

THE
PUBLISHER OF
**HACKING
EXPOSED**

ANTI-SPAM TOOL KIT



CD ROM CONTAINS
POPULAR ANTI-SPAM
TOOLS FROM THE BOOK

PAUL WOLFE, CHARLIE SCOTT & MIKE W. ERWIN

CONTENTS

Acknowledgments	xvii
Introduction.	xix

Part I

1 Forming Your Plan Against Spam	3
A Brief History of Spam	4
Why the Word Spam?	5
The Basics of Fighting Spam	6
Traditional Methods—Filtering by Keyword	6
Open-Relays and Blacklists	6
Advanced Methods and Why They Work	7
Trends Forming Around Spam Legislation	8
Developing E-Mail Policies	9
Organizing Everything	10
Developing an E-Mail Policy	10
Establishing a Resource Plan (Identifying Systems)	13
Conduct Testing and Refinement	14
Spotting Problems Before They Happen	14
Advanced Topics and Cross-Pollination	15
Summary	16

2	Goals and Criteria for Evaluating Spam Control Solutions	17
	The Mail Flow Architecture	18
	The Digital You: Authentication and Repudiation	19
	Goals of a Robust Mail Control System	20
	Restrict Access to Your E-Mail Identities	20
	Identify the Spammers	21
	Identify the Spam	21
	Select the Best Locations	21
	Select the Best Tools	22
	Select for Operational Ease	22
	Bringing It All Together	22
	Selecting Mail Control Components	23
	Breadth (All Forms of Mail-borne Content Filtered)	23
	Depth (Multiple Techniques Used at Multiple Points)	23
	Impact	24
	Operation	24
	Specific Criteria in Selecting Anti-Spam Solutions	24
	Summary	26
3	Methods for Mail Content Control	27
	Building on a Historical Basis	28
	RFC 2505—SMTP and MTA Best Practices	28
	RFC 2635—An Explanation for Why Spam Is Harmful	29
	RFC 3098—A Discussion of Responsible Internet Advertising	29
	Analyzing Spam	29
	Analysis That Targets the Content of the Message	30
	Analysis That Targets the Sender or Intermediaries	34
	Analysis That Targets the Benefactor	39
	New Approaches to Circumvent Advanced Spam Filtering	41
	Summary	42
4	Anti-Spam Implementation Strategies	43
	Choosing the Right Solutions	45
	Key Factors That Affect Your Decision	45
	Recommendations on Solution Robustness	48
	Policy Recommendations	48
	Technical Recommendations	50
	Spam Solutions Covered in this Book	51
	Subscriptions to Network-Based Blacklists	51
	Client-Based Spam Filtering	52

Server-Based Spam Systems	53
Gateway-Based Spam Systems	54
Provider-Based Spam Systems	56
Summary	58

Part II

5 Blocking Spammers with DNS Blacklists	61
Understanding DNS Blacklists	62
Types of DNSBLs	62
Criteria for DNS Blacklists	64
Adding or Removing Entries from a DNS Blacklist	65
Choosing a DNS Blacklist	66
Mail Abuse Prevention System (MAPS)	66
How MAPS Works	67
Subscribing to MAPS	69
SpamCop	69
How SpamCop Works	70
Subscribing to SpamCop	71
Open Relay Database (ORDB)	71
How ORDB Works	72
Subscribing to ORDB	72
Distributed Server Boycott List (DSBL)	72
How DSBL Works	72
Subscribing to DSBL	73
Spamhaus	73
How Spamhaus Works	73
Subscribing to Spamhaus	74
Not Just Another Bogus List (NJABL)	74
How NJABL Works	74
Subscribing to NJABL	75
RFC Ignorant (RFCI)	75
What Makes Someone RFC Ignorant?	76
Subscribing to RFCI	78
Implementing DNSBLs Within Sendmail	78
Configuring Sendmail for IP-Based DNSBLs	79
Configuring Sendmail for Domain-Based RHSBLs	79
Implementing DNSBLs with Postfix	80
Configuring Postfix for IP-Based DNSBLs	80
Configuring Postfix for Domain-Based RHSBLs	80

