Impacto Científico
Revista arbitrada venezolana
del Núcleo LUZ-Costa Oriental del Lago
ISSN: 1836-5042 ~ Depósito legal pp 200602ZU2811
Vol. 3 Nº 1, Enero-Junio 2008, pp. 90 - 107

Técnicas de seguridad en acceso a WEB: crítica de esquemas actuales y propuestas de mejora

David Bracho[1], Carlos Alberto Rincón Castro[2], Alfredo Javier Acurero Álvarez[3] y Neif Guzmán Silva Valero[4]

[1]*Departamento de Computación Facultad Experimental de Ciencias. Universidad del Zulia. drbracho@luz.edu.ve*
[2]*Departamento de Computación Facultad Experimental de Ciencias. Universidad del Zulia.*
[3]*Departamento de Computación. Facultad Experimental de Ciencias. Universidad del Zulia.*
[4]*Consejo Central de Pregrado Vicerrectorado Académico. Universidad del Zulia*

Resumen

El propósito de este artículo es hacer una revisión sobre los trabajos publicados en cuanto a las técnicas de seguridad en acceso WEB. Para ello se expone un análisis descriptivo sobre los mecanismos de seguridad y elementos a proteger durante los accesos WEB, haciendo énfasis en el protocolo Secure Socket Layer (SSL). Actualmente y con el fin de incrementar las investigaciones en el área de las ciencias de la computación, un grupo de investigadores de la Universidad del Zulia (Venezuela) contribuyen con enriquecer esta materia al fortalecer las líneas de investigación: seguridad de aplicaciones bajo ambiente WEB y gestión de riesgo telemático, adscritas a la Unidad Académica de Redes e Ingeniería Telemática. Los protocolos de seguridad de acceso WEB han sido trabajos desarrollados por organizaciones para hacer transparente, rápido y seguro dicho accesos, esto como consecuencia del auge vertiginoso de Internet y del comercio electrónico, integrando incluso, diferentes protocolos y soluciones, algunas de ellas personalizadas, pero siempre a conveniencia de los usuarios, respetando

RECIBIDO: 14/01/2008 ACEPTADO: 24/06/2008

los proveedores, productos y servicios necesarios para realizar sesión, conexión y transmisión de datos en la WEB. La estructuración de los aportes de este artículo está apoyada en una revisión documental que permitió construir el basamento teórico de este trabajo de investigación. Estas teorías conllevaron a evidenciar el funcionamiento, encriptación, arquitectura y estructura, desventajas y limitaciones existentes de los protocolo de seguridad y en especial del SSL. Este trabajo concluye con algunas propuestas que pueden reducir el riesgo de exposición de la información durante los accesos WEB.

Palabras clave: Seguridad WEB, secure socket layer, PKI, handshake, IPSec.

Techniques of Security in Access to WEB: Critic of Present Schemes and Proposals of Improvement

Abstract

The purpose of this article is to review on the work published in terms of security techniques in Web access. This presents a descriptive analysis on the security mechanisms and elements to protect over the WEB access, with emphasis on Secure Socket Layer (SSL). Today, in order to enhance research in the area of computer science, a group of researchers from the University of Zulia (Venezuela) contribute to enrich this area to strengthen the lines of research: application security and low ambient WEB Risk Management Telematic, assigned to the unit Academic Network Engineering and Telematics. The security protocols access WEB work has been developed by organizations to make transparent, fast and secure such access, as a result of this dizzying rise of the Internet and electronic commerce, including integrating different protocols and solutions, some of them customized, but provided for users' convenience, while respecting the vendors, products and services necessary to conduct meeting, connection and data transmission on the Web. The structuring of the contributions of this paper is supported by a document review that built the theoretical foundation of this research. These theories led to reveal the operation, encryption, architecture and structure, disadvantages and limitations of the existing security protocol and especially SSL. This paper concludes with some suggestions that may reduce the risk of exposure of information over the Web access.

Key words: WEB security, secure socket layer, PKI, handshake, IPSec.

Introducción

El crecimiento y masificación de las transacciones electrónicas WEB ha contribuido con facilitar procesos tediosos, comunes y corrientes en fracciones de segundo, ahorrándole al usuario su participación física en el desarrollo de los mismos; es por ello que, más negocios son llevados a la WEB, consolidándose como un factor que ha pasado de lo vanguardista a lo cotidiano, garantizando transparencia e interoperatividad en el quehacer del negocio y de la infraestructura de los servicios WEB.

Debido al auge de los servicios y transacciones virtuales, se han desarrollado e incorporado una serie de elementos que contribuyen directamente al control de la seguridad, destacándose en ella, los mecanismos de seguridad, que son incorporados para proporcionar confidencialidad, integridad y disponibilidad, con el fin de aportar confianza en los usuarios que se sirven de estos productos y servicios.

