La protección de su página web
Con Siempre en SSL

OTA promueve el uso de las mejores prácticas para mitigar las amenazas emergentes a la privacidad, identidad y seguridad a los servicios, agencias gubernamentales, organizaciones y consumidores en línea, aumentando así la confianza en línea.

Actualizado 1 de mayo 2012

Tabla de Contenidos

Resumen ejecutivo

La seguridad y la confianza de los consumidores son los cimientos sobre los que se ha construido el Internet. Hace mucho tiempo que los mejores comercios y empresas de servicios financieros en todo el mundo utilizan la tecnología de Capa de Conexión Segura / Seguridad de la Capa de Transporte SSL / TLS para proteger las comunicaciones y transacciones de sus clientes. Este modelo de seguridad se ha utilizado durante más de una década para garantizar la confianza en los navegadores Web, dispositivos móviles, clientes de correo electrónico y otras aplicaciones de Internet, y sigue siendo fundamentalmente sólido. Los sitios Web y Partes que Confían habitualmente emplean SSL / TLS para proteger información confidencial tal como las contraseñas y los números de tarjetas de crédito. El número de sitios que utilizan SSL / TLS ha aumentado a más del doble desde 2005, y en la actualidad, se estima que más de 4,5 millones de sitios utilizan certificados SSL emitidos por una Autoridad de Certificación.[1]

Pero con el surgimiento de Web 2.0 y las redes sociales, las personas pasan más tiempo en línea y conectadas, y comunican mucho más que tan sólo sus números de tarjetas de crédito. Muchas personas usan Facebook, Gmail y Twitter como su medio principal de comunicación. El panorama de amenazas ha evolucionado también con la proliferación de botnets, malware, pérdida de datos, correo electrónico falsificado, el fraude en línea y otros desafíos de la seguridad y privacidad. Desafortunadamente, las prácticas de seguridad de Internet no siempre han seguido el ritmo de estos cambios. Muchas organizaciones utilizan el protocolo SSL / TLS para cifrar el proceso de autenticación cuando los usuarios acceden a un sitio web, pero no cifrar las páginas siguientes durante la sesión del usuario. Esta práctica es arriesgada ya que deja vulnerables a los visitantes al sitio web a ataques maliciosos en línea, y puede dejar expuestos a millones de usuarios a amenazas sin saber, incluso cuando visitan un sitio web en el que confían.

Online Trust Alliance (OTA) les ha pedido a las comunidades de seguridad, negocios, y publicidades interactivas que trabajen en conjunto para proteger a los consumidores de peligros. Corresponde a todas las partes interesadas a que adopten medidas razonables para proteger la confianza de los consumidores mediante la adopción de mejores prácticas de seguridad de fácil implementación y de acceso a nivel mundial. Una de esas prácticas es *Siempre en SSL* (SSSL), la práctica de utilizar SSL / TLS a través de su sitio entero para proteger a los usuarios con una seguridad persistente, desde el comienzo al fin de la sesión. *Siempre en SSL* es una medida probada, de carácter práctico que debe ser implementado en todos los sitios web donde los usuarios comparten o ven información confidencial.

Este documento explica la necesidad imprescindible de *Siempre en SSL*, y las medidas que se pueden tomar para proporcionar protección absoluta a los usuarios. También incluye descripciones detalladas de cuatro organizaciones-Facebook, Google, PayPal y Twitter-que están liderando el enfoque de *Siempre en SSL* en un esfuerzo de cooperación por hacer que el Internet sea más seguro.

OTA desea agradecer las aportaciones del Comité Directivo de OTA y de los miembros, incluyendo AllClear, DigiCert, Epsilon, IID, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft, PayPal, Pitney Bowes, Publishers Clearing House, Return Path, Secunia, Star Marketing Group, Symantec, TrustSphere y VeriSign, Inc.. Un agradecimiento especial a Alex Rice de Facebook, Adam Langley de Google, Andy Steingruebl de PayPal, John Scarrow de Microsoft, Lui Quentin y Rick Andrews, de Symantec, Bob Lord de Twitter y Craig Spiezle de OTA por sus aportaciones y colaboración en este trabajo.

Las actualizaciones a este informe serán publicadas en https://otalliance.org/aossl.htm. Favor de enviar comentarios a staff@otalliance.org.

[1] Netcraft 02 2012 SSL Encuesta

La necesidad de la protección continua en línea

Actualmente, los usuarios de Web 2.0 tienen acceso a una variedad grande y creciente de servicios que les proporcionan ricas experiencias interactivas y personalizadas mientras buscan, comparten y compran en el Internet. Muchos servicios se basan en las cookies del navegador para que estas experiencias mediante la creación de conexiones persistentes recuerden el estado de la sesión. Cuando un usuario inicia una sesión en un sitio, por lo general tiene que presentar un nombre de usuario y contraseña para autenticar su identidad. El servidor web a continuación, genera un identificador de sesión único para el usuario y lo transmite al navegador de Internet, donde se almacena en caché. A este tipo de archivo con texto único como clave se le llama una "cookie." El explorador Web envía el contenido almacenado en caché de la cookie de vuelta al servidor web cada vez que interactúa con el usuario conectado en el sitio, y la cookie permanece activa hasta que se caduca o se elimina.

