Conciencia Tecnológica
ISSN: 1405-5597
contec@mail.ita.mx
Instituto Tecnológico de Aguascalientes
México

Dávila Muro, Jorge; Luna Ramírez, Enrique
Seguridad y comercio por internet
Conciencia Tecnológica, núm. 13, 2000
Instituto Tecnológico de Aguascalientes
Aguascalientes, México

SEGURIDAD Y COMERCIO POR INTERNET

Jorge Dávila Muro
jdavila@fi.upm.es
Facultad de Informática
Universidad Politécnica de Madrid
España

Enrique Luna Ramírez[1]
fp22067@zipi.fi.upm.es
Depto. Sistemas y Computación
Instituto Tecnológico de Aguascalientes
México

RESUMEN

En el mundo de hoy, el uso de las redes de computadoras está presente en casi todas las actividades humanas, tales como la educación, las transacciones bancarias, las declaraciones de impuestos, y en especial en el comercio, entre otras. Sin embargo, a pesar de su amplio uso, las redes aún enfrentan serios problemas en cuestiones de seguridad. Para resolver estos problemas se han desarrollado diversas tecnologías y modelos. En este artículo, se analizan algunos de ellos en base a un enfoque funcional, realizado de acuerdo al aspecto de seguridad que pretenden resolver. De este análisis se concluye que para hacer segura la red interna de una organización y su comunicación con el exterior, es necesario utilizar diversos mecanismos tecnológicos en conjunto con la planificación y políticas específicas de la organización.

1. INTRODUCCIÓN

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envío, principalmente, de correo electrónico y otros datos, y por empleados corporativos para compartir recursos caros como impresoras. En estas condiciones, la seguridad no recibió mucha atención pues realmente no lo exigía la naturaleza de lo transmitido. Pero ahora, cuando millones de personas usan y pretenden usar las redes para sus transacciones bancarias, compras y declaraciones de impuestos, la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones.

La seguridad es un tema amplio que cubre una amplia variedad de problemas. En su forma más sencilla, se ocupa de garantizar que los curiosos no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios; es decir, se preocupa de evitar que la gente no autorizada acceda a servicios remotos restringidos.

La mayoría de los problemas de seguridad son causados intencionalmente por gente que intenta ganar algo o hacerle daño a alguien. Algunos tipos de usuarios y sus eventuales acciones más comunes que intentan violar la seguridad se listan en la tabla 1. A este tipo de usuarios se les llamará adversarios.

Adversario	Meta
Estudiante	Divertirse husmeando el correo de otra gente.
Hacker	Probar el sistema de seguridad de alguien; robar datos.
Representante de ventas	Indicar que representa a toda Europa, no sólo a Andorra.
Hombre de negocios	Descubrir el plan estratégico.
Ex empleado	Vengar su despido.
Contador	Estafar dinero de una compañía.
Corredor de bolsa	Negar una promesa hecha a un cliente por correo electrónico.
Timador	Robar números de tarjeta de crédito.
Espía	Conocer la fuerza militar de un enemigo.
Terrorista	Robar secretos de guerra bacteriológica.

Tabla Nº 1. Tipos de problemas de seguridad que causan algunos adversarios[1].

Queda claro, en base a esta lista, que hacer segura una red comprende mucho más que simplemente mantener los sistemas libres de errores; implica ser más hábil que los adversarios, a menudo inteligentes, dedicados y a veces bien financiados.

Los problemas de seguridad de las redes pueden dividirse en términos generales en cuatro áreas interrelacionadas: secreto, validación de identificación, no rechazo y control de integridad. El secreto tiene relación con mantener la información fuera del alcance de usuarios no autorizados; esto es lo que normalmente viene a la mente cuando la gente piensa en la seguridad de las redes. La validación de identificación se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios. El no rechazo se encarga de las firmas: ¿cómo comprobar que su cliente realmente colocó una orden electrónica por 10 millones de tornillos a 89 centavos de Dólar cada uno

[1] Doctorando del Instituto Tecnológico de Aguascalientes (México) en la Facultad de Informática de la Universidad Politécnica de Madrid. Este trabajo cuenta con el auspicio del Consejo Nacional de Ciencia y Tecnología de México (CONACYT).

cuando él luego alega que el precio era de 69 centavos? Por último, ¿cómo puede asegurarse de que el mensaje recibido realmente fue el enviado, y no algo que un adversario modificó en el camino o elaboró por su propia cuenta?.

Para todos estos problemas se han desarrollado diversas tecnologías tales como firewalls y protocolos para autenticación, envío de mensajes, seguridad en la Web, y seguridad del comercio electrónico; sin embargo, a pesar de estas tecnologías, aún continúa la investigación y el desarrollo, y por lo tanto el problema sigue abierto.

Este artículo trata de forma empírica el tema de la seguridad en Internet, y más específicamente el problema de seguridad del comercio electrónico a través de la Web. Este trabajo se encuentra estructurado en 6 secciones, partiendo con la introducción sobre la situación actual, y continúa con el análisis del problema de seguridad en la Web y del comercio a través de ésta. Después, se discuten algunas soluciones tecnológicas existentes. Finalmente, se presentan las conclusiones del trabajo.

2. EL PROBLEMA DE SEGURIDAD EN INTERNET

La seguridad en Internet requiere de un conjunto de procedimientos, prácticas, y tecnologías orientadas a proteger los servidores Web, a sus usuarios, y a las organizaciones a las cuales pertenecen. Algunas razones del porqué los servidores Web deben estar protegidos por mecanismos de seguridad son:

- **Comercio**. Muchos servidores Web tienen relación con el comercio y sus transacciones financieras. Los protocolos criptográficos construidos en el navegador Netscape® y en otros browsers fueron creados originalmente para permitir a los usuarios enviar sus números de tarjetas de crédito a través de Internet sin temor alguno. Así es como los servidores Web se han convertido en depósitos de información financiera, haciéndolos un blanco atractivo para muchos adversarios.
- **Información propietaria**. Las organizaciones están utilizando la tecnología Web como una forma fácil de distribuir información ya sea internamente, a sus propios miembros, ó, externamente, a socios alrededor del mundo. Esta información patentada es un blanco para la competencia y los enemigos.
- **Acceso a la red**. Ya que los servidores Web son usados por gente dentro y fuera de una organización, estos se extienden efectivamente a las redes internas y externas de la organización. Su posición privilegiada en la conectividad de toda la red hace a los servidores Web un blanco ideal para el ataque, dado que un servidor Web corrompido puede ser usado para atacar otros puntos internos de la organización.
- **Ampliación de los servidores Web**. Por su naturaleza, los servidores Web están diseñados para ser extendidos. Esta característica hace posible conectar los servidores con bases de datos, y otras aplicaciones en la red de una organización. Si los módulos asociados al servidor no son implementados adecuadamente, estos pueden comprometer la seguridad del sistema entero.
- **Ampliación de los Web browsers**. De la misma forma que los servidores se pueden extender, también lo pueden hacer los clientes Web. Las tecnologías tales como ActiveX, Java, JavaScript, VBScript, y otras pueden enriquecer las aplicaciones Web con nuevas y variadas características que no son posibles sólo con el lenguaje HTML. Desafortunadamente, estas tecnologías también pueden ser subvertidas y empleadas contra los usuarios del browser (a menudo sin el conocimiento de ellos).
- **Interrupción del servicio**. Ya que la tecnología Web está basada en la familia de protocolos TCP/IP, está sujeta al problema la interrupción del servicio: ya sea accidental ó intencionalmente. La gente que usa esta tecnología debe tener cuidado de fallos y prepararse para interrupciones significativas del servicio.
- **Soporte complejo**. Los Web browsers requieren servicios externos tales como DNS (Domain Name Service) e IP (Internet Protocol) para funcionar adecuadamente. Sin embargo, estos servicios pueden ser vulnerables a accidentes y ataques. El hecho de corromper un servicio de más bajo nivel, puede significar problemas tanto para el servicio mismo, como para los browsers.
- **Crecimiento**. El crecimiento explosivo de la Web ha sido dirigido por un ritmo frenético de innovación y desarrollo. Se están desarrollando plataformas y software con nuevas características, a menudo con una mínima consideración sobre aspectos tan importantes como el diseño y la seguridad. La presión del mercado obliga a los usuarios a adoptar estas nuevas versiones para mantenerse competitivos. Sin embargo, el nuevo software puede no ser compatible con las características del anterior ó puede tener nuevas