Sin embargo, las amenazas son cada vez más frecuentes y complejas, con la variante de que muchos usuarios poseen conocimientos avanzados en el área de la computación y telecomunicaciones, lo cual les permite realizar ataques complejos a la infraestructura de servicios WEB, convirtiéndose estas agresiones en un aspecto difícil de prevenir y corregir.

En 1994, el *Internet Architecture Board* (IAB) emitió el reporte "*Security in the Internet Architecture*" (*RFC 1636*), el cual establecía que Internet requería una mayor y mejor seguridad, además, identificaba las áreas claves que requerían mecanismos de seguridad. Entre las principales necesidades quedaron identificadas: el aseguramiento de la infraestructura de red, tanto del monitoreo como del control del tráfico no autorizado y la protección del tráfico usuario_final-usuario_final utilizando mecanismos de autentificación y de encriptamiento. Espinosa y Morales (2000).

En este sentido, los distintos protocolos establecidos para las transacciones WEB, poseen algunos años de creación y por ende, están basados en tecnología antigua, que a pesar de haberse actualizado con mejoras sustanciales, es posible que, éstas no aporten el resultado esperado en toda la dimensión requerida y sea necesario una revisión total, e incluso, un replanteamiento de los mecanismos de seguridad para las transacciones WEB existentes.

Muchos de los mecanismos de seguridad hacen uso de estándares y componentes que pueden considerarse maduros y al no poder soportar más desarrollos que permitan incorporar nuevas funciones, no es posible disminuir los efectos a la exposición y uso que ocasionan las limitaciones y desventajas propias de las tecnologías, considerándose obsoletas e inseguras, generando desconfianza en el usuario final.

Por lo anteriormente planteado, este documento pretende encontrar elementos de seguridad sobre un análisis crítico del protocolo Secure Socket Layer (SSL) como mecanismos de seguridad, con el fin de identificar mejoras sustanciales que incrementen la seguridad de las transacciones WEB. El resto del material se organiza de la siguiente manera: En la sección 2 se expone a la metodología, la cual abarca lo concerniente a trabajos afines revisados sobre el tema de SSL. En la sección 3 se presenta todo lo relacionado con el funcionamiento del SSL, encriptación, arquitectura y estructura, debilidades y limitaciones, así como los últimos avances del mismo. En la sección 4 se muestran otras soluciones vigentes, que surgen como competencia directa al SSL. En la sección 5 se revelan las conclusiones manteniendo como propuesta la vigencia del SSL. Finalmente, en la sección 6 se indican las referencias bibliográficas revisadas.

Metodología

1. Trabajos Afines

En 1999, se indicó que en general SSL 3,0 proporcionaba una excelente seguridad contra la escucha pasiva y de otros tipos de ataques. Sin embargo, este protocolo proporciona solo protección mínima a la confidencialidad, la solidez del protocolo SSL es un punto sensible a mejorar, ello inspirado directamente en las vulnerabilidades detectadas. Wagner y Schneier (1999).

En este mismo orden de ideas, en 2002 se expuso que SSL carecía de muchos de los elementos necesarios para construir un sistema de transacciones seguras en Internet. Para ello, se ha intentado paliar estos fallos desarrollando el mercado y estandarizando otros sistemas diferentes sin que ninguno de ellos haya conseguido desplazar a SSL, básicamente por que es una tecnología rápida, fácil de implementar, barata y cómoda para el usuario. A nivel del comercio que incorpora al SSL es

igualmente sencillo de implementar, no exigiendo servidores con características especiales y recursos computacionales significativos. García y Chouciño (2002).

Así en 2003, se expresó que no es tan fácil prever por cuánto tiempo se mantendrá SSL como protocolo preferido para los accesos WEB; lo lógico sería pensar que en el terreno de las comunicaciones seguras de propósito general se vea desplazado en algún momento por IPSec y en el terreno específico de las aplicaciones de comercio electrónico por SET u otro protocolo diseñado a tal efecto. Morales (2003). En el mismo año, se indicó que SSL era vital para la seguridad WEB ya que proporcionaba un fuerte sentido de la confidencialidad, la integridad del mensaje, y el servidor de autenticación a los usuarios. En el futuro, SSL será capaz de manejar más transacciones a un ritmo más rápido en los dispositivos terminales. La longitud de clave de cifrado y sistemas de cifrado seguirán evolucionando a fin de garantizar la seguridad de información sensible en la WEB, de esta forma, el comercio electrónico será capaz de continuar creciendo en popularidad y en confianza de parte de los usuarios y desarrollando cada vez nuevas aplicaciones en línea. Cisco Systems (2003).

