



Contents

Acknowledgments	xv
Part I Email and Security Background	
Chapter 1 Introduction	3
How This Book Is Organized	3
Part I: Email and Security Background	4
Part II: PKI Basics	4
Part III: Secure Email	4
Part IV: Tokens	4
Part V: Case Studies	5
Part VI: Expectations for the Future	5
Appendices	5
Who Should Read This Book	5
Chapter 2 Understanding Email	7
History and Evolution	8
Internet Email	11
Wow! Email Is Just Like Snail Mail	11
Process	11
Formats	12
Commands	16
Mail Transfer System Architecture	19
Emailing	21
Email Client	21
Webmail	22
Chapter 3 Security Fundamentals	23
Who Wants to Read Your Email?	24
Governments	24
Businesses	26

x Contents

Criminals	27
Hackers	27
Reporters and Bloggers	28
Friends and Family Members	28
Where They Can Read Your Email	28
How They Can Read Your Email	29
Eavesdrop	29
Masquerade	29
What Else Can They Do to the MTS?	30
How You Can Stop Them	30
Security Services	31
Fundamental Services	31
Derivative Services	32
Cryptographic Mechanisms	33
Encryption	33
Digital Signatures	33
One-Way Hash Functions	34
Basic Security Tools	34
Access Control Lists	34
Fake Traffic	34
Logs	34
Nonces	35
Signed Receipts	35
Sequence Numbering	35
Time	35
More Attacks	35
Chapter 4 Cryptography Primer	37
Symmetric Cryptography	38
Types	38
Algorithms	39
Modes	39
Symmetric Key Management	40
Symmetric Integrity Functions	42
Asymmetric Cryptography	45
Public Key Encryption	45
Digital Signatures	47
Asymmetric Key Management	51
Part II PKI Basics	
Chapter 5 Understanding Public Key Infrastructure	55
Trust	56
PKI Architectures	57
Single CA	57
Trust Lists	58
Hierarchical PKI	59

Contents xi

Mesh PKI	61
Cross-Certified PKIs	62
Bridge CAs	64
X.509 Public Key Certificates	66
Tamper-Evident Envelope	66
Basic Certificate Contents	67
Certificate Extensions	68
Subject Type Extensions	69
Name Extensions	69
Key Attributes	70
Policy	71
Additional Information	72
X.509 Certificate Revocation Lists	73
Signed Certificate List	73
CRL Extensions	75
CRL Entry Extensions	77
PKI Components and Users	78
Infrastructure Users	78
Subscribers	79
Replying Parties	79
Infrastructure Components	79
Certification Authorities	80
Registration Authority	83
Repository	84
Archive	84
Part III Secure Email	
Chapter 6 Protecting Email Message Contents	87
Evolution	87
Privacy Enhanced Mail	88
Pretty Good Privacy	89
MIME Object Security Services	90
Message Security Protocol	91
Public-Key Cryptography Standard #7	91
Secure Multipurpose Internet Mail Extensions	91
Protecting Email Content	92
Concepts	93
CMS Content Types	93
Encapsulating	93
Version Numbers	95
Attributes	95
MIME Layer	95
Protecting CMS Content Types	96
Signed Data	96
Enveloped Data	98
Encrypted Data	102

xii Contents

	Digest Data	102
	Authenticated Data	103
	Authenticated-Enveloped Data	104
	Non-Protecting Content Types	104
	Data	105
	Compressed Data	105
	Receipt Syntax	105
	Content Collection	106
	Content with Attributes	107
	Attributes	107
	Content Type	108
	Message Digest	109
	Signing Time	110
	Counter Signatures	110
	S/MIME Capabilities	111
	Encryption Key Preference	111
	Signed Receipts	112
	Content Hints	115
	Content Reference	116
	Signing Certificates	116
	Security Labels	117
	Equivalent Labels	118
	Secure Mail Lists	118
	Algorithms	120
	Generating an S/MIME Message	122
Chapter 7	Protecting Email Passwords, Headers, and Commands	125
	Password Scramble	126
	Connection Security	127
	Transport Layer Security	128
	Handshake Protocol	129
	Record Protocol	132
	IPsec	133
	Security Associations	134
	Authentication Header	136
	Encapsulating Security Payload	137
	Internet Key Exchange (IKE)	139
Part IV	Tokens	
Chapter 8	Tokens and Hardware Security Modules	143
	Evaluation Criteria	144
	Tokens	148
	PC Cards	149
	Smart Cards	151
	Looking under the Hood	153
	Operating Systems and Smart Cards	154

Choosing Smart Cards	154
USB Tokens	155
Software Tokens	156
iButton Tokens	156
Embedded Tokens	157
Hardware Security Modules	158
Network-Attached Multi-User Hardware Security Modules	159
Application Program Interfaces	160
Part V	Case Studies
Chapter 9	Signatures and Authentication for Everyone 165
SAFE Architecture	166
Cryptographic Algorithms	166
PKI Architecture	167
Certificate Policies	169
Certificate, CRL, and OCSP Profiles	169
Tokens and Cryptographic Modules	173
Applications	174
Successes and Shortcomings	175
Lessons Learned	176
Chapter 10	Department of Defense Public Key Infrastructure, Medium Grade Service, and Common Access Card 181
Architectures	182
Cryptographic Algorithms	182
PKI Architecture	183
DEERS/RAPIDS Architecture	184
Certificate Policies	186
Certificate and CRL Profiles	188
Certificate Status Responders	190
Repositories	191
CAC and Cryptographic Modules	193
Applications	194
Success and Shortcomings	196
Lessons Learned	197
Chapter 11	National Institute of Standards and Technology Personal Identity Verification 201
PIV Architecture	203
Cryptographic Algorithms	203
Architecture	205
Certificate Policies	206
Certificate, CRL, and OCSP Profiles	209
Cards and Cryptographic Modules	215
Applications	218
Lessons Learned	220

xiv Contents

Part VI	Expectations for the Future	
Chapter 12	Future Developments	223
	Email	223
	Evolution of Messaging	223
	Stopping spam	225
	Cryptography	229
	Competing Hash Algorithms	229
	Adopting Elliptic Curve Cryptography	231
	Public Key Infrastructure	232
	Trending Architectures	233
	Checking Certificate Status	233
	Online Certificate Status Protocol	234
	Server-Based Certificate Validation Protocol	236
	Authorizing with Attribute Certificates	239
	Delegating with Proxy Certificates	242
	Managing Trust Anchors	244
	Security	245
	Tokens	246
	Physical Access Control	246
	Conclusion	247
Appendix A	ABNF Primer	249
	Rules	249
	Operators	250
	Operator Precedence	251
Appendix B	ASN.1 Primer	253
	Syntax Definition	254
	Simple Types	255
	Structured Types	256
	Implicit and Explicit Tagging	256
	Other Types	257
	Basic Encoding	257
	Distinguished Encoding Rules	258
Appendix C	MIME Primer	259
	Character Sets	260
	Transfer Encoding	261
	Content Type	262
	Multipart Messages	264
Appendix D	RFC Summaries	267
	References	277
	Index	287