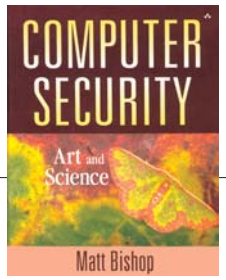
COMPUTER SECURITY Art and Science

Autor: Matt Bishop
Editorial: Addison Wesley
Año 2003 - 1084 páginas
ISBN: 0-201-44099-7
www.awprofessional.com/
www.pearsoned.es



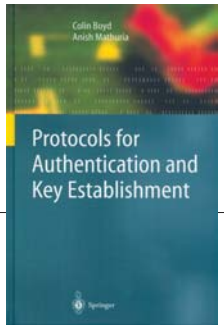
Los expertos suelen decir que las variables que guían al lector en la compra de un libro son múltiples. Sin duda, una de las más influyentes es la apariencia. Por suerte o por desgracia, el elevado número de páginas o la dureza de las cubiertas suelen ser malos referentes en la mensura de la calidad de una obra, pero no siempre es así.

Este es el caso del volumen escrito por **Matt Bishop**. Lo primero que llama la atención son sus más de dos kilos de peso y sus cerca de 1.100 páginas, pero estos indicadores no son los únicos. La interconexión de "ciencia" y "arte" -aludidos en el subtítulo del libro-, refleja con exactitud el espíritu de la obra, que orbita sobre tres ejes. El primero de ellos, la simbiosis existente entre teoría y práctica en el mundo de la seguridad informática: ambas son irrelevantes por separado, pero juntas conforman el modelo ideal. El segundo es la necesidad de diferenciar entre seguridad TI y criptografía. Su simbiosis es provechosa pero lo capital es entender sus mecanismos y protocolos para utilizarlos con propiedad en un contexto determinado. En último lugar, y no por ello menos importante, se enfatiza la obligatoriedad de clarificar que la seguridad informática no es exactamente una ciencia pero tampoco solo arte. Tiene parte de la primera (sus teorías están basadas en construcciones matemáticas, análisis y pruebas) y parte de la segunda (dos ingenieros pueden construir su interacción con sistemas tecnológicos de diferente forma, pero persiguiendo el mismo concepto). La medida de graduación de ambas es, según el autor, la clave de todo.

Dicho esto, sólo queda destacar del volumen glosado la estructuración funcional de sus contenidos en nueve partes y 35 capítulos, en los que se analizan cuestiones como el diseño de políticas de seguridad, la criptografía, la implantación de sistemas y los mecanismos de certificación, entre otras. También cabe recalcar la correcta organización de la materia, los diagramas y esquemas que perfeccionan la información y su extensa bibliografía, que complementa, junto con los apéndices, las cuestiones analizadas.

PROTOCOLS FOR AUTHENTICATION AND KEY ESTABLISHMENT

Autores: Colin Boyd y Anish Mathuria
Editorial: Springer
Año 2003 - 321 páginas
ISBN: 3-540-43107-1
www.springer.de

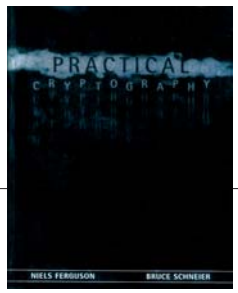


El libro reseñado, como indica su título, está centrado en el análisis de los protocolos de autenticación y gestión de claves que han ido surgiendo a lo largo de la historia del desarrollo criptográfico. Los autores, **Colin Boyd** y **Anish Mathuria** mantienen que en 1978 se inició formalmente su estudio, momento que coincidió con la publicación, por parte de Needham y Schroeder, del primer documento académico. Por aquel entonces, este campo de estudio generó la separación de los investigadores en dos comunidades: la centrada en la criptografía y la especializada en seguridad informática. Desde entonces, el elevado número de protocolos generados por ambas, y por ende su complicado seguimiento literario por parte de investigadores y usuarios finales, ha tenido como resultado la aparición de *Protocols for Authentication and Key Establishment*, volumen que pretende recoger, de forma clara y sencilla, los datos básicos disponibles relacionados con este tema.

Los siete capítulos que conforman la obra están estructurados de la siguiente forma: 1) Introducción a la autenticación y gestión de claves, 2) Objetivos, 3) Protocolos de autenticación basados en algoritmos simétricos, 4) Autenticación y gestión de claves utilizando criptografía de clave pública, 5) Protocolos de intercambio de claves, 6) Protocolos de gestión de claves en grupo, 7) Protocolos basados en contraseñas. Anexo) Normativa para la autenticación y gestión de claves.

