

INDICE

Acerca del Autor	vii
Prefacio	xix
Notas a la versión española	xxi
1. Introducción a los Estándares de Seguridad de las Redes Locales Inalámbricas	1
Comunicaciones inalámbricas: definición	3
Factores de seguridad	3
Robo	4
Control de accesos	4
Autenticación	5
Encriptación	5
Barreras	6
Sistemas de detección de intrusiones	7
IEE	7
WECA	7
Wi – Fi	8
Las múltiples variantes del estándar 802.11	8
FHSS	9
DSSS	10
OFDM	11
Bluetooth	11
Diferencias ente los estándares inalámbricos	12
Conclusión: el papel de la seguridad	12
2. Tecnología	15
Comparaciones	17
homeRF	17
802.11 frente a SWAP	17
La especificación SWAP	18
Integración de voz y datos inalámbricos	18
Bluetooth	18
Hacking inalámbrico	19
NetStumbler	19
Usos del programa NetStumbler	20
Script Kiddies	21
Hechos	21
Tecnología Bluetooth	21
Historia de Bluetooth	22
¿Dónde esta la gracia de Bluetooth?	23
Los saltos de espectro de Bluetooth	24
Conexiones en Bluetooth	24
Cómo reforzar la seguridad	26
¡Conéctame!	26
Conclusión: el futuro de las WLAN	27
3. Factores de Seguridad en las LAN Inalámbricas	29
Activación de la seguridad mediante encriptación	32
Encriptación WEP	32
¿Puede encriptarse 802. 11b?	33

Tarjetas de interfaz de red (NIC)	33
Hawking entre plataformas	33
Escuchas no autorizadas	35
¡Intrusión!	35
Usurpación de personalidad	36
Ataques inalámbricos de denegación de servicios (DoS)	36
Puntos vulnerables	37
La mejor defensa ante un ataque	39
Conclusión: Cómo mantener segura una WLAN	41
4. Problemas en la Seguridad Inalámbrica	43
El estado de la seguridad en las LAN inalámbricas	45
La seguridad de la WLAN	45
Autenticación de datos	46
Autenticación del cliente en un sistema cerrado	47
Autenticación mediante clave compartida	48
RC4	48
Cómo asegurar la privacidad	48
Integridad de los datos	49
Gestión de las claves	50
Vulnerabilidad de la WLAN	51
Ataques sutiles	52
Fallos comunes de seguridad	52
¡Poca seguridad es mejor4 que ninguna!	52
Claves cortas	52
Vectores de inicialización	52
Claves compartidas	53
Comprobación de paquetes	53
Autenticación	53
¡Ubicación!	54
Pautas de ataques activos	54
Ataques pasivos	55
Conclusión	55
5. Definición del Estándar 802.11	57
El estándar 802.11	59
Problemas a considerar	59
La ampliación de estándar de red	61
Redes ad hoc	62
Conjunto extendido de servicios	62
El estándar inalámbrico vía radio	62
El algoritmo estándar	63
Espacios de direccionamiento	63
La seguridad en el estándar 802.11	64
Encriptación	65
Tiempos y gestión de energía	65
Velocidad	66
Compatibilidad	66
Variantes al estándar de 802.11	67
802.11a	67

802.11b	67
802.11d	68
802.11e	68
802.11f	68
802.11g	69
802.11h	69
802.11i	70
Conclusión: Evolución de estándar 802.11	70
6. La Infraestructura de Seguridad de 802.11	71
Seguridad en aplicaciones inalámbricas punto a punto a punto	73
Punto de interceptación	73
Vulnerabilidad inalámbrica	74
La construcción de una infraestructura inalámbrico privada	77
Encriptación vulnerable	77
Infraestructura de seguridad en el comercio	77
Construcción de una infraestructura privada	78
Elementos a proteger	78
Despliegue de la infraestructura inalámbrica	78
Análisis de requerimientos	79
Elección de la variante de 802.11	80
Diseño de la seguridad	82
Monitorización de la actividad	83
Conclusión: el mantenimiento de un infraestructura segura	83
7. La Encriptación 802.11 y la Privacidad Equivalente al Cableado (WEP)	85
¿Por qué WEP?	87
Defensa de los sistemas	87
Funcionamiento de WEP	89
Encriptación para seguridad inalámbrica	89
Claves inseguras	90
El tema de las prestaciones	90
Autenticación inalámbrica	91
Imperfecciones WEP conocidas	93
Control de accesos	93
Seguridad IRL	94
Puntos vulnerables	94
Conclusión: La búsqueda de la seguridad en un mundo inseguro	95
8. Acceso no Autorizados y Privacidad	97
La privacidad, amenazada	99
Ataques pasivos	99
Monitorización de la emisión	100
Ataques activos	101
El <<falso>> punto de acceso	101
Privacidad de datos	102
Compromisos de la privacidad en lugares públicos	102
Protección de la privacidad	103
¿Pública o privada?	104
Una computación más segura	104