2. Mecanismos de Seguridad WEB

La seguridad está estructurada en función de mecanismos que se traducen a su vez en protocolos que buscan minimizar las debilidades y vulnerabilidades al ser expuesta la información en un entorno WEB. Los elementos que forman esta barrera son siete (7) y van más allá del hardware y del software; estos elementos son: Confidencialidad, Integridad, Disponibilidad, No Repudio, Verificación de la Identidad, Validez Legal y Confianza de los Usuarios.

Es por esto que, para dar respuestas efectivas a los elementos anteriormente mencionados, se cuenta con los protocolos de seguridad WEB, como el mecanismo más difundido entre los distintos esquemas de seguridad. Entre los protocolos se encuentran: Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure – HTTP (S-HTTP), Private Communication Tecnology (PCT), IPSec, Cybercash y SET. Pons (2000).

2.1. Secure Socket Layer. Secure Socket Layer (SSL) es un protocolo de propósito general que tecnológicamente es independiente del servicio utilizado en Internet, ya que se sitúa en un nivel superior de la

capa, esto hace que se puedan utilizar servicios como el FTP o TELNET con implementaciones SSL.

El borrador más reciente data de noviembre de 1996, cuando Netscape publicó la versión 3.0. El intento era ser un protocolo de la seguridad que proporcionaba privacidad a las comunicaciones en Internet. El protocolo sincroniza tanto al cliente como al servidor, de manera tal, que es diseñado para evitar que se pueda escuchar por medio de puertas trasera o forzar la falsificación de mensajes. Los objetivos que fundamentan este protocolo estuvieron orientados hacia el aporte de seguridad criptográfica, interoperabilidad, extensibilidad y eficacia relativa. Por tal razón, este es el protocolo dominante en la actualidad en el panorama del comercio electrónico, proporciona confidencialidad, integridad y verificación de la identidad de ambas partes. Friedly (2004).

2.2. Funcionamiento. Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se introducen como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo las ranuras del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice. Al mismo tiempo, proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que éstos sean segmentados en la capa de Transporte para posteriormente ser encapsulados y enviados por las capas inferiores.

La versión más actual de SSL usa los algoritmos simétricos de encriptación DES, 3DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1. Los algoritmos, longitudes de clave y funciones hash de resumen usados en SSL dependen del nivel de seguridad estipulado. Palacios (2006).

En general, se afirma que la encriptación utiliza algoritmos matemáticos que tienen 2 entradas, la cadena de datos como texto plano y el número prefijado como clave y, como salida genera la cadena de datos encriptado como texto cifrado. La desencriptación por el contrario, utiliza algoritmos que toman el texto cifrado y la clave como entradas y genera el texto plano como salida. La clave y el algoritmo utilizado para la encriptación no necesariamente son las mismas utilizadas para la desencriptación, sin la clave para desencriptar la cadena de texto cifrado debería ser difícil poder descifrar el texto.

En tal sentido, la forma más eficiente de poder romper un algoritmo de encriptación es por medio de la fuerza bruta, intentando múltiples claves combinadas. Si la clave es lo suficientemente larga, sería prácticamente imposible romper por medio de procedimientos ordinarios individuales Chou (2002a).

2.2.1. Encriptación con Clave Secreta. Cabe destacar que con los algoritmos de clave secreta, tanto el emisor como el receptor usan la misma clave para encriptar y desencriptar la data. El problema inherente a este mecanismo, es garantizar la confiabilidad del proceso de distribución de la clave, lo cual sería el éxito de éste, el canal utilizado. Chou (2002a). Seguidamente, se presentan las características de la encriptación con clave secreta:

- Es usada para encriptar y desencriptar con claves simples.
- Requiere que tanto emisor como receptor tengan la clave.
- La distribución de la claves es una debilidad.
- No exige muchos ciclos de CPU.
- Su fortaleza recae en la longitud de la clave, que pueden ser rangos entre 40 a 168 bits. Cisco Systems (2003).

2.2.2. Encriptación con Clave Pública. Con los algoritmos de clave pública se incorporan dos procesos por separados: públicos y privados, en donde cada clave pública corresponde a una específica clave privada, lo cual asegura la autentificación. Normalmente, el emisor utiliza la clave pública para encriptar el mensaje y el receptor utiliza la clave privada para desencriptarlo; desafortunadamente este procedimiento requiere y consume mucho recurso computacional, sometiendo al CPU a un proceso de cálculo intenso. Chou (2002a). A continuación se presentan las características de este tipo de encriptación:

- Es una respuesta a las debilidades de la criptografía simétrica.
- La información encriptada con una clave puede ser desencriptada sólo con otra clave.
- Requiere más de 1000 veces ciclos de CPU.
- Se basa en RSA como algoritmo utilizado para habilitar la PKI.
- Inicia con intercambio de claves asimétricas. Cisco Systems (2003).

2.2.3. Encriptación con ambas Claves. Para capitalizar la longitud de ambos tipos de algoritmos, los protocolos de seguridad frecuentemente utilizan la clave pública para transmitir la clave privada. La data transferida se encripta con clave pública, la cual contiene la clave secreta como carga útil, una vez distribuida la clave secreta se garantiza el éxito en la transferencia de la data.

