

Contents

Preface to the Second Edition	xiii
Preface to the First Edition	xvii
I Getting Started	1
1 Introduction	3
1.1 Security Truisms	3
1.2 Picking a Security Policy	7
1.3 Host-Based Security	10
1.4 Perimeter Security	10
1.5 Strategies for a Secure Network	11
1.6 The Ethics of Computer Security	16
1.7 WARNING	18
2 A Security Review of Protocols: Lower Layers	19
2.1 Basic Protocols	19
2.2 Managing Addresses and Names	28
2.3 IP version 6	34
2.4 Network Address Translators	37
2.5 Wireless Security	38
3 Security Review: The Upper Layers	41
3.1 Messaging	41
3.2 Internet Telephony	46
3.3 RPC-Based Protocols	47
3.4 File Transfer Protocols	52
3.5 Remote Login	58
3.6 Simple Network Management Protocol—SNMP	62
3.7 The Network Time Protocol	63
3.8 Information Services	64




3.9	Proprietary Protocols	68
3.10	Peer-to-Peer Networking	69
3.11	The X11 Window System	70
3.12	The Small Services	71
4	The Web: Threat or Menace?	73
4.1	The Web Protocols	74
4.2	Risks to the Clients	79
4.3	Risks to the Server	85
4.4	Web Servers vs. Firewalls	89
4.5	The Web and Databases	91
4.6	Parting Thoughts	91
II	The Threats	93
5	Classes of Attacks	95
5.1	Stealing Passwords	95
5.2	Social Engineering	98
5.3	Bugs and Back Doors	100
5.4	Authentication Failures	103
5.5	Protocol Failures	104
5.6	Information Leakage	105
5.7	Exponential Attacks—Viruses and Worms	106
5.8	Denial-of-Service Attacks	107
5.9	Botnets	117
5.10	Active Attacks	117
6	The Hacker's Workbench, and Other Munitions	119
6.1	Introduction	119
6.2	Hacking Goals	121
6.3	Scanning a Network	121
6.4	Breaking into the Host	122
6.5	The Battle for the Host	123
6.6	Covering Tracks	126
6.7	Metastasis	127
6.8	Hacking Tools	128
6.9	Tiger Teams	132
III	Safer Tools and Services	135
7	Authentication	137
7.1	Remembering Passwords	138

7.2	Time-Based One-Time Passwords	144
7.3	Challenge/Response One-Time Passwords	145
7.4	Lamport's One-Time Password Algorithm	146
7.5	Smart Cards	147
7.6	Biometrics	147
7.7	RADIUS	148
7.8	SASL: An Authentication Framework	149
7.9	Host-to-Host Authentication	149
7.10	PKI	150
8	Using Some Tools and Services	153
8.1	<i>Inetd</i> —Network Services	153
8.2	<i>Ssh</i> —Terminal and File Access	154
8.3	<i>Syslog</i>	158
8.4	Network Administration Tools	159
8.5	Chroot—Caging Suspect Software	162
8.6	Jailing the Apache Web Server	165
8.7	<i>Aftpd</i> —A Simple Anonymous FTP Daemon	167
8.8	Mail Transfer Agents	168
8.9	POP3 and IMAP	168
8.10	Samba: An SMB Implementation	169
8.11	Taming <i>Named</i>	170
8.12	Adding SSL Support with <i>Sslwrap</i>	170
IV	Firewalls and VPNs	173
9	Kinds of Firewalls	175
9.1	Packet Filters	176
9.2	Application-Level Filtering	185
9.3	Circuit-Level Gateways	186
9.4	Dynamic Packet Filters	188
9.5	Distributed Firewalls	193
9.6	What Firewalls Cannot Do	194
10	Filtering Services	197
10.1	Reasonable Services to Filter	198
10.2	Digging for Worms	206
10.3	Services We Don't Like	207
10.4	Other Services	209
10.5	Something New	210

11 Firewall Engineering	211
11.1 Rulesets	212
11.2 Proxies	214
11.3 Building a Firewall from Scratch	215
11.4 Firewall Problems	227
11.5 Testing Firewalls	230
12 Tunneling and VPNs	233
12.1 Tunnels	234
12.2 Virtual Private Networks (VPNs)	236
12.3 Software vs. Hardware	242
V Protecting an Organization	245
13 Network Layout	247
13.1 Intranet Explorations	248
13.2 Intranet Routing Tricks	249
13.3 In Host We Trust	253
13.4 Belt and Suspenders	255
13.5 Placement Classes	257
14 Safe Hosts in a Hostile Environment	259
14.1 What Do We Mean by “Secure”?	259
14.2 Properties of Secure Hosts	260
14.3 Hardware Configuration	265
14.4 Field-Stripping a Host	266
14.5 Loading New Software	270
14.6 Administering a Secure Host	271
14.7 Skinny-Dipping: Life Without a Firewall	277
15 Intrusion Detection	279
15.1 Where to Monitor	280
15.2 Types of IDSs	281
15.3 Administering an IDS	282
15.4 IDS Tools	282
VI Lessons Learned	285
16 An Evening with Berferd	287
16.1 Unfriendly Acts	287
16.2 An Evening with Berferd	290
16.3 The Day After	294

16.4	The Jail	295
16.5	Tracing Berferd	296
16.6	Berferd Comes Home	298
17	The Taking of Clark	301
17.1	Prelude	301
17.2	CLARK	302
17.3	Crude Forensics	303
17.4	Examining CLARK	303
17.5	The Password File	310
17.6	How Did They Get In?	310
17.7	Better Forensics	311
17.8	Lessons Learned	312
18	Secure Communications over Insecure Networks	313
18.1	The Kerberos Authentication System	314
18.2	Link-Level Encryption	318
18.3	Network-Level Encryption	318
18.4	Application-Level Encryption	322
19	Where Do We Go from Here?	329
19.1	IPv6	329
19.2	DNSsec	330
19.3	Microsoft and Security	330
19.4	Internet Ubiquity	331
19.5	Internet Security	331
19.6	Conclusion	332
VII	Appendixes	333
A	An Introduction to Cryptography	335
A.1	Notation	335
A.2	Secret-Key Cryptography	337
A.3	Modes of Operation	339
A.4	Public Key Cryptography	342
A.5	Exponential Key Exchange	343
A.6	Digital Signatures	344
A.7	Secure Hash Functions	346
A.8	Timestamps	347

B Keeping Up	349
B.1 Mailing Lists	350
B.2 Web Resources	351
B.3 Peoples' Pages	352
B.4 Vendor Security Sites	352
B.5 Conferences	353
Bibliography	355
List of  s	389
List of Acronyms	391
Index	397