

Contents

Preface	xiii
Acknowledgement	xv
Glossary	xix
Acronyms and Abbreviations	xxiii
1 Threats and Solutions	1
1.1 The Technical Threats to Communications Security	4
1.2 Authentication	4
1.2.1 Text/Data Message Authentication	6
1.3 Confidentiality	7
1.4 Integrity	8
1.4.1 Digital Signatures	8
1.5 Availability	10
1.5.1 PINs and Passwords	10
1.5.2 Biometric Access Tools	13
1.5.3 Challenge/Response Control	14
1.5.4 Tamperproof Modules	15
1.6 Compromising Emanation/Tempest Threats	16
1.6.1 Compromising Emanation Definitions	16
1.6.2 Compromising Emanation	16
1.6.3 Modulated Harmonics	16
1.6.4 Electronic Coupling	19
1.6.5 Preventative Measures in Electronic Equipment Construction	21
2 An Introduction to Encryption and Security Management	25
2.1 Analogue Scrambling	25
2.1.1 Phonemes and the Structure of Voice Signals	26
2.1.2 Frequency Scrambling	28
2.1.3 Time Element Scrambling	29
2.1.4 Digital Ciphering	30
2.1.5 Digital Stream Ciphering	31
2.1.6 Block Ciphering	33
2.1.7 Summary	37
2.2 Algorithms	38
2.2.1 Symmetrical Cryptography	38
2.2.2 Asymmetrical Cryptography	39
2.2.3 Hash Algorithms	41
2.2.4 MACs (Message Authentication Codes)	41

2.2.5	<i>Digital Signature Algorithms</i>	41
2.2.6	<i>Key Agreement/Exchange Algorithms</i>	42
2.2.7	<i>Summary of Comparisons Between Asymmetric and Symmetric Algorithms</i>	42
2.3	Goodbye DES, Hello AES	43
2.4	Fundamentals in Key Management	44
2.4.1	<i>Key Generation</i>	45
2.4.2	<i>Key Storage</i>	47
2.4.3	<i>Key Distribution</i>	48
2.4.4	<i>Key Changes</i>	51
2.4.5	<i>Key Destruction</i>	54
2.4.6	<i>Separation</i>	55
2.5	Evaluating Encryption Equipment	57
2.5.1	<i>The Main Points of Evaluation</i>	58
3	Voice Security in Military Applications	61
3.1	Analogue Encryption of Naval Long Range, HF Radio Communications	62
3.1.1	<i>Ship Communications Operation</i>	63
3.1.2	<i>The Cipher/Scrambler Features</i>	65
3.1.3	<i>Synchronisation</i>	68
3.1.4	<i>Security Parameters</i>	69
3.1.5	<i>Key Distribution and Management</i>	70
3.2	Stand-alone Digital Cipher Units in Land-based Operations	70
3.2.1	<i>The Ground Force Scenario</i>	71
3.2.2	<i>The Cipher Unit Features</i>	71
3.2.3	<i>Synchronisation</i>	74
3.2.4	<i>Security Parameters</i>	76
3.2.5	<i>Key Management</i>	77
3.3	Radio Integrated Cipher Module	82
3.3.1	<i>Typical Features</i>	83
3.3.2	<i>Cryptographic Parameters</i>	83
3.3.3	<i>Other Security Parameters and Features</i>	83
4	Telephone Security	87
4.1	Specific Threats to Telephone Operations	88
4.1.1	<i>Telephone Security Requirements and Features</i>	89
4.2	Network Technologies	90
4.2.1	<i>Secure Telephone Communication</i>	90
4.2.2	<i>INMARSAT Communications</i>	91
4.3	Telephone Security Solutions	95
4.3.1	<i>STU III/IIB</i>	96
4.3.2	<i>The Alternative Telephone Security</i>	98
4.3.3	<i>Hardware Security Features</i>	101
4.3.4	<i>Telephone Security Architecture and Functions</i>	102
4.4	Key and Access Management	103
4.4.1	<i>The Complete Key System</i>	104
4.4.2	<i>The 'ZUPPA' Network</i>	107
4.5	Network Implementation	108
4.6	Key Distribution	111
4.7	Summary	112
5	Secure GSM Systems	113
5.1	The Basic GSM Architecture	113
5.1.1	<i>System Components</i>	114
5.1.2	<i>The GSM Subsystems</i>	116