Las cookies HTTP y las demás cookies inseguras dejan a los usuarios vulnerables a los ataques

Muchos sitios web utilizan el protocolo HTTPS para cifrar la información de inicio de sesión con un canal de SSL, pero bajan a sus usuarios al protocolo HTTP después de instalar la cookie de sesión. Esto puede proteger la contraseña del usuario, pero la cookie-incluyendo la identificación de sesión, se transmite en texto simple cuando el navegador Web hace solicitudes posteriores al dominio, dejando a los usuarios vulnerables a los ataques de secuestro de sesión. También se les puede dar a los usuarios una falsa sensación de seguridad porque creen incorrectamente que su sesión completa está segura, cuando sólo es el inicio de sesión que está cifrado.

Algunas organizaciones utilizan HTTPS en su sitios enteros, pero se olvidan de marcar las cookies de sesión como seguras. Esto también es un riesgo porque los usuarios suelen escribir direcciones URL parciales (por ejemplo, sin escribir "https://" en forma explícita de antemano), y las cookies están expuestas durante la primera solicitud, antes de que se les redirija a una página HTTPS. Un atacante mirando una red abierta sólo tiene que capturar una sola petición HTTP no cifrada para robar cookies de sus víctimas y secuestrar sus cuentas.

Estos problemas no son nuevos y pueden afectar cualquier sitio Web que use cookies de sesión. Los buscadores de Internet que hacen eco de los términos de consulta de los usuarios son vulnerables a este tipo de ataque. Las organizaciones ya no pueden darse el lujo de seguir siendo complacientes, y la educación en sí de un usuario no es suficiente. El estado general de la seguridad en línea en toda la industria ha llegado a un punto de inflexión, y los sitios web deben cambiar a fin de preservar la confianza de los usuarios.

El secuestro de sesiones es peligrosamente fácil

El secuestro de sesión no es un problema nuevo, pero el lanzamiento de un programa adicional en el navegador Firefox llamado "Firesheep" ha aumentado la conciencia entre los usuarios y los atacantes sobre la inseguridad inherente de las conexiones HTTP sin protección (redes Wi-Fi abiertas). Desarrollado por Eric Butler y Ian Gallagher, Firesheep hace que sea "muy fácil" que un atacante sin conocimientos de programación secuestre la cuenta de alguien en un gran número de sitios web populares. Firesheep encuentra y une redes abiertas, tales como una red Wi-Fi en un café o biblioteca, y utiliza un analizador de paquetes para capturar las cookies que no son seguras. En cuanto alguien visite un sitio web inseguro conocido por Firesheep, el software toma y muestra el nombre de usuario y los servicios a los que esté conectado. El atacante puede hacer doble clic sobre el nombre de la víctima y de inmediato tener acceso a su cuenta.

Firesheep es una innovación en cuanto a integración de funciones y facilidad de uso. Pero, como Butler y Gallagher declararon, Firesheep puso al descubierto la gravedad y el alcance de un problema que los expertos de seguridad advertieron hace muchos años. Las herramientas de software tales como "Hamster", "Ferret", y "CookieMonster" se introdujeron años antes de Firesheep, y también permitían a los atacantes que accedieran a redes abiertas, robaran cookies y secuestraran sesiones de HTTP con relativa facilidad.

Figura 1. Captura de pantalla de Firesheep en la acción

Con estas herramientas a mano, un atacante puede explotar esta vulnerabilidad para obtener acceso total o parcial a la cuenta de la víctima. Algunos sitios toman precauciones para evitar el secuestro completo de los usuarios (por ejemplo, pidiendo la contraseña anterior, cuando un usuario trata de cambiarla), pero en muchos casos, el atacante puede apoderarse totalmente de la cuenta de la víctima, cambiar su contraseña y, potencialmente, secuestrar los otros servicios que están conectados a la cuenta de la víctima.

No es sólo un problema en los cafés

Algunas personas creen que el secuestro de sesión es sólo un problema en los "cafés de Internet" y que la solución es que los usuarios eviten las redes Wi-Fi abiertas. Pero esta es una expectativa poco realista, y la realidad es que las herramientas como Firesheep pueden ser utilizada para interceptar cualquier tráfico de red, inalámbrico o no, que incluya cookies enviadas por las sesiones HTTP sin cifrar. Otro aspecto pasado por alto es el riesgo a las organizaciones empresariales y agencias gubernamentales que utilizan sitios de redes sociales, correo web y aplicaciones web 2.0. Si un empleado tiene acceso a un sitio inseguro y su sesión está secuestrada, el atacante puede usar la cuenta como un vector para propagar código malicioso, o puede tener acceso a activos confidenciales y causar un fallo de seguridad de datos. El daño potencial que podría resultar de tal violación es algo que ningún operador de sitio web quiere enfrentar.

La educación de los usuarios en sí no es suficiente

Como intento de aumentar la conciencia de los usuarios y luchar contra el peligro del secuestro, la Electronic Frontier Foundation (EFF) ha creado su propia extensión para Firefox, HTTPS-Everywhere, lo cual obliga a Firefox a utilizar sólo conexiones HTTPS en ciertos sitios web. Además, la EFF y Access, una organización sin fines de lucro, han creado HTTPS Now, una campaña educativa internacional para mejorar la conciencia y la adopción de *Siempre en SSL* como el "nivel mínimo de seguridad" para navegar el Internet. La campaña incluye un sitio web

donde los usuarios pueden ir a buscar y aportar información acerca de los sitios web que utilizan HTTPS.[2] HTTPS-Everywhere se considera una herramienta que funciona bien en una lista definida de sitios web, pero no protege a los usuarios si visitan sitios con los que no es compatible. Además, HTTPS-Everywhere no es compatible con Chrome, Safari o Internet Explorer, y su valor será limitado hasta que todos los principales navegadores apoyen o incluyan esta funcionalidad por defecto.

