ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

50/2014 1 octubre 2014

David Ramírez Morán

VULNERABILIDADES EN LAS HERRAMIENTAS DE CIFRADO DE INTERNET

VULNERABILIDADES EN LAS HERRAMIENTAS DE CIFRADO DE INTERNET

Resumen:

Durante 2014 se está produciendo una avalancha de noticias sobre vulnerabilidades de las soluciones tecnológicas que dan soporte a la transmisión de información cifrada a través de internet. Estas herramientas son imprescindibles para la utilización segura de los servicios y aplicaciones online, pues proporcionan la confidencialidad que permite la transferencia de información sensible de forma segura. El elevado número de vulnerabilidades detectadas constituye un indicador del interés existente en distintos ámbitos por acceder a la información cifrada que circula por la red.

Abstract:

During 2014 a bunch of news about vulnerabilities in the technology solutions that support transmission of encrypted data on internet have emerged. These tools are essential for the safe use of online services and applications since they provide the confidentiality that allows for the transmission of sensitive information in a safe way. The high number of detected vulnerabilities poses an indicator of the existing interest in various domains to gain access to the encrypted information flowing through the net.

Palabras clave:

Internet, cifrado, vulnerabilidad, heartbleed.

Keywords:

Internet, encryption, vulnerability, heartbleed.

INTRODUCCIÓN

La seguridad de la información en internet es una cuestión primordial para la prestación segura de servicios online tal y como se conocen hoy en día. A medida que aumentan la cantidad y el tipo de servicios prestados cada vez es más necesaria la transferencia de información cifrada, que debe ser protegida para asegurar la confidencialidad y la seguridad de las transacciones.

La puesta en funcionamiento de internet no consideró esta necesidad de implantar medidas de seguridad en un primer momento, dado el entorno controlado en el que sería desplegada. A mediados de los años 90 se implantó la tecnología que permitía esta comunicación segura, que desde principios de 2014 se ha visto seriamente amenazada por varias vulnerabilidades que se han publicado sobre los paquetes de software que implementan o utilizan esta funcionalidad.

Tras una breve descripción de las tecnologías que dan soporte al cifrado de la información en internet, para establecer el contexto necesario para comprender las técnicas que permiten explotar las vulnerabilidades que se han publicado a lo largo de 2014, se analiza el escenario y las tendencias que se están produciendo tanto en la detección como en la publicación de las vulnerabilidades.

CIFRADO DE INFORMACIÓN EN INTERNET

Tal y como fue creada internet en los años 70 y con la implantación de la tecnología web como medio para la compartición de la información en los años 90, utilizando el protocolo Hyper Text Transfer Protocol (HTTP), la información viaja a través de las líneas de comunicación totalmente en claro, de forma que cualquier persona puede acceder a esta información en su tránsito por la red. El problema no se limita a la posibilidad de que un tercero pueda acceder a la información que circula por la red sino que también puede modificarla en su tránsito e incluso puede suplantar el servidor al que se está conectando el cliente y proporcionar información incorrecta o recopilar la información que proporcione el usuario, como nombres de usuario o contraseñas.

Para acabar con estos problemas se desarrolló en primer lugar el protocolo Secure Socket Layer[1] (SSL) y, posteriormente, la evolución de este protocolo denominado Transport Layer

[1] The Secure Sockets Layer (SSL) Protocol Version 3.0 http://tools.ietf.org/html/rfc6101 (Consultado 29/09/2014)

Security[2] (TLS). Estos protocolos son los que están detrás, por ejemplo, de las conexiones seguras HTTPS. Ambos protocolos proporcionan los medios necesarios para conseguir proteger la información que circula por la red en términos de autenticidad, integridad y confidencialidad.

La autenticidad es la propiedad por la que los dos usuarios de una comunicación pueden comprobar que en el otro extremo se encuentra la persona u organización que dice ser. De esta forma, al acceder un usuario a la web de un banco, puede estar seguro de que el servidor al que va a enviar su información pertenece realmente a ese banco. También es posible para el banco realizar una comprobación de que el usuario es quien dice ser, aunque no suele utilizarse salvo en entornos profesionales. Una vez que el usuario comprueba que está en comunicación con su banco gracias a la indicación, en forma de candado cerrado o de texto o fondo en verde, que aparece en la barra de direcciones del navegador, procede a introducir sus datos de usuario para acceder de forma segura a su información financiera.

