

Confidentiality Versus Privacy

8

Protecting Confidentiality

9

Protecting Privacy

10

to

11

12

12

13

Digital Signatures	26
How Digital Signatures Work	26
Digital Signature Algorithms	28
Protocols	29
The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols	30
The Internet Protocol Security Extension (IPsec) Protocols	30
The Secure Multipurpose Internet Mail Extensions (S/MIME)	34
Authentication-Only Protocols	35
Summary	39
Additional Reading	40
<hr/>	
3 Windows and Exchange Security Architecture	41
Learning the Right Lingo	42
Authentication	43
Built-In Accounts and Groups	43
What Happens When You Log On?	46
Access Control and Permissions	47
How Exchange Modifies the Access Control Process	48
Understanding Exchange-Specific Permissions	49
Permissions and Roles	52
Permissions and Mailboxes	54
Summary	57
Additional Reading	57
<hr/>	
4 Threats and Risk Assessment	59
Types of Security Threats	60
What Makes a Target?	61
Attack Versus Defense	62
Classifying Threats	62
Models for Risk Assessment	64
The STAVE Model	65
The STRIDE Model	67
Asset and Threat Assessment for Exchange (or, What Would You Like to Not Lose Today?)	69
Summary	71
Additional Reading	71

5 Physical and Operational Security 73

Physical and Operational Threat Assessment	74
Beefing Up Your Physical Security	75
Securing the Environment	75
Securing Your Hardware	77
A Few Words About Laptops	78
Strengthening Operational Security	79
Keeping Your Secrets Secret	79
Summary	80
Additional Reading	80

PART II Exchange Server Security

6 Windows 2000 Server Security Basics 83

Taking the First Step: Patch Management	83
Where Patches Come From	83
Figuring Out What Needs Patching	85
Using the Microsoft Baseline Security Analyzer (MBSA)	86
Using MBSA From the Command Line	93
Automating Patch Distribution	97
Securing What's Most at Risk: A Checklist	100
Step 1: Patch	101
Step 2: Set Strong Policies	102
Step 3: Lock Down IIS	107
Tightening Things Further	110
Summary	114
Additional Reading	115

7 Installing Exchange with Security in Mind 117

Delegating Control	126
Applying the Finishing Touches	135
Summary	137
Additional Reading	137

8 SMTP Relaying and Spam Control 139

Understanding Relaying	139
Understanding SMTP Store-and-Forward Protocol	139
What Relaying Is	140
Why Relaying Is Necessary Sometimes	141
How Relaying Can Get You in Trouble	141
Controlling Relaying	142
Controlling Access for SMTP Virtual Servers	143
Controlling Who Can Relay	149
Configuring Relaying on SMTP Connectors	150
Verifying Your Relaying Configuration	151
Understanding Spam	152
Common Spam-Blocking Tactics	153
Using Exchange's Spam Control Features	156
Creating a Domain or Sender Filter	156
Activating the Filter	158
Evaluating Third-Party Antispam Products	158
Questions About Cost	159
Questions About Capability	159
Summary	160
Additional Reading	160

9 Content Control, Monitoring, and Filtering 161

Adding Disclaimers	162
Getting to the Message	162
Rolling Your Own Sink	162
Using a Commercial Product	163
Filtering Inbound and Outbound Content	164
Evaluating Filtering Products	165
Reading Other People's Mail	166
Using Message Journaling	167
Granting Permission to Other Mailboxes	168

Using Message Tracking	169
Setting Up Message Tracking: A Quick Review	170
Tracking a Specific Message	171
Searching the Store for Specific Content	171
Searching Mailboxes with Exmerge	172
Summary	175
Additional Reading	175

10 Antivirus Protection 177

Understanding Virus Protection Principles	177
Finding Viruses	178
Cleaning Up Viruses	180
Designing Defense in Depth	180
Perimeter Protection	180
Desktop Protection	182
Exchange Server Protection	182
Everything Else	186
Summary	187
Additional Reading	187

