

# **Computer and Information Security Handbook**

**The Morgan Kaufmann Series in Computer Security**

*Computer and Information Security Handbook*

John Vacca

*Disappearing Cryptography: Information Hiding: Steganography & Watermarking, Third Edition*

Peter Wayner

*Network Security: Know It All*

James Joshi, et al.

*Digital Watermarking and Steganography, Second Edition*

Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker

*Information Assurance: Dependability and Security in Networked Systems*

Yi Qian, David Tipper, Prashant Krishnamurthy, and James Joshi

*Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*

Jean-Philippe Vasseur, Mario Pickavet, and Piet Demeester

*For further information on these books and for a list of forthcoming titles,  
please visit our Web site at <http://www.elsevierdirect.com>*

# Computer and Information Security Handbook

Edited by  
John R. Vacca



AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK  
OXFORD • PARIS • SAN DIEGO • SAN FRANCISCO  
SINGAPORE • SYDNEY • TOKYO

Morgan Kaufmann Publishers is an imprint of Elsevier



Morgan Kaufmann Publishers is an imprint of Elsevier.  
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

This book is printed on acid-free paper.

Copyright © 2009 by Elsevier Inc. All rights reserved.

Exception to the above text:

Chapter 29: © 2009, The Crown in right of Canada.

Designations used by companies to distinguish their products are often claimed as trademarks or registered trademarks. In all instances in which Morgan Kaufmann Publishers is aware of a claim, the product names appear in initial capital or all capital letters. All trademarks that appear or are otherwise referred to in this work belong to their respective owners. Neither Morgan Kaufmann Publishers nor the authors and other contributors of this work have any relationship or affiliation with such trademark owners nor do such trademark owners confirm, endorse or approve the contents of this work. Readers, however, should contact the appropriate companies for more information regarding trademarks and any related registrations.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, scanning, or otherwise—without prior written permission of the publisher.

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone: (+44) 1865 843830, fax: (+44) 1865 853333, E-mail: [permissions@elsevier.com](mailto:permissions@elsevier.com). You may also complete your request online via the Elsevier homepage (<http://elsevier.com>), by selecting "Support & Contact" then "Copyright and Permission" and then "Obtaining Permissions."

#### **Library of Congress Cataloging-in-Publication Data**

Application submitted

#### **British Library Cataloguing-in-Publication Data**

A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-374354-1

For information on all Morgan Kaufmann publications,  
visit our Web site at [www.mkp.com](http://www.mkp.com) or [www.elsevierdirect.com](http://www.elsevierdirect.com)

Printed in the United States of America

09 10 11 12 13 5 4 3 2 1

Working together to grow  
libraries in developing countries

[www.elsevier.com](http://www.elsevier.com) | [www.bookaid.org](http://www.bookaid.org) | [www.sabre.org](http://www.sabre.org)

**ELSEVIER** **BOOK AID** **Sabre Foundation**  
International

*This book is dedicated to my wife, Bee.*



Foreword	xxi
Preface	xxiii
Acknowledgments	xxvii
About the Editor	xxix
Contributors	xxxix

**Part I**  
**Overview of System and Network Security: A Comprehensive Introduction**

<b>1. Building a Secure Organization</b>	<b>3</b>
<i>John Mallery</i>	
<b>1. Obstacles to Security</b>	<b>3</b>
Security Is Inconvenient	3
Computers Are Powerful and Complex	3
Computer Users Are Unsophisticated	4
Computers Created Without a Thought to Security	4
Current Trend Is to Share, Not Protect	4
Data Accessible from Anywhere	4
Security Isn't About Hardware and Software	5
The Bad Guys Are Very Sophisticated	5
Management Sees Security as a Drain on the Bottom Line	5
<b>2. Ten Steps to Building a Secure Organization</b>	<b>6</b>
A. Evaluate the Risks and Threats	6
B. Beware of Common Misconceptions	8
C. Provide Security Training for IT Staff—Now and Forever	9
D. Think “Outside the Box”	10
E. Train Employees: Develop a Culture of Security	12
F. Identify and Utilize Built-In Security Features of the Operating System and Applications	14
G. Monitor Systems	16
H. Hire a Third Party to Audit Security	17
I. Don't Forget the Basics	19
J. Patch, Patch, Patch	20
<b>2. A Cryptography Primer</b>	<b>23</b>
<i>Scott R. Ellis</i>	
<b>1. What is Cryptography?</b>	
<b>What is Encryption?</b>	<b>23</b>
How Is Cryptography Done?	24

<b>2. Famous Cryptographic Devices</b>	<b>24</b>
The Lorenz Cipher	24
Enigma	24
<b>3. Ciphers</b>	<b>25</b>
The Substitution Cipher	25
The Shift Cipher	26
The Polyalphabetic Cipher	29
The Kasiski/Kerckhoff Method	30
<b>4. Modern Cryptography</b>	<b>31</b>
The Vernam Cipher (Stream Cipher)	31
The One-Time Pad	32
Cracking Ciphers	33
The XOR Cipher and Logical Operands	34
Block Ciphers	35
<b>5. The Computer Age</b>	<b>36</b>
Data Encryption Standard	36
Theory of Operation	37
Implementation	38
Rivest, Shamir, and Adleman (RSA)	38
Advanced Encryption Standard (AES or Rijndael)	38
<b>3 Preventing System Intrusions</b>	<b>39</b>
<i>Michael West</i>	
<b>1. So, What is an Intrusion?</b>	<b>39</b>
<b>2. Sobering Numbers</b>	<b>40</b>
<b>3. Know Your Enemy: Hackers Versus Crackers</b>	<b>40</b>
<b>4. Motives</b>	<b>41</b>
<b>5. Tools of the Trade</b>	<b>41</b>
<b>6. Bots</b>	<b>42</b>
<b>7. Symptoms of Intrusions</b>	<b>43</b>
<b>8. What Can You Do?</b>	<b>43</b>
Know Today's Network Needs	44
Network Security Best Practices	45
<b>9. Security Policies</b>	<b>45</b>
<b>10. Risk Analysis</b>	<b>46</b>
Vulnerability Testing	46
Audits	47
Recovery	47
<b>11. Tools of Your Trade</b>	<b>47</b>
Firewalls	47
Intrusion Prevention Systems	47
Application Firewalls	48
Access Control Systems	48
Unified Threat Management	49
<b>12. Controlling User Access</b>	<b>49</b>
Authentication, Authorization, and Accounting	49
What the User Knows	49

What the User Has	50	<b>6. Safeguarding Vital Data by Securing</b>	
The User Is Authenticated,		<b>Local and Network File Systems</b>	<b>76</b>
But Is She Authorized?	50	Directory Structure and Partitioning	
Accounting	51	for Security	76
Keeping Current	51	<b>6. Eliminating the Security Weakness</b>	
<b>13. Conclusion</b>	<b>51</b>	<b>of Linux and Unix Operating</b>	
<b>4. Guarding Against Network</b>		<b>Systems</b>	<b>79</b>
<b>Intrusions</b>	<b>53</b>	<i>Mario Santana</i>	
<i>Tom Chen and Patrick J. Walsh</i>		<b>1. Introduction to Linux and Unix</b>	<b>79</b>
<b>1. Traditional Reconnaissance and Attacks</b>	<b>53</b>	What Is Unix?	79
<b>2. Malicious Software</b>	<b>56</b>	What Is Linux?	80
Lures and “Pull” Attacks	57	System Architecture	82
<b>3. Defense in Depth</b>	<b>58</b>	<b>2. Hardening Linux and Unix</b>	<b>84</b>
<b>4. Preventive Measures</b>	<b>59</b>	Network Hardening	84
Access Control	59	Host Hardening	88
Vulnerability Testing and Patching	59	Systems Management Security	90
Closing Ports	60	<b>3. Proactive Defense for Linux and Unix</b>	<b>90</b>
Firewalls	60	Vulnerability Assessment	90
Antivirus and Antispyware Tools	61	Incident Response Preparation	91
Spam Filtering	62	Organizational Considerations	92
Honeypots	62	<b>7. Internet Security</b>	<b>93</b>
Network Access Control	63	<i>Jesse Walker</i>	
<b>5. Intrusion Monitoring and Detection</b>	<b>63</b>	<b>1. Internet Protocol Architecture</b>	<b>93</b>
Host-Based Monitoring	64	Communications Architecture Basics	94
Traffic Monitoring	64	Getting More Specific	95
Signature-Based Detection	64	<b>2. An Internet Threat Model</b>	<b>100</b>
Behavior Anomalies	65	The Dolev-Yao Adversary Model	101
Intrusion Prevention Systems	65	Layer Threats	101
<b>6. Reactive Measures</b>	<b>65</b>	<b>3. Defending Against Attacks on</b>	
Quarantine	65	<b>the Internet</b>	<b>105</b>
Traceback	66	Layer Session Defenses	106
<b>7. Conclusions</b>	<b>66</b>	Session Startup Defenses	113
<b>5. Unix and Linux Security</b>	<b>67</b>	<b>4. Conclusion</b>	<b>117</b>
<i>Gerald Beuchelt</i>		<b>8. The Botnet Problem</b>	<b>119</b>
<b>1. Unix and Security</b>	<b>67</b>	<i>Xinyuan Wang and Daniel Ramsbrock</i>	
The Aims of System Security	67	<b>1. Introduction</b>	<b>119</b>
Achieving Unix Security	67	<b>2. Botnet Overview</b>	<b>120</b>
<b>2. Basic Unix Security</b>	<b>68</b>	Origins of Botnets	120
Traditional Unix Systems	68	Botnet Topologies and Protocols	120
Standard File and Device Access		<b>3. Typical Bot Life Cycle</b>	<b>122</b>
Semantics	69	<b>4. The Botnet Business Model</b>	<b>123</b>
<b>4. Protecting User Accounts</b>		<b>5. Botnet Defense</b>	<b>124</b>
<b>and Strengthening Authentication</b>	<b>71</b>	Detecting and Removing	
Establishing Secure Account Use	71	Individual Bots	124
The Unix Login Process	71	Detecting C&C Traffic	125
Controlling Account Access	71	Detecting and Neutralizing	
Noninteractive Access	72	the C&C Servers	125
Other Network Authentication		Attacking Encrypted C&C Channels	126
Mechanisms	73	Locating and Identifying the Botmaster	128
Risks of Trusted Hosts and Networks	73	<b>6. Botmaster Traceback</b>	<b>128</b>
Replacing Telnet, rlogin, and FTP		Traceback Challenges	129
Servers and Clients with SSH	73		
<b>5. Reducing Exposure to Threats by</b>			
<b>Limiting Superuser Privileges</b>	<b>74</b>		
Controlling Root Access	74		



