lucid and intelligible manner.

For other titles published in this series, go to http://www.springer.com/

Joseph Migga Kizza

A Guide to Computer Network Security

Springer

Joseph Migga Kizza, PhD
University of Tennessee-Chattanooga
Department of Computer Science
615 McCallie Ave.
Chattanooga TN 37403
326 Grote Hall
USA
joseph-kizza@utc.edu

Series Editor
Professor A.J. Sammes, BSc, MPhil, PhD, FBCS, CEng
CISM Group, Cranfield University,
RMCS, Shrivenham, Swindon SN6 8LA,UK

CCN Series ISSN 1617-7975
ISBN 978-1-84800-916-5 e-ISBN 978-1-84800-917-2
DOI 10.1007/978-1-84800-917-2

Library of Congress Control Number: 2008942999

© Springer-Verlag London Limited 2009
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

springer.com

To the Trio: Immaculate, Josephine,
and Florence

Preface

If we are to believe in Moore's law, then every passing day brings new and advanced changes to the technology arena. We are as amazed by miniaturization of computing devices as we are amused by their speed of computation. Everything seems to be in flux and moving fast. We are also fast moving towards ubiquitous computing. To achieve this kind of computing landscape, new ease and seamless computing user interfaces have to be developed. Believe me, if you mature and have ever program any digital device, you are, like me, looking forward to this brave new computing landscape with anticipation.

However, if history is any guide to use, we in information security, and indeed every computing device user young and old, must brace themselves for a future full of problems. As we enter into this world of fast, small and concealable ubiquitous computing devices, we are entering fertile territory for dubious, mischievous, and malicious people. We need to be on guard because, as expected, help will be slow coming because first, well trained and experienced personnel will still be difficult to get and those that will be found will likely be very expensive as the case is today. Secondly, the security protocols and best practices will, as it is today, keep changing at a first rate which may warrant network administrators to constantly changing them. Thirdly, as the case is today, it will be extremely difficult to keep abreast of the many new vulnerabilities and patches to them. In other words, the computing landscape will change for sure on one side and remain the same on the other.

For these reasons, we need to remain vigilant with better, if not advanced computer and information security protocols and best practices because the frequency of computer network attacks and the vulnerability of computer network systems will likely not abet, rather they are likely to increase as before.

More efforts in developing adaptive and scalable security protocols and best practices and massive awareness, therefore, are needed to meet this growing challenge and bring the public to a level where they can be active and safe participants in the brave new worlds of computing.

This guide is a comprehensive volume touching not only on every major topic in computing and information security and assurance, but it also introduces new computing technologies like wireless sensor networks, a wave of the future, where

security is likely to be a major issues. It is intended to bring massive education and awareness of security issues and concerns in cyberspace in general and the computing world in particular, their benefits to society, the security problems and the dangers likely to be encountered by the users, and be a pathfinder as it initiates a dialog towards developing better algorithms, protocols, and best practices that will enhance security of computing systems in the anticipated brave new world. It does this comprehensively in four parts and twenty-two chapters. Part I gives the reader an understanding of the working of and the security situation of computer networks. Part II builds on this knowledge and exposes the reader to the prevailing security situation based on a constant security threat. It surveys several security threats. Part III, the largest, forms the core of the guide and presents to the reader most of the best practices and solutions that are currently in use. Part IV is for projects. In addition to the algorithms, protocols, and solutions, several products and services are given for each security item under discussion.

In summary, the guide attempts to achieve the following objectives:

1 Educate the public about cyberspace security in general terms and computer systems security in particular, with reference to the Internet,
2 Alert the public to the magnitude of computer network vulnerabilities, weaknesses, and loopholes inherent in the computer network infrastructure
3 Bring to the public attention effective security solutions and best practice, expert opinions on those solutions, and the possibility of ad-hoc solutions
4 Look at the roles legislation, regulation, and enforcement play in computer network security efforts
5 Finally, initiate a debate on developing effective and comprehensive algorithms, protocols, and best practices for information security.

Since the guide covers a wide variety of security topics, algorithms, solutions, and best practices, it is intended to be both a teaching and a reference tool for all interested in learning about computer network security issues and available techniques to prevent information systems attacks. The depth and thorough discussion and analysis of most of the computer network security issues, together with the discussion of security algorithms, and solutions given, makes the guide a unique reference source of ideas for computer network security personnel, network security policy makers, and those reading for leisure. In addition, the guide provokes the reader by raising valid legislative, legal, social, and ethical security issues, including the increasingly diminishing line between individual privacy and the need for collective and individual security.

