



Osborne

*Includes a Security Dictionary and
contributions from topical experts!*

The Complete Reference

Network Security

Examine and implement
security strategies
and discover
proven techniques

Secure Windows®, Linux/
UNIX, Novell and Wireless
Security networks with
logical, concise information

Understand legal
issues and HIPPA
legislation

Roberta Bragg

CISSP, MCSF, Security Security+

Mark Rhodes-Osley

CISSP

Keith Strassberg

CPA, CISSP

MORE THAN 20 CO-AUTHORS AND TECHNICAL REVIEWERS

Contents

Acknowledgments	xxxiii
Introduction	xxxv

Part I Network Security Foundations

1 Network Security Overview	3
Benefits of Good Security Practices	4
Business Agility	4
Return on Investment	6
Security Methodology	9
The Three <i>Ds</i> of Security	10
Five Steps to Better Security	12
Strategy and Tactics	15
The Evolution of Security	17
The Weakest Link	22
There Is No Silver Bullet	23
Business Processes vs. Technical Controls	24
Security Hierarchy	26
Summary	29
References	29
2 Risk Analysis and Defense Models	31
Threat Definition and Risk Analysis	31
Threat Vectors	33
Defense Models	37
The Lollipop Model of Defense	38
The Onion Model of Defense	39
Zones of Trust	41
Segmentation	43
Summary	45
References	45

3 Security Policy Development	47
Developing a Security Policy	48
Security Policy Developers	48
Security Policy Audience	50
Security Policy Organization	50
Security Policy Topics	54
Sample Security Policy Topics	55
Sample Computer System Security Policy Topics	56
Sample Personnel Management Security Policy Topics	68
Sample Physical Security Policy Topics	74
Implementing a Security Policy	78
Summary	79
References	79
4 Security Organization	81
Roles and Responsibilities	81
Security Positions	82
Position Descriptions	82
Security Incident Response Team	87
Separation of Duties	89
Separation of Duties in IT	89
Separation of Duties in System Administration	90
Security Operations Management	91
Security Operations Responsibilities	91
Project Management	91
Security Council	94
Interaction with Human Resources	95
Security Lifecycle Management	96
The Security Process	96
The Security Lifecycle	97
Security Awareness	99
Importance of Security Awareness	99
Objectives of an Awareness Program	99
Increasing Effectiveness	101
Implementing the Program	101
Enforcement	103
Policy Enforcement for Vendors	104
Policy Enforcement for Employees	104
Software-Based Enforcement	104
Information Classification	105
Classification Categories	105
Roles	106
Documentation	106
Importance of Documentation	106
Presentation of Documents	107

Security Audit	107
Managed Security Services	110
Benefits of MSPs	111
Services Performed by MSPs	112
Security Monitoring Services	113
Summary	114
References	114

Part II Access Control

5 Physical Security	117
Classification of Assets	117
Physical Vulnerability Assessment	118
Buildings	118
Computing Devices and Peripherals	118
Documents	119
Records and Equipment	119
Choosing Site Location for Security	119
Accessibility	120
Lighting	120
Proximity to Other Buildings	120
Proximity to Law Enforcement and Emergency Response ..	120
RF and Wireless Transmission Interception	121
Construction and Excavation	121
Securing Assets: Locks, Entry Controls	122
Locks	122
Entry Controls	122
Physical Intrusion Detection	123
Closed-Circuit Television	123
Alarms	124
Mantraps	124
System Logs	124
Summary	124
References	124
6 Authentication and Authorization Controls	127
Authentication	127
Usernames and Password	129
Certificate-Based Authentication	139
Extensible Authentication Protocol (EAP)	144
Biometrics	145
Additional Uses for Authentication	146

Authorization	147
User Rights	148
Role-Based Authorization	148
Access Control Lists (ACLs)	149
Rule-Based Authorization	151
Summary	152
7 Data Security Architecture	153
Principles of Data Security Architecture	154
Confidentiality	154
Privacy	161
Integrity	162
Availability	165
Non-Repudiation	166
Applications of Data Security Architecture	169
Securing Data in Flight	169
Data Storage and File Encryption	171
Digital Rights Management	173
Confidential E-Mail	173
Summary	174
8 Security Management Architecture	175
Acceptable Use Enforcement	175
Examples of AUP Enforcement Wording	176
Developing AUP Enforcement Policy Text	177
Enforcement Processing	179
Administrative Security	180
Preventing Administrative Abuse of Power	180
Management Practices	181
Accountability Controls	181
Activity Monitoring and Audit	183
System and Device Logging	183
Log File Summarization and Reporting	186
System and Network Activity Monitoring	189
Vulnerability Scanning	189
NASA Improves Security	189
Summary	190