Traceback Beyond the Internet	130		
7. Summary	132		
<b>9. Intranet Security</b>	<b>133</b>		
<i>Bill Mansoor</i>			
1. Plugging the Gaps: NAC and Access Control	136		
2. Measuring Risk: Audits	137		
3. Guardian at the Gate: Authentication and Encryption	138		
4. Wireless Network Security	139		
5. Shielding the Wire: Network Protection	141		
6. Weakest Link in Security: User Training	142		
7. Documenting the Network: Change Management	142		
8. Rehearse the Inevitable: Disaster Recovery	143		
9. Controlling Hazards: Physical and Environmental Protection	145		
10. Know Your Users: Personnel Security	146		
11. Protecting Data Flow: Information and System Integrity	146		
12. Security Assessments	147		
13. Risk Assessments	148		
14. Conclusion	148		
<b>10. Local Area Network Security</b>	<b>149</b>		
<i>Dr. Pramod Pandya</i>			
1. Identify network threats	150		
Disruptive	150		
Unauthorized Access	150		
2. Establish Network Access Controls	150		
3. Risk Assessment	151		
4. Listing Network Resources	151		
5. Threats	151		
6. Security Policies	151		
7. The Incident-handling Process	152		
8. Secure Design Through Network Access Controls	152		
9. Ids Defined	153		
10. NIDS: Scope and Limitations	154		
11. A Practical Illustration of NIDS	154		
UDP Attacks	154		
TCP SYN (Half-Open) Scanning	155		
Some Not-So-Robust Features of NIDS	156		
12. Firewalls	158		
Firewall Security Policy	159		
Configuration Script for sf Router	160		
13. Dynamic Nat Configuration	160		
14. The Perimeter	160		
15. Access List Details	162		
16. Types of Firewalls	162		
17. Packet Filtering: IP Filtering Routers	162		
18. Application-layer Firewalls: Proxy Servers	163		
19. Stateful Inspection Firewalls	163		
20. NIDS Complements Firewalls	163		
21. Monitor and Analyze System Activities	163		
Analysis Levels	164		
22. Signature Analysis	164		
23. Statistical Analysis	164		
24. Signature Algorithms	164		
Pattern Matching	164		
Stateful Pattern Matching	165		
Protocol Decode-based Analysis	165		
Heuristic-Based Analysis	166		
Anomaly-Based Analysis	166		
<b>11. Wireless Network Security</b>	<b>169</b>		
<i>Chunming Rong and Erdal Cayirci</i>			
1. Cellular Networks	169		
Cellular Telephone Networks	170		
802.11 Wireless LANs	170		
2. Wireless Ad Hoc Networks	171		
Wireless Sensor Networks	171		
Mesh Networks	171		
3. Security Protocols	172		
WEP	172		
WPA and WPA2	173		
SPINS: Security Protocols for Sensor Networks	173		
4. Secure Routing	175		
SEAD	175		
Ariadne	176		
ARAN	176		
SLSF	177		
5. Key Establishment	177		
Bootstrapping	177		
Key Management	178		
References	181		
<b>12. Cellular Network Security</b>	<b>183</b>		
<i>Peng Liu, Thomas F. LaPorta and Kameswari Kotapati</i>			
1. Introduction	183		
2. Overview of Cellular Networks	184		
Overall Cellular Network Architecture	184		
Core Network Organization	185		
Call Delivery Service	185		
3. The State of the Art of Cellular Network Security	186		
Security in the Radio Access Network	186		
Security in Core Network	187		
Security Implications of Internet Connectivity	188		
Security Implications of PSTN Connectivity	188		

<b>4. Cellular Network Attack Taxonomy</b>	<b>189</b>	Impact of Security Breaches	231
Abstract Model	189	<b>2. Protecting Mission-critical Systems</b>	<b>231</b>
Abstract Model Findings	189	Information Assurance	231
Three-Dimensional Attack Taxonomy	192	Information Risk Management	231
<b>5. Cellular Network Vulnerability Analysis</b>	<b>193</b>	Defense in Depth	233
Cellular Network Vulnerability Assessment Toolkit (CAT)	195	Contingency Planning	233
Advanced Cellular Network Vulnerability Assessment Toolkit (aCAT)	198	<b>3. Information Security from the Ground Up</b>	<b>236</b>
Cellular Network Vulnerability Assessment Toolkit for evaluation (eCAT)	199	Physical Security	236
<b>6. Discussion</b>	<b>201</b>	Data Security	237
<b>References</b>	<b>202</b>	Systems and Network Security	239
 		Business Communications Security	241
<b>13. RFID Security</b>	<b>205</b>	Wireless Security	242
<i>Chunming Rong and Erdal Cayirci</i>		Web and Application Security	246
<b>1. RFID Introduction</b>	<b>205</b>	Security Policies and Procedures	247
RFID System Architecture	205	Security Employee Training and Awareness	248
RFID Standards	207	<b>4. Security Monitoring and Effectiveness</b>	<b>249</b>
RFID Applications	208	Security Monitoring Mechanisms	250
<b>2. RFID Challenges</b>	<b>209</b>	Incidence Response and Forensic Investigations	251
Counterfeiting	209	Validating Security Effectiveness	251
Sniffing	209	<b>References</b>	<b>252</b>
Tracking	209	 	
Denial of Service	210	<b>15. Security Management Systems</b>	<b>255</b>
Other Issues	210	<i>Joe Wright and Jim Harmening</i>	
Comparison of All Challenges	212	<b>1. Security Management System Standards</b>	<b>255</b>
<b>3. RFID Protections</b>	<b>212</b>	<b>2. Training Requirements</b>	<b>256</b>
Basic RFID System	212	<b>3. Principles of Information Security</b>	<b>256</b>
RFID System Using Symmetric-Key Cryptography	215	<b>4. Roles and Responsibilities of Personnel</b>	<b>256</b>
RFID System Using Public-key Cryptography	217	<b>5. Security Policies</b>	<b>256</b>
<b>References</b>	<b>219</b>	<b>6. Security Controls</b>	<b>257</b>
 		<b>7. Network Access</b>	<b>257</b>
<b>Part II</b>		<b>8. Risk Assessment</b>	<b>257</b>
<b>Managing Information Security</b>		<b>9. Incident Response</b>	<b>258</b>
<b>14. Information Security Essentials for IT Managers, Protecting Mission-Critical Systems</b>	<b>225</b>	<b>10. Summary</b>	<b>258</b>
<i>Albert Caballero</i>		 	
<b>1. Information Security Essentials for IT Managers, Overview</b>	<b>225</b>	<b>16. Information Technology Security Management</b>	<b>259</b>
Scope of Information Security Management	225	<i>Rahul Bhaskerand Bhushan Kapoor</i>	
CISSP Ten Domains of Information Security	225	<b>1. Information Security Management Standards</b>	<b>259</b>
What is a Threat?	227	Federal Information Security Management Act	259
Common Attacks	228	International Standards Organization	260
		Other Organizations Involved in Standards	260
		<b>2. Information Technology security aspects</b>	<b>260</b>
		Security Policies and Procedures	261
		IT Security Processes	263
		<b>3. Conclusion</b>	<b>267</b>

