



RFID APLICACIONES, SECURITY, AND PRIVACY

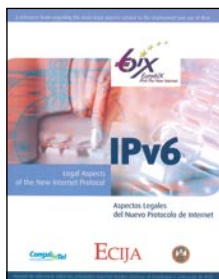
Autores: Simson Garfinkel y Beth Rosenberg (Ed)
Editorial: Addison Wesley
Año 2005 – 556 páginas
ISBN: 0-321-2996-8
www.awprofessional.com

El galardonado investigador en seguridad Simson Garfinkel y la editora y escritora Beth Rosenberg han reunido en este libro una densa pero interesantísima recopilación de artículos y comunicaciones que abordan diferentes aspectos de la tecnología de identificación de radio frecuencia (RFID), destinada, sin duda, a protagonizar estelarmente los grandes titulares en los próximos años. Como era de prever, los autores han prestado especial atención a las cuestiones que suscita esta nueva tecnología en cuanto a seguridad y privacidad.

Hasta dieciocho empresas e instituciones (entre las que se encuentran IDAT Consulting & Education, MIT Media Laboratory o la

Facultad de Derecho de la Wayne State University) han colaborado en esta recopilación que muestra la evolución y proyección de la RFID, evalúa sus riesgos de privacidad y las soluciones propuestas en los campos tanto técnico como empresarial y político. Además, el volumen también repasa las implicaciones de privacidad de otras tecnologías como la tecnología Wi-Fi, Bluetooth, *smart cards*, dispositivos biométricos, las nuevas redes de teléfono móvil y las nuevas tendencias de Internet.

El libro aborda, asimismo, temas como las soluciones técnicas a los contenidos privados que circulan por redes inalámbricas, la legislación vigente al respecto, o la seguridad y el espionaje industrial. ■



IPv6: ASPECTOS LEGALES DEL NUEVO PROTOCOLO EN INTERNET

Autores: Varios
Editorial: Euro6IX
Año 2005 – 304 páginas
ISBN: 84-609-6359-4
www.ecija.com

La firma Écija Abogados, en colaboración con la Universidad de Murcia y Consulintel, ha publicado un libro que recoge los informes realizados por el despacho como socio jurídico del denominado Consorcio Euro6IX, un proyecto europeo responsable de la investigación de una arquitectura apropiada, un diseño, desarrollo, implantación y validación de la primera red pre-comercial paneuropea de Intercambiadores de tráfico nativo IPv6.

Con una estructura claramente divulgativa, el manual presenta de manera conjunta la edición española e inglesa, y está dividido en cuatro capítulos fundamentales: unos conceptos iniciales a modo de introducción, y un capítulo par cada uno de los tres informes realizados para el Consorcio.

Estos informes analizan las implicaciones jurídicas del nuevo protocolo IPv6, de próxima implanta-

ción; el primero analiza cómo podría afectar la adopción de este protocolo a la privacidad de los usuarios, ya que con un el IPv6, las direcciones basadas en un identificador único posibilitan la asociación de dicha IP al nodo o dispositivo que la utiliza, por lo que en casos concretos esta dirección IP tendría la consideración de dato personal; las implicaciones de este cambio en materia de protección de datos y, por último, un estudio de las implicaciones y relaciones que pueden establecerse entre el nuevo protocolo y las normas relativas a los derechos de Propiedad Intelectual (IPRs).

Dado que el objetivo de la publicación es facilitar el acercamiento de IPv6 a los futuros usuarios, los autores han optado por un lenguaje sencillo y han huido de los tecnicismos, además de ofrecer versiones en formato pdf en www.ipv6tf.org/pdf/ipv6legalaspects.pdf. ■



BLACK HAT: PHYSICAL DEVICE SECURITY

Autor: Drew Miller
Editorial: Syngress
Año 2005 – 364 páginas
ISBN: 1-932266-81-X
www.syngress.com

El consultor especializado Drew Miller, especialista en desarrollo de metodologías de seguridad defensivas y la detección de ataque a aplicaciones, ha centrado en Black Hat Physical Device Security su atención en los riesgos asociados al hardware de red. A lo largo de sus nueve capítulos, la obra analiza la evolución de los dispositivos de seguridad, desde los que tan sólo son transistores electrónicos, hasta los más avanzados dotados de software e incide en las vulnerabilidades que poseen. Estas vulnerabilidades del hardware, afirma Miller, no sólo afectan al entorno empresarial ya que implica no sólo a ordenadores, sino además a todos los aparatos que hoy poseen microprocesadores, como los sistemas GPS,

teléfonos móviles, video juegos, y dispositivos biométricos.

El título profundiza en temas como la protección de los dispositivos físicos contra intrusiones, la valoración del riesgo de no poseer un método seguro de comunicaciones o cuáles son las mejores herramientas para evaluar el propio software y hardware que se está desarrollando. Igualmente, repasa cuestiones como la autenticación del personal o los diferentes sistemas de notificación.

Gracias a su experiencia como formador en estrategias de programación defensiva para software y analistas de seguridad, la obra de Miller conforma un manual completo y ordenado que incluye un índice alfabético y tres apéndices. ■



HACKING ÉTICO

Autores: S. Harris, A. Harper, C. Eagle, J. Ness y M. Lester
Editorial: Anaya Multimedia
Año 2005 – 542 páginas
ISBN: 84-415-1874-2
www.anayamultimedia.es

He aquí un título que pretende dotar al profesional de la seguridad del punto de vista del "enemigo", los métodos, habilidades e incluso motivaciones más frecuentes de los *hackers*. A través del denominado *hacking ético*, aquel que no tiene una finalidad espuria y actúa de manera responsable, el lector puede profundizar en las diferentes técnicas de los piratas informáticos, su modo de actuación y la forma en que perpetran los ataques a redes o accesos no permitidos, con el objetivo de que se puedan afrontar y prevenir con mayor éxito.

Se trata, portanto, de un manual que recopila diferentes técnicas de intrusión y tipos de ataques pero que no pierde de vista aspectos como el sistema jurídico, el análisis

de la legislación más reciente concerniente a delitos informáticos o la manera correcta y ética de divulgar las vulnerabilidades.

Los autores, además de incluir métodos como la ingeniería invertida o la variación de parámetros, se han centrado en el funcionamiento de los componentes de cada sistema operativo y sus vulnerabilidades. Dividido en cuatro grandes bloques (La ética del *hacker*, Herramientas y pruebas de presentación, Exploits 101 y Analizar vulnerabilidades), el libro incluye en cada uno de sus capítulos un resumen, un apartado de referencias y una serie de preguntas y respuestas para la autoevaluación, así como un índice alfabético en sus últimas páginas. ■