Part III Network Architecture

9 Network Design Considerations	193
Introduction to Secure Network Design	193
Acceptable Risk	193

Designing Security into a Network	194
Designing an Appropriate Network	195
The Cost of Security	195
Performance	196
Availability	197
Security	199
Wireless Impact on the Perimeter	201
Remote Access Considerations	203
Internal Security Practices	203
Intranets, Extranets, and DMZs	205
Host Hardening	208
Outbound Filtering	209
Summary	212
References	212
10 Network Device Security	213
Switch and Router Basics	213
Switches	214
Routers	216
Routing Protocols	217
Network Hardening	218
Patches	218
Switch Security Practices	218
Access Control Lists	218
Services Not in Use	219
Administrative Practices	221
Internet Control Message Protocol	224
Anti-Spoofing and Source Routing	226
Logging	227
Summary	227
11 Firewalls	229
Understanding Firewalls	229
Firewall Strengths and Weaknesses	230
Firewalls and TCP/IP	232
Packet-Filtering Firewalls	234
Application Gateways	236
Circuit-Level Gateways	238
Stateful Packet-Inspection (SPI) Firewalls	238
Appliance- vs. OS-Based Firewalls	240
Additional Firewall Functions	241
Network Address Translation (NAT)	241
Auditing and Logging	244
Virtual Private Networks	244

Summary	245
References	245
12 Virtual Private Network Security	247
How a VPN Works	248
VPN Protocols	248
IPSec Tunnel Mode Products	249
L2TP over IPSec	249
PPTP	250
SSL VPNs	250
Client/Server Remote Access Vulnerabilities and Threats	251
Remote Dial-In Server Security	251
Remote Client Security	251
Site-to-Site Networking Vulnerabilities and Threats	261
Summary	262
13 Wireless Network Security	263
Radio Frequency Security Basics	265
Layer 1 Security Solutions	266
Data-Link Layer Wireless Security Features, Flaws, and Threats ...	279
802.11 and 802.15 Data-Link Layer in a Nutshell	279
802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats	281
Closed-System ESSIDs, MAC Filtering, and Protocol Filtering	285
Built-in Bluetooth PAN Data-Link Security and Threats ...	285
Wireless Network Hardening Practices and Recommendations ...	287
Introducing the 802.11i Security Standard	287
Wireless Intrusion-Detection Fundamentals	291
Wireless Network Positioning and Secure Gateways	293
Summary	294
14 Intrusion-Detection Systems	295
IDS Concepts	295
Why Intrusion Detection	296
Threat Types	297
First-Generation IDSs	301
Second-Generation IDSs	302
Return on IDS Investment	303
IDS Types and Detection Models	305
Host-Based IDS	305
Network-Based IDS (NIDS)	308
Anomaly-Detection (AD) Model	311
Signature-Detection Model	313

Wireless IDSs	316
What Type of IDS Should You Use?	316
IDS Features	317
IDS End-User Interfaces	317
IDS Management	318
Intrusion-Prevention Systems (IPSs)	320
IDS Performance	323
IDS Logging and Alerting	324
IDS Reporting and Analysis	326
IDS Deployment Considerations	327
IDS Weaknesses	327
IDS Fine-Tuning	330
NIDS Deployment Plan	331
The Future of IDS	332
IDS Products	333
Online IDS Resources	334
Summary	334
15 Integrity and Availability Architecture	335
Version Control and Change Control	336
Documenting and Analyzing Change Control	336
The Change Control Policy	337
Usable Change Control Procedures	338
Patching	340
Determining What Should Be Patched	341
Where to Obtain Patch Notification	341
The Decision-Making Process	342
Audit Patch Application	342
Examples of Patching Processes and Procedures	343
Patch Management Products and Resources	345
Backups	347
Traditional Backup Methods	347
Backup Alternatives and Newer Methodologies	350
Backup Policy	352
System and Network Redundancy	353
Automated Redundancy Methods	355
Operational Procedures That Keep Systems Functional	357
Summary	358
16 Network Role-Based Security	359
E-Mail	360
Protocols and Security Issues	360
Mail Distribution	378
Spam and Spam Control	380

