

# Contents

Introduction	xxvi
Chapter 1: Understanding the Threats: E-mail Viruses, Trojans, Mail Bombers, Worms, and Illicit Servers	1
Introduction	2
Essential Concepts	3
Servers, Services, and Clients	3
Authentication and Access Control	3
Hackers and Attack Types	4
What Do Hackers Do?	4
Attack Types	5
Overview of E-mail Clients and Servers	7
Understanding a Mail User Agent and a Mail Transfer Agent	7
The Mail Delivery Agent	9
When Are Security Problems Introduced?	10
History of E-mail Attacks	10
The MTA and the Robert Morris Internet Worm	11
MDA Attacks	12
Analyzing Famous Attacks	12
Case Study	14
Learning from Past Attacks	14
Viruses	15
Worms	15
Types of Worms	16
Trojans	17
Illicit Servers	17
Differentiating between Trojans and Illicit Servers	18

E-mail Bombing	19
Sniffing Attacks	19
Carnivore	20
Spamming and Security	21
Common Authoring Languages	22
Protecting Your E-mail	23
Protecting E-mail Clients	23
Third-party Applications	23
Encryption	24
Hash Encryption and Document Signing	27
Protecting the Server	27
Summary	28
FAQs	29
Chapter 2: Securing Outlook 2000	31
Introduction	32
Common Targets, Exploits, and Weaknesses	33
The Address Book	35
The Mail Folders	36
Visual Basic Files	37
Attacks Specific to This Client	38
No Attachment Security	38
Default Settings Are Not Secure	38
Zone Security	39
Word 2000 as the Outlook E-mail Editor	39
Security Updates	39
Enabling Filtering	42
Junk E-mail	42
Filtering Keywords	44
Mail Settings and Options	44
HTML Messages	45
Zone Settings	46
Attachment Security	48
Attachment Security After Applying Outlook	
E-mail Security Update	51
Enabling S/MIME	54
Why You Should Use Public Key Encryption	56
Installing and Enabling Pretty Good Privacy (PGP)	57
Installing PGP	58

Understanding Public Key Encryption	62
Generating a Key Pair	65
Exchanging Keys	67
Key Distribution Sites	69
Summary	70
FAQs	71
 Chapter 3: Securing Outlook Express 5.0 and Eudora 4.3	 75
Introduction	76
Outlook Express for Windows	76
Security Settings	77
Secure Mail	78
Security Zones	80
Attachments	82
Outlook Express for Macintosh	85
Junk Mail Filter	85
Message Rules	88
Attachments	89
Case Study: Automated Virus Scanning of Mail Attachments	 90
Eudora for Windows and Macintosh	91
Security	91
Attachments	91
Filtering	93
Enabling PGP for both Outlook Express and Eudora	95
Sending and Receiving PGP-Secured Messages	96
Eudora for Windows	97
Outlook Express for Windows	101
Eudora for Macintosh	103
Outlook Express for Macintosh	105
Automatic Processing of Messages	107
File Attachments and PGP	108
Case Study: Securing File Attachments with PGP	109
Summary	113
FAQs	115
 Chapter 4: Web-based Mail Issues	 119
Introduction	120

Choices in Web-based E-mail Services	121
Why Is Web-based E-mail So Popular?	122
The Cost of Convenience	122
Specific Weaknesses	124
Internet Architecture and the Transmission Path	124
Reading Passwords	126
Case Study	128
Specific Sniffer Applications	131
Code-based Attacks	133
The PHF Bug	134
Hostile Code	135
Taking Advantage of System Trusts	135
Cracking the Account with a “Brute Force” or Dictionary	
Application	136
Physical Attacks	137
Cookies and Their Associated Risks	138
Solving the Problem	139
Using Secure Sockets Layer (SSL)	139
Secure HTTP	139
Practical Implementations	140
Local E-mail Servers	141
Using PGP with Web-based E-mail	141
Making Yourself Anonymous	142
Summary	143
FAQs	144
 Chapter 5: Client-Side Anti-Virus Applications	 147
Introduction	148
McAfee VirusScan 5	150
Availability of VirusScan	151
Updates of Virus Definition Files	152
Installation of VirusScan 5	152
Configuration of VirusScan 5	156
Norton AntiVirus 2000	163
Availability of Norton AntiVirus 2000	163
Updates of Norton AntiVirus 2000	
Definition Files	164
Installation of Norton AntiVirus 2000	165
Configuration of Norton AntiVirus 2000	167
Trend Micro PC-cillin 2000	176