vulnerabilidades desconocidas para los usuarios en general, e incluso para los expertos.

Partes principales del problema de seguridad

1. Asegurar el servidor Web y los datos y funcionalidades que hay en él. Se necesita estar seguro que el servidor puede continuar su operación, que la información en el servidor no es modificada sin autorización, y que la información es distribuida sólo a quienes se quiere que sea distribuida.
2. Asegurar la información que viaja entre el servidor Web y el usuario. Sería deseable asegurar la información que el usuario proporciona al servidor (usernames, passwords, información financiera, etc.), para que no se pueda leer, modificar, ó destruir por otros. Muchas tecnologías de red son especialmente susceptibles al espionaje debido a que la información es transmitida a cada computadora que está en la red de área local.
3. Asegurar la propia computadora del usuario. Sería deseable tener una forma de asegurar a los usuarios que la información, datos, ó programas bajados a sus sistemas no causarán daño alguno. Sería deseable también tener una forma de asegurar que la información bajada es controlada de acuerdo a la licencia o derechos de autor del usuario.

A continuación se describen con mayor detalle estos puntos.

Seguridad en el servidor Web

La seguridad en un servidor Web se plantea en dos dimensiones. Primero, la computadora misma (el servidor) debe ser asegurada utilizando técnicas tradicionales (por ejemplo, uso de passwords, niveles de seguridad, etc.). Estas técnicas permiten que los usuarios autorizados al sistema tengan las facilidades para realizar su propio trabajo, y sólo esas facilidades. Así entonces, se pueden autorizar usuarios anónimos para leer los contenidos de la página Web principal, pero no para alterar los archivos del sistema. Estas técnicas tradicionales evitan también que las personas en Internet que no son usuarios autorizados del sistema, puedan entrar al mismo.

Por otro lado, la seguridad del servidor se complica cuando además de su función como tal, este se utiliza como una computadora tradicional de tiempo compartido. Esto es debido a que el servidor puede ser usado para aprovechar los eventuales fallos de seguridad en el host, y estas a su vez, pueden ser utilizadas para detectar problemas en el servidor. Por ejemplo, un script CGI deficiente puede permitir la modificación de algún archivo de configuración del servidor, de manera que éste funcione con privilegios excesivos para su cometido. Aprovechando los fallos de seguridad del host, un adversario podría crear otro script CGI con privilegios tales que le daría acceso total al sistema. Así, una de las mejores estrategias para mejorar la seguridad del servidor, es minimizar el número de servicios proporcionados por el host en el cual el servidor está instalado y cuidar la calidad de estos. Por ejemplo, si se necesitan un servidor de correo y un servidor Web, lo más conveniente es situarlos en máquinas diferentes.

Seguridad de la información en tránsito

Los riesgos más comunes de seguridad que presenta la información en tránsito son el espionaje, la sustitución o suplantación, y la "negación del servicio". Existen muchas formas de proteger la información del espionaje y de la sustitución cuando esta viaja a través de una red: asegurar físicamente la red, de manera que el espionaje sea imposible, ocultar la información que se desea asegurar en la información visible, y cifrar la información de manera que no pueda ser descifrada por alguien que no posea la clave adecuada. De estas técnicas, el cifrado es la única de utilidad práctica. Asegurar Internet físicamente es imposible. Ocultar la información sólo funciona si la gente de quien se oculta, no sabe de este hecho.

Por otra parte, como ya se mencionó, otro riesgo para la información en tránsito es un ataque de "negación del servicio" resultado de una interrupción en la red. Una "negación del servicio" puede ser el resultado de un evento físico, tal como un corte en la fibra, ó de un evento lógico, tal como un fallo en las tablas de encaminamiento de Internet. O puede ser el resultado de un ataque sostenido que proviene de adversarios en Internet, contra los servidores: el adversario podría tratar de "bombardear" el servidor Web con miles de peticiones cada segundo. En la actualidad no existe una forma práctica de defenderse contra ataques de "negación del servicio", aunque la redundancia y los sistemas de respaldo pueden ayudar a minimizar su impacto y facilitar su detección.

Seguridad en la computadora del usuario

Aunque el lenguaje HTML y los archivos de imágenes no representan una amenaza para los usuarios (más allá de los problemas legales que pudieran surgir del contenido de los archivos), sí limitan las posibilidades

de interacción en las aplicaciones Web. A esto se debe que las compañías estén promoviendo otras tecnologías tales como JavaScript, Java, ActiveX, y la tecnología plug-in. Estos lenguajes de programación y entornos de ejecución proporcionan a los desarrolladores una manera de crear páginas Web "vivas" y otros tipos de aplicaciones que no son posibles con HTML. El poder agregado a estos sistemas activos también ha creado nuevos peligros. Después de su presentación, hubo repetidos problemas de seguridad adjudicados a JavaScript, Java, y ActiveX. También ha habido problemas de seguridad con respecto al plug-in de Netscape Navigator[3].

Así mismo, los desarrolladores de tecnología Web también desean estar protegidos de los usuarios. Las compañías que ponen información pay-per-view en un Web site desean evitar que los usuarios bajen esta información y la compartan con otros que no han pagado por el servicio. Es muy difícil imponer soluciones técnicas que limiten la dispersión de la información una vez que esta ha sido proporcionada al usuario. Si los datos son visualizados en pantalla, esa información puede simplemente copiarse para ser guardada en un archivo ó para su impresión. Aunque se han propuesto un cierto número de sistemas de "protección contra copia" para los datos Web, todos ellos pueden ser violados. Sobre el mejor método disponible para algunas formas de datos binarios está "digital watermarking". Este método consiste en hacer alteraciones ocultas muy pequeñas a los datos para guardar una forma de identificación del material. El usuario no se puede dar cuenta de las alteraciones, y con ello se espera que no se puedan borrar. Imágenes, archivos de sonido, y otros datos marcados se pueden examinar con programas que encuentran y despliegan la información de identificación, mostrando así al propietario y posiblemente el nombre de la persona que hizo la primera copia.