El trabajo de EFF es encomiable, pero la educación del usuario y las herramientas por sí solas no eliminarán las vulnerabilidades de sesiones de administración de sitios web, y no es probable que la gente deje de usar las redes abiertas en cafés, bibliotecas, aeropuertos y otros lugares públicos para acceso al Internet. Los operadores de sitios web deben proteger los datos y la privacidad de sus usuarios, sin importar el navegador o cómo se está utilizando la red. Tomando las medidas necesarias de protección contra un ataque antes de que sea exitoso, las empresas pueden evitar la pérdida de clientes y de incurrir costos agobiantes de litigios y la reparación de la publicidad negativa.

Proteger la experiencia del usuario Con *Siempre en SSL*

Siempre en SSL es una medida de seguridad económica y fundamental que ofrece una protección total a los visitantes a un sitio web. No es un producto, servicio o sustitución de sus certificados SSL existentes, sino más bien un enfoque en la seguridad que reconoce la necesidad de proteger la totalidad de la sesión de un usuario, no sólo la pantalla de inicio de sesión. Siempre en SSL comienza utilizando HTTPS en el sitio entero, pero también significa el establecimiento del indicador seguro para todas las cookies de sesión para evitar que su contenido sea enviado a través de una conexión HTTP. Medidas adicionales, tales como certificados SSL de Validación Extendida (EV) y HSTS, pueden reforzar aún más su infraestructura contra un ataque de “hombre en el medio”.

Todo el mundo lo está haciendo, y usted también debería

Con la aumentada frecuencia y facilidad de los ataques en línea, organizaciones de todo el mundo son objeto de creciente escrutinio para asegurar que todas las transacciones en línea relacionadas con los datos confidenciales estén seguras. Los funcionarios del gobierno y grupos de privacidad están presionando para que las empresas proporcionen *Siempre en SSL*.

En enero de 2011, como respuesta a informes de ataques a SSL, el senador de los E.E.U.U. Charles Schumer (D-NY) envió una carta a Yahoo!, Twitter y Amazon[3] para quitar la "alfombra de bienvenida a los aspirantes a piratas informáticos" que presenta HTTP, y en su lugar les pidió que aceleraran la aplicación de *Siempre en SSL*.

Hoy en día, algunos de los sitios web más grandes y de más confianza del mundo, incluyendo Facebook, Google, PayPal y Twitter, han adoptado *Siempre en SSL*, y están aplicando HTTPS para cifrar todas las comunicaciones desde y hacia sus sitios web, incluidos los datos de promoción y no confidencial. Estas organizaciones reconocen la creciente importancia de la protección persistente, y estamos trabajando duro para proporcionar una experiencia segura para los usuarios en línea a través de la Web.

---

[2] https://www.eff.org/press/archives/2011/04/19-0

[3] http://www.infosecurity-magazine.com/view/16328/senator-schumer-current-internet-security-welcome-mat-for-wouldbe-hackers/

Facebook

Como el sitio más visitado en la web,[4] Facebook tuvo 845 millones de usuarios activos mensuales a finales de diciembre de 2011, con un promedio diario de 483 millones de usuarios activos durante ese mismo mes.[5] Facebook se dedica a proteger la información de la gente, y sus equipos de seguridad han desarrollado sistemas sofisticados para proteger su sitio contra spam, phishing, código malicioso y otras amenazas la seguridad.[6] En enero de 2011, como parte de un gran esfuerzo para hacer más segura su plataforma para los usuarios, Facebook comenzó a implementar *Siempre en SSL* implementando la capacidad de los usuarios de navegar por el sitio a través de HTTPS. La respuesta de los usuarios hacia el cambio fue enorme, con más del 19 por ciento de los usuarios activos de Facebook eligiendo permitir la navegación segura.

La orquestación de la migración de millones de aplicaciones

Facebook se enfrentó a un desafío más desalentador en la migración de su ecosistema de más de un millón de desarrolladores a HTTPS y OAuth 2.0[7], un estándar abierto escrito en colaboración con Yahoo, Twitter, Google y otros. Este fue un esfuerzo importante, porque muchas aplicaciones de terceros se bloquearían cuando los usuarios intentaran navegar con seguridad si no se admitía HTTPS y causaría advertencias de contenido mixto en los navegadores. Para ayudar a los desarrolladores a hacer la transición, Facebook esbozó un plan de seis meses en su plan de trabajo para desarrolladores de sitios y aplicaciones para migrar a HTTPS.[8]

La transición fue rápida para los desarrolladores que habían creado sus aplicaciones con soporte para conexiones seguras, pero para algunos desarrolladores más grandes con una multitud de aplicaciones, se requirieron más tiempo y recursos para encontrar y volver a escribir el código necesario, y hacer las mejoras necesarias a la infraestructura.

Para Facebook, la transición a un enfoque de *Siempre en SSL* y el esfuerzo ha valido la pena. La compañía ahora tiene un estándar único para la autenticación de aplicaciones utilizadas a través de HTTPS que les permite ofrecer una plataforma más sencilla, más segura y confiable. Con la finalización de este paso, Facebook se está centrando ahora sus esfuerzos en la expansión internacional de la infraestructura para llevar la latencia a niveles tolerables. Este es un componente crítico para Facebook, ya que aproximadamente el 80 por ciento de sus usuarios activos se encuentran fuera de América del Norte.

