SEGURIDAD EN REDES TELEMÁTICAS

Autor: Justo Carracedo Gallardo
Editorial: McGraw-Hill
Año: 2004-549 páginas
ISBN: 84-481-4157-1

La producción bibliográfica en español sobre seguridad de las TIC, dirigida principalmente al noble fin de ayudar a la formación de los estudiantes universitarios en esta disciplina tan de moda hoy, está dejando de ser una peladera, y de vez en cuando, un buen profesor tiene oportunidad de ver editada alguna obra con la que contribuir al mejor conocimiento de la materia por la vía de la sistematización razonable de lo que ya se sabe, todo un arte, y que es la asignatura pendiente de ciertos pretendidos sabios de nuestra tierra, que se anuncian como personas que investigan y, a la postre, devienen en copiones mediocres, cuyo único interés en este asunto concreto es que les editen el librito, algo así como el oscuro objeto del deseo de la inmensa mayoría de los habitantes del planeta académico.

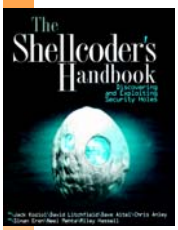
Desde luego no es el caso del autor del volumen que nos ocupa, Justo Carracedo Gallardo, Ingeniero de Telecomunicación y Doctor en Informática, cuya pretensión al escribir la obra, titulada "Seguridad en redes telemáticas" no ha sido otra, en tanto que excelente Catedrático de Escuela Universitaria con destino es el Departamento de Ingeniería y Arquitecturas Telemáticas-Diatel, de la Escuela Universitaria de Ingeniería Técnica de Telecomunicaciones de Madrid (UPM), que enmarcarla en el más puro interés docente, algo que viene a prestigiar todavía más a un profesor que lleva participando en proyectos de investigación nacionales y europeos sobre seguridad en redes telemáticas desde el año 1990, y que es un experto en voto electrónico.

En este libro, el autor se centra con profusión en la aplicación de la criptografía moderna a la seguridad en redes telemáticas, algo muy importante pero que todavía fascina desproporcionadamente a la comunidad de enseñantes, y que tiene como efecto en sus obras y enfoques, el que destinen bastante menos atención a otros aspectos involucrados en la materia, y que entran de lleno en la gestión de los riesgos de seguridad. No obstante, la exposición de Carracedo es impecable para los fines de protección que se plantea y el alcance de la obra, que quedan patentes en el concepto de "seguridad cívica" al que alude el Catedrático en no pocas ocasiones.

Estamos, pues, ante un dignísimo libro técnico, cuya aparición hay que aplaudir. Y es de esperar que, en el futuro, pase a ser una referencia en la bibliografía señalada de otros autores que prueben suerte en la temática. Aunque la verdad, en general, los profesores e investigadores en esto son, digamos, especiales. Tampoco dan ejemplo de elegancia y corrección las compañías editoras, muchas de las cuales ni siquiera incluyen unas breves notas biográficas de los escritores de los libros que editan. Da que pensar.

José de la Peña Muñoz

THE SHELLCODER´S HANDBOOK
Discovering and Exploiting Security Holes



Autores: J. Koziol, D. Litchfield, D. Aitel, C. Anley, S. Eren, N. Mehta, R. Hassell
Editorial: Wiley
Año 2004 – 620 páginas
ISBN: 0-7645-4468-3
www.wiley.com

Este libro, escrito por un equipo de autores integrado por expertos en seguridad corporativa y *hackers-crackers* clandestinos, colaboradores de la lista de distribución sobre rastreo de vulnerabilidades *Bugtrag*, ofrece la información y las herramientas para descubrir vulnerabilidades en software basado en lenguaje C, explotar las mismas y prevenir la aparición de nuevas brechas de seguridad, permitiendo de este modo ir un paso por delante de los posibles atacantes de nuestras aplicaciones y sistemas operativos. Además, los autores proporcionan información sobre técnicas avanzadas para tapar nuevos agujeros que todavía no son conocidos por el público, pero que pueden causar graves consecuencias.

La obra, dividida en cuatro grandes secciones, comienza haciendo una introducción sobre la detección y explotación de vulnerabilidades en binario, con varios ejemplos de estructuras de código ficticias (comenzando por las más sencillas en las plataformas Linux/IA32), para posteriormente avanzar en las vulnerabilidades de otros sistemas operativos más complejos como Windows, Solaris y Tru64.

En una tercera parte, el libro abunda en los métodos empleados por los intrusos para descubrir vulnerabilidades (técnicas automatizadas de inyección de errores, detección de *bugs* mediante *fuzzing*, auditoría del código fuente, búsqueda manual de *bugs* mediante técnicas de ensayo-error, calco de vulnerabilidades, y auditoría de binarios), y dedica la última parte a contenidos de un nivel más avanzado, como nuevas estrategias de carga, cómo escribir *exploits* que funcionen en un entorno hostil, cómo atacar bases de datos relacionales específicas, y algunos fenómenos de nueva naturaleza como los ataques de desbordamiento del kernel, así como la forma de explotar sus vulnerabilidades.

SEGURIDAD EN WIFI

Autor: Stewart S. Miller
Editorial: McGraw Hill
Año 2004 – 270 páginas
ISBN: 84-481-4028-1
www.mcgraw-hill.es

El libro de **Stewart S. Miller**, experto destacado en EEUU en seguridad y gestión de la eficiencia de las TI, ahonda en el amplio despliegue de las comunicaciones inalámbricas en los últimos años, así como los diferentes estándares y especificaciones de seguridad que han surgido de forma paralela. Igualmente, el autor dedica buena parte de las páginas de este volumen a revelar las vulnerabilidades y problemas más frecuentes de esta tecnología, a la vez que propone diferentes medidas y soluciones a adoptar para asegurar convenientemente las redes inalámbricas y los dispositivos móviles.

Los contenidos se distribuyen a lo largo de dieciocho capítulos con la siguiente estructura: Introducción a los estándares de seguridad de las redes locales inalámbricas; Tecnología; Factores de seguridad; Definición del estándar 802.11; La infraestructura de seguridad de 802.11; El cifrado 802.11 y la privacidad equivalente al cableado (WEP); Accesos no autorizados y privacidad; La autenticación en sistemas abiertos; Expansión de espectro por secuencia directa; Consideraciones sobre equipos WiFi; Seguridad multiplataforma para el usuario inalámbrico; Vulnerabilidades y brechas de seguridad; Esquemas de control de acceso; Usuarios en computadoras portátiles inalámbricas (PC y MAC); Seguridad administrativa; Problemas de seguridad en aplicaciones inalámbricas (PDA inalámbricos), y El futuro de la seguridad WiFi.