<b>17. Identity Management</b>	<b>269</b>	<b>19. Computer Forensics</b>	<b>307</b>
<i>Dr. Jean-Marc Seigneur and Dr. Tewfiq El Malika</i>		<i>Scott R. Ellis</i>	
<b>1. Introduction</b>	<b>269</b>	<b>1. What is Computer Forensics?</b>	<b>307</b>
<b>2. Evolution of Identity Management Requirements</b>	<b>269</b>	<b>2. Analysis of Data</b>	<b>308</b>
Digital Identity Definition	270	Computer Forensics and Ethics,	
Identity Management Overview	270	Green Home Plate Gallery View	309
Privacy Requirement	272	Database Reconstruction	310
User-Centricity	272	<b>3. Computer Forensics in the Court System</b>	<b>310</b>
Usability Requirement	273	<b>4. Understanding Internet History</b>	<b>312</b>
<b>3. The Requirements Fulfilled by Current Identity Management Technologies</b>	<b>274</b>	<b>5. Temporary Restraining Orders and Labor Disputes</b>	<b>312</b>
Evolution of Identity Management	274	Divorce	313
Identity 2.0	278	Patent Infringement	313
<b>4. Identity 2.0 for Mobile Users</b>	<b>286</b>	When to Acquire, When to Capture Acquisition	313
Mobile Web 2.0	286	Creating Forensic Images Using Software and Hardware	
Mobility	287	Write Blockers	313
Evolution of Mobile Identity	287	Live Capture of Relevant Files	314
The Future of Mobile User-Centric Identity Management in an Ambient Intelligence World	290	Redundant Array of Independent (or Inexpensive) Disks (RAID)	314
Research Directions	292	File System Analyses	314
<b>5. Conclusion</b>	<b>292</b>	NTFS	315
		The Role of the Forensic Examiner in Investigations and File Recovery	315
<b>18. Intrusion Prevention and Detection Systems</b>	<b>293</b>	Password Recovery	317
<i>Christopher Day</i>		File Carving	318
<b>1. What is an "Intrusion," Anyway?</b>	<b>293</b>	Things to Know: How Time stamps Work	320
Physical Theft	293	Experimental Evidence	321
Abuse of Privileges (The Insider Threat)	293	Email Headers and Time stamps, Email Receipts, and Bounced Messages	322
<b>2. Unauthorized Access by an Outsider</b>	<b>294</b>	Steganography "Covered Writing"	324
<b>3. Malware Infection</b>	<b>294</b>	<b>5. First Principles</b>	<b>325</b>
<b>4. The Role of the "0-day"</b>	<b>295</b>	<b>6. Hacking a Windows XP Password</b>	<b>325</b>
<b>5. The Rogue's Gallery: Attackers and Motives</b>	<b>296</b>	Net User Password Hack	325
<b>6. A Brief Introduction to TCP/IP</b>	<b>297</b>	Lanman Hashes and Rainbow Tables	325
<b>7. The TCP/IP data Architecture and Data Encapsulation</b>	<b>298</b>	Password Reset Disk	326
<b>8. Survey of Intrusion Detection and Prevention Technologies</b>	<b>300</b>	Memory Analysis and the Trojan Defense	326
<b>9. Anti-Malware Software</b>	<b>301</b>	User Artifact Analysis	326
<b>10. Network-based Intrusion Detection Systems</b>	<b>302</b>	Recovering Lost and Deleted Files	327
<b>11. Network-based Intrusion Prevention Systems</b>	<b>303</b>	Email	327
<b>12. Host-based Intrusion Prevention Systems</b>	<b>304</b>	Internet History	327
<b>13. Security Information Management Systems</b>	<b>304</b>	<b>7. Network Analysis</b>	<b>328</b>
<b>14. Network Session Analysis</b>	<b>304</b>	Protocols	328
<b>15. Digital Forensics</b>	<b>305</b>	Analysis	328
<b>16. System Integrity Validation</b>	<b>306</b>	<b>8. Computer Forensics Applied</b>	<b>329</b>
<b>17. Putting it all Together</b>	<b>306</b>	Tracking, Inventory, Location of Files, Paperwork, Backups, and So On	329
		Testimonial	329
		Experience Needed	329
		Job Description, Technologist	329

Job Description Management	330	Two-Router Configuration	357
Commercial Uses	330	Dual-Homed Host	358
Solid Background	330	Network Configuration Summary	358
Education/Certification	330	<b>11. Firewall Installation and Configuration</b>	<b>358</b>
Programming and Experience	331	<b>12. Supporting Outgoing Services Through Firewall Configuration</b>	<b>359</b>
Publications	331	Forms of State	359
<b>9. Testifying as an Expert</b>	<b>332</b>	Payload Inspection	360
Degrees of Certainty	332	<b>13. Secure External Services Provisioning</b>	<b>360</b>
Certainty Without Doubt	334	<b>14. Network Firewalls for Voice and Video Applications</b>	<b>360</b>
<b>10. Beginning to End in Court</b>	<b>334</b>	Packet Filtering H.323	361
Defendants, Plaintiffs, and Prosecutors	334	<b>15. Firewalls and Important Administrative Service Protocols</b>	<b>361</b>
Pretrial Motions	335	Routing Protocols	361
Trial: Direct and Cross-Examination	335	Internet Control Message Protocol	362
Rebuttal	335	Network Time Protocol	362
Surrebuttal	335	Central Log File Management	362
Testifying: Rule 702. Testimony by Experts	335	Dynamic Host Configuration Protocol	363
Correcting Mistakes: Putting Your Head in the Sand	336	<b>16. Internal IP Services Protection</b>	<b>363</b>
<b>20. Network Forensics</b>	<b>339</b>	<b>17. Firewall Remote Access Configuration</b>	<b>364</b>
<i>Yong Guan</i>		<b>18. Load Balancing and Firewall Arrays</b>	<b>365</b>
<b>1. Scientific Overview</b>	<b>339</b>	Load Balancing in Real Life	365
<b>2. The Principles of Network Forensics</b>	<b>340</b>	How to Balance the Load	365
<b>3. Attack Traceback and Attribution</b>	<b>341</b>	Advantages and Disadvantages of Load Balancing	366
IP Traceback	341	<b>19. Highly Available Firewalls</b>	<b>366</b>
Stepping-Stone Attack Attribution	344	Load Balancer Operation	366
<b>4. Critical Needs Analysis</b>	<b>346</b>	Interconnection of Load Balancers and Firewalls	366
<b>5. Research Directions</b>	<b>346</b>	<b>20. Firewall Management</b>	<b>367</b>
VoIP Attribution	346	<b>21. Conclusion</b>	<b>367</b>
<b>21. Firewalls</b>	<b>349</b>	<b>22. Penetration Testing</b>	<b>369</b>
<i>Dr. Errin W. Fulp</i>		<i>Sanjay Bavisi</i>	
<b>1. Network Firewalls</b>	<b>349</b>	<b>1. What is Penetration Testing?</b>	<b>369</b>
<b>2. Firewall Security Policies</b>	<b>350</b>	<b>2. How does Penetration Testing Differ from an Actual “Hack?”</b>	<b>370</b>
Rule-Match Policies	351	<b>3. Types of Penetration Testing</b>	<b>371</b>
<b>3. A Simple Mathematical Model for Policies, Rules, and Packets</b>	<b>351</b>	<b>4. Phases of Penetration Testing</b>	<b>373</b>
<b>4. First-match Firewall Policy Anomalies</b>	<b>352</b>	The Pre-Attack Phase	373
<b>5. Policy Optimization</b>	<b>352</b>	The Attack Phase	373
Policy Reordering	352	The Post-Attack Phase	373
Combining Rules	353	<b>5. Defining What’s Expected</b>	<b>374</b>
Default Accept or Deny?	353	<b>6. The Need for a Methodology</b>	<b>375</b>
<b>6. Firewall Types</b>	<b>353</b>	<b>7. Penetration Testing Methodologies</b>	<b>375</b>
Packet Filter	354	<b>8. Methodology in Action</b>	<b>376</b>
Stateful Packet Firewalls	354	EC-Council LPT Methodology	376
Application Layer Firewalls	354	<b>9. Penetration Testing Risks</b>	<b>378</b>
<b>7. Host and Network Firewalls</b>	<b>355</b>	<b>10. Liability Issues</b>	<b>378</b>
<b>8. Software and Hardware Firewall Implementations</b>	<b>355</b>	<b>11. Legal Consequences</b>	<b>379</b>
<b>9. Choosing the Correct Firewall</b>	<b>355</b>		
<b>10. Firewall Placement and Network Topology</b>	<b>356</b>		
Demilitarized Zones	357		
Perimeter Networks	357		

12.	“Get out of jail free” Card	379
13.	Penetration Testing Consultants	379
14.	Required Skill Sets	380
15.	Accomplishments	380
16.	Hiring a Penetration Tester	380
17.	Why Should a Company Hire You?	381
	Qualifications	381
	Work Experience	381
	Cutting-Edge Technical Skills	381
	Communication Skills	381
	Attitude	381
	Team Skills	381
	Company Concerns	381
18.	All’s Well that Ends Well	382
<b>23.</b>	<b>What Is Vulnerability Assessment?</b>	<b>383</b>
	<i>Almantas Kakareka</i>	
1.	Reporting	383
2.	The “It Won’t Happen to Us” Factor	383
3.	Why Vulnerability Assessment?	384
4.	Penetration Testing Versus Vulnerability Assessment	384
5.	Vulnerability Assessment Goal	385
6.	Mapping the Network	385
7.	Selecting the Right Scanners	386
8.	Central Scans Versus Local Scans	387
9.	Defense in Depth Strategy	388
10.	Vulnerability Assessment Tools	388
	Nessus	388
	GFI LANguard	389
	Retina	389
	Core Impact	389
	ISS Internet Scanner	389
	X-Scan	389
	Sara	389
	QualysGuard	389
	SAINT	389
	MBSA	389
11.	Scanner Performance	390
12.	Scan Verification	390
13.	Scanning Cornerstones	390
14.	Network Scanning Countermeasures	390
15.	Vulnerability Disclosure Date	391
	Find Security Holes Before They Become Problems	391
16.	Proactive Security Versus Reactive Security	392
17.	Vulnerability Causes	392
	Password Management Flaws	392
	Fundamental Operating System Design Flaws	392
	Software Bugs	392
	Unchecked User Input	392
18.	DIY Vulnerability Assessment	393
19.	Conclusion	393

