

Contents

Preface xvii

Acknowledgments xix

List of Figures xxi

List of Tables xxiii

PART I TMN OVERVIEW 1

CHAPTER 1 A Brief History of TMN 3

CHAPTER 2 Architectural Views of the TMN 7

- 2.1 Functional Architecture 7
- 2.2 Physical Architecture 9
- 2.3 Communications/Information Architecture 11
 - 2.3.1 Physical Layer 13
 - 2.3.2 Data Link Layer 13
 - 2.3.3 Network Layer 14
 - 2.3.4 Transport Layer 14
 - 2.3.5 Session Layer 15
 - 2.3.6 Presentation Layer 15
 - 2.3.6.1 Distinguished Encoding Rules 15
 - 2.3.7 Application Layer 16
 - 2.3.7.1 ACSE (Association Control Service Element) 18
 - 2.3.7.2 ROSE (Remote Operations Service Element) 19
 - 2.3.7.3 STASE-ROSE 19
 - 2.3.7.4 FTAM (File Transfer Administration and Maintenance) 20
 - 2.3.7.5 X.500 Directory User Agent 20
 - 2.3.7.6 CMISE (Common Management Information Service Element) 20
 - 2.3.7.6.1 Containment 20
 - 2.3.7.6.2 Addressing MOs 21
 - 2.3.7.6.3 Inheritance 22
 - 2.3.7.6.4 CMISE Services 22
 - 2.3.7.6.5 Managers and Agents 23
 - 2.3.7.7 SMASE (System Management Application Service Element) 24
 - 2.3.7.8 Proper Naming 25

- 2.3.7.8.1 OBJECT IDENTIFIER 26
- 2.3.7.8.2 DistinguishedName 26
- 2.3.7.8.3 Security Audit Trail—An Example 27
- 2.3.7.9 EDI 28
- 2.3.7.10 CORBA 29
- 2.3.7.11 SNMP—Keeping It Simple 30
 - 2.3.7.11.1 A Simple Structure of Management Information 30
 - 2.3.7.11.2 SNMP PDUs 32
 - 2.3.7.11.3 Version 2—Bigger and Better 33
 - 2.3.7.11.4 SNMPv3—A Version for All Seasons 35
- 2.3.8 Security-Related Components of the TMN Stack 37

PART II SECURITY OVERVIEW 39

CHAPTER 3 TMN Attacks and Defenses 41

- 3.1 TMN General Threats and Vulnerabilities 41
 - 3.1.1 Potential Security Attackers 41
 - 3.1.2 Potential Security Threats 42
 - 3.1.2.1 Unauthorized Access 42
 - 3.1.2.2 Eavesdropping 42
 - 3.1.2.3 Masquerade 43
 - 3.1.2.4 Modification of Information 43
 - 3.1.2.5 Repudiation 43
 - 3.1.2.6 Replay, Reroute, Misroute, Delete Messages 43
 - 3.1.2.7 Network Flooding 43
 - 3.1.3 Potential Security Risks 43
 - 3.1.3.1 Theft of Information 43
 - 3.1.3.2 Unauthorized Use of Resources 44
 - 3.1.3.3 Theft of Service 44
 - 3.1.3.4 Denial of Service 44
 - 3.1.3.4.1 Single-User Denial of Service 44
 - 3.1.3.4.2 Networkwide Denial of Service 44
 - 3.1.4 Impacts of Security Risks on the TMN 45
 - 3.1.4.1 Configuration Management—Provisioning 45
 - 3.1.4.2 Performance Monitoring 45
 - 3.1.4.3 Fault Management—Trouble Administration 46
 - 3.1.4.4 Accounting Management 46
 - 3.1.4.4.1 Usage Measurement 46
 - 3.1.4.4.2 Tariffing/Pricing 46
- 3.2 Threats Unique to the TMN 46
 - 3.2.1 Generic TMN Vulnerabilities 47
 - 3.2.2 TMN Domain-Specific Vulnerabilities 47
 - 3.2.2.1 Generic ICEC Threats 48
 - 3.2.2.2 Application Specific Threats 48
 - 3.2.2.2.1 Service Ordering 48
 - 3.2.2.2.2 Trouble Administration 49
 - 3.2.2.2.3 Testing 49
 - 3.2.2.2.4 Performance Management 49
 - 3.2.2.2.5 Alarm Notification 49
- 3.3 Security Services 50

