

# HANDBOOK OF INFORMATION SECURITY

---

**Threats, Vulnerabilities, Prevention,  
Detection, and Management**

---

**Volume 3**

**Hossein Bidgoli**

Editor-in-Chief

*California State University*

*Bakersfield, California*



WILEY

John Wiley & Sons, Inc.

# Contents

Contributors	xv		
Preface	xxiii		
Guide to the Handbook of Information Security	xxvi		
Reviewers List	1051		
Volume Index	1059		
<b>Volume I: Key Concepts, Infrastructure, Standards, and Protocols</b>			
<b>Part 1: Key Concepts and Applications Related to Information Security</b>			
<b>Internet Basics</b>	<b>3</b>		
<i>Hossein Bidgoli</i>			
<b>Digital Economy</b>	<b>15</b>		
<i>Nirvikar Singh</i>			
<b>Online Retail Banking: Security Concerns, Breaches, and Controls</b>	<b>37</b>		
<i>Kent Belasco and Siaw-Peng Wan</i>			
<b>Digital Libraries: Security and Preservation Considerations</b>	<b>49</b>		
<i>Cavan McCarthy</i>			
<b>E-Mail and Instant Messaging</b>	<b>77</b>		
<i>Bhagyavati</i>			
<b>Internet Relay Chat</b>	<b>87</b>		
<i>Paul L. Witt</i>			
<b>Online Communities</b>	<b>97</b>		
<i>Lee Sproull</i>			
<b>Groupware: Risks, Threats, and Vulnerabilities in the Internet Age</b>	<b>110</b>		
<i>Pierre Balthazard and John Warren</i>			
<b>Search Engines: Security, Privacy, and Ethical Issues</b>	<b>126</b>		
<i>Raymond Wisman</i>			
<b>Web Services</b>	<b>151</b>		
<i>Akhil Sahai, Sven Graupner, and Wooyoung Kim</i>			
<b>Electronic Commerce</b>	<b>164</b>		
<i>Charles Steinfield</i>			
<b>EDI Security</b>	<b>179</b>		
<i>Matthew K. McGowan</i>			
<b>Electronic Payment Systems</b>	<b>189</b>		
<i>Indrajit Ray</i>			
<b>Intranets: Principals, Privacy, and Security Considerations</b>	<b>205</b>		
<i>William T. Schiano</i>			
		<b>Extranets: Applications, Development, Security, and Privacy</b>	<b>215</b>
		<i>Stephen W. Thorpe</i>	
		<b>Business-to-Business Electronic Commerce</b>	<b>226</b>
		<i>Julian J. Ray</i>	
		<b>Click-and-Brick Electronic Commerce</b>	<b>242</b>
		<i>Charles Steinfield</i>	
		<b>Mobile Commerce</b>	<b>254</b>
		<i>Vijay Atluri</i>	
		<b>E-Education and Information Privacy and Security</b>	<b>268</b>
		<i>William K. Jackson</i>	
		<b>Security in E-Learning</b>	<b>279</b>
		<i>Edgar R. Weippl</i>	
		<b>E-Government</b>	<b>294</b>
		<i>Shannon Schelin and G. David Garson</i>	
		<b>E-Government Security Issues and Measures</b>	<b>306</b>
		<i>William C. Barker</i>	
		<b>International Security Issues of E-Government</b>	<b>318</b>
		<i>Karin Geiselhart</i>	
		<b>Part 2: Infrastructure for the Internet, Computer Networks, and Secure Information Transfer</b>	
		<b>Conducted Communications Media</b>	<b>337</b>
		<i>Thomas L. Pigg</i>	
		<b>Routers and Switches</b>	<b>350</b>
		<i>Hans-Peter Dommel</i>	
		<b>Radio Frequency and Wireless Communications Security</b>	<b>363</b>
		<i>Okechukwu Ugweje</i>	
		<b>Wireless Channels</b>	<b>387</b>
		<i>P. M. Shankar</i>	
		<b>Security in Circuit, Message, and Packet Switching</b>	<b>400</b>
		<i>Robert H. Greenfield and Daryle P. Niedermayer</i>	
		<b>Digital Communication</b>	<b>415</b>
		<i>Robert W. Heath Jr., William Bard, and Atul A. Salvekar</i>	
		<b>Local Area Networks</b>	<b>428</b>
		<i>Wayne C. Summers</i>	
		<b>Wide Area and Metropolitan Area Networks</b>	<b>444</b>
		<i>Lynn A. DeNoia</i>	
		<b>Home Area Networking</b>	<b>460</b>
		<i>Sherali Zeadally, Priya Kubher, and Nadeem Ansari</i>	

