

# CONTENIDO

---

<b>Introducción</b> .....	<b>xix</b>
<b>Prefacio</b> .....	<b>xxiii</b>
<b>Agradecimientos</b> .....	<b>xxvii</b>
<b>Acerca de los autores</b> .....	<b>xxxii</b>
<b>Capítulo 1 ¿Por qué son diferentes las comunicaciones inalámbricas? .....</b>	<b>1</b>
Introducción .....	1
Protección de los medios de comunicación .....	2
Protección de la intimidad .....	3
Promoción de la seguridad física .....	5
Lo personal y lo público .....	6
La modificación del statu quo .....	7
Previsiones para el sector inalámbrico.....	9
Grados razonables de seguridad .....	10
Problemas y restricciones de carácter legal .....	11
Normativa legal relativa a la seguridad .....	12
Factores de mercado relativos a la seguridad .....	12
Directrices sobre medidas de seguridad.....	13
Redes celulares y tecnologías portadoras .....	16
Tecnologías inalámbricas de primera generación (1G) .....	20
Tecnologías inalámbricas de segunda generación (2G).....	21
Expansión de espectro .....	24
Acceso múltiple por división de código (CDMA).....	25
Acceso múltiple por división del tiempo (TDMA).....	26
Sistema global de comunicaciones móviles (GSM) .....	28

Entornos inalámbricos de tercera generación (3G).....	29
SMS (Short Message Service, servicio de mensajes cortos) .....	30
Entornos inalámbricos de cuarta generación (4G).....	33
Resumen.....	34
<b>Capítulo 2 La guerra de la información en los entornos inalámbricos .....</b>	<b>37</b>
La guerra de la información inalámbrica.....	37
Algunas definiciones de utilidad .....	38
Clasificación de las redes de comunicación inalámbricas .....	42
Esquema de clasificación basado en la arquitectura de red .....	44
Sistemas inalámbricos con una infraestructura fija de soporte .....	44
Sistemas inalámbricos en que los usuarios se comunican directamente mediante uno o más satélites .....	44
Redes de datos inalámbricos completamente móviles .....	45
Sistemas inalámbricos sin otra infraestructura de soporte que los propios nodos móviles.....	46
Clasificación según el tipo de movilidad.....	46
Movilidad restringida con estaciones base fijas .....	47
Redes completamente móviles .....	48
Redes de conmutación de circuitos y redes de conmutación de paquetes .....	48
Teoría de la información .....	50
Entropía .....	51
Capacidad en las redes móviles .....	53
Eficiencia espectral.....	54
Teoría de la decisión .....	58
Gestión de riesgos y arquitectura de seguridad de la información (INFOSEC).....	59
Análisis de riesgos.....	60
Vulnerabilidad .....	61
Amenazas .....	61
Contramidas .....	61
Impacto .....	62
Modelo para una gestión de riesgos económicamente eficiente.....	63
Amenazas tradicionales a los servicios inalámbricos.....	65
¿Por qué es diferente la seguridad en los entornos inalámbricos? .....	66
Seguridad del nivel físico .....	68
Niveles de enlace de datos y de red.....	68
Seguridad de nivel de transporte .....	68
Seguridad del nivel de aplicación.....	69
Medidas de rendimiento y principales compromisos de diseño .....	70
Medidas de rendimiento de alto nivel.....	71
Medidas de rendimiento de bajo nivel .....	72
Ataques de red típicos.....	72
Ataques criptográficos .....	79

Medida de defensa criptográficas .....	81
Gestión de claves .....	84
Amenazas de captura electromagnética .....	85
Resumen.....	87
<b>Capítulo 3 Vulnerabilidades de los sistemas telefónicos .....</b>	<b>89</b>
Facilidad de interceptación .....	90
Interrupción del servicio .....	91
Interrupciones no intencionadas .....	92
Desastres naturales.....	93
Huracanes .....	93
Tornados .....	93
Tormentas de invierno .....	94
Inundaciones.....	94
Terremotos .....	95
Fuego .....	95
Apagones .....	95
Fallos de software.....	96
Interrupciones intencionadas .....	96
Piratería telefónica.....	97
Aspectos legales .....	98
Leyes en los Estados Unidos .....	98
Intimidad .....	98
Criptografía .....	100
Interferencias intencionadas .....	101
El conflicto entre libertad de expresión y confidencialidad en la telefonía celular .....	102
¿Quién está llevando a cabo la interceptación?.....	102
El ciudadano corriente.....	103
Teléfonos inalámbricos.....	103
Teléfonos celulares .....	104
Amigos y vecinos: interceptación no intencionada.....	104
Sistemas de voz .....	104
Sistemas de datos.....	105
Actividades criminales .....	106
Fraude .....	107
Buscapersonas .....	108
Cárteles de la droga .....	108
El campo militar en los Estados Unidos.....	109
Otros países .....	110
ECHELON .....	113
Estaciones terrestres de ECHELON.....	113
Futuras líneas de investigación.....	115
Fuerzas de seguridad .....	116