- 3.3.1 Connection Access Control 50
- 3.3.2 Peer Entity Authentication 50
- 3.3.3 Data Origin Authentication 50
- 3.3.4 Integrity 51
 - 3.3.4.1 Selective Field Integrity 51
 - 3.3.4.2 Whole Message Integrity 51
 - 3.3.4.3 Session Integrity 51
- 3.3.5 Confidentiality 51
 - 3.3.5.1 Selective Field Confidentiality 51
 - 3.3.5.2 Whole Message Confidentiality 52
 - 3.3.5.3 Traffic Flow Confidentiality 52
- 3.3.6 Non-Repudiation 52
 - 3.3.6.1 Non-Repudiation of Origin 52
 - 3.3.6.2 Non-Repudiation of Receipt 52
- 3.3.7 Access Control 53
- 3.3.8 Security Alarm 53
- 3.3.9 Security Audit Trail 55

CHAPTER 4 Basic Security Mechanisms 57

- 4.1 Hashing 57
 - 4.1.1 Keyed Hashing 58
 - 4.1.2 S-key 60
- 4.2 Encryption 60
 - 4.2.1 Symmetric Key Encryption 61
 - 4.2.1.1 Padding 61
 - 4.2.1.2 IV Selection 63
 - 4.2.1.3 Error Propagation 64
 - 4.2.1.4 Triple DES 64
 - 4.2.1.5 Digital Seals 65
 - 4.2.2 Asymmetric Encryption 65
- 4.3 Digital Signatures 66
- 4.4 Certificates 68
- 4.5 Access Control Mechanisms 69
 - 4.5.1 Rules 70
 - 4.5.2 Initiator ACI 71
 - 4.5.2.1 Authenticated Identity Initiator 71
 - 4.5.2.2 Anonymous Authenticated Initiator 71
 - 4.5.2.3 Anonymous Unauthenticated Initiator 72
 - 4.5.3 Request ACI 72
 - 4.5.4 Target ACI 73
 - 4.5.4.1 Access Control Lists 73
 - 4.5.4.2 Capabilities 73
 - 4.5.4.3 Security Labels 73
- 4.6 Diffie–Hellman Key Exchange 73
 - 4.6.1 Ephemeral Diffie–Hellman Key Exchange 74
 - 4.6.2 Certified Diffie–Hellman Parameters 74
- 4.7 Authentication Protocols 74
 - 4.7.1 Challenge-Response Authentication 75
 - 4.7.2 Stateful Authentication 76
- 4.8 Mapping Security Services to Security Mechanisms 78

CHAPTER 5 Support Mechanisms 81

- 5.1 Security Alarms 81
- 5.2 Security Audit Log 82
- 5.3 Key Distribution 82
 - 5.3.1 Key Lists 82
 - 5.3.2 Public Key Distribution 83
- 5.4 Directory 83
 - 5.4.1 Automatic Registration 83
 - 5.4.2 Directory Access Control 85
 - 5.4.3 Multiple Security Domains 86
- 5.5 Protocols for Security 86
 - 5.5.1 Anatomy of Secure Communication Protocols 87
 - 5.5.2 Security In Layers 88
- 5.6 GSS-API—Security In a Box 89
 - 5.6.1 GSS Handshaking 90
 - 5.6.2 GSS Secure Transfer 91
 - 5.6.3 GSS Administrative Interfaces 93
 - 5.6.4 Status Reporting 94
- 5.7 GULS—Soaring Security 94
- 5.8 SSL3—Safe Surf 95
 - 5.8.1 A Firm Handshake 95
 - 5.8.2 Secure Transfer 99
 - 5.8.3 Alerts 100
- 5.9 IPsec 100
 - 5.9.1 A Discrete Handshake 100
 - 5.9.2 Secure Transfer 101
- 5.10 Security Engineering 102

PART III SECURING THE TMN 105**CHAPTER 6 Security of OSI-Based TMN Protocols 107**

