LA SEGURIDAD EN LA RED: CORREO Y COMERCIO ELECTRÓNICO

José Manuel Huidobro.
Ingeniero de Telecomunicación

Nadie duda de las muchas ventajas de estar conectado a la Red y las enormes posibilidades que ello nos brinda para comunicarnos, buscar información y realizar negocios, entre otras facilidades; pero estar conectado a Internet y la navegación por el ciberespacio también nos puede proporcionar enormes quebraderos de cabeza si no tenemos en cuenta algunos aspectos básicos de seguridad y, al igual que cuando salimos de casa de vacaciones, tenemos que tomar algunas precauciones, muchas de ellas de sentido común.

Internet es una red descentralizada, a la que tiene acceso, de una manera muy fácil y económica, cualquier usuario que cuente con un simple terminal y una línea de conexión, fija o móvil, de banda estrecha o ancha. Ello hace que estemos expuestos a numerosos ataques, muchísimos más que si se tratase de una red privada. Los más usuales son los virus, troyanos, gusanos y otros códigos maliciosos, como el *spyware*, *phishing*, etc., además de sufrir las molestias del *spam*, *hoax*, *adware*, *etc*. Estos ataques pueden hacer que lleguemos a perder la información o que ésta sea accesible a extraños, o incluso dejar inutilizado el equipo, aparte de ser una herramienta para cometer innumerables estafas, con casi total impunidad, desde cualquier rincón del mundo.

Cada día es más frecuente utilizar Internet, además de para el correo electrónico, para la realización de transacciones electrónicas. Existen muchos tipos diferentes de amenazas que pueden comprometer la seguridad del correo y el comercio electrónico, pero para contrarrestarlas se han desarrollado varios protocolos y aplicaciones usando, entre otras, las técnicas criptográficas.

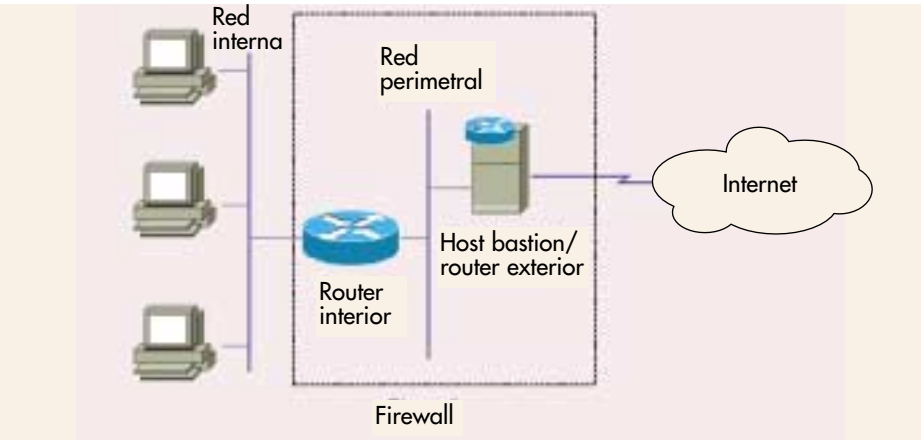
Desde sus comienzos Internet depende de estándares abiertos y este apoyo a los estándares abiertos, junto con el intercambio sin límites de información en Internet, puede hacer que se piense que seguridad e Internet son términos mutuamente excluyentes, pero nada es menos cierto y aunque en el pasado Internet era mucho menos segura que las redes privadas, los esfuerzos por proporcionar una variedad de mecanismos de seguridad al tráfico en Internet han progresado a toda velocidad, de modo que hoy es posible afirmar que puede ser tan segura como una red privada.

Algunas de las medidas de seguridad se están implementado en Internet para hacer de ella una red más segura, además de instalar unos buenos *firewalls* y antivirus, son las diferentes técnicas de cifrado de la información, bien de clave privada o pública (sistemas simétricos y asimétricos) y otros mecanismos a nivel de aplicación, como los que se describen en este artículo.

FIREWALLS. SEGURIDAD ENTRE REDES

Un *firewall* o cortafuegos es un dispositivo «hardware/software» que controla y filtra todo el tráfico entre una red privada e Internet, para evitar que cuando se conectan recursos de la red corporativa o doméstica a una red pública, como es Internet, se pongan en riesgo los datos y los sistemas informáticos.

Los *firewalls* pueden proporcionar protección contra ataques a los protoco-



los o aplicaciones individuales, y ser eficaces en la protección contra impostores. Instrumentan controles de acceso basados en los contenidos de los paquetes de datos que se transmiten entre dos partes o dispositivos en una red. La solución en aplicaciones que requieran de un nivel de seguridad muy elevado pasa por emplear una configuración con zona desmilitarizada o DMZ (*DeMilitarized Zone*). Se trata de utilizar una subred (DMZ) entre las redes interna y externa de manera que un atacante que logre burlar el host bastión no tenga acceso a la red interna.