Aplicaciones .....	117
Vulnerabilidades de los sistemas telefónicos .....	118
Interferencias intencionadas .....	118
Interceptación .....	120
Contra medidas para las interferencias y la interceptación .....	120
Acceso múltiple por división de código (CDMA) .....	122
¿Quién escucha las conversaciones de los teléfonos celulares? .....	122
Fraude .....	123
Contra medidas para el fraude .....	123
Historia de los teléfonos inalámbricos .....	124
Características de los aparatos telefónicos .....	125
Vulnerabilidades de los aparatos móviles .....	125
Contra medidas .....	127
Micrófonos .....	128
Tipos de micrófonos .....	128
Utilización de los micrófonos .....	129
Contra medidas .....	131
Comunicación de datos por radiofrecuencia .....	132
Corto alcance: menor de 30 metros .....	132
Rango medio: de 50 a 300 metros .....	133
La cuestión de la intimidad .....	134
Resumen .....	134
<b>Capítulo 4 Comunicaciones vía satélite .....</b>	<b>137</b>
Historia .....	137
Órbitas de los satélites .....	139
Órbitas geoestacionarias .....	139
Órbita altamente elíptica .....	141
Baja órbita terrestre/media órbita terrestre .....	142
Navegación y seguimiento .....	144
Sistema de posicionamiento global .....	144
Sistema de aumentación de área extensa .....	145
Búsqueda y rescate vía satélite .....	145
Comunicaciones: voz, vídeo y datos .....	146
Voz .....	146
Vídeo, audio y datos .....	147
Internet vía satélite .....	148
Sensores terrestres: imágenes comerciales .....	149
Landsat .....	149
SPOT .....	149
European Remote Sensing .....	150
IKONOS .....	150
Gestión del espectro para los satélites .....	151

Instrumentos y objetivos de la actual política de cifrado para satélites en los Estados Unidos .....	153
Cuestiones asociadas con la política actual de los Estados Unidos.....	153
Estándares FIPS .....	154
Cuestiones de política internacional .....	156
Controles de exportación para cifrado vía satélite: objetivos de los Estados Unidos .....	156
Mecanismos de licencia y lista USML.....	157
Impacto de los controles de exportación .....	157
¿Son efectivos los controles de exportación? .....	159
Cuestiones legales relativas al cifrado vía satélite: intimidad .....	159
Delitos informáticos.....	161
Vigilancia.....	161
Patentes.....	162
Cifrado de clave pública para comunicación vía satélite .....	162
Custodia de claves para comunicación vía satélite.....	163
Impacto sobre la seguridad de la información y sobre las fuerzas y cuerpos de seguridad .....	164
Importancia de la explotación y control del espacio para los Estados Unidos.	165
Disuasión .....	165
Defensa nacional e internacional .....	166
Vigilancia .....	166
Desarrollo, implementación y gestión de estrategias y opciones de cifrado avanzado para satélite .....	166
Planificación, detalles e implementación .....	166
Opciones de servicio para los consumidores de datos .....	170
Marco de trabajo para las cuestiones de política de utilización.....	170
Protección de la intimidad y de los datos personales .....	172
Seguridad de los sistemas de información .....	174
Protección de la propiedad intelectual.....	177
Ejemplo de sistemas de seguridad basados en hardware.....	179
Compromiso entre la tecnología de la información, la seguridad nacional y la intimidad personal.....	180
Una revolución en marcha.....	180
Problemas y potencialidades .....	181
Vulnerabilidad de la información .....	182
Importancia de la información .....	183
Los riesgos existentes.....	184
Guerra de la información.....	184
Resumen.....	185
<b>Capítulo 5 Seguridad criptográfica .....</b>	<b>187</b>
Ocultación.....	188
Principios fundamentales .....	189