- 6.1 In the Beginning—ACSE Security 107
 - 6.1.1 Identification 107
 - 6.1.2 Authentication 108
 - 6.1.3 ASE-Specific Security 109
- 6.2 CMISE Security 109
 - 6.2.1 Electronic Bonding Authenticator—Homegrown Security 110
 - 6.2.1.1 Historical Background 110
 - 6.2.1.2 The Authenticator 111
 - 6.2.1.2.1 Vulnerabilities 112
 - 6.2.1.2.2 Protocol Implications 113
 - 6.2.1.2.3 Operations Implications 113
 - 6.2.1.2.4 DES Padding 114
 - 6.2.1.2.5 Key Management 114
 - 6.2.1.2.6 Future Proofing 115
 - 6.2.2 Selective Field Protection—If ABSolutely Necessary 115
 - 6.2.2.1 Data Representation 117
 - 6.2.2.1.1 Character Strings 117
 - 6.2.2.1.2 Time 117
 - 6.2.2.1.3 Octet Strings 117

	6.2.2.1.4 Bit Strings	117
	6.2.2.1.5 Boolean	117
	6.2.2.1.6 Integers	118
	6.2.2.1.7 Real Numbers	118
	6.2.2.1.8 OBJECT IDENTIFIER	118
	6.2.2.1.9 OBJECT DESCRIPTOR	118
	6.2.2.2 Syntax for Security Transformations	118
	6.2.2.3 DES Padding For ABS	124
6.3	STASE-ROSE	124
	6.3.1 Security Transformations on ROSE PDUs	125
	6.3.2 Peer Entity Authentication	126
	6.3.3 Negotiation of Security Algorithms	127
	6.3.3.1 Defaults	127
	6.3.3.2 Negotiation	129
	6.3.4 Dynamic Update of Security Parameters	132
	6.3.5 STASE-ROSE Services	132
	6.3.5.1 SR-TRANSFER Parameters	132
	6.3.5.1.1 ROSE-PDU	133
	6.3.5.1.2 Encryption-Type	133
	6.3.5.1.3 Encryption-Parameters	133
	6.3.6 Interaction between Application Service Elements	135
	6.3.6.1 Association Establishment	135
	6.3.6.1.1 Association Initiator	135
	6.3.6.1.2 Association Responder	136
	6.3.6.2 Association Release	137
	6.3.6.2.1 Sender	137
	6.3.6.2.2 Receiver	138
	6.3.6.3 Association Abort	138
	6.3.6.3.1 Sender	138
	6.3.6.3.2 Receiver	139
	6.3.6.4 Data Transfer	139
	6.3.6.4.1 Sender	139
	6.3.6.4.2 Receiver	139
	6.3.7 STASE-ROSE Protocol	140
	6.3.7.1 Abstract Syntax Definition of APDUs	140
	6.3.8 Use of GSS API with STASE-ROSE	145
	6.3.8.1 Security Context Negotiation	146
	6.3.8.2 Data Transfer Phase	147
	6.3.9 STASE-ROSE Current Status and Future Developments	148
6.4	Q3 Security	149
6.5	X.500	149
6.6	X.25	150

CHAPTER 7 EDI-Based TMN Security 153

7.1	TLS1 for EDI	153
7.2	Interactive Agent	154
	7.2.1 Message Formatting	154
	7.2.1.1 IA Status Message Detail Format	157
	7.2.1.2 Optional Message Receipts	157
	7.2.2 Message Syntax Definitions	158
	7.2.2.1 ASN.1 Syntax for Basic EDI Messages	159