<b>Public Network Technologies and Security</b> <i>Dale R. Thompson and Amy W. Apon</i>	473	<b>Part 3: Standards and Protocols for Secure Information Transfer</b>	
<b>Client/Server Computing: Principles and Security Considerations</b> <i>Daniel J. McFarland</i>	489	<b>Standards for Product Security Assessment</b> <i>István Zsolt Berta, Levente Buttyán, and István Vajda</i>	809
<b>Peer-to-Peer Security</b> <i>Allan Friedman and L. Jean Camp</i>	501	<b>Digital Certificates</b> <i>Albert Levi</i>	823
<b>Security Middleware</b> <i>Linda Volonino and Richard P. Volonino</i>	512	<b>Internet E-Mail Architecture</b> <i>Robert Gezelter</i>	836
<b>Internet Architecture</b> <i>Graham Knight</i>	522	<b>PKI (Public Key Infrastructure)</b> <i>Radia Perlman</i>	852
<b>TCP/IP Suite</b> <i>Prabhaker Mateti</i>	543	<b>S/MIME (Secure MIME)</b> <i>Steven J. Greenwald</i>	859
<b>Voice-over Internet Protocol (VoIP)</b> <i>Roy Morris</i>	561	<b>PGP (Pretty Good Privacy)</b> <i>Stephen A. Weis</i>	868
<b>Security and Web Quality of Service</b> <i>Tarek F. Abdelzhaer and Chengdu Huang</i>	576	<b>SMTP (Simple Mail Transfer Protocol)</b> <i>Vladimir V. Riabov</i>	878
<b>Mobile Devices and Protocols</b> <i>Min Song</i>	592	<b>Internet Security Standards</b> <i>Raymond R. Panko</i>	901
<b>Bluetooth Technology</b> <i>Brent A. Miller</i>	605	<b>Kerberos</b> <i>William Stallings</i>	920
<b>Wireless Local Area Networks</b> <i>M. S. Obaidat, G. I. Papadimitriou, and S. Obeidat</i>	617	<b>IPsec: AH and ESP</b> <i>A. Meddeb, N. Boudriga, and M. S. Obaidat</i>	932
<b>Security in Wireless Sensor Networks</b> <i>Mohamed Eltoweissy, Stephan Olariu, and Ashraf Wadaa</i>	637	<b>IPsec: IKE (Internet Key Exchange)</b> <i>Charlie Kaufman</i>	944
<b>Cellular Networks</b> <i>Jingyuan Zhang and Ivan Stojmenovic</i>	654	<b>Secure Sockets Layer (SSL)</b> <i>Robert J. Boncella</i>	952
<b>Mobile IP</b> <i>M. Farooque Mesiya</i>	664	<b>PKCS (Public Key Cryptography Standards)</b> <i>Yongge Wang</i>	966
<b>IP Multicast and Its Security</b> <i>Emilia Rosti</i>	680	<b>Public Key Standards: Secure Shell</b> <i>Xukai Zou</i>	979
<b>TCP over Wireless Links</b> <i>Mohsen Guizani and Anupama Raju</i>	693	<b>Security and the Wireless Application Protocol</b> <i>Lillian N. Cassel and Cynthia Pandolfo</i>	995
<b>Air Interface Requirements for Mobile Data Services</b> <i>Harald Haas</i>	712	<b>Wireless Network Standards and Protocol (802.11)</b> <i>Prashant Krishnamurthy</i>	1007
<b>Wireless Internet: A Cellular Perspective</b> <i>Abbas Jamalipour</i>	732	<b>P3P (Platform for Privacy Preferences Project)</b> <i>Lorrie Faith Cranor</i>	1023
<b>Security of Satellite Networks</b> <i>Michele Luglio and Antonio Saitto</i>	754	<b>Volume II: Information Warfare: Social, Legal, and International Issues; and Security Foundations</b>	
<b>Security of Broadband Access Networks</b> <i>Peter L. Heinzmann</i>	772	<b>Part 1: Information Warfare</b>	
<b>Ad Hoc Network Security</b> <i>Pietro Michiardi and Refik Molva</i>	787	<b>Cybercrime and the U.S. Criminal Justice System</b> <i>Susan W. Brenner</i>	3
		<b>Cyberterrorism and Information Security</b> <i>Charles Jaeger</i>	16
		<b>Online Stalking</b> <i>David J. Loundy</i>	40