3. EL PROBLEMA DE SEGURIDAD DEL COMERCIO A TRAVES DE INTERNET

La protección de los números de tarjetas de crédito usados en las transacciones on-line es el ejemplo más citado de contar con sistemas de seguridad para el comercio a través de la Web. Por lo tanto, consideremos este ejemplo y veamos cómo suceden las transacciones usando tarjetas de crédito, qué riesgos existen, y cómo la seguridad en la Web hace su aportación. Considérese una transacción típica en la Web: comprar un CD de una tienda de música con una tarjeta de crédito. En este ejemplo, un usuario a través de su computadora, encuentra una tienda de música en la Web, y revisa el catálogo de la compañía. Encuentra un disco compacto de su interés. Crea una orden con la carta de compra electrónica de la tienda, escribe sus datos, incluyendo el número de la tarjeta de crédito, y la envía. El CD llega por correo. Un mes más tarde, él recibe el estado de cuenta de la tarjeta de crédito. Para este usuario, existen dos riesgos obvios:

- El número de tarjeta de crédito podría ser detectado por algún adversario cuando este viaja a través de Internet. Esa persona pudiera utilizar el número para cometer fraude. Para empeorar las cosas, el dueño de la tarjeta podría no darse cuenta que el número ha sido robado hasta que el estado de cuenta fuera recibido. Por ese tiempo, el límite de crédito de la tarjeta probablemente haya sido excedido con cargos fraudulentos.
- El cargo por la compra podría ser hecho, pero el CD nunca ser entregado en su destino. Cuando el usuario trate de indagar, puede encontrar que no existe esa tienda de música: todo fue un fraude.

Una posible solución a este problema es el protocolo Secure Socket Layer (SSL) de Netscape [2], el cual fue diseñado precisamente para combatir estos dos riesgos. SSL usa el cifrado [4], una técnica matemática para codificar la información, de manera que los datos enviados entre el browser del cliente y el servidor de la tienda de música no puedan ser “interpretados” cuando están en tránsito. SSL también posee un sofisticado sistema de identificación digital para que el cliente tenga cierta seguridad de que la gente que opera el servicio de la tienda de música es quién dice ser. En la siguiente sección se analizará con mayor detalle a SSL.

Con este ejemplo, se ha descrito básicamente el problema de la seguridad del comercio a través de la Web. Las soluciones que se requieren, son a su vez parte del problema general de la seguridad en Internet, y por lo tanto, en la siguiente sección, se analizarán de forma general las soluciones para Internet y cuando sea necesario se matizarán las soluciones del problema específico del comercio.

4. FIREWALLS Y PROTOCOLOS DE SEGURIDAD

Firewalls

Un firewall es un dispositivo (usualmente una computadora que ejecuta un sistema operativo especialmente escrito ó modificado) que aisla la red interna de una organización del resto de Internet, permitiendo sólo conexiones específicas y bloqueando otras. Idealmente, los firewalls están configurados de manera que todas las conexiones externas pasen a

través de puntos monitorizados. Con esta actividad, los firewalls son parte de la estrategia de seguridad de una organización. Desafortunadamente, muchas organizaciones han basado su estrategia de seguridad sólo en los firewalls. Se han dado casos de organizaciones que han tenido serios problemas de seguridad en sus redes internas, y han intentado "resolverlos" usando simplemente un firewall para bloquear el acceso externo. Muchos ataques vienen de empleados deshonestos, y no del exterior, de manera que en estos casos los firewalls desvían la atención de otros problemas igualmente importantes, tales como la vulnerabilidad de la red interna, y la falta de planificación y de políticas corporativas ó institucionales. Así, los firewalls a menudo mejoran la seguridad sólo en cierta medida, y en el proceso, dan un falso sentido de seguridad.

Sin embargo, existen algunas situaciones en las cuales el uso de un firewall se hace necesario. Una de ellas se da cuando una organización debe usar "sistemas heredados" antiguos que no pueden ser asegurados; en este caso se puede usar un firewall para controlar el acceso a este tipo de sistemas.

Así, un firewall debería ser usado sólo para lograr seguridad adicional que opere en conjunto con otros sistemas de seguridad internos, y nunca como un sustituto de los mismos.

¿Cómo se puede situar un servidor Web respecto a un firewall?

Si una organización usa un firewall para proteger su red interna de ataques externos, se tiene una serie de alternativas donde situar el servidor Web:

- Se puede situar el servidor Web fuera del firewall. La ventaja es que el servidor puede estar sujeto a ataques de adversarios, y en caso de que este no resista, no les servirá de mucho para emprender más ataques contra la organización. Cabe destacar que en este caso, el servidor no se verá beneficiado de la protección que el firewall ofrece.
- Se puede situar el servidor Web dentro del firewall. Si se hace esto, será necesario configurar el firewall de manera que éste envíe las transacciones por el puerto TCP 80, permitiendo pasar los paquetes ya sea directamente ó usando un mecanismo compatible (proxying). La ventaja de situar el servidor detrás del firewall es que este no permitirá a los usuarios externos usar algunos servicios de Internet, tales como Telnet y FTP. Sin embargo, si los adversarios logran corromper el servidor debido a un script CGI deficiente, tendrán acceso total a la red interna. Cabe señalar que un servidor Web asegurado adecuadamente no obtiene ningún beneficio cuando se sitúa dentro de un firewall; esto se debe a que un servidor asegurado ofrece sólo dos servicios TCP/IP al mundo externo: http en el puerto 80, y http con SSL en el puerto 443. Si el servidor se sitúa detrás del firewall, se tendría que programar el firewall para que haga las conexiones de entrada en los puertos 80 y 443 entre las computadoras e Internet.
- Una tercera opción es usar dos firewalls: uno para proteger la red interna y otro para proteger el servidor Web. En este caso el sistema se complica considerablemente, favoreciendo la aparición de errores o problemas de seguridad debidos a una deficiente configuración y/o coordinación de los diferentes firewalls.

Autenticación

Casi todas las técnicas de autenticación personal dependen de passwords en cierta medida. Sin embargo, los passwords constituyen una de las mayores vulnerabilidades de los sistemas de seguridad. Las mayores amenazas para la autenticación basada en passwords son:

- Espionaje de las comunicaciones. Un adversario que monitoriza las comunicaciones puede descubrir un password si este se transmite sin protección sobre una línea de comunicación ó una red.
- Replicar. Aún si un password es cifrado para su tránsito, es posible que un adversario pueda monitorizar las comunicaciones para interceptarlo, y enviarlo más tarde a su destino como si fuera legítimo.
- Ensayo y error. Un adversario intenta diferentes passwords hasta lograr el éxito. Si los passwords vienen de un conjunto suficientemente grande de valores posibles, esto sería poco práctico. Sin embargo, con un selector de passwords, existe la posibilidad de escoger valores obvios, tales como la fecha de nacimiento ó el número de teléfono de un usuario. Un adversario puede sacar ventaja significativa simplemente ensayando este tipo de valores como una primera opción (ataques por diccionario).
- Host corrompido. Un adversario ingresa a un sistema de cómputo que contiene una base de datos de passwords.

Teniendo en cuenta las amenazas anteriores, se requieren procedimientos efectivos para la gestión de passwords, el uso responsable de los mismos, y la

disponibilidad de sistemas de autenticación bien diseñados.

