VÍDEO intypedia010es

LECCIÓN 10: ATAQUES AL PROTOCOLO SSL

AUTORES: D. Luciano Bello y Dr. Alfonso Muñoz

R&D Security Researcher (Chalmers University)
R&D Security Researcher. T>SIC Group – UPM

ALICIA

Hola, bienvenidos a Intypedia. En lecciones pasadas aprendimos los fundamentos del funcionamiento del protocolo SSL. Hoy vamos a profundizar en este protocolo, y vamos a ver algunos ataques reales sobre el mismo y cómo mitigarlos. ¡Acompáñanos!

ESCENA 1. ¿ES SEGURO SSL?

ALICIA

Hola Bernardo. En lecciones anteriores aprendimos los fundamentos de la criptografía. También aprendimos cómo se implementa esta criptografía en algoritmos y protocolos reales ampliamente extendidos, entre los que estaba el protocolo SSL que estudiamos en la lección anterior. Sin embargo, de vez en cuando se publican noticias de ataques a este tipo de protocolos y como SSL es un protocolo muy utilizado en Internet, su estudio tiene un interés especial.

BERNARDO

Alicia no te fíes mucho de lo que publica la gente, a mí me parece que SSL es muy seguro y confiable.

ALICIA

Estoy de acuerdo contigo, SSL es inherentemente seguro pues los protocolos que se utilizan tienen un cuerpo teórico fuerte y maduro. Pero incluso así hay aún muchas cosas que pueden salir mal. Por un lado, está la complejidad que, como sabemos, atenta contra la usabilidad. Además, las implementaciones pueden tener fallos en la forma en que han sido programadas. Por último, puede pasar que se desarrollen nuevas técnicas de criptoanálisis, haciendo que

algunos protocolos no sean tan seguros como se esperaba. Esto, sumado al hecho de que la capacidad de computación de los atacantes va en aumento conforme a la ley de Moore, hace que los protocolos necesiten ser revisados y que las antiguas versiones de SSL sean inseguras.

BERNARDO

Espera… ¿entonces me dices que SSL no es tan seguro?

ALICIA

Calma Bernardo, SSL es seguro en su diseño teórico. Pero esto es una condición necesaria aunque no suficiente. Hoy día el uso de este protocolo es vital en el comercio electrónico entre clientes (usuarios) y proveedores de productos. Es común su uso en transacciones cuando compramos un libro por Internet o la banca online. Aunque SSL tiene otros usos como vimos en la lección anterior, es posible que sea más famoso por su uso en la Web. Su uso adecuado permitirá minimizar ataques, algunos clásicos como ataques de hombre en el medio contra la información intercambiada, así como minimizará ataques de suplantación en el acceso a nuestras redes sociales favoritas.

No obstante, la "seguridad real" del protocolo SSL tiene que ser matizada. Por ejemplo, en su uso en la web va mucho más allá de la idea equivocada de que una página es segura si y solo si se muestra el famoso "candado amarillo".

Si te parece bien, vamos a analizar diferentes ataques a este protocolo en los últimos años para hacernos una idea de lo que estamos hablando, finalizando con unas recomendaciones de uso.

BERNARDO

Me parece una idea excelente. Adelante Alicia.

ESCENA 2. FALLOS DE PROGRAMACIÓN EN LAS IMPLEMENTACIONES. CRIPTOANALISIS Y DOWNGRADE

ALICIA

Los fallos de programación juegan malas pasadas muchas veces. Uno de los ejemplos más famosos de ataque a SSL fue la vulnerabilidad anunciada en Mayo de 2008. El investigador argentino Luciano Bello descubrió que se habían implementado incorrectamente funciones aleatorias que se utilizaban en OpenSSL/Debian. Esto producía material "aleatorio" predecible que facilitaba invertir los procesos criptográficos, y como consecuencia de ello certificados X.509, claves SSH e incluso material cifrado se vieron expuestos.