<b>Electronic Attacks</b>	47	<b>Trademark Law and the Internet</b>	381
<i>Thomas M. Chen, Jimi Thompson, and Matthew C. Elder</i>		<i>Ray Everett-Church</i>	
<b>Wireless Information Warfare</b>	59	<b>Online Contracts</b>	392
<i>Randall K. Nichols</i>		<i>G. E. Evans</i>	
<b>Computer Network Operations (CNO)</b>	89	<b>Electronic Speech</b>	408
<i>Andrew Blyth</i>		<i>Seth Finkelstein</i>	
<b>Electronic Protection</b>	101	<b>Software Piracy</b>	418
<i>Neil C. Rowe</i>		<i>Robert K. Moniot</i>	
<b>Information Assurance</b>	110	<b>Internet Gambling</b>	428
<i>Peng Liu, Meng Yu, and Jiwu Jing</i>		<i>Susanna Frederick Fischer</i>	
<b>Part 2: Social and Legal Issues</b>		<b>The Digital Millennium Copyright Act</b>	446
<b>The Legal Implications of Information Security:</b>		<i>Seth Finkelstein</i>	
<b>Regulatory Compliance and Liability</b>	127	<b>Digital Courts, the Law and Evidence</b>	459
<i>Blaze D. Waleski</i>		<i>Robert Slade</i>	
<b>Hackers, Crackers, and Computer Criminals</b>	154	<b>Part 3: Foundations of Information,</b>	
<i>David Dittrich and Kenneth Einar Himma</i>		<b>Computer and Network Security</b>	
<b>Hacktivism</b>	172	<b>Encryption Basics</b>	469
<i>Paul A. Taylor and Jan Ll. Harris</i>		<i>Ari Juels</i>	
<b>Corporate Spying: The Legal Aspects</b>	183	<b>Symmetric Key Encryption</b>	479
<i>William A. Zucker and Scott Nathan</i>		<i>Jonathan Katz</i>	
<b>Law Enforcement and Computer Security Threats</b>	200	<b>Data Encryption Standard (DES)</b>	491
<b>and Measures</b>		<i>Mike Speciner</i>	
<i>Mathieu Deflem and J. Eagle Shutt</i>		<b>The Advanced Encryption Standard</b>	498
<b>Combating the Cybercrime Threat: Developments</b>	210	<i>Duncan A. Buell</i>	
<b>in Global Law Enforcement</b>		<b>Hashes and Message Digests</b>	510
<i>Roderic Broadhurst</i>		<i>Magnus Daum and Hans Dobbertin</i>	
<b>Digital Identity</b>	223	<b>Number Theory for Information Security</b>	532
<i>Drummond Reed and Jerry Kindall</i>		<i>Duncan A. Buell</i>	
<b>Digital Divide</b>	238	<b>Public Key Algorithms</b>	548
<i>Jaime J. Davila</i>		<i>Bradley S. Rubin</i>	
<b>Legal, Social, and Ethical Issues of the Internet</b>	247	<b>Elliptic Curve Cryptography</b>	558
<i>Kenneth Einar Himma</i>		<i>N. P. Smart</i>	
<b>Anonymity and Identity on the Internet</b>	265	<b>IBE (Identity-Based Encryption)</b>	575
<i>Jonathan Wallace</i>		<i>Craig Gentry</i>	
<b>Spam and the Legal Counter Attacks</b>	275	<b>Cryptographic Protocols</b>	593
<i>Charles Jaeger</i>		<i>Markus Jakobsson</i>	
<b>Cyberlaw: The Major Areas, Development,</b>	297	<b>Quantum Cryptography</b>	606
<b>and Information Security Aspects</b>		<i>G. Massimo Palma</i>	
<i>Dennis M. Powers</i>		<b>Key Lengths</b>	617
<b>Global Aspects of Cyberlaw</b>	319	<i>Arjen K. Lenstra</i>	
<i>Julia Alpert Gladstone</i>		<b>Key Management</b>	636
<b>Privacy Law and the Internet</b>	336	<i>Xukai Zou and Amandeep Thukral</i>	
<i>Ray Everett-Church</i>		<b>Secure Electronic Voting Protocols</b>	647
<b>Internet Censorship</b>	349	<i>Helger Lipmaa</i>	
<i>Richard A. Spinello</i>		<b>Digital Evidence</b>	658
<b>Copyright Law</b>	357	<i>Robin C. Stuart</i>	
<i>Randy Canis</i>			
<b>Patent Law</b>	369		
<i>Gerald Bluhm</i>			