5.1.3	<i>The GSM Radio Um Interface</i>	117
5.2	Standard GSM Security Features	118
5.2.1	<i>The AuC</i>	119
5.2.2	<i>The HLR</i>	119
5.2.3	<i>The VLR</i>	120
5.2.4	<i>SIM Card</i>	120
5.2.5	<i>The IMSI & TMSI</i>	121
5.2.6	<i>Standard GSM Encryption</i>	121
5.2.7	<i>Cryptographic Attacks on the GSM Algorithms</i>	126
5.2.8	<i>TDMA Time Division Multiple Access</i>	127
5.2.9	<i>Frequency Hopping</i>	127
5.3	Custom Security for GSM Users	128
5.3.1	<i>The Custom Encryption Process</i>	130
5.3.2	<i>Key Systems</i>	133
5.3.3	<i>Cryptographic Parameters and Algorithms</i>	135
5.3.4	<i>Security Architecture</i>	135
5.3.5	<i>Cipher Unit Hardware Elements</i>	136
5.3.6	<i>System Overview with Secure GSM and Fixed Subscriber Equipment</i>	137
5.4	Key Management and Tools	138
5.4.1	<i>Key Distribution and Loading</i>	138
5.4.2	<i>Chip Cards and Readers</i>	138
5.4.3	<i>Key Signatures</i>	138
5.5	GPRS General Packet Radio Systems	139
5.5.1	<i>Basic GPRS Operation and Security</i>	139
6	Security in Private VHF/UHF Radio Networks	143
6.1	Applications and Features	143
6.1.1	<i>The Ship Group</i>	143
6.1.2	<i>The Escort Group</i>	145
6.1.3	<i>The Close Support Group</i>	145
6.1.4	<i>The Telephone Groups</i>	146
6.2	Threats	146
6.2.1	<i>Confidentiality</i>	146
6.2.2	<i>Integrity</i>	146
6.2.3	<i>Authenticity</i>	147
6.2.4	<i>Access</i>	147
6.3	Countermeasures	147
6.3.1	<i>Protection of Confidentiality</i>	147
6.3.2	<i>Authentication</i>	147
6.3.3	<i>Access Control</i>	149
6.4	Communications Network Design and Architecture	150
6.4.1	<i>The Close Support Group</i>	151
6.4.2	<i>The Escort Group</i>	152
6.4.3	<i>The Ship Group</i>	152
6.5	Hardware Components and Functions	153
6.5.1	<i>Hand-held UHF Radios</i>	153
6.5.2	<i>Base Stations/Repeaters</i>	158
6.5.3	<i>Telephone Patch</i>	160
6.5.4	<i>Security Management Tools</i>	162
6.6	Security and Key Management	162
6.6.1	<i>Functions of the Management Centre</i>	162
6.6.2	<i>Frequency Management</i>	163
6.6.3	<i>Key Management</i>	165
6.7	Other Security Features	168
6.7.1	<i>Remote Key Cancelling</i>	168

6.7.2	<i>Remote Blocking</i>	168
6.7.3	<i>Silent Mode Tracking</i>	168
7	Electronic Protection Measures – Frequency Hopping	171
7.1	ESM	171
7.2	EA	172
7.3	EPM	172
7.3.1	<i>Methods of Attack</i>	172
7.3.2	<i>Spread Spectrum Techniques</i>	177
7.3.3	<i>COMSEC and TRANSEC</i>	182
7.4	Military Applications	183
7.4.1	<i>Applications Requirements</i>	183
7.4.2	<i>Operational Requirements</i>	184
7.4.3	<i>Security Requirements</i>	184
7.4.4	<i>Anti Jamming Requirements</i>	184
7.4.5	<i>Co-location</i>	185
7.4.6	<i>Air Defence Scenario</i>	185
7.4.7	<i>Close Air Support Scenario</i>	187
7.5	Network Architecture and Management	189
7.5.1	<i>Mission Procedures</i>	190
7.6	Characteristics of Frequency Hopping Networks	191
7.6.1	<i>COMSEC</i>	191
7.6.2	<i>TRANSEC</i>	192
7.7	Key/Data Management and Tools	201
7.7.1	<i>Algorithm Data</i>	202
7.7.2	<i>Frequency Data</i>	203
7.7.3	<i>Pre-set Data</i>	203
7.7.4	<i>Configuration Parameters</i>	203
7.7.5	<i>Key Distribution</i>	203
7.7.6	<i>The Time Problem</i>	206
7.8	Hardware Components	207
7.8.1	<i>Airborne Transceiver</i>	207
8	Link and Bulk Encryption	211
8.1	Basic Technology of Link Encryption	211
8.1.1	<i>Frame Modes</i>	211
8.2	The Ciphering Process	212
8.3	Cryptographic Parameters	214
8.3.1	<i>Key Agreement</i>	216
8.4	Key and Network Management	216
8.4.1	<i>Civilian Application</i>	216
8.5	Military Link Security	222
8.5.1	<i>Military Topology and Features</i>	223
9	Secure Fax Networks	227
9.1	Basic Facsimile Technology	228
9.2	The Basic Operation of an Encrypted Fax Machine	229
9.2.1	<i>Fax by Telephone Line</i>	229
9.2.2	<i>Fax by Radio</i>	230
9.2.3	<i>The GB Fax Protocol</i>	230
9.3	Manual/Automatic Key Selection	232
9.3.1	<i>Multi-key Fax Networks</i>	233
9.3.2	<i>Single Key Fax Networks</i>	234
9.3.3	<i>Facsimile Transmission over Radio</i>	235

