Computer Communications and Networks

Series editor
A.J. Sammes
Centre for Forensic Computing
Cranfield University, Shrivenham Campus
Swindon, UK

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.

More information about this series at http://www.springer.com/series/4198

Joseph Migga Kizza

Guide to Computer Network Security

Fourth Edition

Springer

Joseph Migga Kizza
University of Tennessee
Chattanooga, TN, USA

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-55605-5 ISBN 978-3-319-55606-2 (eBook)
DOI 10.1007/978-3-319-55606-2

Library of Congress Control Number: 2017939601

© Springer-Verlag London 2009, 2013, 2015
© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

It has been barely 3 years since our third edition came out, and we are again in need of a new and improved fourth edition. This quick turnaround of editions of a successful book like this is indicative of the rapidly changing technology landscape. We are excited by our growing number of users, and we are indeed indebted to them by continuously keeping a living promise we first made to our readers in the very first edition of maintaining the book materials as up to date as possible. In line with this promise, we have now embarked on this fourth edition. Since our first edition, we have been bringing to our growing ranks of users not only the concept of a changing computer network but also the correspondingly evolving repertoire of security tools, algorithms, and best practices, all mandated by the rapidly changing technology. The traditional computer network we introduced in the first edition with its nicely "demarcated" and heavily defended perimeter wall and well-guarded access points has been going into a transformation as a result of new technologies. Changes have occurred, as we pointed out in both the second and third editions, from within and outside the network, at the server, and most importantly at the boundaries resulting into a *virtualized and elastic network*, with rapid extensions at will, to meet the growing needs of users. These changes are driven by new technological developments and changing user demands and security needs. New developments in system resource virtualization, the evolving cloud computing models, and a growing and unpredictable mobile computing technology are creating new platforms that demand new extensions, usually on the fly and at will, thus making security of the traditional computer network more complex. Also, the rapidly emerging computing technology and the evolving and expanding reach of wireless technologies, broadening the last mile, are rapidly destroying the traditional computer network, the enterprise network, as mobile and home devices are slowly becoming essential parts of the enterprise and at the same time remaining in their traditional public commons, thus creating unpredictable and undefendable enterprise and home networks. When you think of a small mobile device now able to connect to a private enterprise network under BYOD policies and the same device able to be used as a home network device and that at the same time remains connected to networks in public commons, you start to get an image of the *anywhere and everywhere* computing network, a global sprawl of networks within networks, and indeed networks on demand. The ubiquitous nature of these *new* computing networks is creating new and uncharted territories with security nightmare quagmire. What is more worrying is that along with the sprawl, we are getting all types of characters joining amass in the new but rapidly changing technological "ecosystem," for the lack of a better word.

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 computing and mobile systems attacks and the vulnerability of these systems will likely not abet; rather, they are likely to increase. More efforts in developing adaptive and scalable security tools, 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 world of computing.

This guide is a comprehensive volume touching not only on every major topic in computing and information security and assurance but also has gone beyond the security of computer networks as we used to know them, to embrace new and more agile mobile systems and new online social networks that are interweaving into our everyday fabric, if not already, and creating an overgrowing ecosystem of digital and associated social networks. We bring into our ongoing discussion on computer network security a broader view of the new ever-growing ecosystem of fixed, wireless, mobile, and online social networks. As with previous editions, it is intended to bring massive security awareness and education to the security realities of our time, a time when billions of people from the remotest place on earth to the most cosmopolitan world cities are using the smartest, smallest, and more powerful mobile devices loaded with the most fascinating and worrisome functionalities ever known to interconnect via a mesh of elastic computing networks in this ecosystem. We highlight security and privacy issues and concerns in public commons and private bedrooms as users around the globe intersect in this growing digital and social network ecosystem.