## Part III

## Encryption Technology

## 24. Data Encryption 397

*Dr. Bhushan Kapoor and Dr. Pramod Pandya*

1.	Need for Cryptography	398
	Authentication	398
	Confidentiality	398
	Integrity	398
	Nonrepudiation	398
2.	Mathematical Prelude to Cryptography	398
	Mapping or Function	398
	Probability	398
	Complexity	398
3.	Classical Cryptography	399
	The Euclidean Algorithm	399
	The Extended Euclidean Algorithm	399
	Modular Arithmetic	399
	Congruence	400
	Residue Class	400
	Inverses	400
	Fundamental Theorem of Arithmetic	400
	Congruence Relation Defined	401
	Substitution Cipher	401
	Transposition Cipher	402
4.	Modern Symmetric Ciphers	402
	S-Box	403
	P-Boxes	403
	Product Ciphers	404
5.	Algebraic Structure	404
	Definition Group	404
	Definitions of Finite and Infinite Groups (Order of a Group)	404
	Definition Abelian Group	404
	Examples of a Group	404
	Definition: Subgroup	405
	Definition: Cyclic Group	405
	Rings	405
	Definition: Field	405
	Finite Fields $GF(2^n)$	405
	Modular Polynomial Arithmetic Over $GF(2)$	406
	Using a Generator to Represent the Elements of $GF(2^n)$	406
	$GF(2^3)$ Is a Finite Field	407
6.	The Internal Functions of Rijndael in AES Implementation	407
	Mathematical Preliminaries	408
	State	408
7.	Use of Modern Block Ciphers	412
	The Electronic Code Book (ECB)	412
	Cipher-Block Chaining (CBC)	412
8.	Public-key Cryptography	412
	Review: Number Theory	412
9.	Cryptanalysis of RSA	416
	Factorization Attack	416

<b>10. Diffie-Hellman Algorithm</b>	<b>417</b>	X.509 V3 Format	445
<b>11. Elliptic Curve Cryptosystems</b>	<b>417</b>	X.509 Certificate Extensions	445
An Example	418	Policy Extensions	446
Example of Elliptic Curve Addition	418	Certificate Policy	446
EC Security	419	<b>10. PKI Policy Description</b>	<b>447</b>
<b>12. Message Integrity and Authentication</b>	<b>419</b>	<b>11. PKI Standards Organizations</b>	<b>448</b>
Cryptographic Hash Functions	419	IETF PKIX	448
Message Authentication	420	SDSI/SPKI	448
Digital Signature	420	IETF OpenPGP	448
Message Integrity Uses a Hash Function in Signing the Message	420	<b>12. PGP Certificate Formats</b>	<b>449</b>
RSA Digital Signature Scheme	420	<b>13. PGP PKI Implementations</b>	<b>449</b>
RSA Digital Signature and the Message Digest	420	<b>14. W3C</b>	<b>449</b>
<b>13. Summary</b>	<b>421</b>	<b>15. Alternative PKI Architectures</b>	<b>450</b>
<b>References</b>	<b>421</b>	<b>16. Modified X.509 Architectures</b>	<b>450</b>
 		Perlman and Kaufman's User-Centric PKI	450
<b>25. Satellite Encryption</b>	<b>423</b>	Gutmann's Plug and Play PKI	450
<i>Daniel S. Soper</i>		Callas's Self-Assembling PKI	450
<b>1. The Need for Satellite Encryption</b>	<b>423</b>	<b>17. Alternative Key Management Models</b>	<b>450</b>
<b>2. Satellite Encryption Policy</b>	<b>425</b>	 	
<b>3. Implementing Satellite Encryption</b>	<b>426</b>	<b>27. Instant-Messaging Security</b>	<b>453</b>
General Satellite Encryption Issues	426	<i>Samuel J. J. Curry</i>	
Uplink Encryption	428	<b>1. Why Should I Care About Instant Messaging?</b>	<b>453</b>
Extrplanetary Link Encryption	428	<b>2. What is Instant Messaging?</b>	<b>453</b>
Downlink Encryption	429	<b>3. The Evolution of Networking Technologies</b>	<b>454</b>
<b>4. The Future of Satellite Encryption</b>	<b>430</b>	<b>4. Game Theory and Instant Messaging</b>	<b>455</b>
 		Your Workforce	455
<b>26. Public Key Infrastructure</b>	<b>433</b>	Generational Gaps	456
<i>Terence Spies</i>		Transactions	457
<b>1. Cryptographic Background</b>	<b>433</b>	<b>5. The Nature of the Threat</b>	<b>457</b>
Digital Signatures	433	Malicious Threat	458
Public Key Encryption	434	Vulnerabilities	459
<b>2. Overview of PKI</b>	<b>435</b>	Man-in-the-Middle Attacks	459
<b>3. The X.509 Model</b>	<b>436</b>	Phishing and Social Engineering	459
The History of X.509	436	Knowledge Is the Commodity	459
The X.509 Certificate Model	436	Data and Traffic Analysis	460
<b>4. X.509 Implementation Architectures</b>	<b>437</b>	Unintentional Threats	460
<b>5. X.509 Certificate Validation</b>	<b>439</b>	Regulatory Concerns	461
Validation Step 1: Construct the Chain and Validate Signatures	439	<b>6. Common IM Applications</b>	<b>461</b>
Validation Step 2: Check Validity Dates, Policy and Key Usage	439	Consumer Instant Messaging	461
Validation Step 3: Consult Revocation Authorities	440	Enterprise Instant Messaging	461
<b>6. X.509 Certificate Revocation</b>	<b>440</b>	Instant-Messaging Aggregators	462
Online Certificate Status Protocol	441	Backdoors: Instant Messaging Via Other Means (HTML)	462
<b>7. Server-based Certificate Validity Protocol</b>	<b>442</b>	Mobile Dimension	462
<b>8. X.509 Bridge Certification Systems</b>	<b>443</b>	<b>7. Defensive Strategies</b>	<b>462</b>
Mesh PKIs and Bridge CAs	443	<b>8. Instant-messaging Security Maturity and Solutions</b>	<b>463</b>
<b>9. X.509 Certificate Format</b>	<b>444</b>	Asset Management	463
X.509 V1 and V2 Format	445	Built-In Security	463
		Content Filtering	463
		Classic Security	463
		Compliance	464
		Data Loss Prevention	464
		Logging	464
		Archival	464

<b>9. Processes</b>	<b>464</b>
Instant-Messaging Activation and Provisioning	464
Application Review	464
People	464
Revise	464
Audit	464
<b>10. Conclusion</b>	<b>465</b>
Example Answers to Key Factors	466

**Part IV  
Privacy and Access Management**

**28. NET Privacy 469**

*Marco Cremonini, Chiara Braghin and Claudio Agostino Ardagna*

<b>1. Privacy in the Digital Society</b>	<b>469</b>
The Origins, The Debate	469
Privacy Threats	471
<b>2. The Economics of Privacy</b>	<b>474</b>
The Value of Privacy	474
Privacy and Business	475
<b>3. Privacy-Enhancing Technologies</b>	<b>476</b>
Languages for Access Control and Privacy Preferences	476
Data Privacy Protection	478
Privacy for Mobile Environments	480
<b>4. Network Anonymity</b>	<b>482</b>
Onion Routing	483
Anonymity Services	484
<b>5. Conclusion</b>	<b>485</b>

**29. Personal Privacy Policies 487**

*Dr. George Yee and Larry Korba*

<b>1. Introduction</b>	<b>487</b>
<b>2. Content of Personal Privacy Policies</b>	<b>488</b>
Privacy Legislation and Directives	488
Requirements from Privacy Principles	488
Privacy Policy Specification	490
<b>3. Semiautomated Derivation of Personal Privacy Policies</b>	<b>490</b>
An Example	492
Retrieval from a Community of Peers	493
<b>4. Specifying Well-formed Personal Privacy Policies</b>	<b>494</b>
Unexpected Outcomes	494
Outcomes From the Way the Matching Policy Was Obtained	494
<b>5. Preventing Unexpected Negative Outcomes</b>	<b>496</b>
Definition 1	496
Definition 2	496
Rules for Specifying Near Well-Formed Privacy Policies	496

Approach for Obtaining Near Well-Formed Privacy Policies	497
<b>6. The Privacy Management Model</b>	<b>497</b>
How Privacy Policies Are Used	497
Personal Privacy Policy Negotiation	499
Personal Privacy Policy Compliance	502
<b>7. Discussion and Related Work</b>	<b>502</b>
<b>8. Conclusions and Future Work</b>	<b>505</b>

**30. Virtual Private Networks 507**

*Jim Harmening and Joe Wright*

<b>1. History</b>	<b>508</b>
<b>2. Who is in Charge?</b>	<b>511</b>
<b>3. VPN Types</b>	<b>512</b>
IPsec	512
L2TP	512
L2TPv3	513
L2F	513
PPTP VPN	513
MPLS	514
MPVPN™	514
SSH	514
SSL-VPN	514
TLS	514
<b>4. Authentication Methods</b>	<b>515</b>
Hashing	515
HMAC	515
MD5	515
SHA-1	515
<b>5. Symmetric Encryption</b>	<b>516</b>
<b>6. Asymmetric Cryptography</b>	<b>516</b>
<b>7. Edge Devices</b>	<b>516</b>
<b>8. Passwords</b>	<b>516</b>
<b>9. Hackers and Crackers</b>	<b>517</b>