> *"Tenemos mucha más confianza ahora en nuestra capacidad de ofrecer un servicio seguro a través de redes donde de otra manera la privacidad de nuestros clientes habría estado en riesgo."*
>
> – Alex Rice, Facebook

[4] http://www.google.com/adplanner/static/top1000/

[5] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

[6] https://www.facebook.com/blog/blog.php?post=486790652130

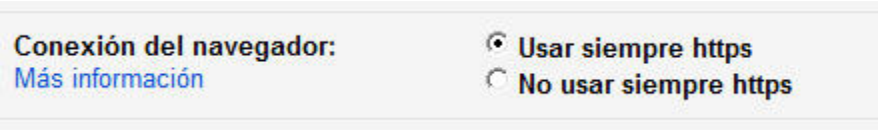
[7] http://oauth.net/2/

[8] https://developers.facebook.com/blog/post/497/

Google

Aunque Google empezó como un buscador de Internet que se ocupaba principalmente de información pública, la empresa ha llegado a ofrecer una experiencia de usuario cada vez más personalizada, y hace tiempo que entienden la importancia de proteger la privacidad de la información personal. Cuando Google creó Gmail y Google Apps, su intención fue construir productos de clase mundial tan sólidos que podría gestionar su propia empresa a base de ellos, por lo que diseñó Gmail y Google Apps para admitir HTTPS desde el principio. Al principio, obligaron el uso de HTTPS para proteger la información de usuario de inicio de sesión. Luego, en julio de 2008, Google lanzó una característica que les dio a todos los usuarios de Gmail y Google Apps la opción de usar siempre HTTPS.

Figura 2. Imagen de la opción HTTPS en Gmail y Google Apps



En enero de 2010, Google decidió hacer HTTPS la configuración por defecto de Gmail y Google Apps,[9] lo que hace aún más fácil que los usuarios protejan su correo electrónico entre su navegador y Google, en todo momento. Esta transición no requiere ningún equipo o hardware adicional, y el impacto en el rendimiento era insignificante. Los investigadores de Google descubrieron que SSL / TLS representa menos del uno por ciento de la carga de CPU en su máquinas de producción de interfaz, menos de 10 KB de memoria por conexión, y menos del dos por ciento de la sobrecarga de su red.

Habilitación de Búsqueda Segura

Proporcionar una experiencia de búsqueda segura era una tarea más compleja. En mayo de 2010, Google presentó una opción de búsqueda cifrada, dando a los usuarios la capacidad de realizar búsquedas con una mejor protección contra el espionaje por parte de terceros. Más recientemente, Google comenzó a utilizar HTTPS como la experiencia de búsqueda por defecto para sus usuarios ingresados. Este cambio cifra las consultas de los usuarios y la página de resultados de Google.[10] El beneficio de la seguridad de este enfoque era claro: los usuarios tienen una experiencia de búsqueda más segura y privada a través del uso de un cifrado total entre sus máquinas y Google. Sin embargo, el ecosistema alrededor de la búsqueda, sobre todo el análisis web y SEO (Posicionamiento en buscadores) es más complejo.

Cuando los usuarios hacen clic en un resultado de búsqueda de Google para visitar un sitio web, una bandera de referencia es proporcionada por el navegador para indicar si la petición actual es el resultado de un enlace de Google. Muchos practicantes de SEO y profesionales de análisis web se basan en esta información para obtener estadísticas de uso o para determinar el impacto de sus esfuerzos de marketing en línea. Sin embargo, cuando los usuarios realizan una búsqueda de forma segura, los términos de la consulta están protegidos. Para los sitios que reciben clics de los resultados de búsqueda de Google, esto significa que todavía sabrán que los usuarios provienen de Google, pero no recibirán información acerca de cada consulta individual.

Sin embargo, tal como Google indica, los sitios aún pueden recibir una lista agregada de las 1.000 consultas de búsqueda mayores que impulsaron el tráfico a su sitio para cada uno de los últimos 30 días a través de Google Webmaster Tools. Esta información ayuda a los webmasters mantener

[9] http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html

[10] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html

estadísticas más precisas sobre su tráfico de usuarios, al tiempo que protege la confidencialidad de los usuarios individuales que tienen HTTPS activado. Por otra parte, cuando un usuario opta por hacer clic en una publicidad que aparece en las páginas de resultados de Google, su navegador seguirá enviando la consulta pertinente sobre la red para que los anunciantes puedan medir la efectividad de sus campañas y para mejorar los anuncios y las ofertas que presenten.

En el futuro, Google planea añadir más apoyo para *Siempre en SSL* a sus productos, y sus investigadores continúan publicando información y asesoramiento sobre SSL / TLS. Google también está abogando fuertemente por esfuerzos más amplios por parte de la industria para implementar SSL de forma más amplia y efectiva, con la visión de la protección de todo el contenido legítimo de la Web para asegurar una experiencia fluida y segura para los usuarios de todo el mundo.[11]

PayPal

Desde 1998, PayPal ha sido el líder global en soluciones de pago en línea, y fue un pionero de SSL / TLS. Para el año 2000, la compañía ya utilizaba HTTPS en todas las páginas después de la pantalla de inicio de sesión de usuario y había comenzado a utilizar HTTPS para proteger la pantalla de inicio de sesión misma para el año 2006. PayPal es también una de las primeras organizaciones en utilizar certificados SSL de Validación Extendida (EV) y comenzó a utilizar EV SSL en todas las páginas de inicio de sesión tan pronto como 2007.[12]

PayPal se enfrentaba a desafíos únicos en cuanto al rendimiento, debido a la naturaleza transaccional de sus servicios. A diferencia de los sitios donde los usuarios pasan un período de tiempo relativamente largo en una sola sesión, PayPal ofrece un mayor porcentaje de sesiones cortas. Y puesto que el handshake SSL / TLS es la parte que más tiempo requiere en el proceso, sabían que tendrían que monitorear y administrar el impacto en el rendimiento potencial en la experiencia del usuario. Sin embargo, en algunos casos, la conversión a HTTPS en realidad acelera el sitio porque pudieron utilizar contenido de los mismos servidores a través de conexiones en el navegador.

