

Information Security Management

HANDBOOK

4th EDITION



Harold F. Tipton
Micki Krause

EDITORS

Suranaree University of Technology



31051000600540



AUERBACH

Contents

Introduction	xi
<i>Micki Krause and Harold F. Tipton</i>	
 DOMAIN 1 ACCESS CONTROL SYSTEMS AND METHODOLOGY	 1
Domain 1.1 Access Control Issues	3
1 Biometric Identification	5
<i>Donald R. Richards</i>	
2 Single Sign-On for the Enterprise	27
<i>John R. Vacca</i>	
 DOMAIN 2 TELECOMMUNICATIONS AND NETWORK SECURITY	 45
Domain 2.1 Network Security	47
3 Secured Connections to External Networks	49
<i>Steven F. Blanding</i>	
Domain 2.2 Internet, Intranet, and Extranet Security	71
4 Firewalls: An Effective Solution for Internet Security	73
<i>E. Eugene Schultz</i>	
5 Internet Security: Securing the Perimeter	83
<i>Douglas G. Conarich</i>	
6 Extranet Access Control Issues	99
<i>Christopher King</i>	
7 Firewall Management and Internet Attacks	115
<i>Lt. Jeffery J. Lowder</i>	
8 Network Layer Security	133
<i>Steven F. Blanding</i>	
9 Transport Layer Security	145
<i>Steven F. Blanding</i>	

10	Application-Layer Security Protocols for Networks	161
	<i>Bill Stackpole</i>	
11	Security of Communication Protocols and Services	179
	<i>William Hugh Murray</i>	
DOMAIN 3	SECURITY MANAGEMENT PRACTICES	193
Domain 3.1	Security Awareness	195
12	Security Awareness Program	197
	<i>Tom Peltier</i>	
Domain 3.2	Organization Architecture	213
13	Enterprise Security Architecture	215
	<i>William Hugh Murray</i>	
14	An Introduction to IPSEC	231
	<i>Bill Stackpole</i>	
Domain 3.3	Risk Management	245
15	Risk Analysis and Assessment	247
	<i>Will Ozier</i>	
16	Protecting High-Tech Trade Secrets	287
	<i>William C. Boni</i>	
17	Information Security Management in the Healthcare Industry	303
	<i>Micki Krause</i>	
DOMAIN 4	APPLICATION AND SYSTEMS DEVELOPMENT SECURITY	321
Domain 4.1	Application Security	323
18	Security Models for Object-Oriented Databases	325
	<i>James Cannady</i>	
DOMAIN 5	CRYPTOGRAPHY	335
Domain 5.1	Crypto Technology and Implementations	337
19	Fundamentals of Cryptography and Encryption	339
	<i>Ronald A. Gove</i>	

20	Principles and Applications of Cryptographic Key Management	367
	<i>William Hugh Murray</i>	
21	Implementing Kerberos in Distributed Systems	389
	<i>Joe Kovara and Ray Kaplan</i>	
22	Getting Started with PKI	475
	<i>Harry DeMaio</i>	
DOMAIN 6	SECURITY ARCHITECTURE AND MODELS.	491
Domain 6.1	Microcomputer and LAN Security	493
23	Microcomputer and LAN Security	495
	<i>Stephen Cobb</i>	
DOMAIN 7	COMPUTER OPERATIONS SECURITY	539
Domain 7.1	Threats	541
24	How to Trap the Network Intruder	543
	<i>Jeff Flynn</i>	
25	A Look at Java Security	551
	<i>Ben Rothke</i>	
DOMAIN 8	BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING.	559
Domain 8.1	Business Continuity Planning.	561
26	Reengineering the Business Continuity Planning Process	563
	<i>Carl B. Jackson</i>	
Domain 8.2	Disaster Recovery Planning	581
27	Restoration Component of Business Continuity Planning.	583
	<i>John Dorf and Marty Johnson</i>	
DOMAIN 9	LAW, INVESTIGATION, AND ETHICS	597
Domain 9.1	Investigation	599
28	Computer Crime Investigation and Computer Forensics	601
	<i>Thomas Welch</i>	

Domain 9.2	Information Ethics	645
29	Ethics and the Internet	647
	<i>Micki Krause</i>	
Domain 9.3	Information Law	663
30	Jurisdictional Issues in Global Transmissions	665
	<i>Ralph Spencer Poore</i>	
DOMAIN 10	PHYSICAL SECURITY	677
Domain 10.1	Threats and Facility Requirements	679
31	Intrusion Detection: How to Utilize a Still Immature Technology	681
	<i>E. Eugene Schultz and Eugene Spafford</i>	
INDEX		697