Viruses and Virus Control	385
Recommendations for Securing E-Mail Servers	390
Proxy Servers	391
Network Connectivity	391
Proxy Connectivity	394
Proxy Security Issues	397
DNS Servers	399
DNS Overview	399
DNS Security	402
Source Code Repository Access	404
Basic Security	404
Advanced Security	404
Web Servers	406
Overview of Web Server Security	406
Types of Attacks	407
Web Server Protection	410
IP Telephony and Streaming Media	413
Common Usage	413
Streaming Media Protocols	414
Key Features of VoIP/Streaming Media Protocols	414
Security Issues of VoIP/Streaming Media Protocols	415
Credit Card Security	416
Common Insecure Practices	416
Securing Credit Card Systems	417
Printers and Faxes	419
Printers	419
Fax Security	420
Special Systems	420
OS Security	420
Intercommunication Security	421
Level of Security Support	421
Auditing	421
SCADA	422
Overview	422
Typical SCADA Topology	422
SCADA Security	423
PBX	426
Hacking a PBX	426
Securing a PBX	427
Summary	428

Part IV Operating System Security

17 Operating System Security Models	431
Operating System Models	431
Access Control Lists	433
MAC vs. DAC	434
Classic Security Models	435
Bell-LaPadula	435
Biba	436
Clark-Wilson	436
TCSEC	436
Labels	439
Reference Monitor	439
Windows 2000/XP Security Reference Monitor	440
Windows NT Security Model and Monitor	442
Trustworthy Computing	442
International Standards for Operating System Security	444
Common Criteria	444
ISO 17799	447
COBIT	448
Summary	449
References	449
18 Common Unix Vulnerabilities	451
Start with a Fresh Install	452
Remove Unneeded Daemons	453
Look at Your Startup Scripts	453
Install OpenSSL	454
Replace Vulnerable Daemons with OpenSSH	454
Do Not Use root for Daemons	456
Change the Port	456
Special Cases	458
Use chroot to Isolate Processes	458
Use TCP Wrappers	459
Audit Your Applications	460
Audit Your cron Jobs	461
Scan for SUID and SGID Files	461
Keep . from Your PATH	462
Audit Your Scripts	462
Know What Ports Are Open	463
Using Netstat	463
Using lsof	464

Run CIS Scans	465
Keep Patches Up to Date	465
Use a Centralized Log Server	466
Configure All Your Daemons to Log	467
Consider Replacing Sendmail	467
Sendmail Replacements	467
Subscribe to Security Lists	470
Summary	470
19 Linux Security	471
Start with a Fresh Install	472
Install a File Scanning Application	472
Tripwire	472
Determine Your Server's Role	474
Watching Commonly Scanned Ports	475
IP Restricting	476
Installing TCP Wrappers	476
Configuring TCP Wrappers	477
Read Your Log Files	479
Create a Centralized Log Server	479
Install a Log Scanning Application	480
Stay on Top of Vulnerabilities	483
Keep Your System Updated	483
Subscribe to Security Lists	483
Summary	484
20 Windows Security	485
The Six Basics of Security Applied to Windows Systems	486
Segment the Network into Areas of Trust	
and Provide Specific Controls at Border Areas	486
Patch Systems	487
Strengthen Authentication Processes	488
Limit the Number of Administrators and Limit	
the Privileges of Administrators	492
Harden Systems Against Known Attacks via System	
Configurations	495
Develop and Enforce Security Policy	
via Accountability, Technology, and Training	498
Threat Analysis, Windows Systems Specifics	498
Mitigation Possibilities, Windows Style	499
Logical Security Boundaries	500
Role-Based Administration	508
Security Configuration and Analysis	510
Group Policy	512

Public Key Infrastructure	517
Securing Windows Communications	519
A Role-Based Approach to Security Configuration	521
Mitigation Application—Security Checklists	523
Summary	524
21 Novell Security	525
NetWare Overview	525
Security Considerations of IP and IPX	526
NetWare Core Protocol (NCP) Packet Signature	527
Novell Directory Services (NDS)	527
NDS Basics	527
NDS Tree	528
NDS vs. Bindery Security	530
NDS Security	531
File-System Security	531
NDS Object Security	536
Rules of NDS Object Security	538
Tips and Best Practices for Securing NetWare	542
Securing the Server	543
Securing the Workstation	545
NCP Packet Signature	545
Login Security and User Accounts	547
General Ideas for NDS Security	551
Be Careful What You Place in the SYS:LOGIN Directory	552
Summary	553
References	553