Una de las ventajas más importantes de un *firewall* es que proporciona un punto de control único para la seguridad en una red. Aunque claro, esto puede ir en contra del propio sistema, ya que también puede ser un punto único de fallo y, por lo tanto, recibir la los ataques concentrados de los intrusos. Los *firewalls* controlan los puertos lógicos de nuestro ordenador, que son los puntos de comunicación del ordenador con la red Internet y cada vez que se establece una conexión se hace a través de alguno de ellos. Por ejemplo a través del puerto 80 se tiene la navegación Web, por el 110 se accede al servicio de POP3 que permite recibir *e-mails;* a través del puerto 25 al servicio SMTP, que permite enviarlos; a través del puerto 21 se pueden realizar operaciones FTP, o transmisión de archivos; a través del puerto 139 la NETBIOS deja abierta toda la información del disco duro a posibles ataques exteriores. Los intrusos pueden escasear nuestros puertos, localizar los abiertos y utilizar las vulnerabilidades de las aplicaciones para causarnos daño.

Los *firewalls* no preservan el carácter privado de los datos y, en la mayoría de los casos, no garantizan la confidencialidad de los mismos-, ni tampoco pueden proteger una red contra los virus ya que no verifican su presencia, por lo que siempre se deben instalar en conjunción con un buen y actualizado antivirus.

CIFRADO DE DATOS

Para preservar la confidencialidad de la información se recurre al cifrado de los datos. Los algoritmos de cifrado (encriptación) más comunes, son:

- **DES** (*Data Encryption Standard-Estándar*) es un codificador de bloque creado por IBM, avalado por el gobierno de los Estados Unidos en 1997. Usa una clave de 56 bits y opera en bloques de 64 bits. Relativamente rápido; se usa para cifrar grandes cantidades de datos simultáneamente.
- **Triple DES** basado en DES. Cifra un bloque de datos tres veces, con tres claves diferentes. Es una alternativa al DES y su uso se incrementa día a día, pues existe la posibilidad de violar el DES con facilidad y rapidez, mediante ataques de fuerza bruta.
- **RC2 y RC4,** diseñados por RSA Data Security Inc. Codificadores de tamaño de clave variable para cifrado rápido. Más veloces que DES, los dos algoritmos se pueden hacer más seguros al seleccionar un tamaño de clave más grande. RC2 es un codificador de bloque mientras que RC4 es un codificador de flujo y es 10 veces más veloz que DES.
- **IDEA** (*International Data Encryption Algorithm*). Creado en 1991 y diseñado para ser eficaz. Ofrece un cifrado muy poderoso, pues usa una clave de 128 bits.
- **RSA.** Llamado así en honor de Rivest, Shamir y Adelman, sus diseñadores. Es un algoritmo de clave pública que soporta una longitud de clave variable y del bloque de texto a encriptar, que debe ser más pequeño que la longitud de la clave. La longitud común de la clave es 512 bits. Es muy lento, por lo que se suele utilizar sólo para el intercambio de claves y la firma electrónica, em pleándose DES u otro algoritmo para el cifrado de la información (texto simple).
- **Diffie-Hellman.** El criptosistema de llave pública más antiguo todavía en uso. No soporta el cifrado ni las firmas digitales. El sistema está diseñado para permitir que dos individuos se pongan de acuerdo en una llave compartida, aunque sólo intercambian mensajes en público.
- **DSA** (*Digital Signature Algorithm*), desarrollado por NIST con base en el llamado algoritmo «El Gamal». El esquema de firma usa el mismo tipo de llaves que Diffie-Hellman, y puede crear firmas más rápido que RSA. Impulsado por NIST como DSS (*Digital Signature Standard*).

Estos mecanismos de cifrado, junto con la firma electrónica que proporcionan las autoridades de certificación, sirven para garantizar la confidencialidad de los mensajes y su autenticidad, garantizando que el remitente es quien dice ser.