Protocolos de autenticación

Cuando la única tecnología disponible para el usuario es un simple dispositivo de comunicaciones tal como un teléfono ordinarios, no se puede hacer gran cosa para enfrentar las amenazas a la seguridad de un sistema. Sin embargo, si el dispositivo terminal es más inteligente, ó si se usan dispositivos auxiliares tales como las tarjetas inteligentes, es posible enfrentar estas amenazas usando protocolos de autenticación entre el usuario y el sistema host que ejecuta la autenticación. Tales protocolos típicamente se construyen en la capa de red ó en la capa de aplicación. Algunos de los elementos más importantes de los protocolos de autenticación son:

- Transformación de Password. El password de un usuario que se comunica a un host es procesado a través de una función, la cual regresa como resultado un password transformado. El host puede aplicar la misma función a su copia almacenada del password, y si los resultados son idénticos, se concluye que el usuario proporcionó el valor correcto. Así, será difícil para un espía obtener el password a partir del valor transmitido.
- Respuesta de Contraseña. El host envía al usuario un valor aleatorio llamado contraseña, diferente para cada petición de autenticación. Este valor debe ser incorporado en la respuesta del usuario, por ejemplo, como una entrada adicional a la función que calcula el password transformado. En el proceso de respuesta, el host confirma que se usó la contraseña correcta. Esto proporciona protección contra ataques de réplica.
- Marca de tiempo. La petición de autenticación del usuario hacia el host lleva la hora actual almacenada en este, por ejemplo, como una entrada adicional a la función que calcula el password transformado. En el proceso de respuesta, verifica que el tiempo proporcionado es razonable. Este es otro método para protegerse contra ataques de réplicas, pero tiene limitaciones prácticas porque depende de que todos los sistemas tengan sus relojes suficientemente sincronizados y que estos sean seguros.
- Password one-time. Este mecanismo es, esencialmente, un password transformado que genera un password on-line diferente cada vez que el password del usuario pasa a través de una función que depende de un valor n, el cual se decrementa en 1 por cada nuevo intento de login. El sistema host mantiene el registro de los valores de n y del último password on-line usado. Un espía que observa un password no puede deducir otros futuros passwords porque la función no tiene inversa. El sistema resultante es relativamente simple de implementar tanto en el sistema cliente como en el sistema host. Este mecanismo protege contra ataques de réplicas y además contra la monitorización del canal de comunicación.
- Firma digital. Las firmas digitales son la base de muchos protocolos de autenticación modernos en los cuales el usuario demuestra tener posesión de una llave privada particular al firmar un mensaje de protocolo, ó un campo en un mensaje. Los datos firmados pueden contener una contraseña ó una marca de tiempo para protegerse contra amenazas de réplica.
- Técnicas zero-knowledge. Las técnicas zero-knowledge o de “conocimiento nulo”[5] (véase[3]) constituyen una tecnología criptográfica basada en sistemas de prueba interactivos. Una técnica de este tipo es un medio por el cual se puede verificar la posesión de información sin que ninguna parte de esa información tenga que revelarse. Estas técnicas pueden ser criptográficamente más fuertes que otras técnicas criptográficas convencionales y pueden usar menos recursos de procesamiento. Sin embargo, muchas de estas técnicas requieren protocolos de intercambio más complejos ya que es necesario transferir más datos, de manera que se consumen más recursos de comunicación.

Buenos protocolos de autenticación, que combinen varios elementos como los descritos anteriormente, son difíciles de diseñar. Los protocolos de autenticación a menudo están combinados con protocolos que hacen uso de llaves de sesión para asegurar que éstas sean utilizadas entre las partes correctas. Véase Diffie, et al.[6] (véase[3]), un paper clásico sobre “the pitfalls of combining authentication protocols with Diffie-Hellman key agreement”. Kerberos es un ejemplo interesante de un sistema de autenticación completo y clásico que incluye protocolos de autenticación sofisticados, basados completamente en criptosistemas simétricos .

Protocolos para la seguridad en el envío de mensajes

Las aplicaciones de envío de mensajes presentan un buen ejemplo de una clase de aplicaciones cuyas necesidades no pueden ser satisfechas solamente por las medidas de seguridad en la red. El envío seguro de mensajes demanda protección en un ambiente en el cual los mensajes pueden cruzar múltiples conexiones

de redes y pueden ser almacenados y reenviados a través de sistemas desconocidos.

Seguridad MIME

Un mensaje en Internet comprende un conjunto de cabeceras y el cuerpo del mensaje. Multipurpose Internet Mail Extensions (MIME) es un conjunto de especificaciones que soportan la estructuración del cuerpo de un mensaje, en términos de las partes de un cuerpo. Las partes de un mensaje pueden ser de varios tipos, tales como texto, imágenes, audio, ó mensajes completos encapsulados. Un mensaje ó parte de él tiene un tipo de contenido que define su estructura y tipo.

The Internet Engineering Task Force ha trabajado en el desarrollo de servicios de seguridad para usarlos en conjunto con los mensajes de formato MIME. Este trabajo, que fue finalizado en 1995, dió como resultado dos tipos de especificaciones que resuelven dos partes diferentes del problema de seguridad MIME:

- Multipartes de seguridad para MIME. Esta especificación define dos estructuras de mensajes (los tipos de contenido MIME) que permiten la firma digital y el cifrado de un mensaje ó parte de este . Los dos tipos de contenido, llamados *multiparte/firmada* y *multiparte/cifrada*, son subtipos de un tipo de contenido MIME más general llamado *multiparte*, que es usado para estructurar los mensajes cuyos cuerpos comprenden varias partes.
- Servicios de seguridad para objetos MIME (MOSS). Esta especificación define un conjunto de procedimientos y formatos para las partes del cuerpo de un mensaje, con firma digital y cifrado MIME, para usarlo en conjunto con los tipos de contenido estructurados definidos en el punto anterior .

El tipo de contenido multiparte/firmada define una estructura que comprende dos partes del cuerpo. La primera parte puede contener cualquier contenido MIME, tal como una parte de un texto, sonido, ó algún tipo estructurado. La firma digital es calculada sobre esta primera parte del cuerpo, incluyendo sus cabeceras MIME. La segunda parte del cuerpo contiene la firma digital y cualquier información de control requerida por un usuario receptor para verificar esa firma. La especificación MOSS define un tipo de contenido MIME llamado *aplicación/firma-moss* que se puede usar en la segunda parte del cuerpo de multiparte/firmada.

La especificación MOSS también describe un procedimiento para generar un mensaje firmado usando multiparte/firmada y aplicación/firma-moss. Este procedimiento se ilustra en la Figura 1.

El primer paso es transformar el contenido del mensaje a una *forma canónica*. Este paso es necesario porque los sistemas de mensajería de Internet está construido sobre un sistema de transporte de texto que sólo transporta mensajes de caracteres codificados en ASCII y no permite el transporte de ficheros binarios de forma transparente. Consecuentemente, según un mensaje avanza hacia su destino, la representación del texto del mensaje puede ser modificada. Sistemas diferentes usan codificaciones de caracteres diferentes. También sistemas diferentes usan convenciones diferentes para representar el final de una línea de texto, por ejemplo, el carácter de retorno de carro (CR), el carácter line feed (LF), ó una secuencia de CR seguida por LF. Un mensaje se puede convertir para usar diferentes codificaciones. Mientras tales conversiones no cambian el significado del mensaje, si introducen el riesgo de invalidar una firma digital valida que no será aceptada como correcta. Para evitar este problema, es necesario que todos los sistemas calculen las firmas digitales bajo una representación común de los mensajes, usando un único método de codificación previamente acordado. Esta representación estándar de un mensaje es conocida como la forma canónica de un mensaje. Esta representación, es procesada por una función hash y es firmada digitalmente. La firma digital y la información de control utilizada se construyen en un nueva parte del cuerpo del mensaje que tiene el tipo de contenido aplicación/ firma-moss. Esta parte del cuerpo incluye la firma y los identificadores de la función hash y el algoritmo de firma utilizado. El contenido multiparte/ firmada se construye entonces, incorporando la parte original del cuerpo que se debe firmar y la parte aplicación / firma-moss.

