



SECRETS & LIES

Digital Security in a Networked World

Autor: Bruce Schneier

Editorial: John Wiley & Sons - Díaz de Santos

Año 2000 - 413 páginas - ISBN: 0-471-25311-1

Sitio: www.diazdesantos.es

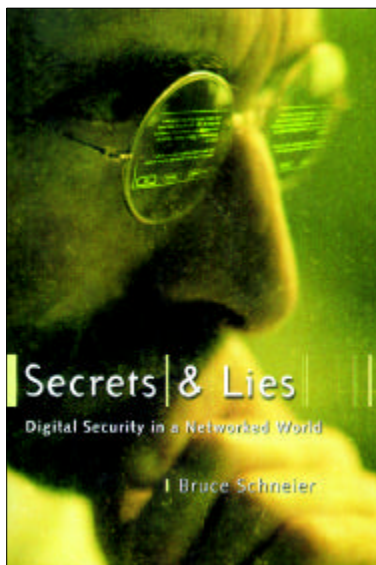
Sin margen de duda, si hay algún reconocido experto en seguridad que se distinga por su vocación divulgadora ese es Bruce Schneier, en cuyo último libro, **Secrets and lies: Digital Security in a Networked World**, editado por **John Wiley & Sons, Inc** publicado el pasado año nos vamos a detener.

El autor (cuyo volumen, ya clásico, *Applied Cryptography. Protocols, algorithms and source code in C*, fue comentado en el número 17 de esta revista -noviembre de 1995-), recoge en la publicación que nos ocupa parte de las reflexiones sobre la disciplina que desde 1998 plasma mensualmente en su universalmente conocido boletín *Cryptogram*, de imprescindible suscripción –gratuita– para todo aquel que desee mantenerse al día en la materia que nos interesa.

Dicho lo anterior, no sorprenderá a los lectores asiduos del boletín citado que la obra ponga de manifiesto su profundo conocimiento de la seguridad, así como sus dotes para transmitir sus saberes.

Entrando en la obra, lo primero que cabe reseñar es que, a diferencia del propósito de *Applied Cryptography*, no nos encontramos estrictamente con un trabajo técnico –si por tal entendemos el formulado en un lenguaje matemático basado en algoritmos y protocolos– aunque la técnica subyazca en todos los capítulos, ni tampoco de administración y organización de la seguridad.

Antes bien sus casi 400 páginas constituyen una fluida, actualizada, documentada y profunda reflexión acerca del alcance y límites de las técnicas usadas en la seguridad, de los errores –a menudo de bulto– que se cometen en su instrumentación, de las cautelas que la más elemental prudencia impone en su aplicación y, en definitiva, una vigorosa llamada de atención a aquellos –muy numerosos, por ser muchos los recién aterrizados a



este campo– que piensan que la seguridad es, en exclusiva, un problema técnico y que por tanto la acumulación de mecanismos redundante, de manera inexorable, en un incremento en los niveles de seguridad.

En síntesis, leyéndolo, se aprecia claramente que la seguridad es un cadena de enorme número y variedad de eslabones, insospechados, sofisticados y multiformes muchos de ellos, permanentemente trabados y mutuamente dependientes, pero siempre tales que la robustez del conjunto, la cadena,

se mide –como el autor asevera en el prefacio– por el eslabón más débil, que no siempre es el más sospechoso. O, como el escritor también afirma: «la seguridad es un proceso, no un producto». O lo que viene a ser igual, de la abismal diferencia entre la teoría y la práctica.

El manual comienza con una breve introducción en la que (tras exponer con ánimo exhaustivo los incidentes de seguridad habidos, tan sólo, en marzo del 2000) presenta el núcleo central de su teoría: la seguridad es un problema enormemente arduo por concernir al sistema en su conjunto y no a sus componentes individuales, cuyas interrelaciones, insospechadas y complejas, pueden producir, y a menudo así acontece, brechas en aquel. Y, aún más, el sistema interactúa con un entorno real, operado por individuos cuya experiencia y sensatez son difícilmente predecibles.

El resto de la obra se articula en tres partes correctamente secuenciadas: *The Landscape, Technologies* y *Strategies*. En la primera, capítulos dos al quinto, se detiene en las amenazas y ataques (imprescindibles, como bien apunta, para responder a la pregunta capital: ¿seguro?, conforme, pero ¿frente a quién y a qué?), para seguir con los adversarios y terminar con los objetivos de la seguridad, que en su opinión trascienden, en mucho, a los clásicos de confidencialidad, inte-

gridad y disponibilidad.

La parte segunda, la más amplia con diferencia (casi 200 páginas), se consagra a estudiar las tecnologías que consolidan la seguridad y de qué tipos de ataques nos protegen. Para ello, empieza por la más básica –la criptografía– y concluye en lo sustancial con los certificados digitales, aunque incorpora al final dos capítulos de difícil entronque en cualquier otra parte: *Security Trick* y *The Human Factor*.

En todos ellos, a pesar de versar sobre materias conocidas, aun el lector más experto descubrirá numerosos aspectos inéditos en los manuales al uso, aspectos que le harán ver con suspicacia todas las tecnologías expuestas. En todo caso, y si tuviese que optar por algunos apartados (lo que dado el nivel general sería para cualquier lector muy problemático), me quedaría con los que sirven de colofón a alguno capítulos: *Choosing an Algorithm or Protocol* (capítulo siete, *Cryptography in Context*), *Future of Secure Computers* (capítulo ocho, *Computer Security*) o *The Future of Network Security* (capítulo once, *Network Security*), o el desmitificador y demolidor *PKI's in the Internet* (capítulo quince, *Certificates and Credentials*).

Finalmente, la tercera y última parte engarza los temas ya tratados para construir un sistema completo de seguridad, evaluando sus vulnerabilidades, sus riesgos (capítulo diecinueve, *Threat Modeling and Risk Assessment*) y verificando la confianza de sus componentes (capítulo veintidós, *Product Testing and Verification*), para construir una política de seguridad que conduzca a la adopción de las pertinentes medidas de protección (capítulo veinte, *Security Policies and Countermeasures*), no como ejercicio teórico, sino antes bien enmarcado en el escenario cotidiano del mundo real.

Destacan singularmente los capítulos veintiuno, *Attack Trees*, y veintitrés, *The Future of Products*, aquél por su originalidad, éste por la previsiblemente atinada visión del porvenir, y ambos por las enseñanzas que transmiten.

En resumen, una valiosa, muy documentada y original obra, no ya por los asuntos tratados, sino por el desarrollo de los mismos y, ante todo, por el punto de vista que adopta: científico –por el aguzado sentido crítico de Schneier– y escéptico –por su dilatada experiencia profesional–. Sin duda alguna, uno de los mejores libros de la materia actualmente en los fondos editoriales, cuyo estudio –que no lectura– se me antoja obligada para cualquier profesional o pretendiente a serlo. n

ARTURO RIBAGORDA

Catedrático de la Universidad Carlos III de Madrid