The volume is venturing into and exposing all sorts of known security problems, vulnerabilities, and dangers likely to be encountered by the users of these devices. In its own way, it is a pathfinder as it initiates a conversation toward developing better tools, algorithms, protocols, and best practices that will enhance the security of systems in the public commons, private and enterprise offices, and living rooms and bedrooms where these devices are used. It does this comprehensively in six parts and 26 chapters. Part I gives the reader an understanding of the working of and the security situation of the traditional 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 tools, algorithms, best practices, and solutions that are currently in use. Part IV goes beyond the traditional computer network as we used to know it to cover new systems and technologies that have seamlessly and stealthily extended the boundaries of the traditional computer network. Systems and other emerging technologies including virtualization, cloud computing, and mobile systems are introduced and discussed. A new Part V ventures into wireless and other technologies creeping into the last mile creating a new security quagmire in the home computing environment and the growing home hotspots. Part VI, the last part, consists of projects.

What Is New in This Edition

There have been considerable changes in the contents of the book to bring it in line with the new developments we discussed above. In almost every chapter, new content has been added, and we have eliminated what looked as outdated and what seem to be repeated materials. Because of the required bedrock content in computer network theory and computer network security fundamentals essential to understand overall content and to gain from the book, the content in some chapters had not changed a great deal since the first edition. But of more interest to our readers and in recognition of the rapidly changing computer network ecosystem, a new chapter on the *Internet of Things (IoT)* has been added. The addition of this chapter has been driven by a number of burning security issues the advent of IoT has brought about to such an extent that some are calling it the old *Wild West* of security, a *security quagmire* that so far does not respect current and standard security protocols and best practices and whose security protocols are yet to be developed and best practices formalized. Throughout the text, the discussion is candid, intended to ignite students' interest and participation in class discussions of the issues and beyond.

Audience

As usual, in summary, the guide attempts to achieve the following objectives:

- Educate the public about computer security in the traditional computer network.
- Educate the public about the evolving computing ecosystem created by the eroding boundaries between the enterprise network, the home network, and the rapidly growing public commons-based social networks, all extending the functionalities of the traditional computer network.
- Alert the public to the magnitude of the vulnerabilities, weaknesses, and loopholes inherent in the traditional computer network and now resident in the new computing ecosystem.
- Bring to the public attention effective security tools, solutions and best practice, expert opinions on those solutions, and the possibility of ad hoc solutions.
- Look at the roles legislation, regulation, and enforcement play in securing the new computing ecosystem.
- Finally, initiate a debate on developing effective and comprehensive security algorithms, protocols, and best practices for new computing ecosystem.

Since the guide covers a wide variety of security topics, tools, algorithms, solutions, and best practices, it is intended to be both a teaching and a reference toolbox for those interested in learning about the security of the evolving computing ecosystem. Learn about available techniques to prevent attacks on these systems. The in-depth and thorough discussion and analysis of most of the security issues of the traditional computer network and the extending technologies and systems, together with the discussion of security algorithms and solutions given, make the guide a unique reference source of ideas for computer network and data security personnel, network security policy makers, and those reading for leisure. In addition, the guide provokes the reader by raising valid legislative, legal, social, technical, and ethical security issues, including the increasingly diminishing line between individual privacy and the need for collective and individual security in the new computing ecosystem.

The guide targets college students in computer science, information science, technology studies, library sciences, and engineering and to a lesser extent students in 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 data- and 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 each chapter: easy and quickly workable exercises whose responses can be easily spotted from the proceeding text and more thought-provoking advanced exercises whose responses may require research outside the content of this book. Also Chap. 25 is devoted to lab exercises. There are three types of lab exercises: weekly and biweekly 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. Links are provided below for cryptographic and mobile security hands-on projects from two successful National Science Foundation (NSF)-funded workshops at the author's university:

- Teaching Cryptography Using Hands-On Labs and Case Studies—http://web2.utc.edu/~djy471/cryptography/crypto.htm
- Capacity Building Through Curriculum and Faculty Development on Mobile Security—http://www.utc.edu/faculty/li-yang/mobilesecurity.php

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, now part of the text.
- *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. Also as we stated above, links are also included at the author's Web site for cryptographic hands-on projects from two successful National Science Foundation (NSF)-funded workshops at the author's university.