Por tal razón, esta variante es una mejora del SSL, garantizando el acuerdo del algoritmo a utilizar y la distribución del mismo. La clave pública permite que se acepte el algoritmo a utilizar, sin que el emisor y el receptor en realidad se encuentre transmitiendo datos ni la clave secreta. En vez de ello, se intercambian las claves públicas y de forma independiente se generan las claves privadas. Chou (2002a). Así, las fases en SSL son:

- Establecimiento de sesión (autentificación; negociación de los parámetros de cifrado y generación de claves.
- Transferencia de datos (proporciona integridad y confidencialidad). Palacios (2006).

2.3. Arquitectura y Estructura del SSL. SSL está diseñado para hacer uso de TCP y proporcionar seguridad en el servicio entre los extremos, es decir, emisor y receptor de mensaje. La arquitectura está conformada por dos (2) importantes conceptos:

- Conexión: enlace lógico cliente-servidor que proporciona tipo adecuado de servicio.
- Sesión: definen una asociación entre un cliente y un servidor (protocolo Handshake). Estos parámetros criptográficos pueden ser compartidas entre múltiples conexiones. Las sesiones evitan la costosa negociación de nuevos parámetros de seguridad para cada conexión. Stallings (1998).

La estructura está conformada por el registro de protocolo de SSL, quien ofrece la seguridad en los servicios de protocolos de las capas más altas, tres (3) protocolos son definidos: Handshake; Change CipherSpec, y Alert and Change Chipre Suite. Palacios (2006). La negociación (Handshake), intercambia los algoritmos; autentifica del servidor y el secreto compartido; tanto para el cliente como para el servidor se especifica información relevante sobre: versión del protocolo, número aleatorio,

identificador de sesión y de forma particular, para el cliente el algoritmo de compresión y para el servidor el conjunto de algoritmos de cifrado.

En este sentido, la certificación envía la cadena de certificados al servidor y a la Autoridad de Certificación (AC) y se valida el certificado por una AC y su vigencia. Luego, toma el control el protocolo Change CipherSpec, en donde el cliente pasa a utilizar los algoritmos y claves negociados, esto es, algoritmos aceptados por el servidor y las claves calculadas a partir del secreto. Finalmente, se activa el protocolo Alert and Change Chipre Suite, el primero gestiona la sesión SSL y los mensajes de error y advertencias y el segundo **indica** que una parte va a cambiar a un Ciphersuite que se ha negociado recientemente. Palacios (2006).

2.4. Debilidades y Limitaciones del SSL. A continuación se mencionan algunas de las debilidades y limitaciones del SSL.

2.4.1. Debilidades. A continuación se listan las debilidades más comunes y serias:

- No está diseñado para el comercio electrónico, exigiendo al emisor enviar información sensible al receptor, comprometiéndola ante posibles fraudes.
- No está concebido para trabajar con otros protocolos de la capa de Transporte diferentes de TCP, como lo es UDP.
- Poca eficiencia al entablar una sesión SSL, sobre todo durante el establecimiento de la conexión.
- Errores propios en la implementación.
- No ofrece disponibilidad.
- Expone las claves privadas al almacenarse en los servidores SSL.
- Permite la recuperación del contenido de sesiones previas.
- No asegura la no intercepción de los mensajes de inicio de sesión del protocolo Handshake.
- Deficiencias en la generación aleatoria de números. Morales (2003).
- No es puesta en práctica la característica que cualquier par de partes (aplicaciones HTTP cliente – servidor) existen múltiples conexiones seguras. Stallings (1998).

2.4.2. Limitaciones. A continuación se mencionan las limitaciones más comunes y serias:

- No Repudio: Falla al máximo, ya que, no hay por defecto establecido ningún método para dejar constancia de cuándo se ha realizado una operación, cuál ha sido y quiénes han intervenido.
- No proporciona formas de emitir recibos válidos que identifiquen una transacción. García y Chouciño (2002).
- La mayoría de las transacciones implementan RSA en vez del acuerdo de intercambio de claves públicas (Diffie – Hellman). Sierra (2006).
- Se obtiene más seguridad en la capa de Transporte a través de otras implementaciones como IPSec. Chou (2002a).
- Restricciones en la longitud de las claves utilizadas. Palacios (2006).
- No utiliza frecuentemente la autenticación de clientes, basta sólo con la del servidor.
- Sólo protege los datos que se encuentren en tránsito, no detenida o en reposo.
- No protege contra la ingeniería social y las cabeceras IP y TCP. Bisel (2007).

2.5. Últimos Avances del SSL. Con el aumento considerable del phishing y otras actividades fraudulentas en Internet que persiguen apropiarse de la información personal de otros usuarios, la autenticación de la identidad se convierte en un aspecto importantísimo.