The guide targets college students in computer science, information science, technology studies, library sciences, engineering, and to a lesser extent students in the arts and sciences who are interested in information technology. In addition, students in information management sciences will find the guide particularly helpful. Practitioners, especially those working in information-intensive areas, will likewise find the guide a good reference source. It will also be valuable to those interested in any aspect of information security and assurance and those simply wanting to become cyberspace literates.

Book Resources

There are two types of exercises at the end of chapter: easy and quickly workable exercises whose responses can be easily spotted from the proceeding text; and more though provoking advanced exercises whole responses may require research outside the content of this book. Also chapter 22 is devoted to lab exercises. There are three types of lab exercises: weekly or bi-weekly assignments that can be done easily with either reading or using readily available software and hardware tools; slightly harder semester long projects that may require extensive time, collaboration, and some research to finish them successfully; and hard open research projects that require a lot of thinking, take a lot of time, and require extensive research.

We have tried as much as possible, throughout the guide, to use open source software tools. This has two consequences to it: one, it makes the guide affordable keeping in mind the escalating proprietary software prices; and two, it makes the content and related software tools last longer because the content and corresponding exercises and labs are not based on one particular proprietary software tool that can go out anytime.

Instructor Support Materials

As you consider using this book, you may need to know that we have developed materials to help you with your course. The help materials for both instructors and students cover the following areas:

- Syllabus. There is a suggested syllabus for the instructor.
- Instructor PowerPoint slides. These are detailed enough to help the instructor, especially those teaching the course for the first time.
- Answers to selected exercises at the end of each chapter
- Laboratory. Since network security is a hands-on course, students need to spend a considerable amount of time on scheduled laboratory exercises. The last chapter of the book contains several laboratory exercises and projects. The book resource center contains several more and updates
- Instructor manual. These will guide the instructor in the day to day job of getting materials ready for the class.
- Student laboratory materials. Under this section, we will be continuously posting the latest laboratory exercises, software, and challenge projects.

These materials can be found at the publisher's website at
http://www.springeronline.com and at the author's site at http://www.utc.edu/Faculty/Joseph-Kizza/

Chattanooga, Tennessee, USA Joseph Migga Kizza
October, 2008.

Contents

Part I Understanding Computer Network Security

1 Computer Network Fundamentals 3
1.1 Introduction 3
1.2 Computer Network Models 4
1.3 Computer Network Types 5
1.3.1 Local Area Networks (LANs) 5
1.3.2 Wide Area Networks (WANs) 6
1.3.3 Metropolitan Area Networks (MANs) 6
1.4 Data Communication Media Technology 7
1.4.1 Transmission Technology 7
1.4.2 Transmission Media 10
1.5 Network Topology 13
1.5.1 Mesh 13
1.5.2 Tree 13
1.5.3 Bus 14
1.5.4 Star 15
1.5.5 Ring 15
1.6 Network Connectivity and Protocols 16
1.6.1 Open System Interconnection (OSI) Protocol Suite 18
1.6.2 Transport Control Protocol/Internet Protocol (TCP/IP) Model 19
1.7 Network Services 22
1.7.1 Connection Services 22
1.7.2 Network Switching Services 24
1.8 Network Connecting Devices 26
1.8.1 LAN Connecting Devices 26
1.8.2 Internetworking Devices 30
1.9 Network Technologies 34
1.9.1 LAN Technologies 35
1.9.2 WAN Technologies 37
1.9.3 Wireless LANs 39
1.10 Conclusion 40

Exercises 40

Advanced Exercises 41

References 41

2 Understanding Computer Network Security 43
2.1 Introduction 43
2.1.1 Computer Security 44
2.1.2 Network Security 45
2.1.3 Information Security 45
2.2 Securing the Computer Network 45
2.2.1 Hardware 46
2.2.2 Software 46
2.3 Forms of Protection 46
2.3.1 Access Control 46
2.3.2 Authentication 48
2.3.3 Confidentiality 48
2.3.4 Integrity 49
2.3.5 Nonrepudiation 49
2.4 Security Standards 50
2.4.1 Security Standards Based on Type of Service/Industry 51
2.4.2 Security Standards Based on Size/Implementation 54
2.4.3 Security Standards Based on Interests 55
2.4.4 Best Practices in Security 56