BERNARDO

Sí… recuerdo algo. Una de las implicaciones fue que se podían reconstruir las claves privadas a través de las claves públicas distribuidas. Sin funciones criptográficas aleatorias los criptosistemas quedaron indefensos.

ALICIA

En efecto, fue un problema puntual finalmente solucionado. No obstante, a los problemas de implementación debe sumarse la capacidad de cómputo cada vez mayor de los atacantes y los avances en criptoanálisis. Estas consideraciones podrían simplificar la creación de certificados digitales falsos creados a la medida.

Un ejemplo de esto puede verse en los resultados publicados en la 25 edición de la Chaos Communication Congress celebrada en Berlín en diciembre de 2008, en la cual investigadores crearon un certificado SSL "válido" aprovechándose de las peculiaridades de emisión de ciertas autoridades de certificación, de un ataque de colisión al algoritmo criptográfico MD5 y de una importante capacidad de cálculo basada en una centena de consolas PlayStation. Es verdad que MD5 ya no se usa en las Autoridades de Certificación para calcular el hash del certificado que va firmado con su clave privada, pero el estándar actual SHA-1 también está comenzando a tener unos problemas similares a los de su homólogo.

Este es un buen ejemplo para justificar por qué la seguridad de los algoritmos criptográficos utilizados en SSL son revisados y actualizados por la comunidad científica. En la medida de lo posible, se debe evitar utilizar versiones del protocolo antiguas o que un atacante fuerce su uso, lo que se conoce como downgrade (downgrade protocol).

BERNARDO

¿Se conoce algún otro tipo de ataque?

ALICIA

Sí, otro ataque curioso fue el descubierto por el investigador Moxie Marlinspike. Al crear un certificado SSL y enviarlo a una Autoridad Certificadora para que lo firme, el campo al que se le suele prestar más atención es el CN (common name) que especifica el nombre del servidor, como puede ser www.ejemplo.org. Moxie Marlinspike descubrió que los estándares de certificado X.509 y SSL definen la cadena CN como una cadena PASCAL (se declara la longitud de la cadena en la posición 0 y se pone la cadena en el resto de posiciones). Curiosamente la mayoría de software de procesamiento de certificados está escrito en C. Dicho software suele manejar la cadena como una cadena C, poniendo un NULL (\0) al final de la cadena para indicar dónde termina. El problema llega cuando alguien obtiene un certificado de la forma www.bancolegitimo.com\0www.atacante.org. Cuando se procesa por un navegador, sólo se leerá la primera parte, www.bancolegitimo.com, permitiendo falsificar fácilmente al banco. La solución más fácil a este problema es que las entidades certificadoras rechacen todos los certificados que contuvieran el carácter NULL.

Cuando se detectan certificados fraudulentos, suelen revocarse gracias al número de serie que incluyen y para esto suele utilizarse el protocolo OCSP (Online Certificate Status Protocol). De nuevo una configuración incorrecta en el mismo facilitaría ataques al protocolo SSL.

BERNARDO

Perdona Alicia, creo que sería bueno definir cómo atacar al protocolo OCSP.

ALICIA

Es verdad. El protocolo OCSP es un protocolo de consulta online para saber si un determinado certificado digital ha sido revocado o no. Para ello, el cliente envía la petición a la dirección de la CRL (Certificate Revocation List), que viene indicada en el propio certificado digital. Si un atacante está haciendo un ataque de hombre en el medio para utilizar uno de estos certificados digitales, entonces también puede interceptar las peticiones OCSP y utilizarlas en su provecho. En un funcionamiento normal, un servidor mediante este protocolo podría enviar una respuesta *Try Later* indicando al cliente que ahora no puede atender una petición. El atacante podría simular esta contestación, que tiene asignado el código 3, para indicar al cliente que ahora no puede atender su petición. Ante esta situación muchos clientes Web aceptarán el certificado digital al no poder corroborar su validez, lo que claramente es un fallo.