Los equipos de seguridad de PayPal eran muy conscientes de que su sitio era un objetivo especialmente atractivo para los ladrones de phishing, hackers y otros criminales cibernéticos, y comenzaron a tomar medidas extraordinarias para proteger a sus clientes y su reputación. Su objetivo era frustrar los ataques de phishing y herramientas activas de ataques tales como sslstrip (a diferencia de Firesheep, que es una herramienta pasiva de escuchar a escondidas, pero que no hace cambiar de ruta o modificar los paquetes de red).[13]

Estos esfuerzos culminaron en el lanzamiento del protocolo HTTP Seguridad Estricta de Transporte (HSTS por sus siglos en inglés), creado en conjunto con Jeff Hodges, un ingeniero de seguridad de PayPal.[14] Esta especificación define un camino para que los sitios web se declaren accesible sólo a través de conexiones seguras, y / o para que los usuarios podrán interactuar con los sitios dados solamente a través de conexiones seguras. Actualmente, HSTS es compatible con Google Chrome y Mozilla Firefox, y sitios como PayPal.com que utiliza HSTS indican explícitamente a los navegadores que sólo utilizarán y aceptarán comunicaciones cifradas, evitando que los usuarios visiten una página HTTP por accidente o que sean dirigidos a páginas HTTP a través de un ataque de phishing o de sslstrip.

[11] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html

[12] https://otalliance.org/resources/EV/index.html

[13] http://www.thoughtcrime.org/software/sslstrip/

[14] http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02

Twitter

Como una red de información en tiempo real, Twitter ha estado a la vanguardia de muchas noticias, especialmente en las zonas del mundo donde se restringe la libertad de expresión. Aunque Twitter ha sido objeto de algunos incidentes de seguridad que se han convertido en noticias, la compañía ha hecho grandes avances al hacer que Twitter sea más seguro para los usuarios.

Twitter ya apoyaba HTTPS para su sitio, clientes de teléfonos inteligentes y su sitio web móvil, incluyendo características tales como el botón Tweet, pero la empresa pronto se movió hacia adelante con un objetivo más ambicioso de la aplicación de *Siempre en SSL*.[15] En mayo de 2011, Twitter anunció que se les proporcionaría a los usuarios la opción de usar siempre HTTPS a través de una configuración definida por el usuario. La respuesta enormemente positiva por parte de los usuarios de Twitter provocó que Twitter acelerara el acceso a todos los usuarios en enero de 2012, por lo cual HTTPS es la opción por defecto para todos los usuarios.

Twitter superó algunos desafíos únicos en la adopción de *Siempre en SSL*. La empresa subcontrata parte de su tráfico a redes de distribución de contenidos (CDN) y tenía como prioridad asegurar que los CDN tuvieran la capacidad de manejar la carga SSL aumentada. La preservación de la capacidad de rastrear las referencias y análisis fue también importante para Twitter y sus socios, y los ingenieros de Twitter volvieron a crear el código para trabajar evitar problemas específicos relacionados con el contenido mixto.

Lecciones aprendidas

Los expertos en seguridad de Facebook, Google, PayPal y Twitter obtuvieron información valiosa, la cual han compartido con OTA como un servicio público para ayudar a los operadores de sitios web a protegerse y proteger a sus usuarios contra el secuestro de sitio y otros ataques. Estas información contiene puntos que deben ser considerados antes de implementar *Siempre en SSL* en su sitio web.

SSL no es computacionalmente costosa

Algunas organizaciones han sido reacias a aplicar *Siempre en SSL* porque perciben que aumentará los gastos generales y operativos de su sitio web. Los certificados SSL / TLS emitidos por una autoridad de certificación no son gratis, pero tienen un costo fijo, y no hay necesidad de sustituir los certificados SSL existentes. Si es necesario asegurar varios nombres de dominio, se puede hacerlo añadiéndolos como Nombres Alternativo del Sujeto (SAN) al comprar sus certificados.

Aparte del costo del certificado SSL, está la cuestión de los requisitos de cómputo y la posible necesidad de adquirir hardware adicional para soportar la carga de CPU.
En los sitios web grandes y populares, parece razonable pensar que el cómputo adicional necesario para cifrar y descifrar los paquetes de red podría suponer un aumento sustancial de los requisitos de hardware. Sin embargo, muchas organizaciones han encontrado que esto no es siempre el caso.