Implementing DNSBLs with Microsoft Exchange	81
Exchange 2000	81
Exchange 2003	82
Summary	88
6 Filtering Spam with SpamAssassin	89
Dossier of a Spam Assassin	90
SpamAssassin = Spam Detective	90
SpamAssassin Rules!	91
SpamAssassin Scores!	91
Killer Features	93
SpamAssassin Gone Commercial	93
Installing SpamAssassin	94
Software and Hardware Requirements	94
Before You Start	98
Installing the Easy Way: From CPAN	99
Installing the Less Easy Way: From Tarball	101
Installing from the Edge: CVS	104
Other Ways to Install	104
Understanding SpamAssassin's Components	105
The spamassassin Utility	105
The Spamd Daemon	106
The Spamc Client	106
The local.cf Configuration File	107
The user_prefs Configuration File	108
Configuring SpamAssassin	109
Per-User Configuration	109
Site-Wide Configuration	110
Spamd Configuration	110
An Introduction to SpamAssassin's Output	111
Looking at a Message	111
Is This the Only Option?	111
Summary	112
7 Catching Spam with SpamAssassin's Bayesian Classifier	113
Implementing SpamAssassin's Bayesian Classifier	114
Looking at SpamAssassin's Bayes-Related Files	114
SpamAssassin's Bayes Rules	115
Automated Learning	116

Training SpamAssassin's Bayesian Classifier	117
Giving sa-learn Input	117
Training with Ham	118
Training with Spam	118
Correcting Mistakes	118
Bayes Database Expiration	119
Getting Bayes Statistics	121
Implementing Bayes System-Wide	122
Bayesian Learning Caveats	123
Summary	124
8 Enhancing and Maintaining SpamAssassin	125
Creating Your Own Rules	126
Where to Create and Modify Rules	127
Components of a Rule	127
Building a Rule	129
Testing the Rule	131
Whitelisting and Blacklisting	131
trusted_networks	131
whitelist_to	132
more_spam_to	132
all_spam_to	133
Localizing	133
ok_locales	133
ok_languages	134
Using MIMEDefang with SpamAssassin	135
MIMEDefang and SpamAssassin	136
MIMEDefang Requirements	136
Using amavisd-new with SpamAssassin	138
amavisd-new and SpamAssassin	139
amavisd-new Requirements	139
Using SpamAssassin as a Gateway to Another Mail Server	140
Summary	141
9 Configuring Popular E-mail Clients for Spam Filtering	143
Configuring Spam Filters on Eudora	144
Watching for Spam with Eudora's SpamWatch	144
Turning On Eudora's SpamWatch	145
Tweaking Eudora's SpamWatch	145
Training Eudora's SpamWatch	146

Configuring Spam Filters on Mozilla Mail	147
Mozilla's Junk Mail Controls	147
Using Mozilla Message Filters with SpamAssassin	149
Configuring Spam Filters in Outlook Express	152
Blocking Senders in Outlook Express	153
Using OE Message Rules with SpamAssassin	156
Configuring Spam Filters on Outlook	158
Configuring Outlook's Junk and Adult Content E-mail Filters	159
Using Outlook Message Rules with SpamAssassin	166
Summary	168

Part III

10 Anti-Spam Clients for Windows	171
SpamBayes	172
How It Works	172
Installing SpamBayes	173
User Knowledge and Machine Learning	174
SpamPal	183
How It Works	183
Installing SpamPal	185
Controlling the World Through Lists	188
SpamCatcher	194
How It Works	194
Installing SpamCatcher	194
Making Contact with the SpamCatcher Network	198
Lyris MailShield Desktop	203
How It Works	204
Installing MailShield Desktop	204
Manipulating MailShield to Suit Your Needs	207
SPAMfighter	212
How It Works	213
Installing SPAMfighter	213
Configuring SPAMfighter	214
SpamButcher	218
How It Works	218
Installing SpamButcher	219
Butchering Spam	220