El factor <<humano>>	105
Definición de los puntos básicos de una política de seguridad	106
Formación	107
Seguridad física	107
Alcance inalámbrico	108
Conclusión: controles de acceso de sentido común	110
9. La Autenticación en Sistemas Abiertas	113
¿Qué es la autenticación en un sistema abierto?	115
Redes 802.11 en Windows XP	115
Gestión de usuarios	115
Gestión de claves en un sistema abierto	118
Problemas de autenticación	118
Algoritmos de encriptación de 802.11b	119
Soporte a la autenticación	119
Autenticación mediante clave compartida	120
Claves secretas	120
El algoritmo WEP	120
Vulnerabilidad estáticas	121
Seguridad NIC	121
Configuraciones de gestión de energía de las NIC inalámbricas	121
Autenticación de sistema abierto a WEP	122
Control de acceso a la red basado en puertos	123
Identificación segura del tráfico inalámbrico	124
Protocolo de autenticación extensible	124
Conclusión: Autenticación de sistema abierto frente a autenticación en sistema cerrado	126
10. Expansión de Espectro por Secuencia Directa	127
DSSS 802.11	129
Estandarización	129
Niveles MAC	130
CSMA	130
Roaming	131
Requerimientos de energía	131
Cómo aumentar la transmisión de datos	132
Seguridad en FHSS	134
Secuencias de salto	134
FHSS frente a DSSS	135
Asignación de frecuencias	135
Seguridad en sistemas abiertos	137
Todo es cuestión de... tiempos	137
Roaming entre sistemas	138
Conclusión: ¡Seguridad es el espectro!	139
11. Consideraciones sobre Equipos WiFi	141
Problemas en el despliegue WiFi	143
Proveedores de equipos inalámbricos	143
Consideraciones sobre equipamiento WLAN	144
Proveedores de equipos	146
Tendencias de mercado	146

Problemas tecnológicos	147
Configuración centrada en los puntos de acceso	147
Configuración de dispositivos móviles	148
Extensiones a los puntos de acceso	149
Transmisiones direccionales	149
Consideraciones sobre costes	149
Los costes de una seguridad efectiva	150
Seguridad cableada frente a seguridad inalámbrica	152
Pruebas de proveedores	152
Conclusión: la próxima generación de equipos inalámbricos	153
12. Seguridad Multiplataforma para el Usuario Inalámbrico	155
Aplicaciones de asignación de WLAN	157
Consideraciones sobre costes	157
WLAN de Macintosh	158
Windows OS	159
Orinoco Wireless	160
Dispositivos de mano	161
Problemas de seguridad inalámbrica multiplataforma	161
Colisiones de vectores de inicialización	162
Reutilización de las claves	162
Paquetes malignos	162
Desencriptación en tiempo real	162
Problemas de seguridad en 802.11	163
Conectividad inalámbrica de Windows XP	165
Autenticación WEP en Windows XP	165
Funcionalidades inalámbricas en Windows XP	166
Proveedores de NIC para WLAN	167
Conclusión: ¡Todos los proveedores deben ir de la mano!	167
13. Vulnerabilidad y Brechas en la Seguridad	169
Interceptación del tráfico de una red inalámbrica	171
802.11 Inalámbrico	171
Ataque de proximidad	172
Asegurar la red	172
¡Ataque WAP!	173
Encriptación	174
Medidas de sentido común	175
Dispositivos plug – and – play en la red	175
Usuarios de Windows	176
Computadoras Macintosh	176
Computadoras con Linux	177
Hawking contra la impresión de la red	177
Servidores de impresión	178
Defensa contra los ataques	179
Conclusión: Limitación de la vulnerabilidad	180
14. Esquemas de Control de Acceso	183
Autenticación	185
Esquemas de autenticación y acceso en Windows XP	186
Procedimientos de control de accesos	186