9.4	Network Architecture	235
9.4.1	<i>Interesting Features of DEFNET</i>	236
9.4.2	<i>Ministry of Defence Subnet</i>	237
9.5	Key Management and Tools	237
9.5.1	<i>Key Management of DEFNET</i>	237
9.5.2	<i>Key Generation</i>	237
9.5.3	<i>Operating Parameters</i>	239
9.5.4	<i>Key and Parameter Distribution</i>	239
9.6	Fax Over Satellite Links	239
10	PC Security	241
10.1	Security Threats and Risks	244
10.2	Implementation of Solutions	244
10.2.1	<i>Unauthorised Read Out of Data Stored on Local Storage Media</i>	244
10.2.2	<i>Unauthorised Read Out of 'Deleted' Data</i>	245
10.2.3	<i>Unauthorised Read Out of Data Stored on a Remote LAN</i>	246
10.2.4	<i>Unauthorised Manipulation of Data Stored on a LAN</i>	247
10.2.5	<i>Eavesdropping on an Untrusted LAN or Public Network</i>	249
10.2.6	<i>Spoofing or Masquerading</i>	249
10.2.7	<i>Unauthorised Manipulation of Data During Transmission over a Public Network</i>	249
10.2.8	<i>Unauthorised Access to/Read Out of/Analysis of/Manipulation of/the Security System</i>	249
10.2.9	<i>'Brute-force' Attack</i>	250
10.2.10	<i>Inefficient Security and Key Management</i>	251
10.2.11	<i>Analysis of Residual Plain Information</i>	251
10.2.12	<i>The Compromise of Information, Due to Loss or Theft of Equipment or the Transfer of Security Personnel</i>	251
10.2.13	<i>The Storage or Transmission of Data in Plain, Due to Loss of Keys or Key Incompatibility</i>	252
10.2.14	<i>Illegal Access to Equipment Under Maintenance or Repair</i>	252
10.2.15	<i>Unauthorised Intrusion into the PC Environment Whilst Connected to a Public or Untrusted Network</i>	252
10.3	Access Protection	253
10.3.1	<i>Access Control Systems</i>	253
10.3.2	<i>Access by Chip Card</i>	254
10.3.3	<i>Access by PC Cards</i>	254
10.3.4	<i>Access by PCMCIA Module</i>	256
10.4	Boot-up Protection by On-board Hardware with Smart Card	256
10.5	LAN Security	256
10.5.1	<i>LAN Workstation Scenario</i>	257
10.5.2	<i>Business Trip Notebook Scenario</i>	258
10.6	Model Application of PC Security	259
10.7	System Administration	264
11	Secure E-mail	265
11.1	The E-mail Scenario	265
11.2	Threats	267
11.2.1	<i>Information Disclosure</i>	267
11.2.2	<i>Modification of Messages</i>	269
11.2.3	<i>Replay Attack</i>	269
11.2.4	<i>Masquerading</i>	269
11.2.5	<i>Spoofing</i>	269
11.2.6	<i>Denial of Service Attack</i>	269
11.3	Type and Motivation of Attackers	270
11.4	Methods of Attack	270

11.5	Countermeasures	271
11.6	Guidelines for E-mail Security	274
12	Secure Virtual Private Networks	275
12.1	Scenario	275
12.2	Definition of VPN	275
12.3	Protocols	277
12.4	Packet Header Formats	278
12.5	Security Association List	281
12.6	Tunnel Table	282
12.7	Routing Tables	282
12.8	Packet Filtering	283
12.9	Threats and Countermeasures	284
12.9.1	<i>Attacks Within the Public Network</i>	285
12.9.2	<i>Attacks Within Nodes of the Trusted Network</i>	285
12.9.3	<i>Attacks Aimed at Gaining Access to the Private Network</i>	285
12.10	Example Application – ‘Diplomatic Network’	285
13	Military Data Communications	289
13.1	Applications	290
13.1.1	<i>Data Over Radio Links</i>	290
13.1.2	<i>Modes of Radio Operation, Automatic Repeat Request and Forward Error Correction</i>	290
13.1.3	<i>Use of GAN Terminals in Battlefield Applications</i>	291
13.2	Data Terminals and Their Operating Features	292
13.3	Technical Parameters	293
13.4	Security Management	294
13.4.1	<i>Access Control</i>	294
13.4.2	<i>Data Encryption</i>	295
13.4.3	<i>Loss of Data</i>	295
13.4.4	<i>TEMPEST</i>	295
13.5	Key Management	295
13.6	Combat Packet Data Networks	296
13.6.1	<i>Packet Radios</i>	296
13.6.2	<i>Packet Data Networks</i>	297
14	Management, Support and Training	301
14.1	Environments of Security Management	303
14.1.1	<i>The Global Environment</i>	303
14.1.2	<i>The Local/Task Environment</i>	306
14.2	Infrastructure and Planning	307
14.2.1	<i>Strategic Goals</i>	308
14.2.2	<i>Tactical Goals</i>	308
14.2.3	<i>Operational Goals</i>	308
14.3	Operational Hierarchies	308
14.4	Training	310
14.5	Customer Support	312
14.6	Troubleshooting	312
14.6.1	<i>The Scanning Stage</i>	312
14.6.2	<i>The Categorisation Stage</i>	313
14.6.3	<i>The Diagnostics Stage</i>	313
14.6.4	<i>Generating Solutions</i>	313
	References	315
	Index	317