Availability of Trend Micro PC-cillin 2000	176
Updates of PC-cillin Virus Definition Files	177
Installation of Trend Micro PC-cillin 2000	178
Configuration of Trend Micro PC-cillin 2000	181
Trend PC-cillin 2000 Configuration Settings	185
Trend Micro PC-cillin 2000 Links	188
Summary	189
FAQs	190
 Chapter 6: Mobile Code Protection	 195
Introduction	196
Dynamic E-mail	196
Active Content	197
Taking Advantage of Dynamic E-mail	197
Composing an HTML E-mail	198
Inserting Your Own HTML File	198
Sending an Entire Web Page	200
Dangers	200
No Hiding Behind the Firewall	201
Mobile Code	201
Java	202
Security Model	203
Playing in the Sandbox	203
Playing Outside the Sandbox	205
Points of Weakness	205
Background Threads	206
Hogging System Resources	206
I Swear I Didn't Send That E-mail	207
Scanning for Files	207
How Hackers Take Advantage	207
Spam Verification	207
Theft of Processing Power	208
Unscrupulous Market Research	208
Applets Are Not That Scary	208
Precautions You Can Take	208
JavaScript	211
Security Model	211
Points of Weakness	212
How Hackers Take Advantage	213
Web-Based E-mail Attacks	213

Are Plug-in Commands a Threat?	213
Social Engineering	213
Precautions to Take	214
ActiveX	215
Security Model	215
Safe for Scripting	216
Points of Weakness	217
How Hackers Can Take Advantage	218
Preinstalled ActiveX Controls	218
Bugs Open the Door	219
Intentionally Malicious ActiveX	219
My Mistake...	220
Trojan Horse Attacks	220
Precautions to Take	220
VBScript	221
Security Model	222
Points of Weakness	222
VBScript, Meet ActiveX	222
How Hackers Take Advantage	223
Social Engineering Exploits	223
VBScript-ActiveX Can Double Team Your Security	223
Precautions to Take	224
Summary	225
FAQs	226
 Chapter 7: Personal Firewalls	 227
Introduction	228
What Is a Personal Firewall?	228
Blocks Ports	230
Block IP Addresses	230
Access Control List (ACL)	231
Execution Control List (ECL)	232
Intrusion Detection	233
Personal Firewalls and E-mail Clients	234
Levels of Protection	235
False Positives	235
Network Ice BlackICE Defender 2.1	236
Installation	236
Configuration	239
E-mail and BlackICE	248

Aladdin Networks' eSafe, Version 2.2	248
Installation	248
Configuration	252
E-mail and ESafe	269
Norton Personal Firewall 2000 2.0	269
Installation	270
Configuration	274
ZoneAlarm 2.1	283
Installation	284
Configuration	287
E-mail and ZoneAlarm	291
Summary	292
FAQs	292
 Chapter 8: Securing Windows 2000 Advanced Server and Red Hat Linux 6 for E-mail Services	 295
Introduction	296
Updating the Operating System	296
Microsoft Service Packs	296
Red Hat Linux Updates and Errata Service Packages	297
Disabling Unnecessary Services and Ports	299
Windows 2000 Advanced Server—Services to Disable	299
The Server Service	300
Internet Information Services (IIS)	302
Red Hat Linux—Services to Disable	304
Inetd.conf	304
Rlogin	305
Locking Down Ports	305
Well-Known and Registered Ports	306
Determining Ports to Block	308
Blocking Ports in Windows	308
Blocking Ports in Linux	310
Inetd Services	310
Stand-Alone Services	310
Maintenance Issues	311
Microsoft Service Pack Updates, Hot Fixes, and Security Patches	312
Case Study	313
Red Hat Linux Errata: Fixes and Advisories	314
Case Study	316

