

Information Security Management Handbook

Sixth Edition

Volume 3

Edited by

Harold F. Tipton, CISSP · Micki Krause, CISSP



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Contents

Preface.....ix
Contributors.....xi

DOMAIN 1 ACCESS CONTROL

1 Expanding PKI-Based Access Control Capabilities with Attribute
Certificates3
ALEX GOLOD

2 Five Components to Identity Management Systems..... 19
KEVIN CASTELLOW

3 Security Weaknesses of System and Application Interfaces Used
to Process Sensitive Information33
SEAN M. PRICE

DOMAIN 2 TELECOMMUNICATIONS AND NETWORK SECURITY

4 Mobile Data Security43
GEORGE G. MCBRIDE

5 Enhanced Security Through Open Standards: A Path to a
Stronger Global Digital Ecosystem57
DAVID O'BERRY

6 Web Application Firewalls73
GEORGES J. JAHCHAN

7 Botnets77
ROBERT M. SLADE

DOMAIN 3 INFORMATION SECURITY AND RISK MANAGEMENT

- 8 Collaborating Information Security and Privacy to Create Effective Awareness and Training89
REBECCA HEROLD
- 9 Security Information and Event Management (SIEM) Technology 111
E. EUGENE SCHULTZ
- 10 The Insider Threat: A View from the Outside.....127
TODD FITZGERALD
- 11 Pod Slurping.....137
BEN ROTHKE
- 12 The USB (Universal Security Burden) Nightmare: Pod Slurping and Other High Storage Capacity Portable Device Vulnerabilities 145
KENNETH F. BELVA
- 13 Diary of a Security Assessment: “Put That in Your Pipe and Smoke It!” 149
KEN M. SHAURETTE
- 14 NERC Compliance: A Compliance Review 163
BONNIE GOINS PILEWSKI AND CHRISTOPHER A. PILEWSKI

DOMAIN 4 APPLICATION SECURITY

- 15 Mashup Security.....189
MANO PAUL
- 16 Format String Vulnerabilities.....199
MANO PAUL
- 17 Fast Scanning Worms.....207
PAUL A. HENRY

DOMAIN 5 CRYPTOGRAPHY

- 18 Message Digests.....217
RALPH SPENCER POORE

19 Quantum Computing: The Rise of the Machine.....227
 ROBBY FUSSELL

DOMAIN 6 SECURITY ARCHITECTURE AND DESIGN

20 Information Flow and Covert Channels.....239
 SEAN M. PRICE

**21 Securing Data at Rest: From Smart Phones to Tapes Defining
 Data at Rest281**
 SAMUEL CHUN AND LEOPOLD KAHNG

DOMAIN 7 OPERATIONS SECURITY

22 Validating Tape Backups.....303
 SANDY BACIK

**DOMAIN 8 BUSINESS CONTINUITY PLANNING AND
 DISASTER RECOVERY PLANNING**

**23 Determining Business Unit Priorities in Business Continuity
 Management.....313**
 KEVIN HENRY

**24 Continuity Program Testing, Maintenance, Training, and
 Awareness323**
 CARL JACKSON

**DOMAIN 9 LEGAL, REGULATIONS, COMPLIANCE, AND
 INVESTIGATION**

25 Bluesnarfing337
 MANO PAUL

26 Virtualization and Digital Investigations347
 MARCUS K. ROGERS AND SEAN C. LESHNEY

DOMAIN 10 PHYSICAL SECURITY

27 Halon Fire Suppression Systems.....367
 CHRIS HARE

28	Crime Prevention through Environmental Design	377
	MOLLIE E. KREHNKE	
29	Data Center Site Selection and Facility Design Considerations.....	393
	SANDY BACIK	
Index	401