Arturo Ribagorda

SEGURIDAD Y COMERCIO EN EL WEB

Autores: Simson Garfinkel y Gene Spafford
Editorial: McGraw Hill/Interamericana de España
1999 - 483 págs - ISBN: 970-10-2142-8
Sitio: www.mcgraw-hill.es

Son numerosos los indicadores que ejemplifican el momento estelar que atraviesa la seguridad de las Tecnologías de Información en nuestro país, y uno de ellos es la continua aparición de libros acerca de la materia en nuestra lengua, sean escritos en ésta o traducidos a ella. Uno de estos últimos, de reciente publicación en Méjico, es Seguridad y Comercio en el *Web*, cuya versión original: *Web Security and Commerce* está fechada en 1996. Escrito por dos prestigiosos consultores a la par que conocidos autores (*Practical Unix Security*, aparecido en 1991, PGP, *Pretty Good Privacy*, de 1995 y *Practical Unix and Internet Security*, editado en 1996) la obra está traducida en Méjico, lo que se aprecia de inmediato en los términos y giros allí habituales mas aquí chocantes por inusuales, aunque correctos en castellano (salvedad hecha del consabido «encriptar» y derivados, que por papanatismo o ignorancia tantas veces aparece a ambas orillas del Atlántico). En todo caso es de agradecer y valorar el conocimiento que de la materia muestra el traductor, lo que, entre otros saludables efectos, lleva a compensar mediante notas complementarias al pie los años transcurridos desde su redacción, que si en otras disciplinas resultarían una nadería en la que nos ocupa constituyen un largo y fructífero periodo que vuelve rápidamente obsoleta cualquier publicación sobre la misma.

Entrando en lo sustancial del libro, lo primero que destaca muy favorablemente en relación a otras obras que tratan la seguridad del comercio electrónico –algunas comentadas últimamente en estas mismas páginas– es la amplitud del panorama que contempla. Así, en lugar de mantenerse en el estudio de los aspectos criptográficos (algoritmos simétricos y asimétricos, certificados, Infraestructuras de clave pública, etc.), el manual, haciendo honor a una parte de su título –Seguridad en el *Web*–, se detiene no sólo en aquellos aspectos, sino también en las facetas de protección del *software* y los datos instalados en el *Web*, prestando también atención a los factores administrativos y legales (éstos, por desgracia y como es fácil colegir, exclusivamente estadounidenses) de la seguridad.

Sin embargo, en contra de lo que pudiera temerse de una visión tan global, la profundidad con que se tratan los puntos de vista comentados es satisfactoria, lo que no obsta para que aquellos lectores que precisen de mayor detalle puedan encontrar cumplidas referencias en forma de direcciones URL y citas bibliográficas.

Frente a estos aciertos la obra adolece –en ocasiones y en algunos detalles– de cierta oscuridad expositiva, que impide en esos casos hacerse una idea cabal de lo expuesto. Además, aquellos temas más vinculados a la criptografía (firma, certificados, etc.) pueden encontrarse mejor recogidos en otros manuales aquí reseñados anteriormente.

El libro se estructura en 19 capítulos, agrupados en seis secciones, y concluye con cinco apéndices. La primera de las secciones, «Introducción», consta de un solo capítulo: «Panorama de la seguridad en el *Web*», que en forma de *pot-pourri* presenta los problemas e introduce las soluciones que se detallan a lo largo del manual.

La segunda sección, una de las más interesantes e instructivas, lleva por título «Seguridad del usuario», y en ella se estudian los riesgos que contraemos los individuos que trabajamos con computadoras conectadas (o incluso que lo han estado en algún momento) a la red. Para mayor utilidad los ejemplos se sacan del Navigator de Netscape o del Internet Explorer de Microsoft, lamentablemente de versiones hoy en día atrasadas, lo que el traductor intenta paliar mediante oportunas notas al pie. Para estudiar estos riesgos, se analizan las amenazas presentes en la red y, de manera muy amena, las vulnerabilidades de los navegadores citados, sean intrínsecas a ellos o consecuencia de una descuidada implementación. No menos interés presentan los capítulos consagrados a desvelar los riesgos de los más populares lenguajes de la red: Java y JavaScript, y a las cautelas a adoptar cuando se descargan programas de la red –Capítulo 4: «Descarga de código máquina mediante Active X y *plug-ins*»–. Para concluir la sección –y bajo el título de «Privacía»– se trata de los problemas de divulgación de información del navegante, por ejemplo mediante *cookies*, y las defensas frente a éstas difusiones de información, incluyendo el uso de anonimizadores durante la navegación por Internet.