Exercises 58

Advanced Exercises 58

References 59

Part II Security Challenges to Computer Networks

3 Security Threats to Computer Networks 63
3.1 Introduction 63
3.2 Sources of Security Threats 64
3.2.1 Design Philosophy 65
3.2.2 Weaknesses in Network Infrastructure and Communication Protocols 65
3.2.3 Rapid Growth of Cyberspace 68
3.2.4 The Growth of the Hacker Community 69
3.2.5 Vulnerability in Operating System Protocol 78
3.2.6 The Invisible Security Threat – The Insider Effect 79

3.2.7 Social Engineering 79
3.2.8 Physical Theft 80
3.3 Security Threat Motives 80
3.3.1 Terrorism 80
3.3.2 Military Espionage 81
3.3.3 Economic Espionage 81
3.3.4 Targeting the National Information Infrastructure 82
3.3.5 Vendetta/Revenge 82
3.3.6 Hate (National Origin, Gender, and Race) 83
3.3.7 Notoriety 83
3.3.8 Greed 83
3.3.9 Ignorance 83
3.4 Security Threat Management 83
3.4.1 Risk Assessment 84
3.4.2 Forensic Analysis 84
3.5 Security Threat Correlation 84
3.5.1 Threat Information Quality 85
3.6 Security Threat Awareness 85

Exercises 86

Advanced Exercises 87

References 88

4 Computer Network Vulnerabilities 89
4.1 Definition 89
4.2 Sources of Vulnerabilities 89
4.2.1 Design Flaws 90
4.2.2 Poor Security Management 93
4.2.3 Incorrect Implementation 94
4.2.4 Internet Technology Vulnerability 95
4.2.5 Changing Nature of Hacker Technologies and Activities 99
4.2.6 Difficulty of Fixing Vulnerable Systems 100
4.2.7 Limits of Effectiveness of Reactive Solutions 101
4.2.8 Social Engineering 102
4.3 Vulnerability Assessment 103
4.3.1 Vulnerability Assessment Services 104
4.3.2 Advantages of Vulnerability Assessment Services 105

Exercises 105

Advanced Exercises 106

References 106

5 Cyber Crimes and Hackers 107
5.1 Introduction 107
5.2 Cyber Crimes 108
5.2.1 Ways of Executing Cyber Crimes 108
5.2.2 Cyber Criminals 111
5.3 Hackers 112
5.3.1 History of Hacking 112
5.3.2 Types of Hackers 115
5.3.3 Hacker Motives 118
5.3.4 Hacking Topologies 121
5.3.5 Hackers' Tools of System Exploitation 126
5.3.6 Types of Attacks 128
5.4 Dealing with the Rising Tide of Cyber Crimes 129
5.4.1 Prevention 129
5.4.2 Detection 130
5.4.3 Recovery 130
5.5 Conclusion 130

Exercises 131

Advanced Exercises 131

References 131

6 Hostile Scripts 133
6.1 Introduction 133
6.2 Introduction to the Common Gateway Interface (CGI) 133
6.3 CGI Scripts in a Three-Way Handshake 134
6.4 Server–CGI Interface 136
6.5 CGI Script Security Issues 137
6.6 Web Script Security Issues 138
6.7 Dealing with the Script Security Problems 139
6.8 Scripting Languages 139
6.8.1 Server-Side Scripting Languages 139
6.8.2 Client-Side Scripting Languages 141

Exercises 143

Advanced Exercises 143

References 143

7 Security Assessment, Analysis, and Assurance 145
7.1 Introduction 145
7.2 System Security Policy 147

7.3 Building a Security Policy 149
7.3.1 Security Policy Access Rights Matrix 149
7.3.2 Policy and Procedures 151
7.4 Security Requirements Specification 155
7.5 Threat Identification 156
7.5.1 Human Factors 156
7.5.2 Natural Disasters 157
7.5.3 Infrastructure Failures 157
7.6 Threat Analysis 159
7.6.1 Approaches to Security Threat Analysis 160
7.7 Vulnerability Identification and Assessment 161
7.7.1 Hardware 161
7.7.2 Software 162
7.7.3 Humanware 163
7.7.4 Policies, Procedures, and Practices 163
7.8 Security Certification 165
7.8.1 Phases of a Certification Process 165
7.8.2 Benefits of Security Certification 166
7.9 Security Monitoring and Auditing 166
7.9.1 Monitoring Tools 166
7.9.2 Type of Data Gathered 167
7.9.3 Analyzed Information 167
7.9.4 Auditing 168
7.10 Products and Services 168