**31. Identity Theft 519**

*Markus Jacobsson and Alex Tsow*

<b>1. Experimental Design</b>	<b>520</b>
Authentic Payment Notification: Plain Versus Fancy Layout	522
Strong Phishing Message: Plain Versus Fancy Layout	525
Authentic Promotion: Effect of Small Footers	525
Weak Phishing Message	527
Authentic Message	528
Login Page	528
Login Page: Strong and Weak Content Alignment	529
Login Page: Authentic and Bogus (But Plausible) URLs	532
Login Page: Hard and Soft Emphasis on Security	532
Bad URL, with and without SSL and Endorsement Logo	535
High-Profile Recall Notice	535

Low-Profile Class-Action Lawsuit	535		
<b>2. Results and Analysis</b>	<b>535</b>		
<b>3. Implications for Crimeware</b>	<b>546</b>		
Example: Vulnerability of Web-Based Update Mechanisms	547		
Example: The Unsubscribe Spam Attack	547		
The Strong Narrative Attack	548		
<b>4. Conclusion</b>	<b>548</b>		
<b>32. VoIP Security</b>	<b>551</b>		
<i>Dan Wing and Harsh Kupwade Patil</i>			
<b>1. Introduction</b>	<b>551</b>		
VoIP Basics	551		
<b>2. Overview of Threats</b>	<b>553</b>		
Taxonomy of Threats	553		
Reconnaissance of VoIP Networks	553		
Denial of Service	554		
Loss of Privacy	555		
Exploits	557		
<b>3. Security in VoIP</b>	<b>558</b>		
Preventative Measures	558		
Reactive	559		
<b>4. Future Trends</b>	<b>560</b>		
Forking Problem in SIP	560		
Security in Peer-to-Peer SIP	561		
End-to-End Identity with SBCs	563		
<b>5. Conclusion</b>	<b>564</b>		
<b>Part V</b>			
<b>Storage Security</b>			
<b>33. SAN Security</b>	<b>567</b>		
<i>John McGowan, Jeffrey Bardin and John McDonald</i>			
<b>1. Organizational Structure</b>	<b>567</b>		
AAA	568		
Restricting Access to Storage	569		
<b>2. Access Control Lists (ACL) and Policies</b>	<b>570</b>		
Data Integrity Field (DIF)	570		
<b>3. Physical Access</b>	<b>571</b>		
<b>4. Change Management</b>	<b>571</b>		
<b>5. Password Policies</b>	<b>571</b>		
<b>6. Defense in Depth</b>	<b>571</b>		
<b>7. Vendor Security Review</b>	<b>571</b>		
<b>8. Data Classification</b>	<b>571</b>		
<b>9. Security Management</b>	<b>572</b>		
Security Setup	572		
Unused Capabilities	572		
<b>10. Auditing</b>	<b>572</b>		
Updates	572		
Monitoring	572		
Security Maintenance	572		
<b>11. Management Access: Separation of Functions</b>	<b>573</b>		
Limit Tool Access	573		
Secure Management Interfaces	573		
<b>12. Host Access: Partitioning</b>	<b>573</b>		
S_ID Checking	574		
<b>13. Data Protection: Replicas</b>	<b>574</b>		
Erasure	574		
Potential Vulnerabilities and Threats	575		
Physical Attacks	575		
Management Control Attacks	575		
Host Attacks	575		
World Wide Name Spoofing	576		
Man-in-the-Middle Attacks	576		
E-Port Replication Attack	576		
Denial-of-Service Attacks	577		
Session Hijacking Attacks	577		
<b>15. Encryption in Storage</b>	<b>577</b>		
The Process	577		
Encryption Algorithms	578		
Key Management	579		
Configuration Management	580		
<b>16. Application of Encryption</b>	<b>580</b>		
Risk Assessment and Management	580		
Modeling Threats	580		
Use Cases for Protecting Data at Rest	581		
Use Considerations	582		
Deployment Options	582		
<b>17. Conclusion</b>	<b>588</b>		
<b>References</b>	<b>589</b>		
<b>34. Storage Area Networking Devices Security</b>	<b>591</b>		
<i>Robert Rounsavall</i>			
<b>1. What is a SAN?</b>	<b>591</b>		
<b>2. SAN Deployment Justifications</b>	<b>591</b>		
<b>3. The Critical Reasons for SAN Security</b>	<b>592</b>		
Why Is SAN Security Important?	592		
<b>4. SAN Architecture and Components</b>	<b>593</b>		
SAN Switches	593		
<b>5. SAN General Threats and Issues</b>	<b>594</b>		
SAN Cost: A Deterrent to Attackers	594		
Physical Level Threats, Issues, and Risk Mitigation	594		
Logical Level Threats, Vulnerabilities, and Risk Mitigation	596		
<b>6. Conclusion</b>	<b>603</b>		
<b>35. Risk Management</b>	<b>605</b>		
<i>Sokratis K. Katsikas</i>			
<b>1. The Concept of Risk</b>	<b>606</b>		
<b>2. Expressing and Measuring Risk</b>	<b>606</b>		
<b>3. The Risk Management Methodology</b>	<b>609</b>		
Context Establishment	609		



- Risk Assessment 610
- Risk Treatment 612
- Risk Communication 614
- Risk Monitoring and Review 614
- Integrating Risk Management into the System Development Life Cycle 614
- Critique of Risk Management as a Methodology 615
- Risk Management Methods 616
- 4. Risk Management Laws and Regulations 620**
- 5. Risk Management Standards 623**
- 6. Summary 625**

**Part VI  
Physical Security**

**36. Physical Security Essentials 629**

*William Stallings*

- 1. Overview 629**
- 2. Physical Security Threats 630**
  - Natural Disasters 630
  - Environmental Threats 631
  - Technical Threats 633
  - Human-Caused Physical Threats 634
- 3. Physical Security Prevention and Mitigation Measures 634**
  - Environmental Threats 634
  - Technical Threats 635
  - Human-Caused Physical Threats 635
- 4. Recovery from Physical Security Breaches 636**
- 5. Threat Assessment, Planning, and Plan Implementation 636**
  - Threat Assessment 636
  - Planning and Implementation 637
- 6. Example: A Corporate Physical Security Policy 637**
- 7. Integration of Physical and Logical Security 639**
- References 643

**37. Biometrics 645**

*Luther Martin*

- 1. Relevant Standards 646**
- 2. Biometric System Architecture 647**
  - Data Capture 648
  - Signal Processing 648
  - Matching 649
  - Data Storage 649
  - Decision 649
  - Adaptation 652
- 3. Using Biometric Systems 652**
  - Enrollment 652

- Authentication 653
- Identification 654
- 4. Security Considerations 655**
  - Error Rates 655
  - Doddington's Zoo 656
  - Birthday Attacks 656
  - Comparing Technologies 657
  - Storage of Templates 658
- 5. Conclusion 659**

**38. Homeland Security 661**

*Rahul Bhaskar Ph.D. and Bhushan Kapoor*

- 1. Statutory Authorities 661**
  - The USA PATRIOT Act of 2001 (PL 107-56) 661
  - The Aviation and Transportation Security Act of 2001 (PL 107-71) 663
  - Enhanced Border Security and Visa Entry Reform Act of 2002 (PL 107-173) 663
  - Public Health Security, Bioterrorism Preparedness & Response Act of 2002 (PL 107-188) 664
  - Homeland Security Act of 2002 (PL 107-296) 665
  - E-Government Act of 2002 (PL 107-347) 666
- 2. Homeland Security Presidential Directives 667**
- 3. Organizational Actions 669**
  - Department of Homeland Security Subcomponents 669
  - State and Federal Organizations 669
  - The Governor's Office of Homeland Security 670
  - California Office of Information Security and Privacy Protection 670
  - Private Sector Organizations for Information Sharing 670
- 4. Conclusion 674**

**39. Information Warfare 677**

*Jan Eloff and Anna Granova*

- 1. Information Warfare Model 677**
- 2. Information Warfare Defined 678**
- 3. IW: Myth or Reality? 678**
- 4. Information Warfare: Making IW Possible 680**
  - Offensive Strategies 680
- 5. Preventative Strategies 685**
- 6. Legal Aspects of IW 686**
  - Terrorism and Sovereignty 686
  - Liability Under International Law 686
  - Remedies Under International Law 687
  - Developing Countries Response 689

