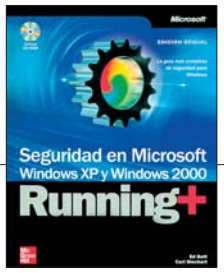
SEGURIDAD EN MICROSOFT WINDOWS XP Y WINDOWS 2000

Autores: Ed Bott y Carl Siechert
Editorial: Osborne McGraw Hill
Año 2003 – 608 páginas
ISBN: 84-481-3807-4
www.mcgrawhill.es



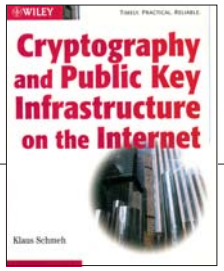
La obra de **Ed Bott** y **Carl Siechert**, redactada con un estilo muy práctico y dotado de una aceptable personalidad visual, se dirige a todos aquellos interesados en conocer de forma detallada el modo de proteger sus equipos personales y sus redes informáticas basadas en los sistemas operativos Windows XP Professional, XP Home Edition y 2000 Professional.

Los autores han acometido la tarea de realizar un detallado recorrido (más de veinte capítulos) por la seguridad técnica implícita en sistemas operativos marca Microsoft (incluidos aspectos tan espinosos como la seguridad en redes inalámbricas), comenzando su "periplo" por los conocimientos más básicos –quizá más propios de Windows 95, 98 o Me– para posteriormente analizar funcionalidades de seguridad propias de los más recientes sistemas operativos del fabricante, tales como el sistema de archivos NTFS, las técnicas de cifrado incorporadas y la compatibilidad con múltiples usuarios, entre otras.

En el volumen glosado cabe resaltar además la inclusión de notas a pie de página, capturas de pantalla y consejos expertos, además de un CD-Rom, que ilustran y guían al lector en los aspectos técnicos más complejos, que exceden, incluso, la temática del libro.

CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE ON THE INTERNET

Autor: Klaus Schmeh
Editorial: John Wiley & Sons
Año 2003 – 472 páginas
ISBN: 0-470-84745-X
www.wiley.com

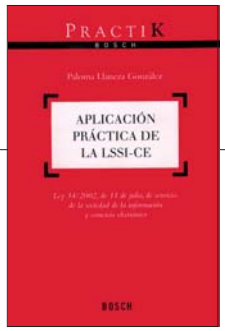


En los últimos tiempos, una de las áreas más recurrentes del mundo de la seguridad TI para autores y editoriales -algunas tan veteranas como Wiley-, es la relacionada con la criptografía en todos sus ámbitos de aplicación. En este caso, el volumen escrito por **Klaus Schemh**, revisión de otro aparecido en 1998 con el título *Safer Net - Cryptography in the Internet and intranet*, se distingue de otros similares por estar centrado en la aplicación de la criptografía y la implantación de infraestructuras de clave pública en proyectos orientados al mundo Internet. Así, los contenidos técnicos comunes en obras de este estilo se encuentran ampliamente tratados en la misma, destacando, además, por el compendio de fuentes de información, así como la catalogación y descripción de organizaciones, personas y empresas que realiza el autor, todas ellas relacionadas directamente con el mundo de la criptografía.

El índice de la obra está dividida en seis partes y dos anexos con la siguiente distribución: **Parte I: ¿Por qué es necesaria la criptografía en Internet?** [Temas: 1) Introducción, 2) ¿Qué es y por qué es tan importante?, 3) ¿Cómo es posible navegar por Internet?]; **Parte II: Los principios de la criptografía** [Temas: 4) Cifrado simétrico, 5) Algoritmos de cifrado simétrico modernos, 6) Cifrado asimétrico, 7) Firma digital, 8) Funciones *hash*, 9) Generadores criptográficos aleatorios] **Parte III: Criptografía avanzada** [Temas: 10) Estandarización en criptografía, 11) Funcionamiento de los modelos de cifras en bloque y transformación de datos para algoritmos asimétricos, 12) Protocolos criptográficos, 13) Autenticación, 14) Sistemas basados en curvas elípticas, 15) Implementación criptográfica]; **Parte IV: Infraestructuras de clave pública** [Temas: 16) PKI, 17) Cómo trabajar con una PKI, 18) Certificados digitales, 19) Servidores de certificados, 20) Aspectos prácticos en el diseño de una PKI] **Parte V: Protocolos criptográficos para Internet** [Temas: 21) Internet y el modelo OSI, 22) Estándares criptográficos para las capas 1 y 2 de OSI, 23) IPSec (capa 3), 24) SSL, TLS y WTLS (capa 4), 24) Estándares criptográficos para WWW (capa 7), 26) Estándares de cifrado para correo-e (capa 7), 27) Sistemas electrónicos de pago (capa 7), 28) Protocolos para la capa de aplicación futuros]; **Parte VI: Más acerca de la criptografía** [Temas: 29) Aspectos políticos, 30) Gente importante, 31) Cómo buscar más información, 32) Los últimos capítulos]. **Anexos** [A) Listado de abreviaturas, B) Bibliografía).