These materials can be found at the publisher's Web site at http://www.springer.com/book/9783319556055 and at the author's Web site at http://www.utc.edu/Faculty/Joseph-Kizza/.

Chattanooga, TN, USA Joseph Migga Kizza
June, 2017

Contents

Part I Introduction to Traditional 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 . . . 6

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 . . . 16

1.6 Network Connectivity and Protocols . . . 16

1.6.1 Open System Interconnection (OSI) Protocol Suite . . . 18

1.6.2 Transmission 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 . . . 28

1.9 Network Technologies . . . 34

1.9.1 LAN Technologies . . . 34

1.9.2 WAN Technologies . . . 36

1.9.3 Wireless LANs . . . 39

1.10 Conclusion . . . 39

References . . . 40

2 Computer Network Security Fundamentals 41
2.1 Introduction 41
2.1.1 Computer Security 43
2.1.2 Network Security 43
2.1.3 Information Security 43
2.2 Securing the Computer Network 44
2.2.1 Hardware 44
2.2.2 Software 44
2.3 Forms of Protection 44
2.3.1 Access Control 45
2.3.2 Authentication 46
2.3.3 Confidentiality 46
2.3.4 Integrity 47
2.3.5 Nonrepudiation 47
2.4 Security Standards 48
2.4.1 Security Standards Based on Type of Service/Industry 49
2.4.2 Security Standards Based on Size/Implementation . . . 52
2.4.3 Security Standards Based on Interests 53
2.4.4 Security Best Practices 53
References 57

Part II Security Issues and Challenges in the Traditional Computer Network

3 Security Threats and Threat Motives to Computer Networks 61
3.1 Introduction 61
3.2 Sources of Security Threats 62
3.2.1 Design Philosophy 63
3.2.2 Weaknesses in Network Infrastructure and Communication Protocols 63
3.2.3 Rapid Growth of Cyberspace 66
3.2.4 The Growth of the Hacker Community 67
3.2.5 Vulnerability in Operating System Protocol 78
3.2.6 The Invisible Security Threat: The Insider Effect . . . 78
3.2.7 Social Engineering 79
3.2.8 Physical Theft 79
3.3 Security Threat Motives 79
3.3.1 Terrorism 80
3.3.2 Military Espionage 80
3.3.3 Economic Espionage 80
3.3.4 Targeting the National Information Infrastructure . . . 81
3.3.5 Vendetta/Revenge 81
3.3.6 Hate (National Origin, Gender, and Race) 82
3.3.7 Notoriety 82

3.3.8 Greed 82
3.3.9 Ignorance 82
3.4 Security Threat Management 82
3.4.1 Risk Assessment 83
3.4.2 Forensic Analysis 83
3.5 Security Threat Correlation 83
3.5.1 Threat Information Quality 84
3.6 Security Threat Awareness 84
References 86

4 Introduction to Computer Network Vulnerabilities 87
4.1 Definition 87
4.2 Sources of Vulnerabilities 87
4.2.1 Design Flaws 88
4.2.2 Poor Security Management 91
4.2.3 Incorrect Implementation 92
4.2.4 Internet Technology Vulnerability 93
4.2.5 Changing Nature of Hacker Technologies and Activities 95
4.2.6 Difficulty of Fixing Vulnerable Systems 96
4.2.7 Limits of Effectiveness of Reactive Solutions 97
4.2.8 Social Engineering 98
4.3 Vulnerability Assessment 100
4.3.1 Vulnerability Assessment Services 100
4.3.2 Advantages of Vulnerability Assessment Services . . . 101
References 103