La integridad es la propiedad que permite comprobar en el extremo receptor que la información que se recibe es correcta, enviada por el emisor y que en su tránsito a través de las redes no se ha visto alterada o modificada por terceras personas. Esta propiedad es la que asegura que la información que llega al usuario se corresponde con la que ha enviado el servidor y viceversa, y que, por tanto, es correcta.

Por último, la confidencialidad es la propiedad que permite cifrar la información para que una tercera persona que disponga de los medios para poder interceptar los datos intercambiados entre los extremos no sea capaz de extraer la información que viaja oculta mediante cifrado en los datos transmitidos.

Tanto en SSL como en TLS la propiedad de autenticidad se consigue mediante la utilización de certificados digitales basados en algoritmos criptográficos de firma digital. Un certificado electrónico puede contener la información que identifica a un usuario, a un servidor o a una máquina física conectada a internet. Para poder comprobar que la información es cierta, se dispone de unas autoridades de certificación que auditan esta información y, una vez validada, la firman mediante un algoritmo matemático que permite al usuario comprobar que la información es correcta al validar esta firma. De esta forma, el usuario confía en la autoridad de certificación como verificadora de la información de identificación que figura en el certificado.

[2] The Transport Layer Security (TLS) Protocol Version 1.2 http://tools.ietf.org/html/rfc5246 (Consultado 29/09/2014)

VECTORES DE EXPLOTACIÓN

Dos son las técnicas por las que las vulnerabilidades detectadas permiten acceder a la información que viaja cifrada a través de internet.

La primera es conseguir hacerse con las claves de cifrado. Una vez que se dispone de esta información, extraer los datos es una operación prácticamente directa pues los algoritmos de cifrado de la información son generalmente públicos y cualquier persona (especialmente un hacker) puede implementar o utilizar un software para descifrar la información una vez que dispone de las claves con las que se ha realizado el cifrado.

La otra técnica es la que se conoce como «man in the middle», por la que el atacante consigue interponerse entre el ordenador del usuario y el servidor al que desea acceder. Para ello, el atacante debe conseguir hacer creer al usuario que está contactando con el servidor deseado, cuando en realidad está accediendo a una máquina intermedia que intercepta el tráfico. El ataque se orquesta en dos pasos. En el primero, el atacante consigue redirigir el tráfico del usuario a la máquina intermedia. En el segundo, el atacante consigue hacerse pasar por el servidor verdadero, que es donde las vulnerabilidades detectadas resultan de aplicación.

El primer paso se consigue generalmente mediante una alteración del funcionamiento del servicio DNS, el encargado de convertir direcciones web en direcciones IP numéricas. Otra alternativa bastante más compleja es que los gestores de la infraestructura de internet desvíen de manera controlada el tráfico destinado a un servidor a otra máquina bajo su control de forma inadvertida para el usuario y para el prestador del servicio.

El resultado en ambos casos es que el tráfico entre el ordenador del usuario y el servidor al que desea acceder, en lugar de ir directamente a este último, llega a una máquina intermedia. Esta máquina intermedia, en la que se descifra la información, se encargará de retransmitirla al servidor genuino y de remitir la respuesta del servidor una vez descifrada al usuario.

A la hora de comprobar la autenticidad es donde las vulnerabilidades detectadas resultan de utilidad para el atacante. Desde la máquina interpuesta el atacante remite un certificado manipulado para que el ordenador del usuario interprete que ha conectado con el servidor genuino y, fruto de las vulnerabilidades, el ordenador no es capaz de detectar la manipulación del certificado. A partir de este punto se establece la conexión y toda la información intercambiada de forma supuestamente segura con el servidor cae en poder del atacante.

VULNERABILIDADES DETECTADAS

El 22 de febrero de 2014, se publicaba una vulnerabilidad[3] en el sistema operativo iOS de Apple[4]. Pese a ser un sistema operativo propietario, donde el usuario no tiene acceso al código fuente, se filtró en internet el código fuente en el que figuraba el error. Se producía por un fallo en la programación en el que se repetía la sentencia «goto fail;» en dos líneas consecutivas. Esta sentencia rápidamente pasó a ser utilizada por los expertos para hacer referencia al error. Como consecuencia del fallo no se comprobaba la validez del certificado recibido del servidor, haciendo posible realizar un ataque «man in the middle».

