Índice

Prólogo 11

Introducción y objetivos 13

Capítulo I Seguridad en comunicaciones GSM 15

1. Arquitectura de GSM 15

MS – Mobile Station 16

BSS – Base Station Subsystem 16

NSS – Network and Switching Subsystem 17

Identificadores de las MS 18

Pila de protocolos 19

Protocolos MS⇔BTS 19

Protocolos BTS⇔BSC 20

Protocolos BSC⇔MSC 20

2. Nivel físico 21

Descripción 21

Modulación 22

MAC: subnivel de acceso al medio 25

Bandas de frecuencia GSM 26

FDMA: división de la banda de frecuencias 26

TDMA: multiplexación en el tiempo 32

Canales físicos y canales lógicos 34

3. El nivel de Red 42

Modo idle y modo dedicado 42

Nivel RR 44

Nivel MM 50

4. Short Messages Services 53
Arquitectura del servicio 53
Contenido de un SMS 53
WAP – Wireless Application Protocol 53
MMS – Multimedia Messaging Service 55
5. El interfaz ME-MS 56
6. Aspectos de seguridad contemplados en GSM 58
Seguridad del protocolo GSM 58
Autenticación GSM 58
Cifrado de las comunicaciones GSM 62
7. Ataques contra comunicaciones GSM 69
Debilidades GSM 69
Infiltración en la red del operador 70
Escucha del canal de radio (señalización) 71
Escucha del canal de radio (datos) 74
Ataque contra la SIM para obtener Ki (con acceso físico) 75
Ataques criptográficos 75
Ataques mediante SMS 85
Suplantación de usuarios 87
Ataque mediante estación base falsa 88
Ataques a la banda Banda Base 102

Capítulo II GPRS 103
1. Introducción a GPRS 103
Dominio de conmutación de circuitos versus dominio de conmutación de paquetes 104
Arquitectura de GPRS 105
El tráfico de datos GPRS 107
EDGE 108
GPRS Routing Area 110
Pila general de protocolos GPRS 111
2. Nivel Físico 112
TDMA 112
Canales lógicos 112
Mapeo de canales lógicos a canales físicos 114

Información de broadcast ... 116
3. Nivel RR ... 117
TBF (Temporary Block Flow) ... 119
4. Nivel LLC ... 120
5. Nivel GMM ... 121
Procedimientos del nivel GMM ... 122
Coordinación de los niveles MM←→GMM ... 122
Identificadores de MS en el nivel GMM ... 122
Estados GMM ... 123
Selección y reselección de celda ... 124
Procedimiento GPRS Attach ... 125
Procedimiento Routing Area Update ... 127
6. Direcciones IP ... 130
Contextos PDP ... 130
El interfaz SGSN ←→ GGSN: GTP ... 132
7. Aspectos de seguridad de GPRS ... 132
Confidencialidad de la identidad del usuario ... 132
Autenticación del usuario ... 133
Cifrado ... 133
8. Ataques ... 136
Ataques activos contra la red core ... 136
Ataques pasivos y semipasivos ... 139
Ataques activos mediante estación base falsa ... 141

Capítulo III UMTS ... 149
1. Introducción a UMTS ... 149
Arquitectura ... 149
Protocolos ... 153
Organización jerárquica ... 155
2. El nivel físico ... 156
Esquema de acceso de radio ... 156
Establecimiento de un canal de radio (RRC protocol) ... 159
Canales físicos, lógicos y de transporte ... 161
HSPA ... 162

3. El nivel MM 164
Gestión de movilidad 164
Reglas de medición 164
Reselección de celda Intra-RAT 165
Reselección de celda inter-RAT, caso GERAN→UTRAN 165
Reselección de celda inter-RAT, caso UTRAN→GERAN 167
Handover 169
4. Aspectos de seguridad 169
Confidencialidad de la identidad del usuario 170
Autenticación y establecimiento de clave 172
Cifrado 178
Protección de integridad 182
Datos de autenticación en el paso entre celdas 184
Datos de autenticación en el handover 186
5. Ataques 189
Ataque pasivo contra handover 189
Ataque activo contra handover 189
Ataque mediante estación base falsa GSM a USIM con soporte para autenticación GSM 190
Ataque mediante estación base falsa GSM a USIM sin soporte para autenticación GSM 191
Ataque mediante estación base falsa UMTS (femtocelda) 194
Otros ataques basados en femtoceldas UMTS 196
Ataques mediante estación base falsa UMTS 198
Viabilidad de una implementación práctica de los ataques con estación base falsa 3G 204

Capítulo IV 4G 205
1. Introducción a 4G 205
Predecesores y tecnologías candidatas 206
LTE y LTE-Advanced 207
E-UTRAN 208
SAE 212
2. Seguridad en 4G 213
Aspectos generales 213
Contexto de seguridad EPS 216
Jerarquía de claves 217

■ ■ ■

Procedimiento de autenticación y establecimiento del cifrado (EPS AKA) 218
Confidencialidad de la identidad del usuario 219
Confidencialidad de los datos de señalización y usuario 219
Integridad 220
Ataques contra LTE 223

Capítulo V Conclusiones y recomendaciones 225
1. Resumen del estado de la seguridad en las comunicaciones móviles 2G/3G-UMTS/4G-LTE 225
2. Recomendaciones para mitigar las vulnerabilidades estudiadas 226
Configuración del terminal para que sólo utilice 3G o superior 226
Desarrollo de software de aviso del modo de cifrado para terminales 227
Soluciones basadas en la detección de estaciones base falsas 228
Soluciones basadas en cifrado a través de los canales CSD de GSM 229
Soluciones basadas en VoIP cifrado 230
Protección de las comunicaciones de datos en niveles superiores 230
Instalación de software de protección en los dispositivos habilitados para comunicaciones de datos móviles 231
Inclusión de los dispositivos con conexión a redes móviles en las políticas de seguridad de las organizaciones 232

Referencias 233

Índice alfabético 259

Otros libros de interés 267