5 Cyber Crimes and Hackers 105
5.1 Introduction 105
5.2 Cybercrimes 106
5.2.1 Ways of Executing Cybercrimes 107
5.2.2 Cybercriminals 109
5.3 Hackers 110
5.3.1 History of Hacking 110
5.3.2 Types of Hackers 113
5.3.3 Hacker Motives 117
5.3.4 Hacking Topologies 120
5.3.5 Hackers' Tools of System Exploitation 124
5.3.6 Types of Attacks 127
5.4 Dealing with the Rising Tide of Cybercrimes 128
5.4.1 Prevention 128
5.4.2 Detection 129
5.4.3 Recovery 129
5.5 Conclusion 129
References 130

6 Scripting and Security in Computer Networks and Web Browsers 133
6.1 Introduction 133
6.2 Scripting 134
6.3 Scripting Languages 134
6.3.1 Server-Side Scripting Languages 135
6.3.2 Client-Side Scripting Languages 135
6.4 Scripting in Computer Network 137
6.4.1 Introduction to the Common Gateway Interface (CGI) 138
6.4.2 Server-Side Scripting: The CGI Interface 140
6.5 Computer Networks Scripts and Security 140
6.5.1 CGI Script Security 141
6.5.2 JavaScript and VBScript Security 143
6.5.3 Web Script Security 144
6.6 Dealing with the Script Security Problems 144
References 145

7 Security Assessment, Analysis, and Assurance 147
7.1 Introduction 147
7.2 System Security Policy 148
7.3 Building a Security Policy 151
7.3.1 Security Policy Access Rights Matrix 151
7.3.2 Policy and Procedures 153
7.4 Security Requirements Specification 157
7.5 Threat Identification 158
7.5.1 Human Factors 158
7.5.2 Natural Disasters 159
7.5.3 Infrastructure Failures 159
7.6 Threat Analysis 161
7.6.1 Approaches to Security Threat Analysis 162
7.7 Vulnerability Identification and Assessment 163
7.7.1 Hardware 163
7.7.2 Software 164
7.7.3 Humanware 165
7.7.4 Policies, Procedures, and Practices 165
7.8 Security Certification 166
7.8.1 Phases of a Certification Process 167
7.8.2 Benefits of Security Certification 167
7.9 Security Monitoring and Auditing 168
7.9.1 Monitoring Tools 168
7.9.2 Type of Data Gathered 169
7.9.3 Analyzed Information 169
7.9.4 Auditing 170
7.10 Products and Services 170
References 171

Part III Dealing with Computer Network Security Challenges

8 Disaster Management 175
8.1 Introduction 175
8.1.1 Categories of Disasters 176
8.2 Disaster Prevention 177
8.3 Disaster Response 179
8.4 Disaster Recovery 179
8.4.1 Planning for a Disaster Recovery 180
8.4.2 Procedures of Recovery 181
8.5 Make Your Business Disaster Ready 183
8.5.1 Always Be Ready for a Disaster 183
8.5.2 Always Back Up Media 184
8.5.3 Risk Assessment 184
8.6 Resources for Disaster Planning and Recovery 184
8.6.1 Local Disaster Resources 184
References 186

9 Access Control and Authorization 187
9.1 Definitions 187
9.2 Access Rights 188
9.2.1 Access Control Techniques and Technologies 189
9.3 Access Control Systems 194
9.3.1 Physical Access Control 194
9.3.2 Access Cards 194
9.3.3 Electronic Surveillance 195
9.3.4 Biometrics 196
9.3.5 Event Monitoring 199
9.4 Authorization 199
9.4.1 Authorization Mechanisms 200
9.5 Types of Authorization Systems 201
9.5.1 Centralized 201
9.5.2 Decentralized 201
9.5.3 Implicit 202
9.5.4 Explicit 202
9.6 Authorization Principles 202
9.6.1 Least Privilege 203
9.6.2 Separation of Duties 203
9.7 Authorization Granularity 203
9.7.1 Fine-Grained Authorization 204
9.7.2 Coarse-Grained Authorization 204
9.8 Web Access and Authorization 204
References 206