PRACTICAL CRYPTOGRAPHY

Autores: Niels Ferguson y Bruce Schneier
Editorial: John Wiley & Sons
Año 2003 - 410 páginas
ISBN: 0-471-22894-X
www.wiley.com



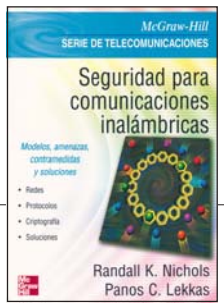
El mercado mundial de la seguridad TI está en constante evolución. No se conoce con exactitud el rumbo concreto y en esto, como en todos los sectores donde existe incertidumbre, la tecnología puede tener una importante baza que jugar. Eso sí, de un tiempo a esta parte es de justicia mencionar que determinadas áreas de esta "feria", y nuestro país no es una excepción, no han dejado de padecer las embestidas de desesperados vendedores de artilugios mágicos, ya sean hardware o software, que incluyen últimamente en las descripciones técnicas de sus productos los vocablos "seguridad" y "cifrado" exclusivamente porque queda bien.

Precisamente, el volumen escrito por **Niels Ferguson** y **Bruce Schneier** pretende cambiar esta percepción errónea que afecta, concretamente, al mundo de la criptografía. Según los autores, los libros de la pasada década han realizado un flaco favor a este campo de investigación, contribuyendo en grado sumo al incremento desmesurado de su aura "mágica". Nada más allá de la realidad. La criptografía es una ciencia, actualmente imperfecta, y en sus aspectos más prácticos se basa este tratado (secuela de otro escrito hace diez años por Schneier, denominado *Applied Cryptography*). Según los autores, los contenidos teóricos en criptografía son importantes, pero aún más lo son su forma de uso y su implementación real en entornos de seguridad TI.

El índice de la obra está dividido en 25 capítulos y cuatro partes con la siguiente distribución: 1) Nuestra filosofía, 2) El contexto de la criptografía, 3) Introducción. **Parte I: Mensajes de seguridad** [Temas: 4) Cifrado en bloque, 5) Modos de cifrado en bloque, 6) Funciones *Hash*, 7) Códigos de autenticación, 8) Canales seguros, 9) Casos prácticos I]; **Parte II: Negociación de claves** [Temas: 10) Generación aleatoria, 11) Números primos, 12) Diffie-Hellman, 13) RSA, 14) Introducción a los protocolos criptográficos, 15) Protocolos de negociación de claves, 16) Casos prácticos II]; **Parte III: Gestión de claves** [Temas: 17) El reloj, 18) Servidores de claves, 19) El sueño de la PKI, 20) La realidad de la PKI, 21) Espíritu práctico de la PKI, 22) Almacén de secretos]; **Parte IV: Variedades** [Temas: 23) Estándares, 24) Patentes, 25) Complicaciones de expertos].

SEGURIDAD PARA COMUNICACIONES INALÁMBRICAS
Modelos, amenazas, contramedidas y soluciones

Editorial: McGraw-Hill
Año 2003 - 563 páginas
ISBN: 84-481-3782-5
www.mcgrawhill.es



El libro de **Randall K. Nichols y Panos C. Lekkas** tiene como público objetivo aquellos profesionales que quieran conocer de una forma sencilla y cercana todo lo relacionado con los distintos elementos de seguridad implicados en las comunicaciones inalámbricas (tecnología, técnicas y metodologías) destinados a proporcionar protección a los activos de información que transitan por este tipo de entornos.

El volumen se encuentra dividido en doce capítulos con la siguiente distribución: 1) ¿Por qué son tan diferentes las comunicaciones inalámbricas?, 2) La guerra de la información en los entornos inalámbricos, 3) Vulnerabilidades de los sistemas telefónicos, 4) Comunicaciones vía satélite, 5) Seguridad criptográfica, 6) Criptografía en la voz, 7) WLAN: redes inalámbricas de área local, 8) Protocolo de aplicaciones inalámbricas (WAP), 9) Seguridad en el nivel de transporte inalámbrico (WTLS), 10) Bluetooth, 11) Voz sobre IP, 12) Perspectivas hardware para la seguridad extremo a extremo en aplicaciones inalámbricas.

Como conclusión cabe destacar que la aridez tecnológica de los distintos temas analizados se encuentra rebajada y amenizada con numerosos ejemplos, comentarios y gráficos incluidos en el mismo, que ayudan en gran medida a su lectura y comprensión.