7. Holistic View of Information Warfare	689	U.S. Government	725
8. Conclusion	690	Other Governments	725
		Libraries	725
		Parents	726
<b>Part VII</b>		<b>3. Content Blocking Methods</b>	<b>726</b>
<b>Advanced Security</b>		Banned Word Lists	726
<b>40. Security Through Diversity</b>	<b>693</b>	URL Block	726
<i>Kevin Noble</i>		Category Block	726
1. Ubiquity	693	Bayesian Filters	727
2. Example Attacks Against Uniformity	694	Safe Search Integration to Search Engines with Content Labeling	727
3. Attacking Ubiquity With Antivirus Tools	694	Content-Based Image Filtering (CBIF)	727
4. The Threat of Worms	695	<b>4. Technology and Techniques for Content-Filtering Control</b>	<b>728</b>
5. Automated Network Defense	697	Internet Gateway-Based Products/Unified Threat Appliances	728
6. Diversity and the Browser	698	<b>5. Categories</b>	<b>732</b>
7. Sandboxing and Virtualization	698	<b>6. Legal Issues</b>	<b>735</b>
8. DNS Example of Diversity through Security	699	Federal Law: ECPA	735
9. Recovery from Disaster is Survival	699	CIPA: The Children's Internet Protection Act	735
10. Conclusion	700	The Trump Card of Content Filtering: The "National Security Letter"	736
		ISP Content Filtering Might Be a "Five-Year Felony"	736
<b>41. Reputation Management</b>	<b>701</b>	<b>7. Issues and Problems with Content Filtering</b>	<b>737</b>
<i>Dr. Jean-Marc Seigneur</i>		Bypass and Circumvention	737
1. The Human Notion of Reputation	702	Client-Based Proxies	737
2. Reputation Applied to the Computing World	704	Open Proxies	739
3. State of the Art of Attack-resistant Reputation Computation	708	HTTP Web-Based Proxies (Public and Private)	739
4. Overview of Current Online Reputation Service	711	Secure Public Web-Based Proxies	739
eBay	711	Process Killing	739
Opinity	713	Remote PC Control Applications	739
Rapleaf	714	Overblocking and Underblocking	740
Venyo	715	Blacklist and Whitelist Determination	740
TrustPlus + Xing + ZoomInfo + SageFire	716	Casual Surfing Mistake	740
Naymz + Trufina	717	Getting the List Updated	740
The GORB	719	Time-of-Day Policy Changing	740
ReputationDefender	720	Override Authorization Methods	740
Summarizing Table	720	Hide Content in "Noise" or Use Steganography	740
5. Conclusion	720	Nonrepudiation: Smart Cards, ID Cards for Access	740
		Warn and Allow Methods	740
<b>42. Content Filtering</b>	<b>723</b>	Integration with Spam Filtering tools	740
<i>Peter Nicoletti</i>		Detect Spyware and Malware in the HTTP Payload	740
1. The Problem with Content Filtering	723	Integration with Directory Servers	740
2. User Categories, Motivations, and Justifications	724	Language Support	741
Schools	725	Financial Considerations Are Important	741
Commercial Business	725	Scalability and Usability	741
Financial Organizations	725	Performance Issues	742
Healthcare Organizations	725	Reporting Is a Critical Requirement	742
Internet Service Providers	725	Bandwidth Usage	742

	Precision Percentage and Recall	742
9.	<b>Related Products</b>	743
10.	<b>Conclusion</b>	743
<b>43.</b>	<b>Data Loss Protection</b>	<b>745</b>
	<i>Ken Perkins</i>	
1.	<b>Precursors of DLP</b>	747
2.	<b>What is DLP?</b>	748
3.	<b>Where to Begin?</b>	753
4.	<b>Data is Like Water</b>	754
5.	<b>You Don't Know What You Don't Know</b>	755
	Precision versus Recall	756
6.	<b>How Do DLP Applications Work?</b>	756
7.	<b>Eat Your Vegetables</b>	757
	Data in Motion	757
	Data at Rest	758
	Data in Use	758
8.	<b>It's a Family Affair, Not Just it Security's Problem</b>	760
9.	<b>Vendors, Vendors Everywhere! Who Do You Believe?</b>	762
10.	<b>Conclusion</b>	762

Part VIII  
**Appendices**

<b>Appendix A</b>	<b>Configuring Authentication Service on Microsoft Windows Vista</b>	<b>765</b>
	<i>John R. Vacca</i>	
1.	<b>Backup and Restore of Stored Usernames and Passwords</b>	765
	Automation and Scripting	765
	Security Considerations	765
2.	<b>Credential Security Service Provider and SSO for Terminal Services Logon</b>	765
	Requirements	766
	Configuration	766
	Security Considerations	766
3.	<b>TLS/SSL Cryptographic Enhancements</b>	766
	AES Cipher Suites	766
	ECC Cipher Suites	767
	Schannel CNG Provider Model	768
	Default Cipher Suite Preference	769
	Previous Cipher Suites	769
4.	<b>Kerberos Enhancements</b>	769
	AES	769
	Read-Only Domain Controller and Kerberos Authentication	770
5.	<b>Smart Card Authentication Changes</b>	770
	Additional Changes to Common Smart Card Logon Scenarios	771

6.	<b>Previous Logon Information</b>	773
	Configuration	774
	Security Considerations	774
<b>Appendix B</b>	<b>Security Management and Resiliency</b>	<b>775</b>
	<i>John R. Vacca</i>	
<b>Appendix C</b>	<b>List of Top Security Implementation and Deployment Companies</b>	<b>777</b>
	List of SAN Implementation and Deployment Companies	778
	SAN Security Implementation and Deployment Companies:	778
<b>Appendix D</b>	<b>List of Security Products</b>	<b>781</b>
	Security Software	781
<b>Appendix E</b>	<b>List of Security Standards</b>	<b>783</b>
<b>Appendix F</b>	<b>List of Miscellaneous Security Resources</b>	<b>785</b>
	Conferences	785
	Consumer Information	785
	Directories	786
	Help and Tutorials	786
	Mailing Lists	786
	News and Media	787
	Organizations	787
	Products and Tools	788
	Research	790
	Content Filtering Links	791
	Other Logging Resources	791
<b>Appendix G</b>	<b>Ensuring Built-in Frequency Hopping Spread Spectrum Wireless Network Security</b>	<b>793</b>
	Accomplishment	793
	Background	793
	Additional Information	793
<b>Appendix H</b>	<b>Configuring Wireless Internet Security Remote Access</b>	<b>795</b>
	Adding the Access Points as RADIUS Clients to IAS	795
	Adding Access Points to the first IAS Server	795

<b>Scripting the Addition of Access Points to IAS Server (Alternative Procedure)</b>	<b>795</b>	<b>Appendix I</b>	<b>Frequently Asked Questions</b>	<b>799</b>
<b>Configuring the Wireless Access Points</b>	<b>796</b>			
<b>Enabling Secure WLAN Authentication on Access Points</b>	<b>796</b>	<b>Appendix J</b>	<b>Glossary</b>	<b>801</b>
<b>Additional Settings to Secure Wireless Access Points</b>	<b>797</b>	<b>Index</b>		<b>817</b>
<b>Replicating RADIUS Client Configuration to Other IAS Servers</b>	<b>798</b>			

*The Computer and Information Security Handbook* is an essential reference guide for professionals in all realms of computer security. Researchers in academia, industry, and government as well as students of security will find the *Handbook* helpful in expediting security research efforts. The *Handbook* should become a part of every corporate, government, and university library around the world.

Dozens of experts from virtually every industry have contributed to this book. The contributors are the leading experts in computer security, privacy protection and management, and information assurance. They are individuals who will help others in their communities to address the immediate as well as long-term challenges faced in their respective computer security realms.

These important contributions make the *Handbook* stand out among all other security reference guides. I know and have worked with many of the contributors and can testify to their experience, accomplishments, and dedication to their fields of work.

John Vacca, the lead security consultant and managing editor of the *Handbook*, has worked diligently to see that this book is as comprehensive as possible. His knowledge, experience, and dedication have combined to create a book of more than 1400 pages covering every important

aspect of computer security and the assurance of the confidentiality, integrity, and availability of information.

The depth of knowledge brought to the project by all the contributors assures that this comprehensive handbook will serve as a professional reference and provide a complete and concise view of computer security and privacy. The *Handbook* provides in-depth coverage of computer security theory, technology, and practice as it relates to established technologies as well as recent advancements in technology. Above all, the *Handbook* explores practical solutions to a wide range of security issues.

Another important characteristic of the *Handbook* is that it is a vendor-edited volume with chapters written by leading experts in industry and academia who do not support any specific vendor's products or services. Although there are many excellent computer security product and service companies, these companies often focus on promoting their offerings as one-and-only, best-on-the-market solutions. Such bias can lead to narrow decision making and product selection and thus was excluded from the *Handbook*.

*Michael Erbschloe*

*Michael Erbschloe teaches information security courses at Webster University in St. Louis, Missouri.*



This comprehensive handbook serves as a professional reference to provide today's most complete and concise view of computer security and privacy available in one volume. It offers in-depth coverage of computer security theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise.

The primary audience for this handbook consists of researchers and practitioners in industry and academia as well as security technologists and engineers working with or interested in computer security. This comprehensive reference will also be of value to students in upper-division undergraduate and graduate-level courses in computer security.

## ORGANIZATION OF THIS BOOK

The book is organized into eight parts composed of 43 contributed chapters by leading experts in their fields, as well as 10 appendices, including an extensive glossary of computer security terms and acronyms.

### Part 1: Overview of System and Network Security: A Comprehensive Introduction

Part 1 discusses how to build a secure organization; generating cryptography; how to prevent system intrusions; UNIX and Linux security; Internet and intranet security; LAN security; wireless network security; cellular network security, and RFID security. For instance:

- Chapter 1, "Building a Secure Organization," sets the stage for the rest of the book by presenting insight into where to start building a secure organization.
- Chapter 2, "A Cryptography Primer," provides an overview of cryptography. It shows how communications may be encrypted and transmitted.
- Chapter 3, "Preventing System Intrusions," discusses how to prevent system intrusions and where an

- unauthorized penetration of a computer in your enterprise or an address in your assigned domain can occur.
- Chapter 4, "Guarding Against Network Intrusions," shows how to guard against network intrusions by understanding the variety of attacks, from exploits to malware and social engineering.
- Chapter 5, "UNIX and Linux Security," discusses how to scan for vulnerabilities; reduce denial-of-service (DoS) attacks; deploy firewalls to control network traffic; and build network firewalls.
- Chapter 6, "Eliminating the Security Weakness of Linux and UNIX Operating Systems," presents an introduction to securing UNIX in general and Linux in particular, providing some historical context and describing some fundamental aspects of the secure operating system architecture.
- Chapter 7, "Internet Security," shows you how cryptography can be used to address some of the security issues besetting communications protocols.
- Chapter 8, "The Botnet Problem," describes the botnet threat and the countermeasures available to network security professionals.
- Chapter 9, "Intranet Security," covers internal security strategies and tactics; external security strategies and tactics; network access security; and Kerberos.
- Chapter 10, "Local Area Network Security," discusses network design and security deployment as well as ongoing management and auditing.
- Chapter 11, "Wireless Network Security," presents an overview of wireless network security technology; how to design wireless network security and plan for wireless network security; how to install, deploy, and maintain wireless network security; information warfare countermeasures: the wireless network security solution; and wireless network security solutions and future directions.
- Chapter 12, "Cellular Network Security," addresses the security of the cellular network; educates readers on the current state of security of the network and its vulnerabilities; outlines the cellular network specific attack taxonomy, also called *three-dimensional attack taxonomy*; discusses the vulnerability assessment tools for cellular networks; and provides

insights into why the network is so vulnerable and why securing it can prevent communication outages during emergencies.