Exercises 168

Advanced Exercises 169

References 169

Additional References 169

Part III Dealing with Network Security Challenges

8 Disaster Management 173
8.1 Introduction 173
8.1.1 Categories of Disasters 174
8.2 Disaster Prevention 175
8.3 Disaster Response 177
8.4 Disaster Recovery 177
8.4.1 Planning for a Disaster Recovery 178
8.4.2 Procedures of Recovery 179
8.5 Make your Business Disaster Ready 181

8.5.1 Always Be Ready for a Disaster 182
8.5.2 Always Backup Media 182
8.5.3 Risk Assessment 182
8.6 Resources for Disaster Planning and Recovery 182
8.6.1 Local Disaster Resources 183

Exercises 183

Advanced Exercises – Case Studies 183

References 184

9 Access Control and Authorization 185
9.1 Definitions 185
9.2 Access Rights 185
9.2.1 Access Control Techniques and Technologies 187
9.3 Access Control Systems 192
9.3.1 Physical Access Control 192
9.3.2 Access Cards 192
9.3.3 Electronic Surveillance 193
9.3.4 Biometrics 194
9.3.5 Event Monitoring 197
9.4 Authorization 197
9.4.1 Authorization Mechanisms 198
9.5 Types of Authorization Systems 199
9.5.1 Centralized 199
9.5.2 Decentralized 200
9.5.3 Implicit 200
9.5.4 Explicit 201
9.6 Authorization Principles 201
9.6.1 Least Privileges 201
9.6.2 Separation of Duties 201
9.7 Authorization Granularity 202
9.7.1 Fine Grain Authorization 202
9.7.2 Coarse Grain Authorization 202
9.8 Web Access and Authorization 203

Exercises 203

Advanced Exercises 204

References 204

10 Authentication 207
10.1 Definition 207
10.2 Multiple Factors and Effectiveness of Authentication 208
10.3 Authentication Elements 210
10.3.1 Person or Group Seeking Authentication 210
10.3.2 Distinguishing Characteristics for Authentication 210
10.3.3 The Authenticator 211
10.3.4 The Authentication Mechanism 211
10.3.5 Access Control Mechanism 212
10.4 Types of Authentication 212
10.4.1 Nonrepudiable Authentication 212
10.4.2 Repudiable Authentication 213
10.5 Authentication Methods 213
10.5.1 Password Authentication 214
10.5.2 Public-Key Authentication 216
10.5.3 Remote Authentication 220
10.5.4 Anonymous Authentication 222
10.5.5 Digital Signature-Based Authentication 222
10.5.6 Wireless Authentication 223
10.6 Developing an Authentication Policy 223

Exercises 224

Advanced Exercises 225

References 225

11 Cryptography 227
11.1 Definition 227
11.1.1 Block Ciphers 229
11.2 Symmetric Encryption 230
11.2.1 Symmetric Encryption Algorithms 231
11.2.2 Problems with Symmetric Encryption 233
11.3 Public Key Encryption 233
11.3.1 Public Key Encryption Algorithms 236
11.3.2 Problems with Public Key Encryption 236
11.3.3 Public Key Encryption Services 236
11.4 Enhancing Security: Combining Symmetric and Public Key Encryptions 237
11.5 Key Management: Generation, Transportation, and Distribution 237
11.5.1 The Key Exchange Problem 237
11.5.2 Key Distribution Centers (KDCs) 238
11.5.3 Public Key Management 240
11.5.4 Key Escrow 242

11.6 Public Key Infrastructure (PKI) 243
11.6.1 Certificates 244
11.6.2 Certificate Authority 244
11.6.3 Registration Authority (RA) 244
11.6.4 Lightweight Directory Access Protocols (LDAP) 244
11.6.5 Role of Cryptography in Communication 245
11.7 Hash Function 245
11.8 Digital Signatures 246

Exercises 247

Advanced Exercises 248

References 248

12 Firewalls 249
12.1 Definition 249
12.2 Types of Firewalls 252
12.2.1 Packet Inspection Firewalls 253
12.2.2 Application Proxy Server: Filtering Based on Known Services 257
12.2.3 Virtual Private Network (VPN) Firewalls 261
12.2.4 Small Office or Home (SOHO) Firewalls 262
12.3 Configuration and Implementation of a Firewall 263
12.4 The Demilitarized Zone (DMZ) 264
12.4.1 Scalability and Increasing Security in a DMZ 266
12.5 Improving Security Through the Firewall 267
12.6 Firewall Forensics 268
12.7 Firewall Services and Limitations 269
12.7.1 Firewall Services 269
12.7.2 Limitations of Firewalls 269