7.2.2.2	ASN.1 Syntax for EDI with Message Integrity	159
7.2.2.3	ASN.1 Syntax for EDI with Non-Repudiation	160
7.2.2.4	ASN.1 Syntax for IA Status	162
7.2.2.5	ASN.1 Syntax for Optional IA Receipts	162
7.2.3	Client Specifications	163
7.2.4	Server Specifications	165
7.2.4.1	SSL Read Processing	167
7.2.4.2	Route Data to Translator	167
7.2.4.3	Receipt Logging	167
7.2.4.4	Message Validation	167
7.2.4.4.1	Message Integrity	167
7.2.4.4.2	Non-Repudiation	168
7.2.4.5	Server Disconnect	168
7.2.4.6	Example of Parsing the Received Message	168
7.2.4.6.1	Basic EDI Message	169
7.2.4.6.2	Message Integrity	169
7.2.4.6.3	Non-Repudiation	171
7.2.4.6.4	IAstatus	174
7.2.4.6.5	IAreceipt	174
7.2.5	Interfaces	175
7.2.5.1	Data Communications Protocol	175
7.2.5.2	EDI Translators	175
7.2.6	Design Considerations	176
7.2.6.1	Multiprocessing/Multithreading	176
7.2.6.2	Non-Persistent Connections	176
7.2.6.3	Resumable SSL3 Sessions	176
7.2.6.4	Connectivity	176
7.2.6.5	Message Priority	176
7.2.7	Operational Concerns	176
7.2.7.1	Security	176
7.2.7.2	Flow Control	176
7.2.7.3	Logging	176
7.2.7.3.1	Logging Levels	177
7.2.7.3.2	Log Files	177
7.2.7.4	Routing	177
7.2.7.5	Firewalls	177
7.2.7.6	Digital Certificates	177
7.2.8	Error Handling/Recovery	177
7.2.9	Implementation Issues	178
7.2.9.1	Interoperability	178
7.2.9.2	Port Assignments	178
7.2.9.3	Partner Responsibilities	178

CHAPTER 8 CORBA-Based TMN Security 179

8.1	Overview of General Inter Orb Protocol (GIOP)	180
8.2	Telecom Non-Repudiation Inter-Orb Protocol (TeNoRIOP)	180
8.2.1	Non-Repudiation for Request	181
8.2.1.1	Digest for Request	182
8.2.1.2	Digital Signature for Request	184
8.2.1.3	Strict Correlation	184
8.2.2	Non-Repudiation for Reply	185

- 8.2.2.1 Digest for Reply 186
- 8.2.2.2 Digital Signature for Reply 187
- 8.3 IDL Syntax for Non-Repudiation Evidence 188
- 8.4 Local API Interface Specification 191
- 8.5 Timing of Non-Repudiation Evidence 193
 - 8.5.1 Timing Agreements 193
 - 8.5.1.1 Non-Repudiation of Origin 193
 - 8.5.1.2 Non-Repudiation of Receipt 193
 - 8.5.1.3 Behavior While Waiting 194
 - 8.5.1.3.1 Trusting Behavior 194
 - 8.5.1.3.2 Cautious Behavior 194
 - 8.5.1.3.3 Suspicious Behavior 194
 - 8.5.1.4 Notifications 195
- 8.6 Non-Repudiation Protocol Machine 195
 - 8.6.1 Message Sender 195
 - 8.6.2 Message Receiver 196

CHAPTER 9 SNMP-Based TMN Security 197

- 9.1 SNMPv1 Security 197
- 9.2 SNMPv2 Security 198
 - 9.2.1 Proper ID Required 198
 - 9.2.2 On the Relativity of Time 199
 - 9.2.3 Secure PDUs 199
- 9.3 SNMPv3 Security 200
 - 9.3.1 User-Based Security Model 201
 - 9.3.1.1 Simple Times 201
 - 9.3.1.2 Key Items 201
 - 9.3.1.3 USM PDUs 202
 - 9.3.1.4 USM APIs 204
 - 9.3.2 View-Based Access Control Model (VACM) 206
 - 9.3.2.1 Who's Calling 206
 - 9.3.2.2 Domain of Discourse 207
 - 9.3.2.3 VACM Services 208

CHAPTER 10 Portraits Gallery 209

PART IV SECURITY MANAGEMENT 221

CHAPTER 11 Management of Security Information 223

- 11.1 Security Administration Functions 224
 - 11.1.1 Login Management 224
 - 11.1.2 Notification Management 225
 - 11.1.3 Access Control Management 225
 - 11.1.4 Management of Encryption Keys 225
- 11.2 Information Model Description 226
 - 11.2.1 Login Management 226
 - 11.2.1.1 Pre- and Post-Login Messages 226
 - 11.2.1.2 User Management 227
 - 11.2.1.3 Password Management 228