SEGURIDAD EN EL CORREO Y COMERCIO ELECTRÓNICO

Además de los algoritmos de cifrado comentados, para aumentar la seguridad del correo y las transacciones económicas, a través de Internet, se utilizan algunos de los estándares de seguridad que se muestran en la tabla siguiente:

Estándar	Función	Aplicación
S-HTTP	Asegura las transacciones en la web	Exploradores, servidores, web aplicaciones para Internet
SSL	Asegura los paquetes de datos en la capa de la red	Exploradores, servidores web, aplicaciones para Internet
S/MIME	Asegura los anexos de correo electrónico en plataformas múltiples	Paquetes de correo electrónico con cifrado RSA y firma digital
PGP	Protege mediante cifrado el correo electrónico	Paquetes de correo electrónico
SET	Asegura las transacciones con tarjeta de crédito	Tarjetas inteligentes, servidores de transacción, comercio electrónico

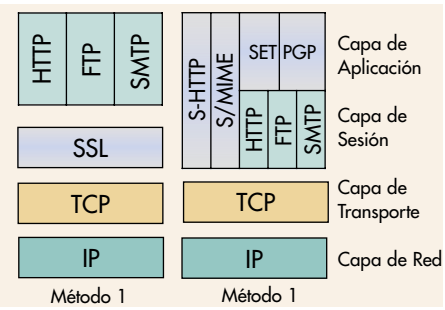
CORREO. PEM, S/MIME Y PGP

Se ha propuesto una variedad de protocolos de seguridad para el correo electrónico (*e-mail*) en Internet, pero sólo uno o dos han tenido aceptación. El correo enriquecido con carácter privado PEM (*Privacy-Enhanced Mail*) es un estándar de Internet para asegurar al correo electrónico usando claves públicas o simétricas. En la actualidad PEM se utiliza poco pues no está diseñado para manejar el moderno correo electrónico multimedia soportado por S/MIME, además de que requiere una jerarquía rígida de autoridades de certificación para emitir las claves.

S/MIME (*Secure/Multipurpose Internet Mail Extensions*) es un estándar del IETF (*Internet Engineering Task Force*) basado en certificados X.509 y en una implementación de Infraestructura de Clave Pública (PKI); proporciona firmas digitales, no-rechazo y encriptación punto a punto. Este nuevo estándar puede utilizar muchos de los algoritmos criptográficos más modernos, pero depende de certificados digitales, por ello también depende de algún tipo de autoridad de certificación, ya sea corporativa o global, para asegurar la autenticación.

S/MIME es un protocolo de seguridad para correo electrónico desarrollado por RSA, Inc., valioso y ampliamente utilizado para certificar la identidad del remitente, proteger los correos electrónicos durante el proceso de transmisión y para validar las credenciales del receptor. Las aplicaciones compatibles con S/MIME pueden enviar y recibir mensajes de correo electrónico seguros (con cifrado y firmado). Este protocolo ha sido adoptado por un amplio número de compañías, entre las que se incluyen Microsoft y Netscape.

PGP (*Pretty Good Privacy*) es una aplicación desarrollada para asegurar los mensajes y archivos que puede emplear una gran variedad de estándares de cifrado; así, los mensajes se pueden cifrar antes de usar un programa de correo electrónico. Probablemente sea la aplicación de seguridad para correo electrónico en Internet más utilizada. PGP está disponible de manera gratuita para la mayoría de los sistemas operativos importantes. PGP se diseñó alrededor del concepto de una red de confianza que permitía a los usuarios compartir sus claves, sin requerir una jerarquía de autoridades de certificación.



COMERCIO. S-HTTP, SSL Y SET

Los estándares se pueden clasificar de acuerdo a si proporcionan seguridad de conexión o de aplicación. Así, el estándar SSL (*Secure Sockets Layer*) está diseñado para mantener comunicaciones seguras en Internet, aunque SSL se usa primariamente con aplicaciones para la web. Por el contrario, Secure HTTP (S-HTTP), está dirigido a proporcionar autentificación y preservar el carácter privado de las aplicaciones y SET (*Secure Electronic Transaction*) va un paso más allá al proporcionar seguridad a las transacciones de comercio electrónico.

S-HTTP y SSL proporcionan autentificación para servidores y navegadores, así como confidencialidad e integridad de los datos para las comunicaciones entre un servidor web y un navegador. S-HTTP está diseñado específicamente para soportar el protocolo de transferencia de hipertexto HTTP, proporcionando la autorización y seguridad de los documentos. SSL ofrece métodos de protección similares, pero asegura el canal de comunicaciones al operar a un nivel más bajo (entre la capa de aplicación y las capas de red y transporte).

Los sistemas SSL y S-HTTP tienen la gran ventaja de la absoluta transparencia para el usuario, que no necesita ningún tipo de preparación ni conocimiento previo, y garantizan plenamente la identidad del vendedor y que sólo él recibirá los datos involucrados en la transacción. En cambio presentan el grave inconveniente de que no se garantiza la identidad del comprador, por lo que puede aparecer el problema del repudio. En la actualidad, la mayoría de las empresas que venden en Internet utilizan este sistema.

Con todos estos mecanismos, correctamente aplicados, podemos casi estar seguros de nuestras transacciones y confiar en mantener la confidencialidad y autenticidad de toda la información, tanto la que circule por la Red como la que tengamos en nuestros sistemas.