Exercises 270

Advanced Exercises 270

References 271

13 System Intrusion Detection and Prevention 273
13.1 Definition 273
13.2 Intrusion Detection 273
13.2.1 The System Intrusion Process 274
13.2.2 The Dangers of System Intrusions 275

13.3 Intrusion Detection Systems (IDSs) 276
13.3.1 Anomaly Detection 277
13.3.2 Misuse Detection 279
13.4 Types of Intrusion Detection Systems 279
13.4.1 Network-Based Intrusion Detection Systems (NIDSs) 280
13.4.2 Host-Based Intrusion Detection Systems (HIDSs) 285
13.4.3 The Hybrid Intrusion Detection System 287
13.5 The Changing Nature of IDS Tools 287
13.6 Other Types of Intrusion Detection Systems 288
13.6.1 System Integrity Verifiers (SIVs) 288
13.6.2 Log File Monitors (LFM) 288
13.6.3 Honeypots 288
13.7 Response to System Intrusion 290
13.7.1 Incident Response Team 290
13.7.2 IDS Logs as Evidence 291
13.8 Challenges to Intrusion Detection Systems 291
13.8.1 Deploying IDS in Switched Environments 292
13.9 Implementing an Intrusion Detection System 292
13.10 Intrusion Prevention Systems (IPSs) 293
13.10.1 Network-Based Intrusion Prevention Systems (NIPSs) 293
13.10.2 Host-Based Intrusion Prevention Systems (HIPSs) 295
13.11 Intrusion Detection Tools 295

Exercises 297

Advanced Exercises 297

References 298

14 Computer and Network Forensics 299
14.1 Definition 299
14.2 Computer Forensics 300
14.2.1 History of Computer Forensics 301
14.2.2 Elements of Computer Forensics 302
14.2.3 Investigative Procedures 303
14.2.4 Analysis of Evidence 309
14.3 Network Forensics 315
14.3.1 Intrusion Analysis 316
14.3.2 Damage Assessment 321
14.4 Forensics Tools 321
14.4.1 Computer Forensic Tools 322
14.4.2 Network Forensic Tools 326

Exercises 327

Advanced Exercises 328

References 328

15 Virus and Content Filtering 331
15.1 Definition 331
15.2 Scanning, Filtering, and Blocking 331
15.2.1 Content Scanning 332
15.2.2 Inclusion Filtering 332
15.2.3 Exclusion Filtering 333
15.2.4 Other Types of Content Filtering 333
15.2.5 Location of Content Filters 335
15.3 Virus Filtering 336
15.3.1 Viruses 336
15.4 Content Filtering 344
15.4.1 Application Level Filtering 344
15.4.2 Packet-Level Filtering and Blocking 346
15.4.3 Filtered Material 347
15.5 Spam 348

Exercises 350

Advanced Exercises 350

References 350

16 Standardization and Security Criteria: Security Evaluation of Computer Products 351
16.1 Introduction 351
16.2 Product Standardization 352
16.2.1 Need for the Standardization of (Security) Products 352
16.2.2 Common Computer Product Standards 353
16.3 Security Evaluations 354
16.3.1 Purpose of Evaluation 354
16.3.2 Security Evaluation Criteria 354
16.3.3 Basic Elements of an Evaluation 355
16.3.4 Outcomes/Benefits 355
16.4 Major Security Evaluation Criteria 357
16.4.1 Common Criteria (CC) 357
16.4.2 FIPS 358
16.4.3 The Orange Book/TCSEC 358

16.4.4 Information Technology Security Evaluation Criteria (ITSEC) 361
16.4.5 The Trusted Network Interpretation (TNI): The Red Book 361
16.5 Does Evaluation Mean Security? 362