Analogía de la llave y la cerradura .....	190
Claves de transposición .....	192
Claves de sustitución .....	193
Principios de Kerckhoff .....	194
Sistemas de cifrado combinados .....	195
Criptanálisis clásico .....	196
Criptografía digital.....	198
Generación de números pseudoaleatorios.....	202
¿Qué es aleatorio? .....	203
Generadores de números pseudoaleatorios.....	204
Semillas para números aleatorios y entropía .....	205
¿Podemos utilizar la semilla como clave? .....	206
El cuaderno de un solo uso .....	207
El sistema DES .....	208
El efecto de avalancha .....	210
Un estándar contra las cuerdas: DES ya no es suficientemente fuerte .....	211
Técnicas modernas de ruptura de un sistema de cifrado .....	212
Velocidad de procesamiento de las claves .....	212
Ataques por fuerza bruta.....	213
Ataques estándar .....	215
Ataques avanzados.....	217
Dos límites para el cifrado .....	218
Cifrado de bloque y cifrado de flujo.....	219
Consideraciones de diseño de los sistemas de cifrado de flujo .....	221
El problema de sincronización de los sistemas de cifrado de flujo .....	223
Sumarizaciones de mensaje no basadas en clave.....	224
SHA .....	226
SHA-1 en el modo de cifrado .....	226
HORNET .....	227
Descripción del acumulador de entropía .....	229
Generación del sincronismo, del relleno y de las claves del cifrado de datos... ..	231
AES (Advanced Encryption Standard) .....	235
Gestión de claves: generación y distribución de claves.....	237
Sistemas de clave pública: la segunda revolución .....	240
Sistema de distribución de clave pública y algoritmo de Diffie-Hellman .....	241
Firmas digitales.....	242
Autoridades de certificación .....	243
Utilización de criptografía de clave pública para la gestión de claves .....	245
Algoritmos .....	245
Dificultad de los sistemas matemáticos .....	247
Sistemas de factorización entera.....	248
Seguridad .....	248
Implementación .....	249
Sistemas basados en logaritmos discretos .....	250
Seguridad.....	250

Implementación .....	251
El criptosistema de curvas elípticas (ECC).....	251
Seguridad.....	253
Implementación.....	253
Comparación de los sistemas criptográficos de clave pública.....	254
Eficiencia .....	256
Requisitos de procesamiento .....	256
Comparación de los tamaños de clave.....	256
Ancho de banda .....	257
El problema de los logaritmos discretos sobre curvas elípticas en los dispositivos inalámbricos.....	258
Generación de claves en los dispositivos inalámbricos para los tres tipos de sistemas de clave pública.....	259
Ancho de banda en los dispositivos inalámbricos .....	259
Escalabilidad.....	260
Potencia de procesamiento.....	261
Tarjetas inteligentes .....	262
Redes de telefonía celular .....	264
Dispositivos PDA/computadoras de mano .....	265
BSAFE Crypto-C.....	266
Criptografía en hardware embebido: dispositivos FPGA y ASIC .....	267
Panorámica de las FPGA .....	269
Criptografía basada en FPGA.....	270
Resultados.....	271
Resumen.....	273
<b>Capítulo 6 Criptología de la voz.....</b>	<b>275</b>
Todo empezó con SIGSALY.....	275
El Forschungsstelle de Vetterlein .....	277
Digitalización de la información de voz mediante SIGSALY .....	279
Panorámica del proceso de cifrado de SIGSALY para un único canal de vocoder .....	284
Criptología de las señales de voz.....	285
El habla: producción y propiedades no lingüísticas .....	286
La estructura del lenguaje.....	287
Fonemas .....	288
Lingüística histórica .....	289
Sistemas de escritura.....	290
Modelo clásico fuente-filtro .....	293
Modelo general fuente-filtro.....	294
Espectrograma continuo de la voz.....	295
Muestreo de la forma de onda de voz.....	299
La transformada de Fourier .....	306
Transformada rápida de Fourier (FFT).....	308