APLICACIÓN PRÁCTICA DE LA LSSI-CE

Autora: Paloma Llaneza
Editorial: Bosch
Año 2003 – 363 páginas
ISBN: 84-7676-813-3
www.bosch.es

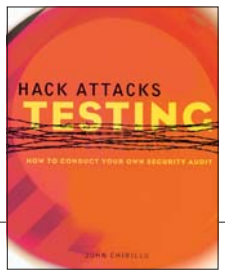


Paloma Llaneza, una activa y reputada profesional en la materia, aborda en su reciente obra los contenidos de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, y más concretamente, sobre su aplicación práctica "a pie de obra", según cita la propia autora. De esta forma, el volumen, a modo de introducción, recoge la casuística del entorno regulado, los problemas de aplicación previsibles, la postura de las administraciones llamadas a aplicarla, así como la documentación que permita al lector encarar los asuntos relacionados con la Ley, entre otros temas. Expresamente, cabe destacar entre sus capítulos el dedicado al deber de retención de datos relativos a las comunicaciones-e y a sus posibles vías de desarrollo reglamentario, aún por definir.

El libro, dividido en cuatro capítulos, se estructura del siguiente modo: **1: Lo imprescindible** [Temas: 1) La doble faz de la LSSI-CE, 2) Conceptos: el anexo de definiciones, 3) Ámbito de aplicación, 4) Obligaciones comunes a todos los PSSI, 5) Cuestiones relativas a la protección de la propiedad intelectual, 6) Otros contenidos ajenos a la regulación de los SSI, 7) La solución de los conflictos, 8) Las infracciones y su sanción]; **2: El control de los contenidos. El régimen especial de los PSI** [Temas: 1) Responsabilidad por contenidos propios, 2) Tratamiento de los ajenos 3) El deber de retención de datos relativos a las comunicaciones-e]; **3: Aspectos relativos al comercio-e** [Temas: 1) Concepto, 2) Validez de los contratos celebrados por medios electrónicos, 3) Contratos incluidos y contratos excluidos, 4) Contratación con consumidores y usuarios]; **4: Obligaciones en relación con la protección de datos personales** [Temas: 1) Cómo recoger datos, 2) La recogida de datos con fines comerciales, 3) Cómo tratar y transferir los datos recogidos].

HACK ATTACKS TESTING
How to conduct your own security audit

Autor: John Chirillo
Editorial: John Wiley & Sons
Año 2003 – 540 páginas
ISBN: 0-471-22946-6
www.wiley.com



El presente volumen de **John Chirillo** continua en la línea de otras obras del afamado consultor ya glosadas en esta revista (véase SIC 53). En esta ocasión, con su estilo claro y conciso, aborda los temas relativos a la auditoría de seguridad de los sistemas informáticos.

A modo de camino de iniciación, el autor ofrece un recorrido por las distintas herramientas presentes en el mercado para este propósito, divididas por sistemas operativos (Linux, Mac, Unix y Windows), para orientar al lector sobre los procedimientos utilizados en la comprobación de la eficacia de los elementos que conforman un sistema de seguridad TIC (abarcando las políticas de seguridad, la defensa perimetral y los planes de contingencia), a modo de análisis de vulnerabilidades *ad hoc*.

Hack Attacks Testing se divide en cuatro partes, catorce capítulos y dos anexos que responden a la siguiente estructura: **Parte I: Construyendo nuestro sistema de auditoría** [Temas: 1) Instalación y configuración básica de Windows 2000 y 2000 Server, 2) En Linux y Solaris, 3) Soluciones para sistemas Mac OS X, 4) Configurando un análisis de vulnerabilidades]; **Parte II: Usando herramientas de auditoría para Windows** [Temas: 5) Cerberus Internet Scanner, 6) Cybercop Scanner, 7) Internet Scanner, 8) Riesgos en el uso de programas para el rastreo de vulnerabilidades, 9) Tigersuite 4.0]; **Parte III: Usando herramientas de auditoría para Mac OS X y NIX** [Temas: 10) hping/2, 11) Nessus Security Scanner, 12) Nmap, 13) SAINT, 14) SARA]; **Parte IV: Evaluación de las vulnerabilidades** [Temas: 15) Análisis comparativos]; Anexos [A) Comandos y atajos para Linux y Unix B) Contenidos del CD-Rom].