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 . . . 211
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 . . . 213
10.4.2 Repudiable Authentication . . . 213
10.5 Authentication Methods . . . 214
10.5.1 Password Authentication . . . 214
10.5.2 Public Key Authentication . . . 217
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
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 . . . 232
11.2.2 Problems with Symmetric Encryption . . . 233
11.3 Public Key Encryption . . . 234
11.3.1 Public Key Encryption Algorithms . . . 236
11.3.2 Problems with Public Key Encryption . . . 237
11.3.3 Public Key Encryption Services . . . 237
11.4 Enhancing Security: Combining Symmetric and Public Key Encryptions . . . 238
11.5 Key Management: Generation, Transportation, and Distribution . . . 238
11.5.1 The Key Exchange Problem . . . 238
11.5.2 Key Distribution Centers (KDCs) . . . 239
11.5.3 Public Key Management . . . 241
11.5.4 Key Escrow . . . 243
11.6 Public Key Infrastructure (PKI) . . . 245
11.6.1 Certificates . . . 245
11.6.2 Certificate Authority . . . 246
11.6.3 Registration Authority (RA) . . . 246
11.6.4 Lightweight Directory Access Protocols (LDAP) . . . 246
11.6.5 Role of Cryptography in Communication . . . 246

11.7 Hash Function 246
11.8 Digital Signatures 247
References 250

12 Firewalls 251
12.1 Definition 251
12.2 Types of Firewalls 254
12.2.1 Packet Inspection Firewalls 255
12.2.2 Application Proxy Server: Filtering Based on Known Services 260
12.2.3 Virtual Private Network (VPN) Firewalls 263
12.2.4 Small Office or Home (SOHO) Firewalls 263
12.3 Configuration and Implementation of a Firewall 264
12.4 The Demilitarized Zone (DMZ) 267
12.4.1 Scalability and Increasing Security in a DMZ 269
12.5 Improving Security Through the Firewall 269
12.6 Firewall Forensics 270
12.7 Firewall Services and Limitations 272
12.7.1 Firewall Services 272
12.7.2 Limitations of Firewalls 272
References 274

13 System Intrusion Detection and Prevention 275
13.1 Definition 275
13.2 Intrusion Detection 275
13.2.1 The System Intrusion Process 276
13.2.2 The Dangers of System Intrusions 277
13.3 Intrusion Detection Systems (IDSs) 278
13.3.1 Anomaly Detection 279
13.3.2 Misuse Detection 281
13.4 Types of Intrusion Detection Systems 282
13.4.1 Network-Based Intrusion Detection Systems (NIDSs) 282
13.4.2 Host-Based Intrusion Detection Systems (HIDS) . . . 287
13.4.3 The Hybrid Intrusion Detection System 289
13.5 The Changing Nature of IDS Tools 290
13.6 Other Types of Intrusion Detection Systems 290
13.6.1 System Integrity Verifiers (SIVs) 290
13.6.2 Log File Monitors (LFM) 290
13.6.3 Honeypots 291
13.7 Response to System Intrusion 292
13.7.1 Incident Response Team 293
13.7.2 IDS Logs as Evidence 293
13.8 Challenges to Intrusion Detection Systems 294
13.8.1 Deploying IDS in Switched Environments 294

13.9 Implementing an Intrusion Detection System 295
13.10 Intrusion Prevention Systems (IPSs) 295
13.10.1 Network-Based Intrusion Prevention Systems (NIPSs) 295
13.10.2 Host-Based Intrusion Prevention Systems (HIPSs) 297
13.11 Intrusion Detection Tools 299
References 300