El siguiente software del que se informó que estaba afectado por una vulnerabilidad fue GnuTLS[5], una implementación libre de código abierto de los protocolos SSL/TLS. Al igual que el fallo anterior, un error de programación hacía que se omitieran las validaciones de los certificados recibidos. En junio se detectó una nueva vulnerabilidad[6] de este software que afectaba a las aplicaciones cliente que utilizaban esta librería. La incorrecta validación del certificado enviado por el servidor al ordenador del usuario podía ocasionar la caída de la aplicación o la ejecución de código en el ordenador del usuario.

El 8 de abril se conocía la noticia del que se considera el fallo más grave de los últimos años en el entorno de la seguridad de la información. En este caso el software afectado era OpenSSL[7], una implementación libre de código abierto de los protocolos SSL/TLS, de las más utilizadas en servidores con sistemas operativos Unix, Linux o BSD, en sistemas con sistema operativo Google Chrome OS, además de en numerosas aplicaciones de usuario.

La extrema gravedad de esta vulnerabilidad[8] radicaba en la posibilidad de acceder al contenido almacenado en la memoria del servidor, donde, además de la información transmitida por los usuarios, como nombres de usuario y contraseñas, podía encontrarse también la clave privada del servidor.

La vulnerabilidad se producía en la funcionalidad «heartbeat» (latido del corazón) del protocolo TLS, motivo por el que surgió en internet el término «Heartbleed» (desangramiento) como metáfora de la pérdida de información que se producía debido a la vulnerabilidad.

---

[3] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1266 (Consultado 29/09/2014)
[4] http://www.spiegel.de/fotostrecke/apple-software-probleme-bei-gesicherten-verbindungen-fotostrecke-111478.html (Consultado 29/09/2014)
[5] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0092 (Consultado 29/09/2014)
[6] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3466 (Consultado 29/09/2014)
[7] http://www.openssl.org/ (Consultado 30/09/2014)
[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 (Consultado 30/09/2014)

Un factor que contribuyó a la gravedad de este error es que no requería ningún equipo especial ni otro tipo de vulnerabilidades para su explotación. Sólo era necesario realizar una conexión al servidor utilizando un programa específicamente desarrollado. Esta conexión, a todos los efectos, no se podía distinguir de la de un usuario lícito del sistema porque se encontraba correctamente cifrada. Por tanto, no había posibilidad de filtrarla mediante los equipos de protección tradicionales como firewall e IDS (Intrusion Detection System).

El 13 de mayo era el entorno .NET de Microsoft, con el que se desarrollan aplicaciones para servidores y clientes de servicios online, el que se veía afectado por una vulnerabilidad en la verificación de los certificados[9] con consecuencias similares al fallo «goto fail;» .

El último error relacionado con los protocolos SSL/TLS se ha detectado en el código de la librería NSS[10] para establecer conexiones cifradas que utilizan los navegadores Mozilla Firefox y Google Chrome en todos los sistemas operativos, y el sistema operativo Google Chrome OS. Debido a la vulnerabilidad, un certificado falsificado se podía validar como correcto, permitiendo, al igual que en el fallo «goto fail;», ataques «man in the middle» o de suplantación del servidor sujetos a las mismas limitaciones.

ANÁLISIS

Los ataques contra las herramientas de cifrado de las comunicaciones de internet están afrontando el problema a través de vías indirectas en lugar de atacar directamente el algoritmo de cifrado. Esto se puede interpretar como una prueba de que estos algoritmos presentan un elevado grado de seguridad y que actualmente suponen una herramienta efectiva para proteger la información que circula por la red. Sin embargo, no debe descartarse que, con la siempre creciente potencia computacional de acuerdo a la Ley de Moore por la que cada 2 años se duplica la potencia de los microprocesadores, estos algoritmos pueden dejar de ser seguros en algún momento con los parámetros con los que se utilizan actualmente. Es por este motivo por el que los atacantes están recurriendo a técnicas alternativas con las que conseguir las claves utilizadas en la comunicación explotando las vulnerabilidades que presentan los protocolos de comunicaciones y las aplicaciones que los utilizan.