- 11.2.1.4 Channel Management 230
- 11.2.1.5 Session Management 231
- 11.2.1.6 Security MOs Management 232
- 11.2.2 Notification Management 232
- 11.2.3 Access Control 236
 - 11.2.3.1 Targets 236
 - 11.2.3.2 Rules 237
 - 11.2.3.3 Initiators 237
 - 11.2.3.3.1 Access Control Lists 237
 - 11.2.3.3.2 Capabilities 237
 - 11.2.3.3.3 Security Labels 237
 - 11.2.3.4 Authentication for Access Control 238
 - 11.2.3.5 MOs for Access Control 238
- 11.2.4 Key Management 240

PART V SECURITY OPERATIONS 243

CHAPTER 12 Security Functions and Operations 245

- 12.1 Prevention Services 245
- 12.2 Detection Security Services 246
- 12.3 Illustrative Scenarios 246
 - 12.3.1 Authentication and Access Control Scenario 246
 - 12.3.2 NEL Alarm Detection, Containment, and Recovery 248

CHAPTER 13 Security Management Functions and Operations 251

- 13.1 Prevention 252
 - 13.1.1 BML 252
 - 13.1.2 SML 254
 - 13.1.3 NML 254
 - 13.1.4 EML 254
 - 13.1.5 NEL 254
- 13.2 Detection 254
 - 13.2.1 BML 254
 - 13.2.2 SML 254
 - 13.2.3 NML 255
 - 13.2.4 EML 255
 - 13.2.5 NEL 255
- 13.3 Containment and Recovery 255
 - 13.3.1 BML 255
 - 13.3.2 SML 256
 - 13.3.3 NML 256
 - 13.3.4 EML 256
 - 13.3.5 NEL 257
- 13.4 Security Administration 257
 - 13.4.1 BML 257
 - 13.4.2 SML 257
 - 13.4.3 NML 258
 - 13.4.4 EML 258
 - 13.4.5 NEL 259

- 13.5 Security Management Scenarios 259
 - 13.5.1 Establish/Change Privileges 259
 - 13.5.2 Audit Detection of a Security Violation,
Containment, and Recovery 262

CHAPTER 14 Future Enhancements to the TMN Security 267

- 14.1 Secure Interworking 267
 - 14.1.1 Application-Based Security 267
 - 14.1.2 CMP/CORBA 268
- 14.2 Public Key Infrastructure 268
- 14.3 Internal Certification of External Entities 268
- 14.4 External Certification Authorities 268
- 14.5 Security Alarm Management 268
- 14.6 Security Audit Trail Management 269
- 14.7 X Interface Security 269
- 14.8 F Interface Security 269
- 14.9 Update of Related Standards 269

Abbreviations 271

Suggested Reading 277

References 279

Index 285

About the Author 296

List of Figures

Figure 2.1: TMN Management Functional Areas and Layers—illustrative entries	8
Figure 2.2: Functional components of an Operation System Function Block	9
Figure 2.3: Example of a TMN physical architecture	10
Figure 2.4: The lower layer of the ISO model	11
Figure 2.5: OSI layering	13
Figure 2.6: Seven layer OSI stack	14
Figure 2.7: Makeup of an Application Service Element	16
Figure 2.8: ASE service primitives	17
Figure 2.9: Application layer constituents	18
Figure 2.10: Interleaved replies to multiple requests	19
Figure 2.11: A security audit trail MO	21
Figure 2.12: Example of a management information tree	21
Figure 2.13: Example of a containment relationship	22
Figure 2.14: Example of an inheritance tree	23
Figure 2.15: Manager and agent systems	24
Figure 2.16: Symmetric CMIP interface	24
Figure 2.17: Cascading management	24
Figure 2.18: Basic setup for systems using CMISE	25
Figure 2.19: Minimum configuration for systems using SMASE	25
Figure 2:20: Example of a directory schema for a people directory	27
Figure 2.21: SNMPv3 architecture	35
Figure 2.22: Main interactions of security modules	38
Figure 4.1: Structure of MD5 for one 512-bit block	59
Figure 4.2: MD5 operating on a whole message	59
Figure 4.3: DES encryption and decryption in the ECB mode	62
Figure 4.4: DES encryption in the CBC mode	62
Figure 4.5: DES decryption in the CBC mode	62
Figure 4.6: Example of the RSA procedure	66
Figure 4.7: Signing and verifying	67
Figure 4.8: Partial order of security services	80