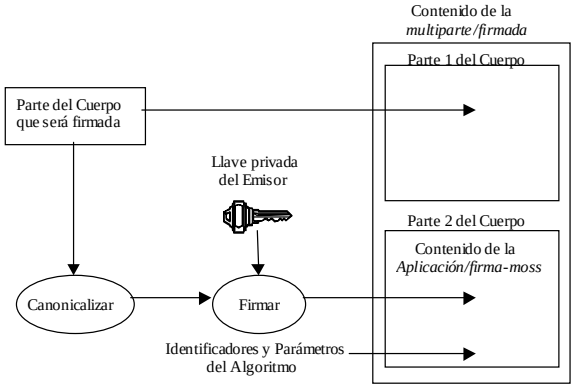

Figura Nº 1: Generación de firma digital MOSS

El cifrado usa un proceso diferente y diferentes tipos MIME. El tipo multiparte/cifrada define una estructura que comprende dos partes del cuerpo. En este caso, la segunda parte contiene una versión cifrada de alguna otra parte MIME (tal como texto, sonido, ó una estructura multiparte). La primera parte del cuerpo contiene la información de control necesaria para descifrar la segunda parte, por ejemplo, los identificadores del algoritmo utilizado y la información de la llave empleada. La especificación MOSS define un tipo de contenido MIME, *aplicación/llaves-moss*, para su uso en la primera parte del cuerpo de multiparte/cifrada. La especificación MOSS también describe un procedimiento para generar un mensaje cifrado usando multiparte/cifrada y aplicación/llaves-moss. Este procedimiento se muestra en la Figura 2.

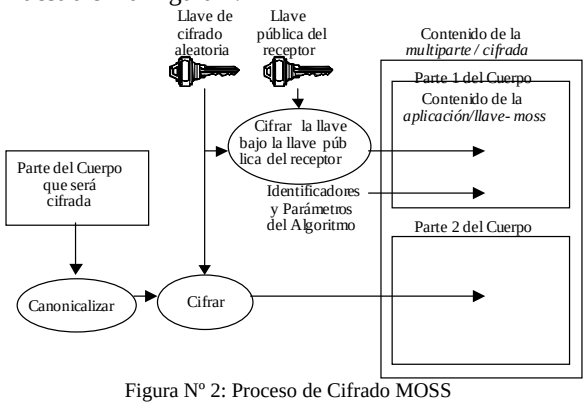

Figura Nº 2: Proceso de Cifrado MOSS

El proceso es como sigue:

- Paso 1. La parte del cuerpo que se cifrará, se transforma en su forma canónica MIME y que es usada por todos los sistemas.
- Paso 2. Se genera una nueva llave aleatoria para el cifrado de los datos y a su vez esta llave es cifrada bajo el control de una llave pública RSA[3] para cada receptor del mensaje. Estas copias cifradas de la llave de cifrado de datos y la información de control usada se construyen en una nueva parte del cuerpo del tipo aplicación/llaves-moss.
- Paso 3. La parte del cuerpo del paso 1 se cifra con el algoritmo simétrico.
- Paso 4. Se construye el contenido multiparte/ cifrada incorporando la parte del cuerpo aplicación/llaves-moss y la parte del paso 3.

La parte del cuerpo aplicación/llaves-moss incluye las copias protegidas de la llave de cifrado de los datos para cada receptor, y un identificador del algoritmo utilizado.

La especificación MOSS no designa una forma estándar para identificar a los poseedores de los pares de llaves públicas ó para gestionar esos pares de llaves. Sin embargo, MOSS si define tipos de contenido MIME para transferir una petición de una parte remota y la información de la llave pública, incluyendo sus certificados de la llave pública, entre las partes. Estos tipos de contenido pueden ser usados como herramientas para construir un sistema completo de gestión de llaves.

S/MIME

En paralelo con el desarrollo de las especificaciones MOSS por la Internet Engineering Task Force, un grupo privado conducido por RSA Data Security, Inc. desarrolló otra especificación para transferir digitalmente información firmada y cifrada en MIME. Esta especificación es conocida como S/MIME. Mientras los objetivos de los proyectos MOSS y S/MIME eran bastante similares, las soluciones finales terminaron siendo completamente diferentes. Esto debido principalmente a que S/MIME construido sobre una base de estándares llamados los Estándares para el cifrado de llaves públicas (PKCS), también fue desarrollado por RSA Data Security, Inc.

Los estándares PKCS, que fueron publicados por primera vez en 1993, incluyen una especificación, denotada PKCS #7, que define las estructuras de los datos y los procedimientos para firmar y cifrar digitalmente otras estructuras de datos. El tratado hecho en S/MIME consistía simplemente en especificar como aplicar PKCS #7 para proteger una parte del cuerpo MIME, generando una nueva estructura de datos que ella misma se convierte en un contenido MIME. Esto proporciona la base para los servicios de seguridad mismos, a decir, los servicios básicos para la protección de un mensaje.

S/MIME define un tipo de contenido MIME llamado el tipo *aplicación/x-pkcs7-mime*. El propósito de este tipo de contenido es proporcionar una representación protegida de cualquier parte del cuerpo MIME desprotegida. Con S/MIME, los diferentes casos de firma digital, cifrado, y firma digital más cifrado son considerados variantes de una transformación básica de los datos ó proceso envolvente. Las siguientes variantes corresponden a diferentes tipos de datos estructurados definidos en PKCS #7:

- Datos firmados. La representación de la parte del cuerpo que se quiere proteger se construye en una estructura de datos que incluye una firma digital

sobre esos datos junto con los identificadores del algoritmo y los certificados de la llave pública (opcional), y otra información relativa al firmante.

- Datos encapsulados. La representación de la parte del cuerpo que se quiere proteger es cifrada de forma simétrica y después incorporada en una estructura de datos que incluye una copia de la llave de cifrado para cada receptor, protegida con la llave pública de un par de llaves RSA, junto con los identificadores del receptor y los identificadores del algoritmo.
- Datos firmados y encapsulados. Esta estructura combina el procesamiento asociado a ambos tipos: datos firmados y datos encapsulados.

El proceso para generar el contenido S/MIME para alguna parte del cuerpo MIME, firmada digitalmente, se ilustra en la Figura 3.