Chapter 13, “RFID Security,” describes the RFID tags and RFID reader and back-end database in detail.

## Part 2: Managing Information Security

Part 2 discusses how to protect mission-critical systems; deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, and penetration testing; and conduct vulnerability assessments. For instance:

Chapter 14, “Information Security Essentials for IT Managers: Protecting Mission-Critical Systems,” discusses how security goes beyond technical controls and encompasses people, technology, policy, and operations in a way that few other business objectives do.

Chapter 15, “Security Management Systems,” examines documentation requirements and maintaining an effective security system as well as conducting assessments.

Chapter 16, “Information Technology Security Management,” discusses the processes that are supported with enabling organizational structure and technology to protect an organization’s information technology operations and IT assets against internal and external threats, intentional or otherwise.

Chapter 17, “Identity Management,” presents the evolution of identity management requirements. It also surveys how the most advanced identity management technologies fulfill present-day requirements. It discusses how mobility can be achieved in the field of identity management in an ambient intelligent/ubiquitous computing world.

Chapter 18, “Intrusion Prevention and Detection Systems,” discusses the nature of computer system intrusions, the people who commit these attacks, and the various technologies that can be utilized to detect and prevent them.

Chapter 19, “Computer Forensics,” is intended to provide an in-depth familiarization with computer forensics as a career, a job, and a science. It will help you avoid mistakes and find your way through the many aspects of this diverse and rewarding field.

Chapter 20, “Network Forensics,” helps you determine the path from a victimized network or

system through any intermediate systems and communication pathways, back to the point of attack origination or the person who should be held accountable.

Chapter 21, “Firewalls,” provides an overview of firewalls: policies, designs, features, and configurations. Of course, technology is always changing, and network firewalls are no exception. However, the intent of this chapter is to describe aspects of network firewalls that tend to endure over time.

Chapter 22, “Penetration Testing,” describes how testing differs from an actual “hacker attack” as well as some of the ways penetration tests are conducted, how they’re controlled, and what organizations might look for when choosing a company to conduct a penetration test for them.

Chapter 23, “What Is Vulnerability Assessment?” covers the fundamentals: defining vulnerability, exploit, threat, and risk; analyzing vulnerabilities and exploits; and configuring scanners. It also shows you how to generate reports, assess risks in a changing environment, and manage vulnerabilities.

## Part 3: Encryption Technology

Part 3 discusses how to implement data encryption, satellite encryption, public key infrastructure, and instant-messaging security. For instance:

Chapter 24, “Data Encryption,” is about the role played by cryptographic technology in data security.

Chapter 25, “Satellite Encryption,” proposes a method that enhances and complements satellite encryption’s role in securing the information society. It also covers satellite encryption policy instruments; implementing satellite encryption; misuse of satellite encryption technology; and results and future directions.

Chapter 26, “Public Key Infrastructure,” explains the cryptographic background that forms the foundation of PKI systems; the mechanics of the X.509 PKI system (as elaborated by the Internet Engineering Task Force); the practical issues surrounding the implementation of PKI systems; a number of alternative PKI standards; and alternative cryptographic strategies for solving the problem of secure public key distribution.

Chapter 27, “Instant-Messaging Security,” helps you develop an IM security plan, keep it current, and make sure it makes a difference.



## Part 4: Privacy and Access Management

Part 4 discusses Internet privacy, personal privacy policies, virtual private networks, identity theft, and VoIP security. For instance:

Chapter 28, “Net Privacy,” addresses the privacy issues in the digital society from various points of view, investigating the different aspects related to the notion of privacy and the debate that the intricate essence of privacy has stimulated; the most common privacy threats and the possible economic aspects that may influence the way privacy is (and especially is not currently) managed in most firms; the efforts in the computer science community to face privacy threats, especially in the context of mobile and database systems; and the network-based technologies available to date to provide anonymity when communicating over a private network.

Chapter 29, “Personal Privacy Policies,” begins with the derivation of policy content based on privacy legislation, followed by a description of how a personal privacy policy may be constructed semiautomatically. It then shows how to additionally specify policies so that negative unexpected outcomes can be avoided. Finally, it describes the author’s Privacy Management Model, which explains how to use personal privacy policies to protect privacy, including what is meant by a “match” of consumer and service provider policies and how nonmatches can be resolved through negotiation.

Chapter 30, “Virtual Private Networks,” covers VPN scenarios, VPN comparisons, and information assurance requirements. It also covers building VPN tunnels; applying cryptographic protection; implementing IP security; and deploying virtual private networks.

Chapter 31, “Identity Theft,” describes the importance of understanding the human factor of ID theft security and details the findings from a study on deceit.

Chapter 32, “VoIP Security,” deals with the attacks targeted toward a specific host and issues related to social engineering.

## Part 5: Storage Security

Part 5 covers storage area network (SAN) security and risk management. For instance:

Chapter 33, “SAN Security,” describes the following components: protection rings; security and

protection; restricting access to storage; access control lists (ACLs) and policies; port blocks and port prohibits; and zoning and isolating resources.

Chapter 34, “Storage Area Networking Security Devices,” covers all the issues and security concerns related to SAN security.

Chapter 35, “Risk Management,” discusses physical security threats, environmental threats, and incident response.

## Part 6: Physical Security

Part 6 discusses physical security essentials, biometrics, homeland security, and information warfare. For instance:

Chapter 36, “Physical Security Essentials,” is concerned with physical security and some overlapping areas of premises security. It also looks at physical security threats and then considers physical security prevention measures.

Chapter 37, “Biometrics,” discusses the different types of biometrics technology and verification systems and how the following work: biometrics eye analysis technology; biometrics facial recognition technology; facial thermal imaging; biometrics finger-scanning analysis technology; biometrics geometry analysis technology; biometrics verification technology; and privacy-enhanced, biometrics-based verification/authentication as well as biometrics solutions and future directions.

Chapter 38, “Homeland Security,” describes some principle provisions of U.S. homeland security-related laws and Presidential directives. It gives the organizational changes that were initiated to support homeland security in the United States. The chapter highlights the 9/11 Commission that Congress charted to provide a full account of the circumstances surrounding the 2001 terrorist attacks and to develop recommendations for corrective measures that could be taken to prevent future acts of terrorism. It also details the Intelligence Reform and Terrorism Prevention Act of 2004 and the Implementation of the 9/11 Commission Recommendations Act of 2007.

Chapter 39, “Information Warfare,” defines information warfare (IW) and discusses its most common tactics, weapons, and tools as well as comparing IW terrorism with conventional warfare and addressing the issues of liability and the available legal remedies under international law.

## Part 7: Advanced Security

Part 7 discusses security through diversity, online reputation, content filtering, and data loss protection. For instance:

Chapter 40, “Security Through Diversity,” covers some of the industry trends in adopting diversity in hardware, software, and application deployments. This chapter also covers the risks of uniformity, conformity, and the ubiquitous impact of adopting standard organizational principals without the consideration of security.

Chapter 41, “Reputation Management,” discusses the general understanding of the human notion of reputation. It explains how this concept of reputation fits into computer security. The chapter presents the state of the art of attack-resistant reputation computation. It also gives an overview of the current market of online reputation services. The chapter concludes by underlining the need to standardize online reputation for increased adoption and robustness.

Chapter 42, “Content Filtering,” examines the many benefits and justifications of Web-based content filtering such as legal liability risk reduction, productivity gains, and bandwidth usage. It also explores the downside and unintended consequences and risks that improperly deployed or misconfigured systems create. The chapter also looks into methods to subvert and bypass these systems and the reasons behind them.

Chapter 43, “Data Loss Protection,” introduces the reader to a baseline understanding of how to investigate and evaluate DLP applications in the market today.

*John R. Vacca*  
*Editor-in-Chief*  
*[jvacca@frognet.net](mailto:jvacca@frognet.net)*  
*[www.johnvacca.com](http://www.johnvacca.com)*

---

## Acknowledgments

There are many people whose efforts on this book have contributed to its successful completion. I owe each a debt of gratitude and want to take this opportunity to offer my sincere thanks.

A very special thanks to my senior acquisitions editor, Rick Adams, without whose continued interest and support this book would not have been possible. Assistant editor Heather Scherer provided staunch support and encouragement when it was most needed. Thanks to my production editor, A. B. McGee, and copyeditor, Darlene Bordwell, whose fine editorial work has been invaluable. Thanks also to my marketing manager, Marissa Hederson, whose efforts on this book have been greatly appreciated. Finally, thanks to all the other people at Computer Networking and Computer and Information Systems Security, Morgan Kaufmann Publishers/Elsevier Science & Technology Books, whose many talents and skills are essential to a finished book.