14 Computer and Network Forensics 303
14.1 Definition 303
14.2 Computer Forensics 304
14.2.1 History of Computer Forensics 305
14.2.2 Elements of Computer Forensics 306
14.2.3 Investigative Procedures 307
14.2.4 Analysis of Evidence 313
14.3 Network Forensics 319
14.3.1 Intrusion Analysis 320
14.3.2 Damage Assessment 324
14.4 Forensic Tools 325
14.4.1 Computer Forensic Tools 325
14.4.2 Network Forensic Tools 327
References 328

15 Virus and Content Filtering 331
15.1 Definitions 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 343
15.4.1 Application-Level Filtering 344
15.4.2 Packet-Level Filtering and Blocking 345
15.4.3 Filtered Material 346
15.5 Spam 347
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 Standardization of (Security) Products 352
16.2.2 Common Computer Product Standards 353

16.3 Security Evaluations 353
16.3.1 Purpose of Security Evaluation 354
16.3.2 Security Evaluation Criteria 355
16.3.3 Basic Elements of an Evaluation 356
16.3.4 Outcome/Benefits 356
16.4 Major Security Evaluation Criteria 358
16.4.1 Common Criteria (CC) 358
16.4.2 FIPS 359
16.4.3 The Orange Book/TCSEC 359
16.4.4 Information Technology Security Evaluation Criteria (ITSEC) 362
16.4.5 The Trusted Network Interpretation (TNI): The Red Book 362
16.5 Does Evaluation Mean Security? 363
References 364

17 Computer Network Security Protocols 365
17.1 Introduction 365
17.2 Application-Level Security 366
17.2.1 Remote Authentication Dial-In User Service (RADIUS) 367
17.2.2 Terminal Access Controller Access Control System (TACACS+) 368
17.2.3 Pretty Good Privacy (PGP) 369
17.2.4 Secure/Multipurpose Internet Mail Extension (S/MIME) 371
17.2.5 Secure HTTP (S-HTTP) 372
17.2.6 Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) 375
17.2.7 Secure Electronic Transactions (SET) 375
17.2.8 Kerberos 377
17.3 Security in the Transport Layer 380
17.3.1 Secure Socket Layer (SSL) 380
17.3.2 Transport Layer Security (TLS) 384
17.4 Security in the Network Layer 385
17.4.1 Internet Protocol Security (IPsec) 385
17.4.2 Virtual Private Networks (VPN) 389
17.4.3 VPN Tunneling Technology, PPTP, and L2TP 392
17.5 Security in the Physical Layer 393
17.5.1 Point-to-Point Protocol (PPP) 393
17.5.2 Other Network Physical Layer Security Protocols Include 395
References 396

18 Security in Wireless Networks and Devices 397
18.1 Introduction 397
18.2 Types of Wireless Broadband Networks 398
18.2.1 Wireless Personal Area Networks (WPANs) 398
18.2.2 Wireless Local Area Networks (WLANs) (Wi-Fi) 401
18.2.3 WiMAX LAN 401
18.2.4 4G (LTE) and 5G: Enhancing Mobile Broadband 408
18.2.5 Mobile Cellular Network 408
18.3 Development of Cellular Technology 412
18.3.1 First Generation 412
18.3.2 Second Generation 412
18.3.3 Third Generation 413
18.3.4 Fourth Generation (4G/LTE) 414
18.4 Other Features of Mobile Cellular Technology 414
18.4.1 Universality 414
18.4.2 Flexibility 415
18.4.3 Quality of Service (QoS) 415
18.4.4 Service Richness 415
18.4.5 Mobile Cellular Security Protocol Stack 415
18.5 Security Vulnerabilities in Cellular Wireless Networks 416
18.5.1 WLAN Security Concerns 418
18.5.2 Best Practices for Wi-Fi Security 424
References 426