<b>Digital Watermarking and Steganography</b> <i>M. A. Suhail, B. Sadoun, and M. S. Obaidat</i>	664	<b>Hacking Techniques in Wireless Networks</b> <i>Prabhaker Mateti</i>	83
<b>Law Enforcement and Digital Evidence</b> <i>J. Philip Craiger, Jeff Swauger, and Mark Pollitt</i>	679	<b>Computer Viruses and Worms</b> <i>Robert Slade</i>	94
<b>Forensic Computing</b> <i>Mohamed Hamdi, Nouredine Boudriga, and Mohammad S. Obaidat</i>	702	<b>Trojan Horse Programs</b> <i>Adam L. Young</i>	107
<b>Computer Forensics Procedures and Methods</b> <i>J. Philip Craiger</i>	715	<b>Hoax Viruses and Virus Alerts</b> <i>Robert Slade</i>	119
<b>Computer Forensics—Computer Media Reviews in Classified Government Agencies</b> <i>Michael R. Anderson</i>	750	<b>Hostile Java Applets</b> <i>David Evans</i>	126
<b>Forensic Analysis of UNIX Systems</b> <i>Dario V. Forte</i>	763	<b>Spyware</b> <i>Tom S. Chan</i>	136
<b>Forensic Analysis of Windows Systems</b> <i>Steve J. Chapin and Chester J. Maciag</i>	781	<b>Mobile Code and Security</b> <i>Song Fu and Cheng-Zhong Xu</i>	146
<b>Operating System Security</b> <i>William Stallings</i>	796	<b>Wireless Threats and Attacks</b> <i>Robert J. Boncella</i>	165
<b>UNIX Security</b> <i>Mark Shacklette</i>	806	<b>WEP Security</b> <i>Nikita Borisov</i>	176
<b>Linux Security</b> <i>A. Justin Wilder</i>	822	<b>Bluetooth Security</b> <i>Susanne Wetzel</i>	184
<b>OpenVMS Security</b> <i>Robert Gezelter</i>	853	<b>Cracking WEP</b> <i>Pascal Meunier</i>	198
<b>Windows 2000 Security</b> <i>E. Eugene Schultz</i>	870	<b>Denial of Service Attacks</b> <i>E. Eugene Schultz</i>	207
<b>Software Development and Quality Assurance</b> <i>Pascal Meunier</i>	885	<b>Network Attacks</b> <i>Edward Amoroso</i>	220
<b>The Common Criteria</b> <i>J. McDermott</i>	897	<b>Fault Attacks</b> <i>Hamid Choukri and Michael Tunstall</i>	230

## **Volume III: Threats, Vulnerabilities, Prevention, Detection, and Management**

### **Part 1: Threats and Vulnerabilities to Information and Computing Infrastructures**

<b>Internal Security Threats</b> <i>Marcus K. Rogers</i>	3
<b>Physical Security Threats</b> <i>Mark Michael</i>	18
<b>Fixed-Line Telephone System Vulnerabilities</b> <i>Mak Ming Tak, Xu Yan, and Zenith Y. W. Law</i>	30
<b>E-Mail Threats and Vulnerabilities</b> <i>David Harley</i>	40
<b>E-Commerce Vulnerabilities</b> <i>Sviatoslav Braynov</i>	57
<b>Hacking Techniques in Wired Networks</b> <i>Qijun Gu, Peng Liu, and Chao-Hsien Chu</i>	70

### **Part 2: Prevention: Keeping the Hackers and Crackers at Bay**

<b>Physical Security Measures</b> <i>Mark Michael</i>	263
<b>RFID and Security</b> <i>Stephen A. Weis</i>	289
<b>Cryptographic Privacy Protection Techniques</b> <i>Markus Jakobsson</i>	300
<b>Cryptographic Hardware Security Modules</b> <i>Nicko van Someren</i>	311
<b>Smart Card Security</b> <i>Michael Tunstall, Sebastien Petit, and Stephanie Porte</i>	326
<b>Client-Side Security</b> <i>Charles Border</i>	342
<b>Server-Side Security</b> <i>Slim Rekhis, Nouredine Boudriga, and M. S. Obaidat</i>	355
<b>Protecting Web Sites</b> <i>Dawn Alexander and April Giles</i>	370