BERNARDO

Alicia, ¿entonces me quieres decir que es fácil engañar a un sistema cuando el usuario accede por https?

ALICIA

No sólo eso. Si bien muchos problemas pueden mitigarse teniendo nuestros programas al día, hay un elemento del sistema que es muy difícil de actualizar: el usuario.

ESCENA 3. ENGAÑANDO AL USUARIO. VULNERANDO SSL EN LA WEB

ALICIA

En la práctica la manera más fácil de vulnerar la seguridad proporcionada por el protocolo SSL/TLS consiste en engañar al usuario haciéndole pensar que lo está utilizando cuando en realidad no es así.

BERNARDO

Yo diría que eso no es posible Alicia. Cuando me conecto a mi banco de forma segura, veo el candado amarillo en mi navegador, lo cual me indica que el acceso a la página es seguro y por tanto se habrá validado correctamente el certificado digital que autentica al banco.

ALICIA

Por desgracia Bernardo, esa fue una mala manera de educar a personal no técnico sobre cómo validar si se estaba utilizando o no el protocolo SSL. En la realidad, es importante considerar muchas otras condiciones que te comento a continuación.

BERNARDO

Espera un momento. Ya sé que si mi máquina ha sido comprometida, por ejemplo mediante un troyano, se puede engañar y mostrar un candado amarillo en el navegador Web mostrando que está cifrado SSL cuando en realidad no es así.

ALICIA

Bueno Bernardo, si realmente tienes un troyano en tu máquina, éste tendrá el control total y será capaz no sólo de engañarte, sino de capturar tus contraseñas, redirigir tu tráfico de datos o de autenticación, etc. Pero posiblemente los ataques más interesantes son aquellos que no tienen acceso interno a tu máquina, clásicamente ataques de hombre en el medio cuyo principal objetivo es interceptar una comunicación entre un cliente y un servidor y ver o alterar la información en tránsito.

BERNARDO

Y si yo me conecto a una página mediante https, ¿eso es posible?

ALICIA

Pues depende de la complejidad del ataque. Algunos se podrán solucionar con un mínimo de formación por parte del usuario, otros, mucho más sofisticados, serán difícilmente detectables.

El ejemplo de ataque de hombre en el medio más simple consiste en crear un certificado digital falso. Es decir, cuando un usuario se conecta vía https a su banco online, un atacante se conecta en medio de los dos y envía su certificado al cliente haciéndose pasar por el banco. El navegador Web detecta que el certificado digital no es el reconocido e indica visualmente al usuario si desea aceptar la conexión. La mayoría de los usuarios sin formación en seguridad lo aceptarán, pulsando SÍ, con lo que el atacante estará en medio y podrá realizar lo que desee con los datos en tránsito, así como con las claves capturadas. Una vez se acepte el certificado, el protocolo SSL hará su funcionamiento normal y el usuario observará el candado amarillo correspondiente. Por el contrario, si un usuario con un mínimo de conocimientos pulsara NO, el ataque no tendría lugar.

BERNARDO

Vaya, no había caído en eso. ¿Hay otros ataques similares a SSL?

ALICIA

Otro ataque más peculiar consiste en el uso de la herramienta SSLstrip. Moxie Marlinspike en 2009 presentó en la conferencia de seguridad informática BlackHat una herramienta que automatiza un ataque de hombre en el medio al protocolo SSL. La idea es sencilla, cuando se llama a una página Web, se sustituyen todos los enlaces https por http, con la intención que la comunicación entre el cliente y el atacante sea por http y la comunicación entre atacante y servidor por https. Para engañar más al usuario, se aprovecha de ciertos trucos, como por ejemplo simular el “candado amarillo” cargando esta imagen en el favicon.

Otros ataques más sofisticados tienen que ver con el robo de certificados o la suplantación de Autoridades de Certificación como vimos anteriormente.