> *"Si usted deja de leer ahora, sólo tienes que recordar una sola cosa:*
>
> *SSL / TLS no requiere más computación. Hace diez años que podría haber sido cierto, pero no es sólo el caso ahora. Usted también puede darse el lujo de habilitar HTTPS para los usuarios."*
>
> *Adam Langley, Google*

[15] https://dev.twitter.com/docs/tweet-button/faq

Los investigadores de Google, por ejemplo, han realizado una amplia investigación sobre la carga computacional relacionada con *Siempre en SSL* y encontrado que no se requiere hardware adicional para implementar en su entorno de Informática. La mayoría de la evidencia sugiere que los avances tecnológicos han reducido al mínimo el impacto del cómputo de SSL / TLS, pero es una buena idea verificar el rendimiento de su servidor Web para saber cuál es la penalización de rendimiento de su entorno.[16]

La latencia de redes presenta problemas de rendimiento

El uso de HTTPS en un sitio entero sí incurre alguna latencia de red, debido en gran parte a las conexiones adicionales necesarias entre el cliente y el servidor para completar el protocolo del handshake SSL / TLS.[17] Esto puede ser un tema particularmente difícil cuando se trata de largas distancias, especialmente para los usuarios internacionales en lugares donde está limitado el ancho de banda de red, o para los sitios donde los usuarios inician un alto volumen de sesiones SSL / TLS relativamente cortas. La latencia no es un problema trivial de resolver. Sin embargo, la penalización de rendimiento se pueden manejar con una planificación adecuada, y las sociedades de servicios financieros ya han demostrado que pueden proporcionar experiencias de navegación de baja latencia al mismo tiempo que implementan un cifrado de alta seguridad por defecto.[18] Además, investigadores de Google están experimentando con nuevas tecnologías tales como "False Start", que ha comprobado reducir la latencia asociada con un handshake SSL / TLS un 30 por ciento.[19]

Un desarrollo de Web seguro hace más fácil la transición

Prácticas de desarrollo seguro, si se siguen desde un principio, pueden dar lugar a sitios web seguros y aplicaciones Web que cuesten aproximadamente lo mismo para desarrollar pero que son mucho más económicos a la larga.[20] El tener que ubicar y reescribir el código puede ser un proceso largo y costoso, especialmente para grandes organizaciones con muchos productos. Todos los sitios construidos hoy en día deben usar HTTPS por defecto y siempre redirigir las conexiones HTTP a HTTPS de inmediato, especialmente en caso de los formularios Web. Hay muchos otros aspectos que hay que tener en cuenta, recursos tales como MozillaWiki y grupos como Open Web Application Security Project (OWASP) proporcionan directrices generales que puede ser seguidas para construir aplicaciones y servicios Web seguros.[21]

El contenido mixto crea una complejidad

El contenido mixto es un tema complicado que surge de la naturaleza hipervínculada del Internet. La mayoría de los sitios web muestran contenido de múltiples fuentes, a menudo por parte de terceros. Si una sola parte de este contenido está vinculada a con un enlace HTTP, podría poner en peligro la seguridad de un sitio que de otra manera estaría seguro, permitiendo que un atacante activo explote la carga de una hoja de estilo en cascada o el código JavaScript.[22] Del mismo modo, cuando una página HTTPS carga una imagen, iframe o fuente a través de HTTP, un atacante intermedio puede interceptar el recurso HTTP. Además, los sitios como Facebook están

[16] http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html

[17] http://www.semicomplete.com/blog/geekery/ssl-latency.html

[18] http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf

[19] http://googleonlinesecurity.blogspot.com/2010/05/extending-ssl-to-google-search.html

[20] https://www.owasp.org/index.php/OWASP_Guide_Project

[21] https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines

[22] https://www.eff.org/https-everywhere/deploying-https

comenzando a exigir el uso de SSL / TLS para evitar contenido mixto, y bloquearán las aplicaciones y contenidos que no utilizan HTTPS.[23] Para evitar estos problemas, los sitios web deben evitar acceder a los archivos a través de HTTP en su código. Esto incluye, pero no se limita, a los siguientes elementos:

- Archivos y enlaces de imagen en la etiqueta <img>
- Archivos CSS (.css)
- Archivos JavaScript (js.)
- Contenido embebido de medios y iframe (Flash, etc)
- URLs en sus etiquetas <html> o DOCTYPE
- Las llamadas a API y SDK externos (por ejemplo, el SDK de Facebook)

Los enlaces relativos son una forma de evitar el tema de la mezcla de contenidos seguros y no seguros, ya que no especifican HTTP o HTTPS. Sin embargo, los vínculos relativos pueden ser aprovechados para enviar spam a buscadores o para ataques "302", por lo que se debe tener en cuenta sus necesidades al momento de decidir cómo y dónde utilizar enlaces relativos.[24]

Implementación de *Siempre en SSL* para su página web

Las empresas que toman en serio la protección de sus clientes y su reputación empresarial a largo plazo pondrán en marcha *Siempre en SSL*. OTA ha esbozado las medidas que se pueden tomar para poner en práctica *Siempre en SSL* y proteger a sus usuarios. El nivel de protección y la garantía que se pueden brindar dependen de las características de seguridad que se pongan en práctica, las cuales se resumen en la Tabla 1.

Tabla 1. Resumen de siempre de Medidas de Seguridad SSL

Función de seguridad	Buen	Mejor	El Mejor
HTTPS persistente	✓	✓	✓
Las cookies conjunto con la bandera de seguro	✓	✓	✓
HTTPS persistentes con Extended Validation		✓	✓
Seguridad en el Transporte HTTP estricta (HSTS)			✓

Hacer cumplir HTTPS persistentes en todas las páginas Web

En primer lugar, *Siempre en SSL* se trata de hacer lo más fácil posible para los visitantes a utilizar siempre HTTPS cuando están en su sitio web, independientemente de la página en que están. El protocolo HTTPS es el protocolo basado en el mismo texto como HTTP, excepto que se ejecuta sobre una conexión cifrada con SSL / TLS sesión. Éstos son algunos de los pasos que debe seguir para hacer cumplir HTTPS:

- Instale un certificado SSL / TLS de una autoridad de certificados de terceros
- Cambie de puerto 80 al puerto 443 para todas las conexiones al servidor Web
- Especificar el nivel de cifrado (por ejemplo, de 128-bit).

