



SECURE COMMUNICATIONS

Applications and management

Autor: Roger J. Sutton

Editorial: John Wiley & Sons

Año: 2002 – 332 páginas – ISBN: 0-471-49904-8

www.wiley.com - www.diazdesantos.es

Creo no equivocarme si afirmo que ésta es la primera vez que acogemos en esta sección a un libro consagrado a la seguridad en las comunicaciones. Y es que, al contrario de lo que acontece con los tratados acerca de la seguridad en ordenadores y redes –editados en aluvión desde hace una década–, aquellos versados en la citada materia se publican con cuentagotas, llegando raramente a los anaqueles de las librerías. Posiblemente lo anterior traiga causa en la dificultad que para los responsables de seguridad suponga asumir un protagonismo en la protección de las comunicaciones, que transcurren más o menos en una caja negra (aunque no inexpugnable) entre los equipos terminales o, lo que es igual si de datos se trata, por el circuito de datos.

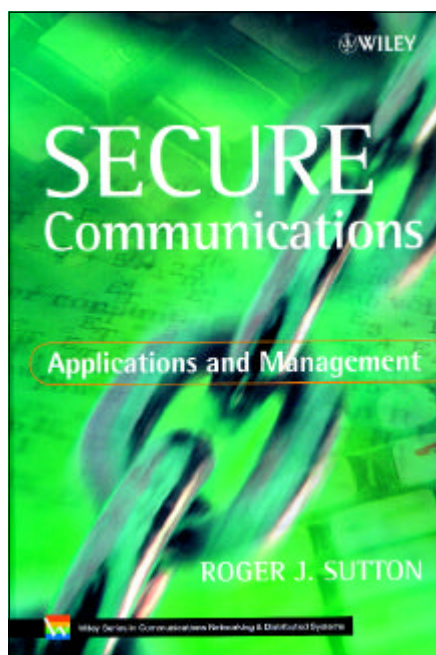
En todo caso, y aunque sólo fuese por conocer las limitaciones de seguridad que los equipos y canales de comunicación comportan, parece inexcusable para los antedichos responsables conocer la seguridad que aquellos canales incorporan y, en los casos en que sea posible, cómo incrementar la misma.

Pues bien, de todo lo anterior versa el tratado que en esta ocasión reseñamos, **SECURE COMMUNICATIONS. Applications and management**, escrito por Roger J. Sutton, experto de la reputada firma helvética Cripto AG (como es sabido, Suiza es uno de los más afamados países en cuanto al desarrollo de productos criptográficos), y publicado por la editorial John Wiley & Sons, LTD en el presente año.

Lo primero que se aprecia en la obra –favorablemente– son las numerosas figuras y tablas que jalonan toda la obra, pues aunque algunas de las primeras sean muy densas, su lectura contribuye poderosamente a la comprensión de las tecnologías y sistemas tratados. Sin embargo, y ya en el debe del autor, procede apuntar que la redacción es, en muchas de sus partes, farragosa y oscura, obligando a repetidas lecturas para el cabal entendimiento de lo presentado.

En otro orden, cumple destacar una marcada tendencia a centrarse en sistemas y redes propias de ambientes militares y ausentes de los civiles. Ello es claramente apreciable en los capítulos tercero y decimotercero, de títulos respectivos tan ilustrativos como: *Voice Security in Military Applications* y *Military Data Communication*. Pero no son sólo éstos, pues en otros muchos –casi todos– se hallan uno o varios apartados de interés para dichos círculos, pero de escasa motivación para los profesionales en general.

Entrando en su estructura, el libro se puede considerar conformado por tres partes o divisiones, si bien ningún agrupamiento o denominación común así lo manifieste. La primera, que podríamos denominar introductoria, está constituida por los dos primeros capítulos y se dedica a presentar



los fundamentos conceptuales y técnicos de la materia. Son un total de sesenta páginas que los lectores no iniciados precisarán ulteriormente, pero que los profesionales podrán orillar sin que ello merme su capacidad de comprensión del resto de la obra, ni les hurte de alguna visión particular de los prolegómenos de la disciplina de la seguridad, con la excepción, quizá, de dos o tres apartados que seguidamente indicamos. Los capítulos aquí incluidos son *Threats and Solutions* y *An Introduction to Encryption and Security Management*. En aquél, sobresale el tercer apartado –dedicado a las amenazas que presentan las emanaciones electromagnéticas–, y en éste, el primero, ocupado parcialmente en las técnicas de seconfonía (*scrambling*), aunque también es de cierto interés el último, de evaluación de cifradores.