<b>Database Security</b>	380	<b>Part 3: Detection, Recovery, Management, and Policy Considerations</b>	
<i>Michael Gertz and Arnon Rosenthal</i>			
<b>Medical Records Security</b>	395	<b>Intrusion Detection Systems Basics</b>	685
<i>Normand M. Martel</i>		<i>Peng Ning and Sushil Jajodia</i>	
<b>Access Control: Principles and Solutions</b>	406	<b>Host-Based Intrusion Detection System</b>	701
<i>S. De Capitani di Vimercati, S. Paraboschi, and Pierangela Samarati</i>		<i>Giovanni Vigna and Christopher Kruegel</i>	
<b>Password Authentication</b>	424	<b>Network-Based Intrusion Detection Systems</b>	713
<i>Jeremy L. Rasmussen</i>		<i>Marco Cremonini</i>	
<b>Computer and Network Authentication</b>	439	<b>The Use of Agent Technology for Intrusion Detection</b>	730
<i>Patrick McDaniel</i>		<i>Dipankar Dasgupta</i>	
<b>Antivirus Technology</b>	450	<b>Contingency Planning Management</b>	744
<i>Matthew Schmid</i>		<i>Marco Cremonini and Pierangela Samarati</i>	
<b>Biometric Basics and Biometric Authentication</b>	459	<b>Computer Security Incident Response Teams (CSIRTs)</b>	760
<i>James L. Wayman</i>		<i>Raymond R. Panko</i>	
<b>Issues and Concerns in Biometric IT Security</b>	471	<b>Implementing a Security Awareness Program</b>	766
<i>Philip Statham</i>		<i>K. Rudolph</i>	
<b>Firewall Basics</b>	502	<b>Risk Management for IT Security</b>	786
<i>James E. Goldman</i>		<i>Rick Kazman, Daniel N. Port, and David Klappholz</i>	
<b>Firewall Architectures</b>	515	<b>Security Insurance and Best Practices</b>	811
<i>James E. Goldman</i>		<i>Selahattin Kuru, Onur Ihsan Arsun, and Mustafa Yildiz</i>	
<b>Packet Filtering and Stateful Firewalls</b>	526	<b>Auditing Information Systems Security</b>	829
<i>Avishai Wool</i>		<i>S. Rao Vallabhaneni</i>	
<b>Proxy Firewalls</b>	537	<b>Evidence Collection and Analysis Tools</b>	840
<i>John D. McLaren</i>		<i>Christopher L. T. Brown</i>	
<b>E-Commerce Safeguards</b>	552	<b>Information Leakage: Detection and Countermeasures</b>	853
<i>Mark S. Merkow</i>		<i>Phil Venables</i>	
<b>Digital Signatures and Electronic Signatures</b>	562	<b>Digital Rights Management</b>	865
<i>Raymond R. Panko</i>		<i>Renato Iannella</i>	
<b>E-Mail Security</b>	571	<b>Web Hosting</b>	879
<i>Jon Callas</i>		<i>Doug Kaye</i>	
<b>Security for ATM Networks</b>	584	<b>Managing a Network Environment</b>	893
<i>Thomas D. Tarman</i>		<i>Jian Ren</i>	
<b>VPN Basics</b>	596	<b>E-Mail and Internet Use Policies</b>	908
<i>G. I. Papadimitriou, M. S. Obaidat, C. Papazoglou, and A. S. Pomportsis</i>		<i>Nancy J. King</i>	
<b>VPN Architecture</b>	612	<b>Forward Security Adaptive Cryptography: Time Evolution</b>	927
<i>Stan Kurkovsky</i>		<i>Gene Itkis</i>	
<b>IP-Based VPN</b>	624	<b>Security Policy Guidelines</b>	945
<i>David E. McDysan</i>		<i>Mohamed Hamdi, Noureddine Boudriga, and M. S. Obaidat</i>	
<b>Identity Management</b>	636	<b>Asset-Security Goals Continuum: A Process for Security</b>	960
<i>John Linn</i>		<i>Margarita Maria Lenk</i>	
<b>The Use of Deception Techniques: Honeypots and Decoys</b>	646	<b>Multilevel Security</b>	972
<i>Fred Cohen</i>		<i>Richard E. Smith</i>	
<b>Active Response to Computer Intrusions</b>	664		
<i>David Dittrich and Kenneth Einar Himma</i>			

<b>Multilevel Security Models</b> <i>Mark Stamp and Ali Hushyar</i>	<b>987</b>	<b>Security Policy Enforcement</b> <i>Cynthia E. Irvine</i>	<b>1026</b>
<b>Security Architectures</b> <i>Nicole Graf and Dominic Kneeshaw</i>	<b>998</b>	<b>Guidelines for a Comprehensive Security System</b> <i>Hossein Bidgoli</i>	<b>1041</b>
<b>Quality of Security Service: Adaptive Security</b> <i>Timothy E. Levin, Cynthia E. Irvine, and Evdoxia Spyropoulou</i>	<b>1016</b>		