2.5.1. Criptografía activada por Servidor (SGC). SGC es una extensión SSL creada originalmente para instituciones financieras exentas de las restricciones de exportación para USA. Con SGC, los niveles de cifrado se controlan mediante el servidor y no dependen del sistema cliente. Una vez eliminadas estas restricciones de exportación, los certificados SSL habilitados para SGC empezaron a emitirse para todos los tipos de sitios WEB y no sólo para las instituciones financieras autorizadas a finales de los años noventa. Soporta como cifrado mínimo 128 bits y como máximo 256 bits. Verising (2006).

2.5.2. SSL de Extended Validation (EV SSL). EV SSL es un nuevo estándar cuyo fin es combatir el aumento de amenazas en Internet (phishing y spoofing). Requiere un proceso estricto de autenticación de sitio WEB y se considera el "punto de referencia" del sector del comercio electrónico para autenticar la identidad legítima de un sitio WEB, en tal sentido, para emitir certificados EV SSL, la AC debe someterse a una auditoría rigurosa de WEBTrust. Verising (2006).

2.5.3. Aceleramiento de Transacciones Seguras. Un servidor SSL ejecuta procesos en el servidor WEB realizando todas las funciones SSL y "escucha" tráfico SSL por el puerto 443. **El número de conexiones SSL que un servidor puede soportar en software depende exclusivamente del CPU. Chou (2002b).**

2.5.4. Servidores SSL Asistido por Adaptadores de Tarjetas e Integrado a Enrutadores. Los adaptadores de tarjetas SSL alivian algunas de las cargas de procesamiento SSL en los servidores WEB. Residen en el interior del servidor en una de las ranuras genéricas, para escuchar únicamente el tráfico que transita por el puerto 443.

Se dice entonces que, algunas funciones son descargadas en la tarjeta y el cálculo SSL de direccionamiento es lo que más recurso computacional consume. Para eliminar la carga de SSL proveniente del servidor WEB, una implementación puede ser designada a realizarse dentro de un enrutador como tal, una limitante de esta modalidad es que no funcionan con equipos genéricos, por el contrario son propietarios. En todo caso un acelerador SSL integrado con un contenido enrutado, puede ser más caro que un adaptador de tarjeta de SSL, percibiéndose los beneficios de éste en el largo plazo. Chou (2002b).

2.5.5. Implementación de Modelos de Negociación. Cuando hacemos referencia al rendimiento del SSL observamos que está directamente relacionado con el mecanismo de cifrado, de esa forma se tiene que el peor rendimiento lo generó 3DES, seguidamente RC2, luego IDEA y DES (con rendimientos similares entre sí) y finalmente el RC4. Cada cifrado está diferentemente influenciado por la frecuencia de variación de los ciclos del CPU. Rapuano y Zimeo (2007).

Sin embargo y dependiendo del modelo de interacción preestablecido, B2B se afecta directamente el CPU, a tal punto de que, se consigue disminuir el impacto del SSL y su proceso de encriptar y desencriptar y la

merma en el rendimiento de los servidores puede ser cuantificada entre un 5 a 10%. Esto se logra si todas las interacciones entre los negocios son llevadas a cabo dentro de un período de sesiones y sólo un SSL Handshake se realiza al comienzo del período de sesiones y un promedio de 50 interacciones se llevan a cabo en cada período de sesiones. La equiparación de los períodos de sesiones seguras con períodos de sesiones del negocio permite un máximo de la reducción de SSL Handshake y, por tanto, el principal gasto de SSL se debe a la encriptación/desencriptación de la información intercambiada. García y col (2007).

En la práctica, cuando se analiza SSL y el efecto en la escalabilidad en los servidores, el resultado confirma que las cargas de procesos seguros y la intensidad del uso del CPU, permiten manejar más usuarios antes de que el equipo se sobrecargue, si se cuenta con más de un procesador, es decir, 2 o 4.

Además, es posible por medio de filtros definir una estrategia de control de sobrecarga evitando así la degradación del rendimiento del servidor. Sobre la base de este análisis, una adaptación del control de sobrecarga fundamentada en la diferenciación de la conexión y del control de admisión SSL permite distinguir nuevas conexiones SSL para ser resumidas todas y limitadas a aceptarse como una nueva conexión SSL, con un número máximo posible de recursos, sin sobrecargar el servidor, mientras todas la conexiones maximizan el número de transacciones completadas exitosas. Guitart y col (2007).

2.5.6. Protocolo de Contraseña Simple. Los Softwares gratuitos rompen contraseñas de 6 caracteres en 30 minutos y de 8 caracteres en 6 horas. Para disminuir este riesgo se debe tener un sistema estricto de normas de uso de contraseñas e ir migrando a un sistema de autentificación en SSL bajo el uso de certificados digitales que reemplacen las mismas.