19 Security in Sensor Networks 429
19.1 Introduction 429
19.2 The Growth of Sensor Networks 430
19.3 Design Factors in Sensor Networks 431
19.3.1 Routing 431
19.3.2 Power Consumption 434
19.3.3 Fault Tolerance 434
19.3.4 Scalability 434
19.3.5 Production Costs 434
19.3.6 Nature of Hardware Deployed 434
19.3.7 Topology of Sensor Networks 435
19.3.8 Transmission Media 435
19.4 Security in Sensor Networks 435
19.4.1 Security Challenges 435
19.4.2 Sensor Network Vulnerabilities and Attacks 436
19.4.3 Securing Sensor Networks 438
19.5 Security Mechanisms and Best Practices for Sensor Networks 439

19.6 Trends in Sensor Network Security Research 440
19.6.1 Cryptography 440
19.6.2 Key Management 441
19.6.3 Confidentiality, Authentication, and Freshness 442
19.6.4 Resilience to Capture 442
References 443

20 Other Efforts to Secure Data in Computer Networks and Beyond 445
20.1 Introduction 445
20.2 Legislation 445
20.3 Regulation 446
20.4 Self-Regulation 447
20.4.1 Hardware-Based Self-Regulation 447
20.4.2 Software-Based Self-Regulation 448
20.5 Education 448
20.5.1 Focused Education 449
20.5.2 Mass Education 450
20.6 Reporting Centers 450
20.7 Market Forces 451
20.8 Activism 451
20.8.1 Advocacy 451
20.8.2 Hotlines 452
Reference 453

Part IV The Emergence of the Digital and Social Network Ecosystem

21 Virtualization Technology and Security 457
21.1 Introduction 457
21.2 History of Virtualization 458
21.3 Virtualization Terminologies 459
21.3.1 Host CPU/Guest CPU 459
21.3.2 Host OS/Guest OS 459
21.3.3 Hypervisor 460
21.3.4 Emulation 460
21.4 Types of Computing System Virtualization 460
21.4.1 Platform Virtualization 460
21.4.2 Network Virtualization 468
21.4.3 Storage Virtualization 469
21.4.4 Application Virtualization 469
21.5 The Benefits of Virtualization 470
21.5.1 Reduction of Server Sprawl 470
21.5.2 Conservation of Energy 470
21.5.3 Reduced IT Management Costs 470
21.5.4 Better Disaster Recovery Management 470

21.5.5 Software Development Testing and Verification . . . 471
21.5.6 Isolation of Legacy Applications . . . 471
21.5.7 Cross-Platform Support . . . 471
21.5.8 Minimizing Hardware Costs . . . 471
21.5.9 Faster Server Provisioning . . . 471
21.5.10 Better Load Balancing . . . 472
21.5.11 Reduce the Data Center Footprint . . . 472
21.5.12 Increase Uptime . . . 472
21.5.13 Isolate Applications . . . 472
21.5.14 Extend the Life of Older Applications . . . 472
21.6 Virtualization Infrastructure Security . . . 473
21.6.1 Hypervisor Security . . . 473
21.6.2 Securing Communications Between Desktop and Virtual Infrastructure . . . 474
21.6.3 Security of Communication Between Virtual Machines . . . 474
21.6.4 Threats and Vulnerabilities Originating from a VM . . . 474
References . . . 475

22 Cloud Computing Technology and Security . . . 477
22.1 Introduction . . . 477
22.2 Cloud Computing Infrastructure Characteristics . . . 478
22.3 Cloud Computing Service Models . . . 480
22.4 Cloud Computing Deployment Models . . . 482
22.5 Virtualization and Cloud Computing . . . 482
22.6 Benefits of Cloud Computing . . . 483
22.7 Cloud Computing, Power Consumption and Environmental Issues . . . 486
22.8 Cloud Computing Security, Reliability, Availability, and Compliance Issues . . . 487
22.8.1 Cloud Computing Actors, Their Roles, and Responsibilities . . . 488
22.8.2 Security of Data and Applications in the Cloud . . . 490
22.8.3 Security of Data in Transition: Cloud Security Best Practices . . . 496
22.8.4 Service-Level Agreements (SLAs) . . . 496
22.8.5 Data Encryption . . . 497
22.8.6 Web Access Point Security . . . 497
22.8.7 Compliance . . . 497
References . . . 500