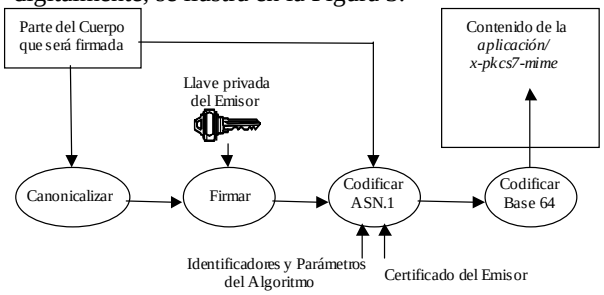

Figura Nº 3: Generación de la Firma digital S/MIME

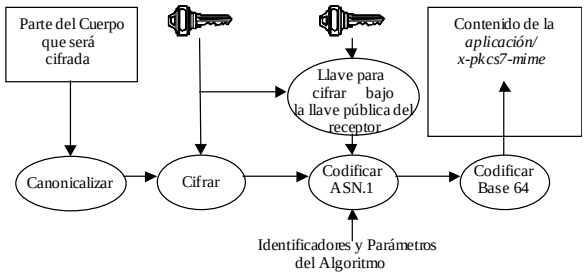

Figura Nº 4: Proceso de Cifrado S/MIME

El proceso de firma digital S/MIME requiere poner en forma canónica la representación de la parte de entrada del cuerpo, la transformación criptográfica, y la conversión de la cadena de datos binarios resultante a una forma que pueda cruzar un sistema de transferencia de mensajes basado en texto. El último paso usualmente sigue un proceso llamado *Base 64 Encoding*, un medio común para transferir datos binarios con MIME. PKCS #7 usa la notación estandarizada internacionalmente llamada Abstract Syntax Notation One (ASN.1), a diferencia del protocolo usado por MOSS que usa el estilo de codificación de caracteres. El proceso para generar el contenido S/MIME para cifrado se ilustra en la Figura 4.

El proceso completo es el mismo que el utilizado para la firma digital S/MIME, excepto que la variante de datos encapsulados del PKCS #7 se usa en lugar de la variante de datos firmados, resultando una transformación criptográfica diferente.

Pretty Good Privacy (PGP)

Pretty Good Privacy es un software para la protección de mensajes bastante popular que es ampliamente usado por usuarios esporádicos de la comunidad de Internet[7]. La popularidad de PGP se debe principalmente al hecho de que la mayoría de la gente lo adquiere gratuitamente. PGP es distribuido sin cargo alguno por The Massachussetts Institute of Technology (MIT) en los Estados Unidos[8]. Una versión comercial también está disponible. Desde una perspectiva técnica, PGP es muy similar a MOSS y S/MIME. Usa funciones de firma digital y cifrado para proporcionar los servicios básicos de protección de mensajes. PGP define su propio formato de protección de mensajes, el cual puede ser incrustado en una parte del cuerpo MIME si se requiere. El aspecto principal de PGP que lo distingue de los otros protocolos para la protección de mensajes descritos hasta ahora es que este define su propio sistema de gestión de pares de llaves públicas, incluyendo su propia forma de certificados de llave pública. Desafortunadamente, este sistema de gestión de llaves no es compatible con los estándares de la infraestructura de llave pública reconocidos [3]. PGP ha demostrado ser un sistema efectivo para proteger e-mails esporádicos entre los usuarios de Internet, pero muchos no lo consideran apropiado para soportar comercio electrónico de gran escala [3].

Protocolos para la seguridad en la Web

El campo de los protocolos para la seguridad en la Web ha tenido un desarrollo y crecimiento acelerado en los últimos años. Uno de los protocolos más usados para propósitos de seguridad en la Web es SSL, comentado en una sección anterior. El protocolo HTTP seguro (S-HTTP) constituye otra alternativa. Se han desarrollado otros protocolos para propósitos especiales, tal como el protocolo Secure Electronic Transaction (SET) para los pagos con tarjeta bancaria (discutido más adelante).

Secure Sockets Layer (SSL)

SSL fue inicialmente concebido como un protocolo para la seguridad Web, pero actualmente es una nueva capa de protocolos que opera sobre el protocolo TCP de Internet. Se puede usar para proteger la

comunicación de cualquier protocolo de aplicación que opere normalmente sobre TCP, por ejemplo, HTTP, FTP, ó TELNET. El uso más común de SSL consiste en proteger las comunicaciones HTTP: en particular, una URL que comienza con "https://" indica el uso de HTTP bajo la protección de SSL. Este protocolo también proporciona un cierto rango de servicios de seguridad para las sesiones cliente-servidor[9]. Los servicios de seguridad que presta son:

- Autenticación del servidor. El servidor se autentica hacia el cliente, demostrando la posesión de una llave privada particular. Es importante para un cliente, estar seguro de que realmente se está comunicando con el servidor correcto y no con algún otro sitio que se presente como tal.
- Autenticación del cliente. Este servicio de seguridad opcional autentica al cliente hacia el servidor, otra vez demostrando la posesión de una llave privada particular por parte de aquel.
- Integridad. Los datos transferidos en la sesión son protegidos con un valor de verificación de la integridad para asegurar que cualquier intento de modificar los datos en tránsito, sea detectado. Esto protege tanto al cliente como al servidor contra algún adversario que pudiera causar daño al modificar el contenido de la información enviada y/o alterar la dirección de envío.
- Confidencialidad. Los datos transferidos en la sesión pueden ser cifrados para protegerlos contra su captura por espías electrónicos. Esto es particularmente importante, ya que existe protección contra agentes externos a la sesión que pudieran detectar alguna otra información personal cuando se transmite hacia el servidor.

SSL consiste en dos subprotocolos: el protocolo SSL Record y el protocolo SSL Handshake. El protocolo SSL Record define el formato básico para todos los datos enviados en la sesión. Proporciona compresión de datos, generación de un valor para la verificación de la integridad sobre los datos, cifrado de los mismos, y la seguridad de que el receptor pueda determinar la longitud correcta de los datos. Se incluye un número de secuencia de registro para protegerse contra el reordenamiento de los datos por parte de un adversario activo. Para que el protocolo SSL Record pueda calcular un valor para la verificación de la integridad y usar el cifrado, es necesario establecer llaves criptográficas tanto en el cliente como en el servidor. El protocolo soporta el cambio a un conjunto diferente de algoritmos de protección y llaves en cualquier momento. El protocolo SSL Handshake se usa para negociar los algoritmos de protección que se utilizarán para autenticar al cliente y al servidor, uno respecto del otro, transmitir los certificados de llave pública requeridos, y establecer las llaves de sesión para su uso en la validación de la integridad y en los procesos de encriptación del protocolo SSL Record. Se pueden utilizar diferentes algoritmos de establecimiento de llaves, incluyendo RSA key transport, Diffie-Hellman key agreement, and the U.S. government's KEA algorithm[3]. Cuando se establece una nueva sesión, es posible usar nuevamente llaves de sesión existentes de comunicaciones anteriores. Las llaves de sesión tienen asociado un identificador de sesión que se usa para este propósito. El protocolo SSL Handshake es un protocolo de más alto nivel que el protocolo SSL Record en el sentido de que este último contiene al primero. En el primer par de mensajes intercambiados en una sesión, el protocolo SSL Record no puede cifrar ó calcular los valores para la verificación de la integridad porque las llaves no son conocidas aún; sin embargo, el protocolo está diseñado de manera que no presente ningún problema de seguridad.