Windows Vulnerability Scanner (ISS System Scanner)	317
Linux Vulnerability Scanner (WebTrends Security Analyzer)	320
Logging	325
Windows 2000 Advanced Server	325
Linux	325
Common Security Applications	326
Firewall Placement	327
Summary	330
FAQs	331
 Chapter 9: Microsoft Exchange Server 5.5	 333
Introduction	334
Securing the Exchange Server from Spam	334
Configuring the IMS To Block E-mail Attacks	335
Exchange and Virus Attacks: Myths and Realities	341
Learning from Recent Attacks	343
Case Study: Preparing for Virus Attacks	345
Exchange Maintenance	347
Service Packs	347
Plug-ins and Add-ons	351
Third-party Add-ons	351
Microsoft Utilities	352
Content Filtering	353
Case Study: Content Scanning	356
Attachment Scanning	357
Recovery	359
Backing Up Data	360
Restoring Data	363
Summary	363
FAQs	365
 Chapter 10: Sendmail and IMAP Security	 367
Introduction	368
Sendmail and Security: A Contradiction in Terms?	368
Sendmail's History	368
Threats to SendMail Security	370
Anatomy of a Buffer Overflow	370
A Buffer Overflow Illustrated	371



Sendmail and the Root Privilege	372
Fixes	373
Stay Current	373
Stay Informed	374
Protect Your Resources	375
Minimize Risk	375
Alternatives: Postfix and Qmail	377
Postfix	377
Qmail	378
Comparing Your Options	379
Configuring Sendmail	380
Internet Message Access Protocol (IMAP)	381
The IMAP Advantage	381
Understanding IMAP Implementations	383
UW IMAP	383
Cyrus IMAP	384
One IMAP, Many Choices	385
Administering the Server	385
The Users	385
The Mail Store	386
Protecting the Messages	387
Strengthening Authentication	387
Securing Access	388
From the Client Side	390
IMAP Summary	390
Recovery	391
Backing Up Data	392
Restoring Data	393
The Bottom Line on Backup	393
Summary	394
FAQs	394
 Chapter 11: Deploying Server-side E-mail	
Content Filters and Scanners	397
Introduction	398
Overview of Content Filtering	398
Filtering by Sender	403
Filtering by Receiver	403
Subject Headings and Message Body	404
Overview of Attachment Scanning	404

Attachment Size	407
Attachment Type (Visual Basic, Java, ActiveX)	407
McAfee GroupShield	408
Installation of GroupShield	408
Configuration	412
Specific Settings	418
Trend Micro ScanMail for Exchange Server	419
Installation of ScanMail	419
Configuration	421
Specific Settings	422
Additional ScanMail Offerings	424
Content Technologies' MAILsweeper for Exchange 5.5	425
Installation of MAILsweeper	425
Configuration	427
Specific Settings	428
Firewall and E-mail Content Scanning	428
Content Technologies' MIMESweeper for	
CheckPoint's Firewall-1	429
Axent Raptor Firewall	430
Attack Detection and System Scanning	431
Attacks	431
Real-time, Third-party Services	433
Evinci	434
Securify	434
Summary	435
FAQs	435
<b>Appendix: Secrets</b>	<b>437</b>
Lesser-known Shortcuts	438
Under-documented Features and Functions	438
Disable an ActiveX Control	440
For Experts Only (Advanced features)	441
Web Pages on Mobile Code Security Topics	441
Outlook Web Access (OWA)	442
Using SendMail To Refuse E-mails with the Love Letter Virus	442
Troubleshooting and Optimization Tips	444
<b>Index</b>	<b>447</b>