A pesar de ello, una práctica común consiste en usar una misma contraseña para varias cuentas, incrementando los ataques maliciosos que pretenden adueñarse de las mismas. Para esto, existe el Protocolo de Contraseña Simple (SPP), el cual hace uso de 2 técnicas: desafío/respuesta, y un servidor de boletos a la vez. El servidor nunca conoce la contraseña del cliente en ningún momento y la validación es diferente en cada tipo de servidor. Con SPP se garantizan 4 propiedades, entre ellas: la seguridad, la cual está basada en dos hipótesis siendo éstas que SPP se ubi-

ca en el tope de SSL y que una contraseña simple es una cadena de 8 o más caracteres aleatorios. Gouda y col (2007).

3. Otras Soluciones Vigentes

Con el fin de corregir las deficiencias encontradas en el SSL, han surgido una serie de protocolos que de forma complementaria o sustitutiva funcionan.

3.1. Transport Layer Security (TLS). Este protocolo, integra en un esquema tipo SSL al sistema operativo, a nivel de la capa TCP/IP, para que el efecto "túnel" que se implementó con SSL sea realmente transparente a las aplicaciones que se están ejecutando. Se diferencia de él en varios aspectos fundamentales:

- En el protocolo Handshake los clientes sólo contestan con un mensaje si son SSL.
- Las claves de sesión se calculan de forma diferente y a la hora de intercambiar las claves, TLS no soporta el algoritmo simétrico privados.
- Utiliza dos campos más en el MAC que SSL, lo que lo hace más seguro. García y Chouciño (2002).

3.2. Secure – HTTP (S-HTTP). Es una extensión del protocolo HTTP cuya finalidad es la transmisión de datos de forma segura sobre la WEB entre un cliente y un servidor. Trabaja sobre la capa de Aplicación cifrando el contenido de los mensajes entre las dos máquinas usando para ello un sistema de cifrado basado en una pareja de claves pública y privada. La autenticación inicial es en ambos extremos mediante el uso de firmas digitales. La integridad de los datos se asegura utilizando MAC. La principal diferencia con SSL, es en cuanto al diseño, ya que, fue concebido para la transmisión de mensajes individuales de forma segura. Morales (2003).

3.3. Secure Electronic Transation (SET). Es un estándar abierto y multiplataforma, en el que se especifican protocolos, formatos de mensaje, certificados, etc., sin limitación alguna respecto al lenguaje de programación, sistema operativo o tipo de máquina usados. Es independiente del medio de comunicación utilizado y se puede transportar directamente mediante TCP, correo electrónico y HTTP en páginas WEB. Utili-

za estándares criptográficos reconocidos y ampliamente usados. Emplea el mismo estándar para los formatos de los mensajes que SSL y se basa en el uso de la criptografía de clave pública efectuando una autenticación de todas las partes participantes en la transacción bajo certificados digitales. Es más lento y complejo que SSL. García y Chouciño (2002).

3.4. IPSec. Proporciona autenticación, confidencialidad e integridad de datos, trabaja en la capa de Red y posee protecciones efectivas contra la repetición de tramas, es capaz de trabajar con UDP y otros protocolos de la capa de Transporte y, se presenta como el verdadero sustituto de SSL. A continuación se mencionan las diferencias significativas con SSL:

- Control de acceso: conexiones permanentes.
- Usuarios: no importa la procedencia y pertinencia de los usuarios.
- Software cliente: garantiza conexiones de todos los recursos de la red y se cuenta con variables de control de acceso en las diferentes aplicaciones.
- Confidencialidad y autenticidad: alto nivel de cifrado y autentificación.
- Criticidad de los recursos accedidos: altos y variables con definición de niveles de jerarquías.
- Criticidad de las funciones realizadas: altos y variables con definición de niveles de jerarquías.
- Nivel técnico de los usuarios: moderado a alto.
- Implantación, flexibilidad y escalabilidad: de fácil y rápida implantación y mantenimiento y flexible ante futuras modificaciones. Morales (2003).

Sin embargo existen algunas consideraciones para el uso correcto del IPSec:

- El software debe estar instalado en el cliente y SSL debe estar incluido en el navegador.
- La traducción de direcciones de red coexisten con el IPSec. Bisel (2007).

3.5. Otros. Existen otros protocolos de seguridad de accesos WEB, no tan difundidos o exitosos, que bien vale mencionar como lo son: Servidores Seguros. García y Chouciño (2002); Private Communication Technology (PCT) y CyberCash. Morales (2003).