iHateSpam	227
How It Works	228
Installing iHateSpam	228
Turning iHate to Action	229
SpamNet	231
How It Works	232
Installing SpamNet	232
Netting Spam with SpamNet	233
KnockKnock	236
How It Works	236
Installing KnockKnock	236
Knocking on a Spammer's Door	237
Knocking KnockKnock	241
POPFile	242
How It Works	242
Installing POPFile	242
POP Goes the Spammers	244
11 Anti-Spam Servers for Windows	249
iHateSpam Server Edition	250
How It Works	250
Installing iHateSpam	250
Hating Spam in the Enterprise	254
GFI MailEssentials	266
How It Works	266
Installing GFI MailEssentials	267
Configuring the Essentials	269
Trend Micro Spam Prevention Service	276
How It Works	276
Installing SPS	276
12 Anti-Spam Tools for Macs	283
PostArmor	284
How It Works	284
Installing	284
Use Your Armor!	288
POPmonitor	292
How It Works	292
Installing	292
Operating POPmonitor	295

Spamfire	297
How It Works	298
Installing	298
Firing Up the Spammers	299
MailGoGoGo	302
How It Works	302
Installing	303
Getting Spam to Go Go Go...	304
Mail Gone, Gone, Gone	305
Summary	306
13 Anti-Spam Tools for Linux	307
Vipul's Razor	308
Examining the Razor	309
Downloading and Installing Razor	310
Using Razor	311
Distributed Checksum Clearinghouse	313
Welcome to the Clearinghouse	313
Downloading and Installing DCC	314
Running DCC	315
Bogofilter	315
Installing Bogofilter	315
Running Bogofilter	316
SpamBayes	317
Installing SpamBayes	317
Using SpamBayes	318
Quick Spam Filter	319
Downloading and Installing QSF	319
Running QSF	319
The SpamBouncer	321
Installing and Configuring the SpamBouncer	321
What You'll See	323
A Pleasant Surprise	324
Summary	324

Part IV

14 Know Your Enemy	327
Profile of an "E-mail Direct Marketer"	328
Spam Tools	328
The Purveyors of Spam	332

Getting to Know the Product (Spam)	335
Anatomy of an E-mail Header	335
Spam Examples	339
Red Alert: Reporting Known Spammers	343
Direct E-mail	343
DNS Blacklists	344
Update Your Own Anti-Spam Tool	344
Summary	344
15 Advanced Topics and Fine Tuning	345
The Black, the White, and the Grey	346
Roll-Your-Own Blacklist	346
Blacklisting with a Bite	346
What in the World Is Greylisting	347
The Complete MX Relay Defense	348
Defense by Disguise	349
Use Graphics Instead of Text	349
Use the HTML ASCII Equivalence	349
Use a Scripting Language (JavaScript)	350
Spam-bots and How They Work	351
Harvesting with Our Perl Reaper	353
Spam-bots Patented: the End of the World Must Be Near...	354
What Is the Robots.txt File	354
Where Can I Get More Info on Robots?	356
Siphoning a 55-Gallon Drum of Spam	356
Reversing the Spam-bot Spigot	358
The Reverse Dictionary Defense	358
The DDoS Detection Defense	359
What to Send Once You've Identified Them	359
Summary	360
16 Fighting Spam Defensively	361
Win Before Fighting	362
E-mail Addresses	362
Challenge/Response: The Next Weird Thing	367
Future Spam-Fighting	369
Keeping Your Own House Clean	369
Open Relays	369
Securing Your Resources	372
Spyware: Another Spam Pathway	375
Pop-ups: The New Spam	375

Anti-Spam Tool Kit

True Spyware	376
Anti-Spyware Tools	376
Summary	381
Glossary Definitions and Acronyms	383
A Selected Anti-Spam Resources	387
E-mail and Spam-Related RFCs	388
Papers, Whitepapers, and Treatises	388
Spam and the Law	389
DNS Blacklists	389
SpamAssassin Resources	390
E-mail Clients	390
E-mail Servers	391
Anti-Spam Client Tools for Windows	391
Anti-Spam Servers for Windows	394
Anti-Spam Tools for the Macintosh	394
Anti-Spam Tools for Linux	395
Other Tactics and Tools	396
U.S. Government Sites Concerning Spam	397
B About the CD-ROM	399
How to Use the CD-ROM	400
Anti-Spam Tools on the CD	400
Links to Additional Tools	401
Problems with the CD	401
Index	403