Exercises 362

Advanced Exercises 363

References 363

17 Computer Network Security Protocols 365
17.1 Introduction 365
17.2 Application Level Security 366
17.2.1 Pretty Good Privacy (PGP) 368
17.2.2 Secure/Multipurpose Internet Mail Extension (S/MIME) 368
17.2.3 Secure-HTTP (S-HTTP) 369
17.2.4 Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) 373
17.2.5 Secure Electronic Transactions (SET) 373
17.2.6 Kerberos 375
17.3 Security in the Transport Layer 378
17.3.1 Secure Socket Layer (SSL) 378
17.3.2 Transport Layer Security (TLS) 382
17.4 Security in the Network Layer 382
17.4.1 Internet Protocol Security (IPSec) 382
17.4.2 Virtual Private Networks (VPN) 387
17.5 Security in the Link Layer and over LANS 391
17.5.1 Point-to-Point Protocol (PPP) 391
17.5.2 Remote Authentication Dial-In User Service (RADIUS) 392
17.5.3 Terminal Access Controller Access Control System (TACACS+) 394

Exercises 394

Advanced Exercises 395

References 395

18 Security in Wireless Networks and Devices 397
18.1 Introduction 397
18.2 Cellular Wireless Communication Network Infrastructure 397
18.2.1 Development of Cellular Technology 400
18.2.2 Limited and Fixed Wireless Communication Networks 404
18.3 Wireless LAN (WLAN) or Wireless Fidelity (Wi-Fi) 406
18.3.1 WLAN (Wi-Fi) Technology 406
18.3.2 Mobile IP and Wireless Application Protocol (WAP) 407
18.4 Standards for Wireless Networks 410
18.4.1 The IEEE 802.11 410
18.4.2 Bluetooth 411
18.5 Security in Wireless Networks 413
18.5.1 WLANs Security Concerns 413
18.5.2 Best Practices for Wi-Fi Security 419
18.5.3 Hope on the Horizon for WEP 420

Exercises 420

Advanced Exercises 421

References 422

19 Security in Sensor Networks 423
19.1 Introduction 423
19.2 The Growth of Sensor Networks 424
19.3 Design Factors in Sensor Networks 425
19.3.1 Routing 425
19.3.2 Power Consumption 428
19.3.3 Fault Tolerance 428
19.3.4 Scalability 428
19.3.5 Product Costs 428
19.3.6 Nature of Hardware Deployed 428
19.3.7 Topology of Sensor Networks 429
19.3.8 Transmission Media 429
19.4 Security in Sensor Networks 429
19.4.1 Security Challenges 429
19.4.2 Sensor Network Vulnerabilities and Attacks 431
19.4.3 Securing Sensor Networks 432
19.5 Security Mechanisms and Best Practices for Sensor Networks 433

19.6 Trends in Sensor Network Security Research 434
19.6.1 Cryptography 435
19.6.2 Key Management 435
19.6.3 Confidentiality, Authentication, and Freshness 436
19.6.4 Resilience to Capture 436

Exercises 437

Advanced Exercises 437

References 438

20 Other Efforts to Secure Information and Computer Networks 439
20.1 Introduction 439
20.2 Legislation 439
20.3 Regulation 440
20.4 Self-Regulation 440
20.4.1 Hardware-Based Self-Regulation 441
20.4.2 Software-Based Self-Regulation 441
20.5 Education 442
20.5.1 Focused Education 443
20.5.2 Mass Education 444
20.6 Reporting Centers 444
20.7 Market Forces 444
20.8 Activism 445
20.8.1 Advocacy 445
20.8.2 Hotlines 446

Exercises 446

Advanced Exercises 447

References 447

21 Security Beyond Computer Networks: Information Assurance 449
21.1 Introduction 449
21.2 Collective Security Initiatives and Best Practices 450
21.2.1 The U.S. National Strategy to Secure Cyberspace 450
21.2.2 Council of Europe Convention on Cyber Crime 452

References 453

Part IV Projects

22 Projects 457
22.1 Introduction 457
22.2 Part I: Weekly/Biweekly Laboratory Assignments 457
22.3 Part II: Semester Projects 461
22.3.1 Intrusion Detection Systems 461
22.3.2 Scanning Tools for System Vulnerabilities 464
22.4 The Following Tools Are Used to Enhance Security in Web Applications 466
22.4.1 Public Key Infrastructure 466
22.5 Part III: Research Projects 467
22.5.1 Consensus Defense 467
22.5.2 Specialized Security 467
22.5.3 Protecting an Extended Network 467
22.5.4 Automated Vulnerability Reporting 467
22.5.5 Turn-Key Product for Network Security Testing 468
22.5.6 The Role of Local Networks in the Defense of the National Critical Infrastructure 468
22.5.7 Enterprise VPN Security 468
22.5.8 Perimeter Security 469
22.5.9 Enterprise Security 469
22.5.10 Password Security – Investigating the Weaknesses 469

Index 471