

SYNGRESS

NETWORK AND SYSTEM SECURITY

John R. Vacca



Contents

Foreword	XV
Acknowledgments	XVII
About the Editor	XIX
List of Contributors	XXI
Introduction	XXIII
Chapter 1: Building a Secure Organization.....	1
1. Obstacles to Security.....	1
Security Is Inconvenient.....	2
Computers Are Powerful and Complex	2
Computer Users Are Unsophisticated.....	2
Computers Created Without a Thought to Security	3
Current Trend Is to Share, Not Protect	3
Data Accessible from Anywhere	4
Security Isn't About Hardware and Software	4
The Bad Guys Are Very Sophisticated	5
Management Sees Security as a Drain on the Bottom Line	5
2. Ten Steps to Building a Secure Organization.....	6
A. Evaluate the Risks and Threats	7
B. Beware of Common Misconceptions.....	9
C. Provide Security Training for IT Staff—Now and Forever	11
D. Think “Outside the Box”	13
E. Train Employees: Develop a Culture of Security.....	17
F. Identify and Utilize Built-In Security Features of the Operating System and Applications	18
G. Monitor Systems.....	22
H. Hire a Third Party to Audit Security.....	25
I. Don't Forget the Basics	26
J. Patch, Patch, Patch	28

Chapter 2: A Cryptography Primer.....	33
1. What Is Cryptography? What Is Encryption?	34
How Is Cryptography Done?	34
2. Famous Cryptographic Devices	35
The Lorenz Cipher	35
Enigma	36
3. Ciphers	37
The Substitution Cipher	37
The Shift Cipher	38
The Polyalphabetic Cipher.....	44
The Kasiski/Kerckhoff Method.....	46
4. Modern Cryptography	47
The Vernam Cipher (Stream Cipher)	47
The One-Time Pad	48
Cracking Ciphers	49
Some Statistical Tests for Cryptographic Applications by Adrian Fleissig.....	50
The XOR Cipher and Logical Operands.....	51
Block Ciphers	53
5. The Computer Age	54
Data Encryption Standard	55
Theory of Operation.....	55
Implementation	56
Rivest, Shamir, and Adleman (RSA)	57
Advanced Encryption Standard (AES or Rijndael)	57
Chapter 3: Preventing System Intrusions	59
1. So, What Is an Intrusion?	60
2. Sobering Numbers	60
3. Know Your Enemy: Hackers versus Crackers	61
4. Motives	63
5. Tools of the Trade.....	63
6. Bots	64
7. Symptoms of Intrusions	65
8. What Can You Do?.....	66
Know Today's Network Needs.....	68
Network Security Best Practices.....	69
9. Security Policies	70
10. Risk Analysis	72
Vulnerability Testing.....	72
Audits.....	72
Recovery	73
11. Tools of Your Trade.....	73
Firewalls.....	74
Intrusion Prevention Systems.....	74

Application Firewalls	75
Access Control Systems	76
Unified Threat Management	76
12. Controlling User Access	77
Authentication, Authorization, and Accounting	77
What the User Knows	77
What the User Has	78
The User Is Authenticated, But Is She Authorized?	79
Accounting	79
Keeping Current	80
13. Conclusion	80
Chapter 4: Guarding Against Network Intrusions	83
1. Traditional Reconnaissance and Attacks	83
2. Malicious Software	88
Lures and “Pull” Attacks	91
3. Defense in Depth	92
4. Preventive Measures	93
Access Control	93
Vulnerability Testing and Patching	94
Closing Ports	95
Firewalls	95
Antivirus and Antispyware Tools	96
Spam Filtering	98
Honeypots	99
Network Access Control	100
5. Intrusion Monitoring and Detection	101
Host-Based Monitoring	102
Traffic Monitoring	102
Signature-Based Detection	103
Behavior Anomalies	103
Intrusion Prevention Systems	104
6. Reactive Measures	104
Quarantine	104
Traceback	105
7. Conclusions	106
Chapter 5: Unix and Linux Security	109
1. Unix and Security	109
The Aims of System Security	109
Achieving Unix Security	110
2. Basic Unix Security	111
Traditional Unix Systems	111
Standard File and Device Access Semantics	113

4. Protecting User Accounts and Strengthening Authentication.....	115
Establishing Secure Account Use	116
The Unix Login Process	116
Controlling Account Access	117
Noninteractive Access	118
Other Network Authentication Mechanisms	119
Risks of Trusted Hosts and Networks	120
Replacing Telnet, rlogin, and FTP Servers and Clients with SSH	120
5. Reducing Exposure to Threats by Limiting Superuser Privileges	121
Controlling Root Access	121
6. Safeguarding Vital Data by Securing Local and Network File Systems.....	123
Directory Structure and Partitioning for Security	124
Chapter 6: Eliminating the Security Weakness of Linux and UNIX Operating Systems.....	127
1. Introduction to Linux and Unix	127
What Is Unix?	127
What Is Linux?	129
System Architecture	131
2. Hardening Linux and Unix	134
Network Hardening	134
Host Hardening	141
Systems Management Security	144
3. Proactive Defense for Linux and Unix.....	145
Vulnerability Assessment.....	145
Incident Response Preparation.....	146
Organizational Considerations	147
Chapter 7: Internet Security.....	149
1. Internet Protocol Architecture.....	149
Communications Architecture Basics	150
Getting More Specific	152
2. An Internet Threat Model	161
The Dolev–Yao Adversary Model.....	162
Layer Threats.....	163
3. Defending Against Attacks on the Internet.....	171
Layer Session Defenses.....	171
Session Startup Defenses	184
4. Conclusion	191
Chapter 8: The Botnet Problem.....	193
1. Introduction.....	193
2. Botnet Overview.....	194
Origins of Botnets	195
Botnet Topologies and Protocols.....	195