Seguridad física	187
Control de acceso a los puntos de acceso	188
Seguridad física de los puntos de acceso	188
Problemas de gestión de los puntos de acceso seguros	189
Medidas preventivas	191
MAC the Knife	192
VPN	192
Problemas de direccionamiento IP	193
Conclusión: Cómo asegurar un control de accesos <<seguro>>	194
15. Usuarios de Computadoras Portátiles Inalámbricas (PC y MAC)	197
Seguridad física de la computadora portátil	199
Protección	199
Soluciones hardware	200
Infraestructura de clave pública	203
Dispositivos biométricos portátiles	203
Reducción de las vulnerabilidades de WEP	204
Una WLAN más segura	206
Diferencias entre plataformas	206
Soporte de red para computadoras portátiles inalámbricas	207
Cómo incrementar la seguridad móvil	208
Usuarios remotos	208
Conclusión: evolución de la seguridad en la computadora portátil	209
16. Seguridad Administrativa	211
Soluciones de autenticación	213
Contraseñas	214
Construcción del cortafuegos	214
Sistemas de detección de instrucciones (IDS)	215
IDS basada en servidor	215
IDS basada en red	216
IDS de servidor frente a IDS de red	217
¿Por qué es necesario un IDS?	217
La computadora como tomadora de decisiones	218
Las personas reales	219
Evaluación de la vulnerabilidad de la seguridad	219
Evaluación de riesgos	220
Conclusión: ¡la mejor defensa es un buen ataque!	222
17. Problemas de Seguridad en Aplicaciones Inalámbricas (PCA Inalámbricas)	225
Protección de la información	227
Los datos de PDA	227
En busca de la seguridad	228
Funcionalidad de seguridad	228
Control de accesos	228
HotSync	229
Infrarrojos	229
Cómo construir una política de seguridad móvil efectiva	229
Protección de los recursos móviles	229
Conectividad inalámbrica	230

Seguridad HotSync	231
Autenticación por infrarrojos	232
Establecimiento de una política de seguridad	232
Consideraciones sobre privacidad	233
Por qué los PDA requieren privacidad	234
Mantenimiento del control de accesos	234
Encriptación de datos	234
Escurrid	234
Acceso a la intranet desde el PDA	235
Cómo se integran los hacher en la ecuación	235
Problemas de seguridad	236
Los PDA como herramientas de diagnóstico	236
PocketDOS	236
Proveedores de servicios inalámbricos	237
GoAmerica Communications	237
SprintPCS	237
La red IP inalámbrica de AT & T	238
Conclusión: Computación inalámbrica móvil	238
18. El Futuro de la Seguridad WiFi	241
Legislación sobre privacidad	243
Patriot Act, 2001 (USPA)	243
Ley Graham – Leach – Billey (GLB), 2001	243
Ley sobre informes de capacidad de crédito (Fair Credit Reporting Act), 1970, 1996 (FCRA)	243
Ley de protección de la privacidad online de la infancia (Childre´n Online Privacy Protection Act), 1998 (COPPA)	244
Ley sobre transmisión y responsabilidad de datos médicos (Health Insurance Portability and Accountability Act) (HIPPA) [21 de agosto de 1996]	244
Computación universal	244
Computación móvil inalámbrica	245
Seguridad evolutiva	245
Encriptación básica	245
WEP	245
Protección de accesos	246
Ataques de denegación de servicio	246
Evolución de los estándares	246
La competencia entre estándares	247
Cómo aumentar la seguridad en las comunicaciones inalámbricas	248
Dispositivos biométricos	249
Evaluación de los puntos fuertes y débiles de un WLAN	250
La combinación con tecnologías WLAN del futuro	250
Sistemas inteligentes	251
Datos encriptadas	251
Evolución de los sistemas operativos de las plataformas	251
La seguridad en Windows XP	252
Macintosh OS X	252
Palm y Pocket PC	252
Linux	253

Windows OS	253
Prevención de los intentos de instrucción en la red	253
Servidores de red	254
Servidores de ficheros	254
Servidores de impresión	254
Conclusión: el futuro de las redes inalámbricas	255
Índice	257