Otra parte, la más sucinta del tratado, la constituye el decimocuarto y último capítulo, que lleva por nombre *Management, Support and Training*, donde se atiende a las facetas vinculadas a la gestión. Es una especie de cajón de sastre, donde se puede encontrar desde el marco (legal, internacional, económico, etc.) en el que se desarrolla la materia, hasta el organigrama de un departamento de seguridad.

Finalmente, la parte más extensa y singular –y que desde luego constituye la razón de ser de la obra– se desarrolla desde el capítulo tercero al duodécimo, donde se exponen los aspectos más técnicos de los equipos, redes y sistemas de comunicación. Aunque nada lo indique, es evidente un agrupamiento de los capítulos comprendidos en esta parte, de modo que los primeros tratan de la

seguridad en comunicaciones de voz (aunque quizá digitalizada) y los últimos de las de datos. Así, entre aquellos procede destacar el cuarto, *Telephone Security* (aunque determinados apartados sólo sean de interés en los ámbitos de la defensa), y sobre todo el quinto, *Secure GSM Systems*, muy amplio y actualizado, llegando a abarcar hasta los sistemas GPRS, o de segunda generación y media. Sin embargo, son de menor audiencia el anteriormente citado tercero y el sexto, *Security in Private VHF/UHF Radio Networks*.

En lo que concierne a la seguridad de los datos –campo mucho más manido para los potenciales lectores–, se puede suponer que comienza con el capítulo décimo, *PC Security*, extendiéndose hasta el ya comentado decimotercero, a través de los de títulos respectivos, *Secure E-mail* y *Secure Virtual Private Network*. Quizá sorprendentemente, si sólo en el título nos fijamos, el de más rentable lectura es el décimo, que expone puntos de vista inéditos en los libros a los que estamos habituados, lo que no acontece con los otros dos, ni con el decimotercero por su carácter muy especializado en lo militar.

Entre ambos grupos de capítulos se localizan el séptimo, octavo y noveno, respectivamente: *Electronic Protection Measure-Frequency Hopping, Link and Bulk Encryption* y *Secure Fax Networks*. El primero y segundo de marcada orientación hacia lo militar, y el tercero –de temática poco usual en los libros de seguridad– de mayor espectro de interés.

A pesar de todo lo anterior, la estructuración expuesta no es tan tajante como pudiera aventurarse. En efecto, en cada capítulo de los que tratan plataformas, redes y sistemas específicos, no sólo se hallan aspectos singulares a los mismos, sino que también se exponen aquellas amenazas específicas al medio (herciano o físico) por el que transitan las informaciones que se tratan de proteger. Y aun más, también se presentan los conceptos y estudian los fundamentos tecnológicos más básicos sobre los que se construyen los sistemas, combinando así una visión diríamos que de alto nivel –plataformas y sistemas–, con otra de nivel más bajo –conceptos y fundamentos tecnológicos–. Todo ello provoca ciertas repeticiones –en capítulos distintos– de los mismos conceptos o tecnologías.

A este respecto, y en descargo del autor, cabe decir que dicho planteamiento, obviamente deliberado, le evita desarrollar unos capítulos introductorios desmesuradamente extensos, que de este modo –como se ha comentado– quedan reducidos a dos y de moderada amplitud. Además, el lector típico –que no es el que lee la obra de principio a fin, sino aquel que sólo se detiene en los capítulos que le pueden servir en su quehacer– se encuentra con capítulos autocontenidos y por tanto de mucha más fácil lectura.

En síntesis, un libro inusual por su temática e interesante por esto mismo, pero con una orientación muy acusada hacia los ambientes vinculados con la defensa, lo que le resta atractivo para la generalidad de potenciales lectores. n

ARTURO RIBAGORDA GARNACHO

Catedrático y Director
del Dpto. de Informática
UNIVERSIDAD CARLOS III
arturo@inf.uc3m.es