Figure 5.1: Life cycle of a secure communications protocol	88
Figure 5.2: In-stack secure communication protocol	90
Figure 5.3: GSS out-of-stack secure communications protocol	90
Figure 5.4: GSS-API handshaking sequence	91
Figure 5.5: GSS-API secure transfer phase	92
Figure 5.6: SSL3 handshake protocol	96
Figure 5.7: Example of tunnel mode authentication and transport mode encryption	101
Figure 6.1: Encryption in the application	116
Figure 6.2: Negotiation of security algorithms	129
Figure 6.3: SR-TRANSFER Service Primitives	133
Figure 6.4: Interaction during association establishment	136
Figure 6.5: Interaction during association release	137
Figure 6.6: Interaction during association abort	138
Figure 6.7: Interaction during data transfer	139
Figure 6.8: Use of GSS-API with STASE-ROSE at association establishment time	146
Figure 6.9: Use of GSS-API with STASE-ROSE during data transfer	147
Figure 7.1: IA Client-server interaction	155
Figure 7.2: Message format architecture for mandatory messages	156
Figure 8.1: Non-Repudiation for request	182
Figure 8.2: Non-Repudiation for reply	185
Figure 8.3: Message sender protocol machine	195
Figure 8.4: Message receiver protocol machine	196
Figure 9.1: Secure Gateways (SG) protecting TMN entities	197
Figure 9.2: Using hashing for encryption/decryption	203
Figure 9.3: A view tree family	207
Figure 10.1: TMN security communications protocols	209
Figure 10.2: GULS—for all OSI-compliant protocols	210
Figure 10.3: SSL3/TLS1 for TCP/IP only	211
Figure 10.4: IPsec—for IP only	212
Figure 10.5: TR40—for ACSE-using protocols	213
Figure 10.6: Application-Based Security—for CMIP only	214
Figure 10.7: STASE-ROSE for ROSE-based protocols	215
Figure 10.8: GSS-API	216
Figure 10.9: Interactive Agent—for EDI only	217
Figure 10.10: TeNorIOP—for CORBA only	218
Figure 10.11: SNMPv2 and SNMPv3 security	219
Figure 11.1: Example of security manager and managed systems	223
Figure 11.2: Possible name bindings (containment) for login management MOs	227
Figure 11.3: Notification management interactions	235
Figure 11.4: Inheritance of notification management MO classes	235
Figure 11.5: Possible name binding for notification management MOs	236
Figure 11.6: Access control MO class inheritance hierarchy	239
Figure 11.7: Relationship of access control MOs	239
Figure 12.1: Authentication and access control	247
Figure 12.2: NE alarm detection of a security violation, containment, and recovery	249
Figure 13.1: Partitioning of TMN security functionality	252
Figure 13.2: Establish/change privileges	260
Figure 13.3: Audit detection of a security violation, containment, and recovery	263

List of Tables

Table 3.1: Summary of Security Threats and Risks	45
Table 3.2: Security Services against Security Threats	54
Table 3.3: Security Services Correlated with Security Risks	55
Table 4.1: Security Mechanisms to Provide Security Services	78
Table 4.2: Security Mechanisms to Protect against Security Threats	79
Table 5.1: Context-Level Calls	92
Table 5.2: Per-Message Calls	93
Table 5.3: Credential Management Calls	93
Table 5.4: Support Calls	93
Table 5.5: Fatal Error Codes	94
Table 5.6: Informatory Status Codes	94
Table 6.1: Negotiated Algorithms	128
Table 6.2: Encryption-Type Values	133
Table 6.3: Components of EncryptionParameters	134
Table 9.1: IN and OUT Parameters of USM Service Primitives	204
Table 9.2: IN and OUT Parameters for USM Authentication Primitives	205
Table 9.3: IN and OUT Parameters for Privacy Primitives	206
Table 13.1: Security Management	253