Part V Application Security

22 Principals of Application Security	557
Web Application Security	557
SQL Injection	558
Forms and Scripts	563
Cookies and Session Management	565
General Attacks	567
Web Application Security Conclusions	568
Regular Application Security	568
Running Privileges	569
Application Administration	570
Integration with OS Security	571
Application Updates	572
Spyware and Adware	574

Network Access	575
Regular Application Security Conclusions	575
Embedded Applications Security	576
Security of Embedded Applications	576
Embedded Applications Security Conclusions	577
Remote Administration Security	577
Reasons for Remote Administration	577
Remote Administration Using a Web Interface	577
Authenticating Web-Based Remote Administration	578
Custom Remote Administration	579
Summary	580
23 Writing Secure Software	581
The Golden Rule—Be Careful Whom You Trust	581
Buffer Overruns	582
Integer Overflow Attacks	585
Cross-Site Scripting Issues	588
SQL Injection Attacks	594
The Golden Secure Rule	597
Summary	598
24 J2EE Security	599
Java and J2EE Overview	599
The Java Language	599
Attacks on the JVM	601
The J2EE Architecture	602
Servlets	602
JavaServer Pages (JSP)	604
Enterprise JavaBeans (EJB)	605
Containers	607
Authentication and Authorization	608
J2EE Authentication	608
J2EE Authorization	610
Protocols	611
HTTP	611
HTTPS	613
Web Services Protocols	615
IIOP	616
JRMP	618
Proprietary Communication Protocols	619
JMS	619
JDBC	619
Summary	620

25	Windows .NET Security	623
	Core Security Features of .NET	624
	Managed Code	624
	Role-Based Security	628
	Code Access Security	631
	AppDomains and Isolated Storage	641
	Application-Level Security in .NET	644
	Using Cryptography	644
	.NET Remoting Security	652
	Securing Web Services and Web Applications	653
	Summary	656
26	Database Security	657
	General Database Security Concepts	657
	Understanding Database Server Security Layers	659
	Server-Level Security	659
	Network-Level Security	659
	Operating System Security	661
	Understanding Database-Level Security	662
	Database Administration Security	663
	Database Roles and Permissions	664
	Object-Level Security	665
	Using Other Database Objects for Security	667
	Using Application Security	669
	Limitations of Application-Level Security	670
	Supporting Internet Applications	671
	Database Backup and Recovery	673
	Determining Backup Constraints	674
	Determining Recovery Requirements	674
	Types of Database Backups	675
	Keeping Your Servers Up-to-Date	676
	Database Auditing and Monitoring	676
	Reviewing Audit Logs	677
	Database Server Monitoring	678
	Summary	680

Part VI Response

27	Disaster Recovery and Business Continuity	683
	Disaster Recovery	683
	Business Continuity	684
	The Four Components of Business Continuity	685

Third-Party Vendor Issues	694
Awareness and Training Programs	694
Summary	700
28 Attacks and Countermeasures	703
Attacks	703
Malicious Mobile Code	704
Manual Cracking	715
Countermeasures	721
Secure the Physical Environment	721
Keep Patches Updated	722
Use an Antivirus Scanner	724
Use a Firewall	725
Secure User Accounts	726
Secure the File System	727
Secure Applications	731
Back Up the System	736
Automate Security	736
Create a Computer Security Defense Plan	737
Summary	738
References	738
29 Incident Response and Forensic Analysis	739
Incident Response Plans	739
Incident Detection	740
Incident Response and Containment	742
Recovery and Resumption	744
Review and Improvement	745
Forensics	746
Legal Requirements	746
Evidence Acquisition	747
Evidence Analysis	751
Summary	760
References	760
30 Legal Issues: The Laws Affecting Information	761
Security Professionals	761
Network Regulations: Defining Computer Crimes	761
Intrusions and Network Attacks: The Computer Fraud and Abuse Act	762
Unauthorized Access to Electronic Communications: The Electronic Communications Privacy Act	768
Other Cyber Crimes	771

Information Security Regulation: The Emerging Duty of Care	772
Gramm-Leach-Bliley Safeguards	773
Sarbanes-Oxley Act	775
HIPAA Privacy and Security Rules	776
California Section 1798.82	778
Voluntary Standards	779
The Future of Duty of Care: Enforcement Actions and Civil Lawsuits?	780
Compliance with Laws in Conducting an Incident Response	
Overview	782
Law Enforcement Referrals—Yes or No?	782
Preservation of Evidence	783
Protecting the Confidentiality of the Response: Privilege Issues	785
Summary	787
Glossary	789
Index	815