CRIPTOLOGÍA Y SEGURIDAD

Autor: Jorge Dávila Muro
Edita: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones
Año: 2008 – 144 páginas
ISBN (13): 978-84-7402-352-7

De vez en cuando, surge una supernova en el universo de la edición de obras en castellano de corte científico-técnico. Y es el caso de ésta, escrita en prosa fina y tono divulgativo, en la que se aborda llanamente la historia de la Criptología y su relación estrechísima con la protección de la información en innumerables escenarios: social, político, militar, comercial...

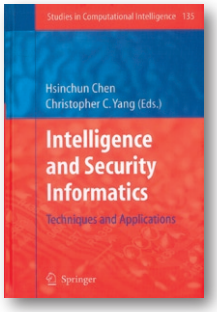
Su autor, **Jorge Dávila Muro**, Profesor Titular de Universidad, trabaja en la Facultad de Informática de la Universidad Politécnica de Madrid (UPM), en la que dirige el Laboratorio de Criptografía; es, además, colaborador habitual de SIC y uno de los grandes expertos españoles en la materia: un joven científico de casta, que concibe el saber como un todo por lo que, pese a su juventud, va para sabio, si no lo es ya.

El libro se enmarca en las iniciativas de edición de Cuadernos Cátedra ISDEFE-UPM/ETSIT (Escuela Técnica Superior de Ingenieros de Telecomunicación), y está prologado por el Secretario de Estado-Director del Centro Nacional de Inteligencia-CNI y del Centro Criptológico Nacional-CCN, Alberto Saiz Cortés, que reconoce la valía de Dávila, un especialista "*... Con el que el personal del Centro Criptológico Nacional contrasta habitualmente opiniones y pareceres sobre cuestiones técnicas*".

La obra es corta –tiene 144 páginas–, de lectura rápida y apta prácticamente para todos los públicos, hecho que no le resta rigor. Está dividida en 54 capítulos más un anexo con dos capítulos. Y en esta dimensión, el autor ofrece su mirada experta desde el principio, el origen de la cifra, hasta los retos de hoy, como pueden ser los representados por las criptografías cuánticas y algunos otros, expresados en el capítulo titulado "¿Qué problemas quedan por resolver en la criptografía actual?".

No cabe duda: el trabajo es meritorio por su pretensión divulgativa, y bien merece que se saque media hora al día para leerlo. Si uno se lo propone, en tres horas está razonablemente aprehendido. El premio es atractivo: conocer, fijar conceptos, asombrarse en ocasiones y entender con perspectiva la historia apasionante de la Criptología, que como el profesor Dávila dice: "*... No es una ciencia de reciente aparición ni parece seguir el frenético desarrollo que otras actividades tecnológicas emergentes tienen. La criptografía, más que una ciencia, se ha comportado como un arte durante los últimos casi 5.000 años. En las últimas décadas han surgido nuevos e impensables escenarios de uso, como pueden ser la Sociedad de la Información e Internet, y en ellos, la Criptología sin duda está teniendo y tendrá un nuevo renacer*". ■

José de la Peña



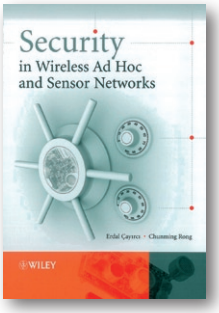
INTELLIGENCE AND SECURITY INFORMATICS Techniques and Applications

Autores: Hsinchun Chen y Christopher C. Yang
Editorial: Springer
Año: 2008 – 460 páginas
ISBN 978-3-540-69207-2
www.springer.com

La obra aquí reseñada recopila los avances llevados a cabo por diversos investigadores en el campo de la Informática de la Inteligencia y la Seguridad (*Intelligence and Security Informatics,* ISI), una ciencia multidisciplinar que utiliza diversas metodologías, modelos, algoritmos e instrumentos avanzados de TI para crear políticas públicas que permitan luchar contra el terrorismo a nivel nacional e internacional, habiendo adquirido gran popularidad tras los atentados del 11 de septiembre de 2001 en Nueva York.

El libro está dividido en cuatro secciones, entre las que se reparten 22 trabajos cuyos autores proceden de nueve países ubicados en distintos continentes. Los trabajos de investigación recogidos en la primera sección ponen el foco en el uso de la informática como herramienta para el desarrollo de acciones terroristas y en la minería de datos, tratando asuntos como la automatización de la extracción de eventos para proteger un dominio o la detección multi-lingüe del contenido de una web terrorista.

Los textos ubicados en la segunda parte de la obra versan sobre la inteligencia y el análisis de delitos, abordando, entre otros aspectos, el hallazgo de pistas mediante la extracción de información de bases de datos criminales, o la gestión de información personal para tareas de inteligencia. El contenido de la tercera sección está relacionado con el control de los accesos, la protección de la infraestructura y la privacidad; mientras que en la última parte, se tratan materias relativas a los campos de la vigilancia y de la respuesta ante emergencias. ■



SECURITY IN WIRELESS AD HOC AND SENSOR NETWORKS

Autores: Erdal Çayirci y Chunming Rong
Editorial: Wiley
Año: 2009 – 257 páginas
ISBN 978-0-470-02748-6
www.wiley.comwww.awprofessional.com

Centrado en la seguridad de las transmisiones en redes inalámbricas *ad hoc*, redes de sensores y redes acopladas (WASMs), el presente título proporciona al lector en un primer apartado los fundamentos y los conceptos básicos para comprender los aspectos ligados a la protección de las redes WASM, que de forma más detallada se abordan en la segunda parte del texto.

Así, en el segundo bloque de la obra se explican las primitivas criptográficas para después exponer los retos y las soluciones relativos a cuestiones básicas como el arranque (*bootstrapping*), la distribución de claves y su integridad. Igualmente, se enseña en el libro a resolver contratiempos relacionados con la privacidad, el anonimato, la detección de intrusos, el análisis del tráfico, el control de accesos, la resistencia a daños, la disponibilidad y la validez. A continuación los autores profundizan en problemas relacionados con el *routing* seguro, como las capacidades de autoformación, la auto-organización y la auto-recuperación de las redes *ad hoc*; y posteriormente, el texto detalla otros problemas específicos de las redes WASMs.

El libro contiene, además, un capítulo muy breve dedicado a guerra electrónica y operaciones de información, y en su parte final otro sobre los estándares relacionados con las diferentes materias tratadas a lo largo del texto: X.800 y RFC 2828, WEP (*Wired Equivalent Privacy*) y WPA (*Wi-Fi Protected Access*). ■