3. Typical Bot Life Cycle	198
4. The Botnet Business Model	200
5. Botnet Defense	201
Detecting and Removing Individual Bots	201
Detecting C&C Traffic.....	202
Detecting and Neutralizing the C&C Servers	203
Attacking Encrypted C&C Channels.....	204
Locating and Identifying the Botmaster.....	205
6. Botmaster Traceback	207
Traceback Challenges.....	208
Traceback Beyond the Internet.....	210
7. Summary.....	213
Chapter 9: Intranet Security	217
1. Plugging the Gaps: Network Access Control and Access Control	222
2. Measuring Risk: Audits.....	223
3. Guardian at the Gate: Authentication and Encryption.....	225
4. Wireless Network Security	226
5. Shielding the Wire: Network Protection	228
6. Weakest Link in Security: User Training	231
7. Documenting the Network: Change Management	231
8. Rehearse the Inevitable: Disaster Recovery	233
9. Controlling Hazards: Physical and Environmental Protection	236
10. Know Your Users: Personnel Security	238
11. Protecting Data Flow: Information and System Integrity.....	239
12. Security Assessments	240
13. Risk Assessments	241
14. Conclusion	242
Chapter 10: Local Area Network Security.....	245
1. Identify Network Threats	246
Disruptive.....	246
Unauthorized Access	247
2. Establish Network Access Controls.....	247
3. Risk Assessment.....	248
4. Listing Network Resources	248
5. Threats	249
6. Security Policies	249
7. The Incident-Handling Process	250
8. Secure Design through Network Access Controls	251
9. Intrusion Detection System Defined.....	252
10. Network-Based IDS: Scope and Limitations	253
11. A Practical Illustration of NIDS	254
UDP Attacks	254
TCP SYN (Half-Open) Scanning.....	254
Some Not-So-Robust Features of NIDS.....	259

12. Firewalls.....	259
Firewall Security Policy.....	260
Configuration Script for sf Router.....	262
13. Dynamic NAT Configuration	262
14. The Perimeter	263
15. Access List Details.....	264
16. Types of Firewalls.....	265
17. Packet Filtering: IP Filtering Routers.....	266
18. Application-Layer Firewalls: Proxy Servers	266
19. Stateful Inspection Firewalls.....	266
20. Network-Based IDS Complements Firewalls.....	266
21. Monitor and Analyze System Activities.....	267
Analysis Levels	268
22. Signature Analysis.....	268
23. Statistical Analysis	269
24. Signature Algorithms.....	269
Pattern Matching	269
Stateful Pattern Matching.....	270
Protocol Decode-Based Analysis.....	271
Heuristic-Based Analysis	272
Anomaly-Based Analysis	272
Chapter 11: Wireless Network Security	275
1. Cellular Networks.....	276
Cellular Telephone Networks	277
802.11 Wireless LANs	278
2. Wireless Ad Hoc Networks	279
Wireless Sensor Networks	279
Mesh Networks.....	280
3. Security Protocols.....	280
Wired Equivalent Privacy	281
WPA and WPA2	282
SPINS: Security Protocols for Sensor Networks	283
4. Secure Routing	286
SEAD	286
Ariadne.....	288
ARAN	288
SLSP	289
5. Key Establishment.....	290
Bootstrapping.....	290
Key Management.....	292
Chapter 12: Cellular Network Security	299
1. Introduction.....	299
2. Overview of Cellular Networks.....	300

Overall Cellular Network Architecture	301
Core Network Organization	302
Call Delivery Service	304
3. The State of the Art of Cellular Network Security	305
Security in the Radio Access Network.....	305
Security in Core Network	306
Security Implications of Internet Connectivity	308
Security Implications of PSTN Connectivity	309
4. Cellular Network Attack Taxonomy	309
Abstract Model	310
Abstract Model Findings.....	310
Three-Dimensional Attack Taxonomy.....	315
5. Cellular Network Vulnerability Analysis	317
Cellular Network Vulnerability Assessment Toolkit	319
Advanced Cellular Network Vulnerability Assessment Toolkit.....	323
Cellular Network Vulnerability Assessment Toolkit for Evaluation	326
6. Discussion	329
Chapter 13: Radio Frequency Identification Security.....	333
1. Radio Frequency Identification Introduction.....	333
RFID System Architecture.....	333
RFID Standards	336
RFID Applications.....	338
2. RFID Challenges	339
Counterfeiting	340
Sniffing	340
Tracking	340
Denial of Service.....	341
Other Issues	342
Comparison of All Challenges.....	345
3. RFID Protections.....	346
Basic RFID System	347
RFID System Using Symmetric-Key Cryptography	349
RFID System Using Public-Key Cryptography	353
Index.....	361