23 Mobile Systems and Corresponding Intractable Security Issues 503
23.1 Introduction 503
23.2 Current Major Mobile Operating Systems 504
23.3 Security in the Mobile Ecosystems 504
23.3.1 Application-Based Threats 506
23.3.2 Web-Based Threats 507
23.3.3 Network Threats 507
23.3.4 Physical Threats 508
23.3.5 Operating System-Based Threats 508
23.4 General Mobile Devices Attack Types 509
23.5 Mitigation of Mobile Devices Attacks 511
23.5.1 Mobile Device Encryption 513
23.5.2 Mobile Remote Wiping 513
23.5.3 Mobile Passcode Policy 514
23.6 Users Role in Securing Mobile Devices 514
References 515

24 Internet of Things (IoT): Growth, Challenges, and Security 517
24.1 Introduction 517
24.2 Overview and Growth of Internet of Things 519
24.3 Architecture and Networking of IoT 520
24.3.1 Architecture and Protocol Stack of IoTs 520
24.3.2 Challenges of Using TCP/IP Architecture over the IoT 523
24.4 IoT Governance, Privacy, and Security Challenges 525
24.4.1 Governance and Privacy Concerns 526
24.4.2 Security Challenges 527
24.4.3 Autonomy 527
24.4.4 Computational Constraints 528
24.4.5 Discovery 528
24.4.6 Trust Relationships 529
References 530

Part V Securing the Last Frontiers – The Home Front

25 Conquering the Last Frontier in the Digital Invasion: The Home Front 535
25.1 Introduction 535
25.2 The Changing Home Network and Hotspots 536
25.2.1 Cable LAN 536
25.2.2 Wireless Home Networks 537
25.2.3 Types of Broadband Internet Connections 540
25.2.4 Smart Home Devices 541

25.3 Data and Activities in the Home LAN . . . 541
25.3.1 Work Data . . . 541
25.3.2 Social Media Data . . . 542
25.3.3 Banking and Investment Data . . . 542
25.3.4 Health Devices . . . 542
25.3.5 Home Monitoring and Security Devices . . . 542
25.4 Threats to the Home and Home LAN . . . 543
25.4.1 Most Common Threats to Homes and Home LANs . . . 544
25.4.2 Actions to Safeguard the Family LAN . . . 544
25.4.3 Using Encryption to Protect the Family LAN . . . 545
25.4.4 Protecting the Family LAN with Known Protocols . . . 546
References . . . 548

Part VI Hands-On Projects

26 Projects . . . 551
26.1 Introduction . . . 551
26.2 Part 1: Case Studies . . . 551
26.3 Part 2: Weekly/Biweekly Laboratory Assignments . . . 552
26.4 Part 3: Semester Projects . . . 555
26.4.1 Intrusion Detection Systems . . . 555
26.4.2 Scanning Tools for System Vulnerabilities . . . 558
26.5 The Following Tools Are Used to Enhance Security in Web Applications . . . 558
26.5.1 Public Key Infrastructure . . . 558
26.6 Part 4: Research Projects . . . 559
26.6.1 Consensus Defense . . . 559
26.6.2 Specialized Security . . . 559
26.6.3 Protecting an Extended Network . . . 559
26.6.4 Automated Vulnerability Reporting . . . 560
26.6.5 Turn-Key Product for Network Security Testing . . . 560
26.6.6 The Role of Local Networks in the Defense of the National Critical Infrastructure . . . 560
26.6.7 Enterprise VPN Security . . . 560
26.6.8 Perimeter Security . . . 561
26.6.9 Enterprise Security . . . 561
26.6.10 Password Security: Investigating the Weaknesses . . . 561

Index . . . 563