Conclusiones

Como conclusión de esta investigación se puede afirmar que los protocolos de acceso WEB están orientados a proporcionar seguridad para los 7 elementos sin desmejorar unos en beneficio de otros. Hasta ahora ningún protocolo por sí solo ha logrado cubrir todas las necesidades de seguridad por completo de forma eficiente. De hecho, las mejores soluciones exigen implementaciones complejas y costosas, que afectan los procesos mismos del negocio al clasificar los servicios como medulares y colaterales, relegando a éstos últimos a utilizar los recursos computacionales en segundo plano, prolongando el tiempo de ejecución y culminación.

A pesar de su longevidad, SSL no parece ser sustituido totalmente en el corto plazo como protocolo de seguridad, incluso sin garantizar la disponibilidad y el no repudio, (elementos de seguridad); el panorama inmediato parece no verse afectado, ello se debe a la sencillez, transparencia y flexibilidad de acoplamiento con otros esquemas de seguridad, especialmente donde SSL es vulnerable. Protocolos como TLS e IPSec, que surgieron como competidores y sustitutos de SSL, lo que han logrado es un perfecto ajuste tal que, se complementan eficientemente con resultados en rendimiento y seguridad sobresalientes.

Otro elemento a considerar es el uso intenso que incurre en el proceso de PKI (256 bits) en el CPU, lo cual no pareciera importar mucho hoy día cuando la evolución de la arquitectura de los microprocesadores (2 - 4 procesadores físicos con 2 - 4 núcleo internos) ofrecen mayor capacidad de procesamiento a un costo razonable.

Investigaciones recientes muestran que bajo esquemas de modelos de negociación preestablecidas éstos logran reducir la merma en el procesamiento del CPU de los servidores entre un 5 - 10%, sin tener que afectar la longitud de las claves PKI. Pareciera que éste es el momento propicio para retomar investigaciones antiguas que tratan encripta-

ción/desencriptación de las claves PKI que anteriormente no podían implementarse básicamente por los recursos computacionales exigidos.

Por tal razón, un factor que puede afectar el uso de las PKI largas es el sistema legal de restricciones de exportaciones de USA, que limita las mismas a 256 bits. Desde soluciones simples como el uso del PPC pasando por servidores SSL asistidos por aceleradores de tarjetas hasta el EC SSL son garantías de la continuidad del SSL. De hecho, otras implementaciones sobre SSL han logrado suplir los elementos de seguridad ausentes en éste como es el caso de TLS e IPSec.

Sin embargo, y aunque SSL puede proteger los datos mientras éstos se encuentren en tránsito a través de una red, ahora bien, está protección podría no ser suficiente para algunas aplicaciones de propósitos específicos. Es por ello que, el desarrollo de un servicio WEB que asuma las funciones de intermediario, tomando como modelo el esquema de intercambio de información SET, parece ser una alternativa atractiva. Éste no pretende sustituir o desplazar al SSL, sino por el contrario, complementarlo y aportar robustez en instancias donde el SSL ha evidenciado debilidad o limitación, sin desmejorar la transparencia, sencillez y velocidad del mismo. El servicio WEB pudiera estar en una condición pasiva y pasar a una activa cuando se invoque en función de la transacción WEB a realizar para una institución específica, con la cual se va a trabajar. Para ello, éste debe estar acreditado y certificado por la institución y/o alguna otra entidad certificadora.

En este sentido, una vez activado se habilita el servicio WEB y se procede a efectuar el proceso de orquestación e interacción entre el cliente y el servidor, intercambiando información necesaria para poder iniciar, ejecutar y finalizar el servicio escogido, el cual solamente lo puede ofrecer la institución o empresa propietaria del servicio WEB. Es éste quien se encargaría de filtrar la información sensible a ser manipulada, evitando así, la exposición innecesaria de información confidencial enviada entre el cliente y el servidor, sobre todo en instantes relativos al procedimiento de iniciación del proceso de negociación y de finalización del protocolo SSL.

El servicio WEB sería ahora el que se encargaría de administrar y gestionar los parámetros cifrados, método de intercambio de claves, secretos de claves a soportar, entre otros, y es quien negocia tanto con el

cliente como el servidor, pasos previos a la ejecución del protocolo SSL, puesto que una vez hecho esto, es cuando el protocolo SSL toma el control del proceso y deja en un estado de pasivo al servicio WEB.

De esta forma este servicio WEB, retoma el control de las gestiones cuando el protocolo SSL finaliza su proceso. Para este momento el servicio WEB, habiendo generado las validaciones respectivas, conserva la información sensible a ser utilizada para falsificación de identidad, suministrada tanto por el cliente como por el servidor, procediendo a eliminar cualquier huella de la data generada una vez haya finalizado el proceso.

Lo anteriormente expuesto es una propuesta que nos orienta hacia la realización de nuevos estudios, desarrollos e implementaciones que bien puedan someter al SSL a una revisión profunda que conlleve a una reingeniería parcial o total, en aquellas áreas donde presentan debilidades y limitaciones serias para generar una nueva versión del SSL o un nuevo protocolo derivado de éste.