PART III Communications Security

11 Securing Internet Communications 191

Using TLS/SSL with SMTP	191
Requesting an SSL Certificate	192
Enabling STARTTLS	199
Using IPsec	201
Understanding the Windows IPsec Implementation	204
Creating IPsec Policies	207
Publishing MAPI RPCs with ISA Server	215
Creating the Publishing Rules	216
Allowing the Exchange Server to Proxy Authentication Traffic	217
Configuring Outlook	218
Summary	218
Additional Reading	219

12 E-Mail Encryption 221

Understanding the Exchange–PKI Combination	221
Planning Your Encryption Infrastructure	222
Detailing Your Specific PKI Goals	222
Designing Your CA Infrastructure	225
Diving in to Digital Certificates	232
Understanding Enrollment	236
Understanding the Exchange KMS	237
Understanding Revocation	238
Server Performance Guidelines	240
Installing Certificate Services	241
Installing Certificate Services	242
Using Web Enrollment	244
Using the Exchange KMS	246
Configuring and Managing Certificate Services	251
Delegation and Segregation	251
Building Trusts and Trust Lists	252
Backing up and Restoring the CA	253
Fine-Tuning CA Security	254
Summary	255
Additional Reading	255

PART IV Client Security

13 Securing Outlook 259

Understanding Outlook's Security Features	259
The Outlook Security Update	260
Attachment Security	260
Address Book and Object Model Security	263
Security Zone Changes	263
S/MIME Security	264
Customizing the Outlook Security Update	265
Installing the Security Package	265
Installing the Trusted Code Control	266
Creating a Public Folder for Security Settings	266

Filling out the Template	267
Deploying Outlook Security Settings	271
Customizing Settings for End Users	272
Using S/MIME	273
Managing Certificates	273
Setting S/MIME Options	276
Signing or Encrypting a Message	278
Reaching into Outlook's Toolbox	279
Converting Inbound HTML Mail to Plaintext	279
Encrypting RPC Traffic	280
Summary	281
Additional Reading	281
<hr/>	
14 Securing Outlook Web Access	283
Understanding Outlook Web Access	283
Front-End and Back-End Servers	283
Understanding Outlook Web Access Authentication	285
Controlling Access to Outlook Web Access	288
Controlling Access to Servers	289
Setting Permissible Authentication Methods	289
Using Form-Based Authentication	291
Controlling Access for Specific Users	294
Using Outlook Web Access Segmentation	294
Using SSL with Outlook Web Access	297
Enabling SSL for OWA	298
Automatically Redirecting Non-SSL Requests	298
Enabling Password Changes Through Outlook Web Access	299
Load Balancing SSL Traffic with Outlook Web Access	302
Controlling Content Caching	303
Securing Outlook Web Access with Firewalls	304
Opening the Correct Firewall Ports	306
Protecting FE/BE Communications	309
Publishing Outlook Web Access with ISA Server	313
Creating the Web Listener	314
Creating the Outlook Web Access Destination Set	315
Creating the Web Publishing Rule	317

Applying the Finishing Touches

318

17 Security Logging 347

Understanding Security Logging	347
How Windows 2000 Auditing Works	348
What Windows 2000 Puts in the Event Logs	348
Using Auditing in Windows 2000	349
What's in the Log Entry?	349
Controlling What Gets Audited	349
Automated Analysis Tools	354
What to Audit and Why	357
Account Management Events	357
Account Logon Events	358
Logon Events	359
Privilege Use	359
Summary	360
Additional Reading	360

PART VI Appendices

A The Ten Immutable Laws 363

The Ten Immutable Laws of Security	363
The Ten Immutable Laws of Security Administration	369

B Permissions Guide 377

Permissions on Objects in the Exchange Configuration Tree	378
Permissions on the Server Object and Its Children	381
Permissions on Other Objects in the Configuration Tree	382
Permissions Set on Public Key Services Objects	383
Permissions on Objects in the Domain Naming Context	384

Index 387