Secure HTTP (S-HTTP)

S-HTTP fue diseñado por Enterprise Integration Technologies en respuesta a los requerimientos de CommerceNet, un consorcio enfocado a la promoción del establecimiento de tecnologías necesarias para el comercio electrónico basado en Internet[10]. S-HTTP fue diseñado como una extensión de seguridad para HTTP, que es esencialmente un protocolo de transacción de respuesta-a-petición. Esto hace a S-HTTP diferente a SSL, que es un protocolo para la protección de una sesión. La función principal de S-HTTP es proteger mensajes de petición ó respuesta de transacciones individuales, similar a la forma en que un protocolo de seguridad de mensajes protege los mensajes de correo electrónico. De hecho, S-HTTP está construido en gran medida sobre la base de los protocolos para la seguridad de mensajes.

Los servicios de seguridad proporcionados por S-HTTP son los mismos que los proporcionados por SSL, es decir, autenticación, integridad (por medio de un valor de verificación de la integridad), y confidencialidad (por medio de cifrado), con la adición de una opción para firmas digitales, que puede proporcionar una base para el servicio de seguridad adicional de no-rechazo. El S-HTTP proporciona gran flexibilidad para la protección de mensajes y la gestión de llaves. Los formatos específicos para la protección de mensajes que se utilizan incluyen el PKCS #7. Las llaves de cifrado se pueden establecer a través de RSA key transport con la envoltura PKCS #7; estas se pueden preestablecer por medios manuales, ó incluso

se pueden establecer de tickets de Kerberos. Como en el caso de SSL, se señala que S-HTTP es una especificación que está sujeta a cambios continuos.

Protocolos para la seguridad en las aplicaciones de comercio electrónico

Las aplicaciones del comercio electrónico pueden hacer uso de las características de seguridad de la mensajería electrónica y de los protocolos Web. Sin embargo, existen requisitos adicionales en escenarios específicos de comercio electrónico. Existen dos áreas relacionadas al comercio en las cuales se necesitan protocolos de seguridad en las capas más altas: la primera es el área bien establecida de Electronic Data Interchange (EDI); la segunda es el área de pagos con tarjeta bancaria a través de Internet.

EDI en Internet

Una de las formas más establecidas para el comercio electrónico es EDI, el cual comenzó a emerger como una ayuda importante a las transacciones de negocios vía electrónica en los 1980s. EDI significa el intercambio máquina-a-máquina de transacciones de negocios. EDI es usado ampliamente, por ejemplo, en la industria automotriz, redes portuarias, marina mercante, etc.

Los formatos de mensajes de EDI están estandarizados. Existen dos familias principales de los estándares de EDI:

- Los estándares X12, desarrollados bajo los auspicios del Instituto Nacional Americano de Estándares (ANSI) por el Comité de Estándares Acreditados (ASC) [11]. Estos estándares son usados predominantemente en Estados Unidos.
- Los estándares EDIFACT (EDI para la Administración, el Comercio, y el Transporte), establecidos por la Comisión Económica de las Naciones Unidas para Europa.

Previo al surgimiento de Internet como un recurso de las comunicaciones para propósitos comerciales, EDI generalmente recaía en la contratación de proveedores de servicios de Redes de Valor Añadido (Value-Added Network, VAN). Las VANs comúnmente proporcionan servicios de comunicaciones de datos y, además, dan asistencia a sus clientes en áreas tales como configuración de software, seguridad, recuperación de datos perdidos, etc. Las comunicaciones EDI no han usado, históricamente, los protocolos de Internet. Más bien, han empleado una combinación de tecnologías, que incluyen líneas dedicadas de comunicación, enlaces dial-up, emulación de terminales mainframe, y redes de datos de paquetes conmutados. La comercialización de Internet ha abierto más opciones para EDI. Primero, si las EDI VANs se conectan a Internet, esto proporciona a los clientes medios de comunicación de bajo costo. Alternativamente, los usuarios de EDI podrían optar por no usar los servicios de una VAN, y realizar transacciones EDI directamente con sus socios comerciales vía Internet. A tales usuarios se les presenta la oportunidad de llevar a cabo transacciones EDI con un rango amplio de socios comerciales y ahorrar dinero evitando los cargos de una VAN. Sin embargo, si se toma esta opción, los servicios de valor añadido se pueden perder. La tecnología natural para el transporte del tráfico EDI sobre Internet es la mensajería electrónica. Ya que MIME proporciona una estructura ideal para almacenar tráfico especializado de mensajería tal como es el caso de EDI, los desarrolladores de los estándares de Internet han definido un conjunto de tipos de contenidos MIME para transmitir el tráfico EDI. Estos tipos de contenidos MIME se pueden usar para transferir los mensajes EDI entre un usuario EDI y una VAN, ó entre un usuario EDI y otro. Ya que se usan diferentes estándares para los formatos de los mensajes EDI, se han definido tres tipos de contenidos MIME diferentes:

- Un tipo MIME para transferir cualquier intercambio ANSI X12 formateado de acuerdo a los estándares ANSI ASC X12.
- Un tipo MIME para transferir cualquier intercambio EDI formateado de acuerdo a los estándares EDIFACT.
- Un tipo MIME para transferir un mensaje EDI ó una colección de mensajes EDI de acuerdo a alguna regla convencional de formato diferente a ANSI X12 ó a EDIFACT. Este tipo puede ser usado sólo dentro del contexto de un acuerdo comercial bilateral y explicitado entre el emisor y el receptor de un mensaje.

Para mayor información sobre el uso de Internet para EDI, se recomienda ver RFC 1865 por Houser, Griffin, y Hage .

Seguridad EDI

Ya que los intercambios de EDI son estructuras complejas, que potencialmente contienen partes de muchas transacciones de negocios diferentes, ambos formatos de intercambio ANSI X12 y EDIFACT definen sus propios mecanismos internos de seguridad. Por ejemplo, un intercambio ANSI X12 está definido

para ser una estructura doblemente anidada, construida de una secuencia de segmentos de datos, como se muestra en la Figura 5.

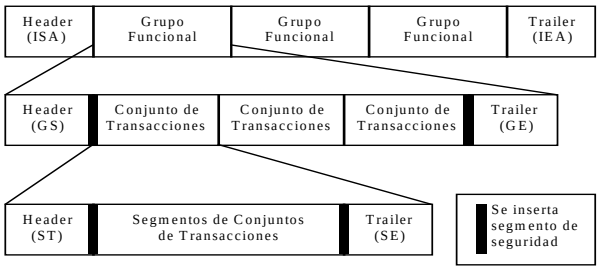

Figura Nº 5: Estructura de Intercambio ANSI X12

Un intercambio incluye uno ó más grupos funcionales, cada uno representando una colección de formas de negocios relacionadas entre sí. Un grupo funcional incluye uno ó más conjuntos de transacciones, cada uno representando una forma de negocio. El estándar ANSI X12.58 especifica como la seguridad se puede proporcionar ya sea en una ó ambas granularidades de los grupos funcionales y de los conjuntos de transacciones. Los servicios de seguridad proporcionan datos con autenticación, confidencialidad, y/o integridad, con datos opcionales para evitar el rechazo (si se usan firmas digitales). ANSI X12.58 define los segmentos de seguridad insertados en grupos funcionales y/o conjuntos de transacciones como se indica en la Figura 5. Estos segmentos transfieren tales datos como identificadores de llave, valores para verificar la integridad, firmas digitales, y marcas de tiempo.