Thanks to my wife, Bee Vacca, for her love, her help, and her understanding of my long work hours. Also, a

very, very special thanks to Michael Erbschloe for writing the Foreword. Finally, I wish to thank all the following authors who contributed chapters that were necessary for the completion of this book: John Mallery, Scott R. Ellis, Michael West, Tom Chen, Patrick Walsh, Gerald Beuchelt, Mario Santana, Jesse Walker, Xinyuan Wang, Daniel Ramsbrock, Bill Mansoor, Dr. Pramod Pandya, Chunming Rong, Prof. Erdal Cayirci, Prof. Gansen Zhao, Liang Yan, Peng Liu, Thomas F La Porta, Kameswari Kotapati, Albert Caballero, Joe Wright, Jim Harmening, Rahul Bhaskar, Prof. Bhushan Kapoor, Dr. Jean-Marc Seigneur, Christopher W. Day, Yong Guan, Dr. Errin W. Fulp, Sanjay Bavisi, Almantas Kakareka, Daniel S. Soper, Terence Spies, Samuel JJ Curry, Marco Cremonini, Chiara Braghin, Claudio Agostino Ardagna, Dr. George Yee, Markus Jacobsson, Alex Tsow, Sid Stamm, Chris Soghoian, Harsh Kupwade Patil, Dan Wing, Jeffrey S. Bardin, Robert Rounsavall, Sokratis K. Katsikas, William Stallings, Luther Martin, Jan Eloff, Anna Granova, Kevin Noble, Peter Nicoletti, and Ken Perkins.



## About the Editor



John Vacca is an information technology consultant and bestselling author based in Pomeroy, Ohio. Since 1982 John has authored 60 books. Some of his most recent works include *Biometric Technologies and Verification Systems* (Elsevier, 2007); *Practical Internet Security* (Springer, 2006); *Optical Networking Best Practices*

*Handbook* (Wiley-Interscience, 2006); *Guide to Wireless Network Security* (Springer, 2006); *Computer Forensics: Computer Crime Scene Investigation, 2nd Edition* (Charles River Media, 2005); *Firewalls: Jumpstart for Network and Systems Administrators* (Elsevier, 2004); *Public Key Infrastructure: Building Trusted Applications and Web Services* (Auerbach, 2004); *Identity Theft* (Prentice Hall/PTR, 2002); *The World's 20 Greatest Unsolved Problems* (Pearson Education, 2004); and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA's space station program (Freedom) and the International Space Station Program from 1988 until his early retirement from NASA in 1995.



## Contributors

- Claudio Agostino Ardagna (Chapter 28)**, Dept. of Information Technology, University of Milan, Crema, Italy
- Jeffrey S. Bardin (Chapter 33)**, Independent Security Consultant, Barre, Massachusetts 01005
- Jay Bavis (Chapter 22)**, President, EC-Council, Albuquerque, New Mexico 87109
- Gerald Beuchelt (Chapter 5)**, Independent Security Consultant, Burlington, Massachusetts 01803
- Rahul Bhaskar (Chapter 38)**, Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834
- Rahul Bhaskar (Chapter 16)**, Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834
- Chiara Braghin (Chapter 28)**, Dept. of Information Technology, University of Milan, Crema, Italy
- Albert Caballero CISSP, GSEC (Chapter 14)**, Security Operations Center Manager, Terremark Worldwide, Inc., Bay Harbor Islands, Florida 33154
- Professor Erdal Cayirci (Chapters 11, 13)**, University of Stavanger, N-4036 Stavanger, Norway
- Tom Chen (Chapter 4)**, Swansea University, Singleton Park, SA2 8PP, Wales, United Kingdom
- Marco Cremonini (Chapter 28)**, Dept. of Information Technology, University of Milan, Crema, Italy
- Sam Curry (Chapter 27)**, VP Product Management, RSA, the Security Division of EMC, Bedford, Massachusetts 01730
- Christopher Day, CISSP, NSA:IEM (Chapter 18)**, Senior Vice President, Secure Information Systems, Terremark Worldwide, Inc., Miami, Florida 33131
- Scott R. Ellis, EnCE (Chapters 2, 19)**, RGL – Forensic Accountants & Consultants, Forensics and Litigation Technology, Chicago, Illinois 60602
- Jan H. P. Eloff (Chapter 39)**, Extraordinary Professor, Information & Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria, and Research Director SAP Meraka UTD/SAP Research CEC, Hillcrest, Pretoria, South Africa, 0002
- Michael Erbschloe (Foreword)**, Teaches Information Security courses at Webster University, St. Louis, Missouri 63119
- Errin W. Fulp (Chapter 21)**, Department of Computer Science, Wake Forest University, Winston-Salem, North Carolina 27109
- Anna Granova (Chapter 39)**, Advocate of the High Court of South Africa, Member of the Pretoria Society of Advocates, University of Pretoria, Computer Science Department, Hillcrest, Pretoria, South Africa, 0002
- Yong Guan (Chapter 20)**, Litton Assistant Professor, Department of Electrical and Computer Engineering, Iowa State University, Ames, Iowa 50011
- James T. Harmening (Chapters 15, 30)**, Computer Bits, Inc., Chicago, Illinois 60602
- Markus Jakobsson (Chapter 31)**, Principal Scientist, CSL, Palo Alto Research Center, Palo Alto, California 94304
- Almantas Kakareka (Chapter 23)**, Terremark World Wide Inc., Security Operations Center, Miami, Florida 33132
- Bhushan Kapoor (Chapters 16, 24, 38)**, Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834
- Sokratis K. Katsikas (Chapter 35)**, Department of Technology Education & Digital Systems, University of Piraeus, Piraeus 18532, Greece
- Larry Korba (Chapter 29)**, Ottawa, Ontario, Canada K1G 5N7.
- Kameswari Kotapati (Chapter 12)**, Department of Computer Science and Engineering, The Pennsylvania State University, University Park, Pennsylvania 16802
- Thomas F. LaPorta (Chapter 12)**, Department of Computer Science and Engineering, The Pennsylvania State University, University Park, Pennsylvania 16802
- Peng Liu (Chapter 12)**, College of Information Sciences and Technology, The Pennsylvania State University, University Park, Pennsylvania 16802
- Tewfiq El Maliki (Chapter 17)**, Telecommunications labs, University of Applied Sciences of Geneva, Geneva, Switzerland

- John R. Mallery (Chapter 1)**, BKD, LLP, Kansas City, Missouri 64105-1936
- Bill Mansoor (Chapter 9)**, Information Systems Audit and Control Association (ISACA), Rancho Santa Margarita, California 92688-8741
- Luther Martin (Chapter 37)**, Voltage Security, Palo Alto, California 94304
- John McDonald (Chapter 33)**, EMC Corporation, Hopkinton, Massachusetts 01748
- John McGowan (Chapter 33)**, EMC Corporation, Hopkinton, Massachusetts 01748
- Peter F. Nicoletti (Chapter 42)**, Secure Information Systems, Terremark Worldwide, Miami, Florida
- Kevin Noble, CISSP GSEC (Chapter 40)**, Director, Secure Information Services, Terremark Worldwide Inc., Miami, Florida 33132
- Pramod Pandya (Chapters 10, 24)**, Department of Information Systems and Decision Sciences, California State University, Fullerton, California 92834
- Harsh Kupwade Patil (Chapter 32)**, Department of Electrical Engineering, Southern Methodist University, Dallas, Texas 75205
- Ken Perkins (Chapter 43)**, CIPP (Certified Information Privacy Professional), Sr. Systems Engineer, Blazent Incorporated, Denver, Colorado 80206
- Daniel Ramsbrock (Chapter 8)**, Department of Computer Science, George Mason University, Fairfax, Virginia 22030
- Chunming Rong (Chapters 11, 13)**, Professor, Ph.D., Chair of Computer Science Section, Faculty of Science and Technology, University of Stavanger, N-4036 Stavanger, Norway
- Robert Rounsavall (Chapter 34)**, GCIA, GCWN, Director, SIS – SOC, Terremark Worldwide, Inc., Miami, Florida 33131
- Mario Santana (Chapter 6)**, Terremark, Dallas, Texas 75226
- Jean-Marc Seigneur (Chapters 17, 41)**, Department of Social and Economic Sciences, University of Geneva, Switzerland
- Daniel S. Soper (Chapter 25)**, Information and Decision Sciences Department, Mihaylo College of Business and Economics, California State University, Fullerton, California 92834-6848
- Terence Spies (Chapter 26)**, Voltage Security, Inc., Palo Alto, California 94304
- William Stallings (Chapter 36)**, Independent consultant, Brewster Massachusetts 02631
- Alex Tsow (Chapter 31)**, The MITRE Corporation, Mclean, Virginia 22102
- Jesse Walker (Chapter 7)**, Intel Corporation, Hillboro, Oregon 97124
- Patrick J. Walsh (Chapter 4)**, eSoft Inc., Broomfield, Colorado 80021
- Xinyuan Wang (Chapter 8)**, Department of Computer Science, George Mason University, Fairfax, Virginia 22030
- Michael A. West (Chapter 3)**, Independent Technical Writer, Martinez, California 94553
- Dan Wing (Chapter 32)**, Security Technology Group, Cisco Systems, San Jose, California 95123
- Joe Wright (Chapters 15, 30)**, Computer Bits, Inc., Chicago, Illinois 60602
- George O.M. Yee (Chapter 29)**, Information Security Group, Institute for Information Technology, National Research Council Canada, Ottawa, Canada K1A 0R6