Está claro que en un caso hipotético se podrían generar certificados válidos de entidades comerciales concretas para fuerzas gubernamentales, por ejemplo por orden judicial, que permitiría hacer un hombre en el medio, difícilmente detectable, en tanto en cuanto el

certificado sería válido y firmado por una autoridad competente. Esto se podría realizar, por ejemplo, para un certificado digital con un número de serie concreto.

BERNARDO

Ya veo que los atacantes son muy astutos.

ALICIA

Espera, que hay más. En otros casos el robo de certificados firmados por una autoridad de confianza puede suponer muchos problemas. Un ejemplo famoso en Marzo de 2011 fue la línea de negocio de certificados SSL de la empresa de seguridad Comodo.

Uno de sus partners (que vendía certificados SSL) fue comprometido de forma que lanzó peticiones de firmado de certificados SSL sin la correspondiente verificación. Esto produjo la emisión de varios certificados digitales SSL falsos, es decir, certificados válidos para determinados sitios como mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com, etc. Estos certificados eran completamente válidos para cualquier navegador Web.

El impacto de este ataque implica que, cualquier persona u organismo con capacidad de implementar un ataque de hombre en el medio sería capaz de "transmitir" una web https falsa de Yahoo, Google y otros sin que el navegador protestase. Por suerte, estos certificados han podido revocarse por su número de serie; no obstante, este hecho destaca la problemática actual de Internet de obtener certificados digitales sin la adecuada validación por parte de los suministradores.

Como puedes ver Bernardo, en la práctica se intenta vulnerar la seguridad del protocolo SSL de forma directa o indirecta, atacando al protocolo, al software o a los usuarios que finalmente lo utilizan.

ESCENA 4. USO SEGURO DE SSL. RECOMENDACIONES

BERNARDO

Es muy interesante Alicia lo que me comentas… ¿Entonces qué puedo hacer para utilizar el protocolo SSL de manera más segura?

ALICIA

Las recomendaciones básicas consistirían en utilizar la versión más moderna del protocolo SSL debidamente configurado e intentar que las implementaciones de dicho protocolo estén corregidas de fallos conocidos. Esto no siempre es posible y depende de la necesidad de mantener la compatibilidad entre sistemas. En el caso de su uso en la Web, te daré cinco consejos para mitigar problemas conocidos:

1. Mantener el navegador web actualizado para que la implementación del protocolo SSL está libre de vulnerabilidades conocidas.

2. Añadir en la url (cuando sea posible) la dirección directa https de la página a la que nos deseamos conectar. El add-on para firefox “HTTPS Everywhere” puede ayudar a automatizar esto.

3. Denegar acceso a una página Web cuando el certificado no sea válido. Esto es especialmente crítico para el acceso a cuentas bancarias, datos personales, etc. En otro caso, el usuario baremará la relación riesgo-acceso a esa web.

4. Configurar los navegadores web para que hagan comprobaciones OCSP por defecto y que si la conexión OCSP falla, el certificado por defecto no sea dado por bueno. Esto evitará ataques basados en negación de servicio al OCSP y uso de certificados revocados.

5. Ciertos complementos software podrían ayudar a detectar plagios. Por ejemplo, en firefox el add-on “Certificate Patrol” monitoriza cambios en servidores https de forma que si un día el certificado de SSL de Gmail es diferente al registrado, notifica ese cambio.

BERNARDO

Bueno Alicia, me ha quedado bastante más claro el asunto de la seguridad en SSL, creo que con esto es suficiente. En la web de intypedia hay información adicional sobre este interesante tema. ¡Hasta pronto!

ALICIA

¡Adiós!

Guión adaptado al formato intypedia a partir del documento entregado por el D. Luciano Bello (Chalmers University) y Alfonso Muñoz (Universidad Politécnica de Madrid).

Madrid, España, Septiembre de 2011

http://www.intypedia.com

http://twitter.com/intypedia