Aplicación de una ventana a los segmentos de señal .....	308
Modelado de predicción lineal .....	311
Cuantización y PCM .....	313
Transmisión de señales de voz .....	316
Sincronización .....	316
Criptografía de las señales de voz .....	318
Cifradores analógicos .....	319
Inversores de frecuencia .....	320
Divisores de banda .....	321
Divisor de doble banda.....	321
Desplazador de banda.....	322
Inversor de banda .....	323
Inversor-desplazador de banda .....	323
Divisor de n bandas .....	323
Cifrados basados en transformadas .....	327
Cifradores en el dominio del tiempo (TDS).....	328
Cifrado de elementos temporales .....	330
Salto de ventana.....	331
Ventana deslizante .....	333
Cifradores bidimensionales.....	333
Cifradores digitales.....	335
Codificación de fuente de la voz .....	337
Vocoder de formantes .....	337
Vocoder de canal.....	338
Vocoder de predicción lineal (LP).....	339
Coeficientes de reflexión.....	341
Coeficientes de cociente logarítmico de área .....	341
Modelo sinusoidal .....	343
Análisis de parámetros sinusoidales .....	344
Estándares.....	345
Criptoanálisis de los sistemas de voz .....	345
Herramientas y parámetros para el criptoanálisis de la voz .....	346
Aplicación del espectrógrafo de sonido al criptoanálisis .....	347
Métodos analógicos .....	351
Criptoanálisis de los sistemas de cifrado digital.....	351
Cancelación de ruido .....	352
Criptoanálisis de los vocoders basados en técnicas de predicción lineal ..	353
Consideraciones acerca del criptoanálisis de los sistemas de clave pública	354
Criptoanálisis del algoritmo A5.....	354
Resumen.....	355
<b>Capítulo 7 WLAN: redes inalámbricas de área local .....</b>	<b>357</b>
Medios de transmisión inalámbrica .....	359
Sistemas infrarrojos .....	359



Sistemas de radio de banda estrecha .....	359
Sistemas de radio de banda ancha: expansión de espectro.....	360
Expansión de espectro por salto de frecuencia (FHSS).....	360
Expansión de espectro por secuencia directa (DSSS).....	361
Productos y estándares WLAN.....	362
¿La seguridad del estándar 802.11?.....	362
IEEE 802.11b.....	363
Cómo dotar de seguridad a las redes WLAN.....	364
Escuchas ilegales .....	364
Acceso no autorizado .....	364
Interferencias aleatorias e intencionadas .....	365
Amenazas físicas .....	366
Contramidas .....	367
Expansión de espectro por salto de frecuencia (FHSS).....	367
Expansión de espectro por secuencia directa (DSSS).....	368
Infrarrojos (IR) .....	370
Sistemas de banda estrecha .....	370
El estándar WEP .....	371
Cifrado.....	371
Autenticación.....	373
Defectos conocidos del protocolo WEP.....	375
Otras técnicas de autenticación .....	375
Seguridad física.....	376
Resumen.....	377
<b>Capítulo 8 Protocolo de aplicaciones inalámbricas (WAP) .....</b>	<b>379</b>
Comparación de los modelos TCP/IP, OSI y WAP.....	380
Cómo funciona WAP.....	383
Estado de las cuestiones de seguridad en WAP.....	384
Virus .....	387
Autorización .....	388
No repudio .....	388
Autenticación.....	389
Sesiones seguras .....	389
Productos de seguridad.....	389
ClearTrust control, de Securant Technologies.....	393
Arquitectura de seguridad WAP.....	394
Seguridad marginal .....	395
Acceso inalámbrico a Internet .....	395
Middleware inalámbrico.....	395
Resumen.....	396

<b>Capítulo 9 Seguridad en el nivel de transporte inalámbrico (WTLS) .....</b>	<b>397</b>
Secure Sockets Layer .....	397
Protocolo de registro.....	399
Protocolo de negociación SSL.....	400
Seguridad de nivel de transporte .....	401
Ventajas y desventajas de SSL/TLS .....	402
Netscape .....	403
Microsoft .....	403
Entrust .....	403
EAP-TLS .....	403
Alternativas a SSL/TLS.....	406
IP Security (IPSec) .....	406
Protocolo AH.....	407
Protocolo ESP.....	408
Modos de transporte y de túnel .....	408
Shell segura (SSH) .....	409
Protocolo de nivel de transporte SSH.....	410
Comparación entre las implementaciones SSH y TLS.....	411
Protocolo LEAP .....	412
Seguridad del nivel de transporte inalámbrico y WAP .....	413
Fundamentos de la seguridad del nivel de transporte inalámbrico.....	414
Protocolo de negociación WTLS.....	415
Protocolo de alerta WTLS .....	416
Protocolo de cambio de cifrado WTLS .....	416
Ventajas y desventajas de WTLS .....	417
Vulnerabilidades de WTLS .....	417
Implementaciones de WTLS .....	418
Información adicional .....	420
 <b>Capítulo 10 Bluetooth .....</b>	 <b>421</b>
Especificaciones básicas de Bluetooth .....	422
Tecnología Bluetooth .....	422
Desarrollo de las especificaciones Bluetooth .....	423
Decisiones de diseño .....	424
Picorredes.....	426
Arquitectura de seguridad de Bluetooth .....	427
Redes dispersas .....	429
La pila de protocolos Bluetooth .....	430
Funciones de seguridad en el nivel de banda base.....	431
Funciones de seguridad del protocolo de descubrimiento de servicios .....	433
Funciones de seguridad en el nivel de enlace .....	434
Saltos de frecuencia .....	435
Establecimiento del canal .....	436