[23] http://googleonlinesecurity.blogspot.com/2011/06/trying-to-end-mixed-scripting.html

[24] http://www.dummies.com/how-to/content/prevent-someone-from-hijacking-your-web-sites-sear.html

Inicialmente, usted puede optar por activar esta como una característica opcional para los usuarios. Pero en el largo plazo, la práctica recomendada es hacer que HTTPS por defecto, y dar a los usuarios la opción de desactivar si es necesario. Mediante la aplicación de todo el sitio el uso de HTTPS, puede proporcionar el nivel mínimo de seguridad necesario para hacer de la seguridad significativo o garantías de la intimidad de sus usuarios.

Garantizar la correcta aplicación de los certificados SSL

Para habilitar HTTPS, debe utilizar un válido de SSL / TLS certificado de una entidad emisora de certificados de terceros (CA). Mientras que un certificado autofirmado cifrar las comunicaciones entre el usuario y el sitio web, sólo un certificado emitido por una CA le dice a sus clientes de que la identidad del dominio ha sido verificado por una fuente confiable. Si la conexión utiliza un certificado autofirmado, el navegador web puede identificarla como un riesgo potencial y mostrar un mensaje de error advirtiendo al usuario que el sitio puede no ser seguro para visitar. Selección de la entidad de certificación de la derecha es muy importante.

Asegúrese de que el CA se trabaja con las prácticas mantiene estrictas medidas de seguridad y cuenta con una infraestructura robusta, con buena atención al cliente. Otras consideraciones incluyen la autenticación de la CA y las prácticas de emisión de certificados, la fiabilidad y la velocidad de sus sistemas de validación de certificados, un informe de auditoría anual de un conocido, empresa de auditoría independiente, y una garantía de que la entidad emisora a la altura de sus declaraciones y compromisos.

Además, asegúrese de que su certificado SSL incluye todos los certificados intermedios en la cadena de confianza. Problemas con el certificado puede causar muchos navegadores web para bloquear a los usuarios acceder a su sitio, o para mostrar un mensaje de advertencia de seguridad cuando se accede a su sitio. Sitios como Facebook que hacen cumplir la validación estricta también puede bloquear el contenido de sus usuarios si su cadena de certificados tiene problemas. Hay varias herramientas de terceros de análisis SSL disponibles que puede utilizar para comprobar su SSL / TLS puesta en práctica y corregir los errores o advertencias.

Establecer la bandera de seguro para todas las cookies de sesión

Una cookie de sesión se puede configurar opcionalmente con un "seguro" del pabellón, que indica al navegador que ponerse en contacto con el servidor de origen a través de HTTPS sólo cada vez que envía esta cookie. El atributo de seguro debe ser considerado consejo de seguridad desde el servidor a la aplicación del usuario, lo que indica que es del interés de la sesión para proteger el contenido de las cookies. Esta medida ayuda a evitar que las cookies sean enviadas a través de HTTP, incluso si el usuario accidentalmente hace (o es obligado a hacer) una solicitud del explorador al servidor Web a través de HTTP.

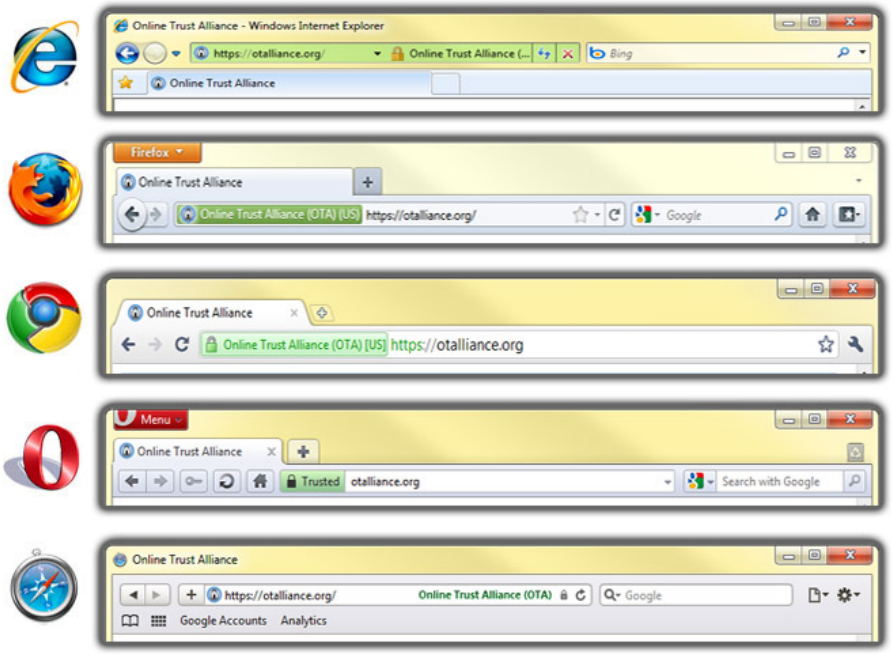
Mejorar la seguridad y la confianza con los certificados de Validación Extendida

Para una mayor protección frente a ataques como sslstrip, la OTA recomienda que considere la implementación de sitios web con Extended Validation (EV) de certificados SSL. Sitios EV garantizados someterse a un riguroso proceso de verificación establecido por el CA Browser Forum, una colaboración de más de 30 autoridades de certificación líderes y proveedores de navegadores de software.