La sección tercera, «Certificados Digitales», más convencional y ampliamente tratada en otros libros de igual temática que éste[1], contempla en cuatro capítulos que totalizan más de 80 páginas, la estructura de los certificados de clave pública y sus distintos tipos, con especial y notoria dedicación a los usos de los certificados de servidor y la creación, instalación y mantenimiento de los de cliente, así como a los riesgos que ambos comportan. Igualmente, se tratan con intensidad la identificación y autenticación de usuario, enfatizando el empleo de los certificados para tales cometidos. Con menor atención también se repasan las Autoridades de Certificación y las Infraestructuras de clave pública. Para concluir, en un último capítulo: «Firmas de código y el Authenticode de Microsoft», se estudian estos nuevos procedimientos que avalan el *software* distribuido por Internet. Para ello, se pormenoriza cómo firmar y verificar código y cómo obtener un certificado de editor de *software*.

Curiosamente tras esta sección, y no antes como ocurre de ordinario, se halla la de título: «Criptografía» –tradicional y obligada en cualquier tratado sobre seguridad–, que con buen criterio no presta atención a los aspectos más trillados de esta disciplina, sino que antes bien se detiene en los protocolos criptográficos, en las limitaciones a la exportación de productos que instrumentan algoritmos de cifrado y en las leyes que regulan el cometido de estos productos en numerosos países (con muy interesantes resúmenes en las tablas 11.2 y 11.3).

El capítulo que concluye esta sección: «Los protocolos SSL y TLS», sin profundizar teóricamente en ninguno de ellos –lo que para el primero se hace en el apartado C–repasa las características constructivas y rasgos de implementación y uso del SSL, mencionando muy de pasada –tan solo media página– el TLS.

A continuación, la sección bajo nombre: «Seguridad de servidores *web*», –junto con la segunda la más interesante del libro– recorre los problemas de seguridad de estos servidores y las estrategias conducentes a su protección. Para ello, tras dos capítulos en los que se estudian los riesgos que corren estas máquinas y las herramientas y procedimientos de seguridad –incluido un apartado sobre seguridad física– y otro más interesante y completo acerca de los sistemas de control de acceso– con ilustrativos ejemplos para el administrador, se termina con el capítulo 15: «Programación segura con CGI y API», posiblemente el más logrado de esta quinta sección, en el que se enseñan técnicas de programación para hacer más segura la escritura de código CGI y API.

La sección sexta: «Comercio y Sociedad» es la más ligera del manual y se entretiene en temas que preocupan a los usuarios más que a los administradores de seguridad. El capítulo que abre la sección: «Pagos digitales» presenta un extenso tratamiento de las transacciones implicadas en el pago mediante medios telemáticos, desde las más convencionales y antiguas tarjetas de crédito hasta los últimos desarrollos en esta materia: Digicash, Cybercash, SET, etc. A continuación, en «*Software* de bloqueo y tecnologías de censura» se transita por ciertos aspectos inusuales en libros de seguridad, como los programas que limitan el acceso a contenidos supuestamente inapropiados para algunos navegantes como los adolescentes. Especialmente se considera el sistema PICS (*Platform for Internet Content Selection*), que puede estudiarse con más detenimiento en el apéndice D de la última sección del libro. Para cerrar esta sección, los dos últimos capítulos se detienen en aspectos legales, sea en su vertiente civil –capítulo 18: «Consideraciones legales: civiles»–, como penal –capítulo 19: «Consideraciones legales: penales»–. En todo caso, ambos intrascendentes desde nuestra óptica por estar enfocados a la legislación estadounidense.

Como colofón, la séptima sección aglutina cuatro apéndices técnicos y uno más con un amplio conjunto de referencias comentadas donde ampliar cualquier pregunta acerca de la seguridad.

En síntesis, una obra dedicada a los administradores de seguridad, de interés variable –elevado en los temas más inusuales (secciones dos y cinco), más intrascendente en los más manidos (secciones tres y cuatro)–, y algo obsoleta –a pesar de los esfuerzos del traductor–, que en todo caso no merece ser desdeñada, aunque sólo sea como libro de esporádica consulta. ■

[1] *Recuérdese DIGITAL CERTIFICATES: Applied Internet Security, aquí comentado en el penúltimo número de esta revista.*

Arturo Ribagorda
Catedrático de la Universidad
Carlos III de Madrid