Referencias bibliográficas

Bisel, L. (2007). The Role of SSL in Cybersecurity (documento en línea). Disponible en: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?&arnumber=4140966 (consulta: 6-9-2007).

Cisco Systems (2003). Introduction to Secure Sockets Layer (documento en línea). Disponible en: http://www.cisco.com/en/US/netsol/ns340/ns394/ns50/ns140/networking_solutions_white_paper09186a0080136858.shtml (Consulta: 20-5-2007).

Chou, W. (2002a). Inside SSL: The Secure Sockets Layer Protocol (documento en línea). Http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/6294/22429/0104664 4.pdf?arnumber=1046644 (Consulta: 20-6-2007)

Chou, W (2002b). Inside SSL: Accelerating Secure Transactions (documento en línea). Disponible en: http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/6294/22323/01041177.pdf (Consulta: 20-6-2007).

Espinosa, R. y Morales, G. (2000). Una arquitectura de seguridad para IP (documento en línea). Disponible en: http://delta.cs.cinvestav.mx/~gmorales/OwnSecurity/IPSec.pdf. (Consulta: 2-10-2007).

Friedly, N. (2004). TLS/SSL (documento en línea). Disponible en: http://nfriedly.com/stuff/Nathan_%20Friedly_SSL_TLS.doc. (Consulta: 7-6-2007).

García, D., García, R., Entrialgo, J., García, J., García M. (2007). Evaluation of the effect of SSL overhead in the performance of e-business servers operating in B2B scenarios. (documento en línea). Disponible en: http://portal.acm.org/citation.cfm?id=1296629&CFID=46629701&CFTOKEN=29373195. (Consulta: 12-6-2007).

García, M. y Chouciño J. (2002). Seguridad en Internet: SSL (documento en línea). Disponible en: http://www.govannom.org/seguridad/criptografia/seg_WEB.pdf (Consulta: 22-6-2007).

Gouda, M., Liu, A., Leung, L., Alam M. (2007). SPP: An anti-phishing single password protocol (documento en línea). Disponible en: http://www.cse.msu.edu/~alexliu/publications/Password/sppjournal.pdf (Consulta: 9-7-2007).

Guitart, J., Carrera, D., Beltran V., Torres, J., Ayguadé, E. (2007). Designing an overload control strategy for secure e-commerce applications (documento en línea). Disponible en: http://www.sciencedirect.com/science?_ob=MImg&_imagekey= B6VRG-4P4FV9Y-2-1&_cdi=6234&_user=3445010&_orig=search&_coverDate= 10%2F24%2F2007&_sk=999489984&view=c&wchp=dGLbVlbzSkzk&md5=38d6dfc83579658265a663e67e9cf352&ie=/sdarticle.pdf (Consulta: 10-9-2007).

Morales, J. (2003). SSL, Secure Sockets Layer y Otros Protocolos Seguros para el Comercio Electrónico (documento en línea). Disponible en: http://blog.unlugarenelmundo.es/?page_id=127 (Consulta: 23-6-2007).

Palacios, R. (2006). Protocolo de Seguridad en la capa de Transporte: Secure Socket Layer (SSL) (documento en línea). Disponible en: http://www.iit.upcomillas.es/palacios/seguridad_dr/tema4_ssl.pdf (Consulta: 13-5-2007).

Pons, M. (2000). Seguridad en Comercio Electrónico (documento en línea. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m013c.htm (Consulta: 8-6-2007).

Rapuano S. y Zimeo E. (2007). Measurement of performance impact of SSL on IP data transmissions (documento en línea). Disponible en: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V42-4P940K9-3 T&_cdi=5746&_user=3445010&_orig=search&_coverDate=07%2F27%2F2007&_sk=999999999&view=c&wchp=dGLbVtzzSkWA&md5=c997840d2f9d9d2c20fb9ecebc93833b&ie=/sdarticle.pdf (Consulta: 18-10-2007).

Stallings, W. (1998). SSL: Foundation for WEB Security (documento en línea). Disponible en: http://www.cisco.com/WEB/about/ac123/ac147/archived_issues/ipj_1-1/index.html. (Consulta: 2-5-2007).

Sierra, J. (2006). Criptografía Asimétrica: "Sistema de Cifrado basado en clave pública" Disponible en: http://www.iit.upcomillas.es/palacios/seguridad/cap05.pdf (Consulta: 9-7-2007).

Verisign (2006). Los últimos avances de la tecnología SSL (documento en línea). Disponible en: http://www.verisign.es/static/038828.pdf (Consulta: 12-5-2007).

Wagner, D. y Schneier, B. (1999). Wagner, David y Schneier Bruce. Analysis of the SSL 3.0 Protocol (documento en línea). Disponible en: http://www.schneier.com/paper-ssl.pdf (Consulta: 3-5-2007).