Cualquier protección que sea interna al intercambio es independiente de que el intercambio sea transportado vía Internet u otros medios de comunicación. Sin importar los medios de comunicación, este tipo de protección puede ser importante porque conjuntos de transacciones diferentes pueden necesitar protección en forma diferente, por ejemplo, transacciones firmadas ó cifradas para diferentes partes. Además, cuando un intercambio EDI circula vía Internet, es posible aplicar protocolos estándares de seguridad para mensajería a los mensajes ó partes de su cuerpo. Por ejemplo, los tipos de contenidos EDI MIME mencionados anteriormente son totalmente compatibles con los protocolos de seguridad MIME como es el caso de S/MIME. Generalmente, es sensato usar autenticación y protección de la integridad a este nivel y, dependiendo de la aplicación, también puede ser sensato usar protección de confidencialidad. El uso de tales servicios de seguridad es recomendado porque el intercambio interno, en su totalidad, puede no estar protegido adecuadamente. Sin embargo, la protección de un mensaje completo en Internet no es necesariamente un substituto para la seguridad de los conjuntos de transacciones ó de los grupos funcionales usando las opciones de seguridad X12 ó EDIFACT.

Pagos con tarjeta bancaria: el protocolo SET

Las organizaciones Visa y MasterCard se unieron para desarrollar SET: un protocolo que soporta los pagos con tarjeta bancaria como parte de las compras electrónicas por Internet[12]. Los principales participantes en el entorno SET son:

- Emisor. Una institución financiera que emite tarjetas bancarias (tarjetas de crédito ó tarjetas de débito), comúnmente portando un logotipo (ejemplos, Visa y Mastercard).
- Dueño de la tarjeta. Está registrado con el emisor correspondiente para llevar a cabo comercio electrónico.
- Comerciante. Un vendedor de bienes, servicios, ó información, que acepta el pago en forma electrónica.
- Contrayente. Una institución financiera que ayuda a los comerciantes proporcionándoles un servicio para procesar transacciones con tarjeta bancaria (ejemplo, Redbank).

Los participantes secundarios que forman parte de la infraestructura SET son:

- Puerta de pago. Un sistema que proporciona servicios de comercio electrónico on-line a los comerciantes. Tal sistema es operado normalmente por un contrayente; el puerto de pago necesitará una interfaz con el contrayente para soportar la autorización y la captura de las transacciones.
- Autoridades de certificación. Los componentes de la infraestructura que certifican las llaves públicas de los dueños de las tarjetas, comerciantes, y/o contrayentes.

Al ejecutar una transacción de pago electrónico, los participantes principales comúnmente interactúan como sigue. El dueño de la tarjeta desea realizar una compra al comerciante y le envía una orden de pago on-line. El comerciante se comunica con su contrayente vía una puerta de pago, comúnmente reenviando todo ó parte de la orden de pago del dueño de la tarjeta, para que este autorice y capture la transacción. La captura es hecha por el contrayente. La autorización puede requerir una transacción de consulta en dirección del emisor: si todo está bien, la autorización se hace usando redes financieras existentes (No Internet).

En este entorno, la tecnología de llave pública se usa para soportar varias funciones, que incluyen:

- Cifrado de instrucciones de pago en una forma que asegure que el número de tarjeta bancaria de un usuario nunca será expuesto mientras es transferido por Internet, ni tampoco será expuesto a los sistemas de los comerciantes (donde pudiera estar en riesgo de corrupción).
- Autenticación (opcional) de los dueños de tarjetas hacia los comerciantes y los contrayentes, para protegerse contra el uso de tarjetas robadas por individuos no autorizados.
- La autenticación de comerciantes hacia los dueños de tarjetas y contrayentes, para protegerse contra impostores establecidos en sites de Internet donde se presentan como comerciantes legítimos y llevan a cabo transacciones fraudulentas.
- Autenticación de los contrayentes hacia los dueños de tarjetas y comerciantes, para protegerse contra alguien que se presenta como un contrayente para ser capaz de descifrar información sobre instrucciones de pago.
- Protección de la integridad de la información de la transacción, para prevenirse contra interferencias en Internet.

Otros modelos de pago por Internet

Existen otros esquemas propuestos que están en operación para proteger los pagos en Internet. Algunos ejemplos de estos esquemas actualmente en uso son:

- CyberCash[13]. Actúa como un intermediario entre comerciantes en la Web y bancos emisores de tarjetas de crédito. Tanto los comerciantes como los clientes se registran como clientes de CyberCash. Las transacciones de CyberCash son protegidas usando criptografía de llave pública, en cuyo caso CyberCash proporciona la gestión de llaves como un sistema cerrado.
- CheckFree[14]. Constituye una versión para Internet del sistema de verificación tradicional de pagos (en papel).
- First Virtual. Soporta pagos con tarjeta de crédito por Internet usando mensajes e-mail. No emplea cifrado.

5. CONCLUSIONES

- Una primera conclusión de este análisis sobre los aspectos de seguridad tratados en éste artículo es que se constata que las redes digitales de comunicación son inherentemente inseguras y que deben ser provistas, necesariamente, de mecanismos que permitan a los usuarios utilizarlas asumiendo el menor riesgo posible. Esta condición necesaria, que a veces no es suficiente, es aún más exigible cuando se trata de realizar comercio a través de ellas o se transfieren datos personales de carácter inherentemente confidencial.
- Los mecanismos que se han analizado, sugieren que el tema de seguridad es más que simplemente mantener los sistemas libres de errores; implica protegerse contra adversarios (hackers...) que no sólo son gente capacitada si no que además bien organizada e incluso financiada.
- Una conclusión no menos importante está relacionada con el hecho de verificar que la seguridad en las redes no es exclusivo de la capa de aplicación en los protocolos, si no más bien cada una de las diferentes capas tiene algo con que contribuir. Sin embargo, las soluciones más generales se encuentran en la capa de aplicación.
- Finalmente, la tendencia a la estandarización y a la creación de protocolos más poderosos, si bien indican que aún no hay algo definitivo, son una buena señal que permite confiar en que las actividades a través de las redes serán cada ves más seguras y por lo tanto, así mismo lo será el comercio a través de ellas.

6. REFERENCIAS

[1] Tanenbaum, A.S.; "Redes de Computadoras", 3ª Ed., *Prentice Hall*,1997.

[2] Garfinkel, S.; Spafford, G.; "Web Security & Commerce", 1st Ed., *O'Reilly & Associates, Inc*., 1997.

[3] Ford, W.; Baum, M.S.; "Secure Electronic Commerce", *Prentice Hall PTR*, 1997.

[4] Schneier, B.; "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, *John Wiley & Sons, Inc*., 1997.

[5] Nechvatal, J.; "Public Key Cryptography", *Contemporary Cryptology: The Science of Information Integrity* (New York: IEEE Press, 1992), pp. 178-228.

[6] Diffie, W.; Van Oorschott, P.C., and Wiener, M.J.; "Authentication and Authenticated Key Exchanges", *Designs, Codes and Cryptography*, Vol. 2, No. 2, (June 1992), pp. 107-126.

[7]http://www.oreilly.com/catalog/pgp/noframes.html

[8] http://web.mit.edu/network/pgp.html

[9] http://www.counterpane.com/ssl.html

[10] http://www.commerce.net

[11] http://www.disa.org

[12]http://www.visa.com ó http//www.mastercard.com

[13] http://www.cybercash.com

[14] http://www.checkfree.com