Este proceso de verificación confirma la identidad y la existencia de operadores de sitios web que utilizan fuentes confiables de terceros. Los usuarios que visitan un sitio Web asegurado con los

certificados EV SLL podrá ver una barra verde y el nombre de la organización en la barra de direcciones, proporcionando seguridad visual de la identidad del operador del sitio web.

Figura 3. Navegadores Web que muestran el uso de certificados SSL con EV



La OTA recomienda que las organizaciones responsables de implementar un certificado EV en cualquier sitio que requiere una conexión segura. Los departamentos de TI deben ayudar a los usuarios finales de gestión y en la comprensión de que los certificados EV será proteger la seguridad de los usuarios y reducir la vulnerabilidad de la organización de los ataques. Todos los usuarios deben actualizar a los navegadores que soportan certificados EV y todos los sitios web para realizar transacciones en línea deberían evaluar los certificados EV como parte de su estrategia de seguridad y protección de la marca.

Implementación de HSTS para prevenir ataques activos

Las conexiones HTTPS a menudo se inician cuando los visitantes son redirigidos de una página HTTP o al hacer clic en un enlace (tal como un botón de inicio de sesión) que los dirige a un sitio HTTPS. Sin embargo, es posible poner en marcha un ataque por parte de un intermedio durante esta transición de una conexión no segura a una conexión segura, ya sea de forma pasiva o engañando a la víctima a hacer clic en un enlace HTTP a un sitio web legítimo (a través de un correo electrónico de phishing, por ejemplo).

La mejor defensa contra este tipo de ataques es la implementación de la Seguridad de Transporte HTTP estricta (HSTS) para su sitio web. Esta especificación permite que un sitio web se declare accesible sólo a través de conexiones seguras, y / o que los usuarios interactúen con los ciertos sitios solamente a través de conexiones seguras. HSTS es compatible con Google Chrome y Mozilla Firefox, y los sitios como PayPal.com que utilizan HSTS indican expresamente a los navegadores que sólo aceptarán las comunicaciones cifradas.[25] El uso de HSTS ayuda a evitar

[25] http://hacks.mozilla.org/2010/08/firefox-4-http-strict-transport-security-force-https/

que los atacantes roben las cookies de sesión cuando los usuarios son redirigidos de HTTP a HTTPS, y actualmente es la defensa más fuerte contra el phishing y los ataques de intermedios.

Conclusión

En el pasado, muchos expertos han aconsejado a los diseñadores y los operadores web a usar SSL / TLS para proteger la autenticación de sus usuarios, las transacciones financieras y otras actividades importantes, pero muchas organizaciones se han mostrado inseguros a cifrar sus sitios enteros debido a las preocupaciones sobre el costo, el rendimiento y otras cuestiones . Sin embargo, el Internet ha llegado a un punto de inflexión donde es evidente que el uso selectivo de HTTPS ya no es suficiente para proteger a los usuarios móviles de hoy, quienes siempre están en línea. SSL / TLS en sí sigue siendo fundamentalmente sólida, pero Firesheep fue un llamado de atención para los operadores de sitios web para proteger la experiencia entera del usuario, no sólo la página de inicio de sesión o el formulario de compras. En resumen, SSL es como un cinturón de seguridad en un automóvil: Siempre debe utilizarse en el tránsito.

Siempre en SSL no es una "bala de plata" para detener a los ladrones en línea, y debe implementarse como parte de una estrategia de seguridad global para proteger a los usuarios cuando interactúan con su sitio web. Sin embargo, es un enfoque comprobado para detener el sidejacking y otros ataques de intermedios, y ya no es computacionalmente costoso para la gran mayoría de las organizaciones. Tal como Facebook, Google, PayPal, Twitter y otros han demostrado, es posible que incluso los sitios web más grandes y complejos ofrezcan una rica experiencia al usuario a través de HTTPS. Cuestiones tales como la latencia y el contenido mixto pueden presentar dificultades, pero las directrices y las mejores prácticas descritas en este documento ayudarán a manejar estos problemas y optimizar el rendimiento para los usuarios.

Más importante aún, *Siempre en SSL* puede ayudar a proteger la confianza que tienen los usuarios en su sitio web. La protección de la confianza y la confianza de los consumidores es un problema muy difícil que no se puede resolver a través de medios puramente técnicos. A cierto nivel, los usuarios simplemente tienen que confiar en el sistema, y como Ken Thompson, uno de los autores principales de UNIX, escribió una vez: "quizás es más importante confiar en las personas que crearon el software."[26] Tomando un enfoque de *Siempre en SSL* se puede ayudar a dar a los usuarios la seguridad de saber que usted toma su seguridad y privacidad en serio, y que usted está tomando las medidas necesarias para protegerlos.

Acerca de la Alianza de Confianza en Línea (OTA, por sus siglos en inglés)

La OTA es una organización independiente sin fines de lucro con la misión de desarrollar y promover las mejores prácticas y políticas públicas que mitiguen las amenazas emergentes a la privacidad, identidad y seguridad a los servicios en línea, las organizaciones y los consumidores, aumentando así la confianza en línea. Al facilitar un diálogo abierto con las agencias de la industria, negocios y gobierno para trabajar en colaboración, la OTA está haciendo progresos para hacer frente a diversas formas de abusos, amenazas y prácticas en línea que amenazan con socavar la confianza en línea y aumentar la demanda de regulaciones.

https://www.otalliance.org/

[26] http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

Traducción de inglés a español por DigiCert.