Gestor de seguridad .....	438
Autenticación .....	441
Autenticación con el cifrado de bloque SAFER+.....	443
Cifrado .....	444
Modos de cifrado .....	444
Negociación de la longitud de clave .....	445
Cifrado con el sistema de cifrado de flujo E <sub>0</sub> .....	446
Amenazas a la seguridad de Bluetooth .....	448
Interferencias intencionadas .....	449
Agujeros de seguridad de Bluetooth.....	449
Resumen y evaluación de seguridad .....	451
<b>Capítulo 11 Voz sobre IP.....</b>	<b>453</b>
VoIP en general .....	453
El atractivo de VoIP .....	453
Estándares VoIP .....	454
El ascenso de las tecnologías VoIP .....	455
Tráfico de red.....	458
El dilema de la facturación y la interoperabilidad.....	458
Interoperabilidad.....	459
Tarifas de larga distancia competitivas.....	459
Problemas de implementación.....	459
Los fabricantes.....	460
Problemas técnicos para las llamadas con VoIP .....	464
Codificación de la voz.....	464
Vulnerabilidades de seguridad de las redes de voz.....	464
Características de confidencialidad, integridad y disponibilidad .....	465
VoIP y el entorno de seguridad inalámbrico .....	465
Redes privadas.....	466
WEP.....	466
Confidencialidad, integridad y disponibilidad en las implementaciones VoIP .....	466
Suplantación IP.....	467
Intercepción y escuchas en las transmisiones de voz a través del aire.....	468
Denegación de servicio.....	469
Resumen.....	470
<b>Capítulo 12 Perspectivas hardware para la seguridad extremo a extremo en las aplicaciones inalámbricas .....</b>	<b>471</b>
Clasificación de los sistemas de comunicaciones.....	473
Arquitecturas cliente-servidor y arquitecturas igualitarias .....	473
Comunicaciones basadas en conmutación de circuitos y en conmutación de paquetes o tramas .....	475

Difusión y unidifusión .....	481
Comunicaciones terrestres e inalámbricas .....	484
Medio de transmisión (punto a punto, LAN, WAN o LAN-WAN-LAN) .....	485
Naturaleza de la transmisión: diferencias entre voz y datos (de audio, de vídeo y alfanuméricos) .....	486
Cantidad, velocidad y predecibilidad de la información transmitida .....	494
Seguridad de las comunicaciones sensible al protocolo .....	495
Evolución hacia los entornos inalámbricos .....	500
Estructuras de cifradores para dispositivos inalámbricos .....	501
Intercepción y vulnerabilidad en los sistemas inalámbricos.....	502
Técnicas ESM para comunicaciones y receptores de intercepción .....	506
CVR .....	506
IFM .....	507
Superheterodino de banda estrecha con sintonización YIG .....	508
Superheterodino de banda ancha con sintonización YIG .....	509
Receptor ESM con análisis espectral .....	509
Receptor canalizado.....	510
Receptor compresivo .....	510
Receptor de célula Bragg acusto-óptica .....	511
Tecnología SAW .....	511
Intercepción de sistemas de expansión de espectro por secuencia directa .....	515
Intercepción de sistemas de salto de frecuencia .....	517
Reconocimiento de la modulación y procesamiento de salida de un sistema COMINT .....	522
Enfoque basado en la teoría de la decisión .....	526
Señales con modulación analógica .....	527
Señales moduladas digitalmente.....	527
Enfoque basado en redes neuronales .....	529
Implicaciones .....	530
AMPS (Advanced Mobile Phone Services) .....	530
TDMA (Time Division Multiple Access) IS-136 .....	530
GSM .....	531
CDMA de banda ancha y de banda estrecha .....	532
Transmisión encubierta .....	533
Conclusiones .....	534
<b>Bibliografía .....</b>	<b>537</b>
<b>Índice .....</b>	<b>547</b>