Existe un interés claro en conseguir descifrar la información que circula por internet. Prueba de ello es que la práctica totalidad de los sistemas informáticos utilizados de forma general

[9] http://support2.microsoft.com/kb/2960358 (Consultado 30/09/2014)
[10] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1568 (Consultado 30/09/2014)

para acceder a internet se han visto afectados, tanto los sistemas propietarios como los de código abierto.

En el caso de Heartbleed, por afectar a una plataforma de código abierto ampliamente utilizada, se ha propagado rápidamente por internet la información sobre las iniciativas que se han tomado para corregir el error. Su gravedad puede haber sido el motivo por el que se haya potenciado la revisión del código de otras herramientas de cifrado y de ahí que se hayan descubierto tantas vulnerabilidades de herramientas relacionadas en tan poco tiempo.

Heartbleed es una vulnerabilidad muy importante por haber permitido a los atacantes hacerse con las claves de cifrado utilizadas por los servidores. En el caso de que los atacantes hubieran conseguido almacenar el tráfico cifrado durante un periodo de tiempo, ahora tendrían capacidad de descifrar toda esta información tan solo con aplicar las claves obtenidas. Esto ha dado lugar a un creciente interés por las técnicas Perfect Forward Secrecy (PFS)[11] por las que un escenario como el que se ha producido no tendría tan graves implicaciones. En estas técnicas se utilizan claves de cifrado distintas para cada comunicación por lo que, aunque se accediera a la clave secreta de cifrado como ha ocurrido con Heartbleed, no sería posible descifrar comunicaciones basadas en esa clave que se hubieran llevado a cabo en el pasado.

Resulta relevante el fenómeno que se está produciendo con las vulnerabilidades de los sistemas por el que se les asigna un nombre con el que darles publicidad. El motivo, según el CEO de la empresa de seguridad que publicó la vulnerabilidad Heartbleed[12], es darle mayor visibilidad para que se arreglase el problema más rápidamente. Esta misma empresa se encargó de crear una página web, www.heartbleed.com, para la difusión de toda la información relacionada con la vulnerabilidad.

Desde Heartbleed se ha producido otra vulnerabilidad de gravedad que también ha recibido una denominación de alto impacto: Shellshock. Esta denominación, sin embargo, se corresponde con varias marcas comerciales y no existe una página web específica.

Estas medidas constituyen una plataforma para que los descubridores de las vulnerabilidades puedan reivindicar su autoría, aunque también se puede interpretar como una señal de la creciente concienciación existente para que las vulnerabilidades sean corregidas cuanto antes, porque un equipo vulnerable puede suponer una herramienta útil para un atacante.

[11] https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy (Consultado 30/09/2014)
[12] http://www.theguardian.com/technology/2014/apr/24/heartbleed-why-did-a-computer-bug-have-a-name

CONCLUSIONES

Todo sistema informático es susceptible de presentar vulnerabilidades y las herramientas de cifrado de la información tampoco están exentas. Independientemente de su naturaleza comercial o libre y de si se trata de código abierto o no, estas vulnerabilidades no sólo se están detectando sino que están siendo explotadas para conseguir acceso a información confidencial.

Las vulnerabilidades de las herramientas de cifrado son especialmente sensibles porque afectan a lo más preciado en los sistemas: la información. Además, su explotación puede proporcionar considerables beneficios económicos por el robo de información financiera, confidencial, comercial o de propiedad intelectual, lo que resulta de gran interés para los delincuentes.

La aparición de múltiples vulnerabilidades tan seguidas constituye un indicador de la sensibilización que los desarrolladores tienen respecto a la seguridad de la información. Sin embargo, queda patente una falta de recursos dedicados a la revisión exhaustiva de los sistemas y aplicaciones de forma preventiva.

Existe un creciente interés en que las vulnerabilidades que presentan los sistemas se difundan con rapidez por toda la red para que las personas implicadas puedan aplicar las soluciones a la mayor brevedad. A este interés está contribuyendo la búsqueda de notoriedad que los expertos están demostrando como venía siendo habitual en los foros hacking, con la importante diferencia de que estas vulnerabilidades están llegando a la prensa general.

Por último, es necesario recordar que la explotación de este tipo de vulnerabilidades en España, aunque sólo sea con fines de análisis o investigación, puede ser constitutivo de delito. Las personas interesadas en analizar el problema deben mantener las precauciones necesarias para hacerlo en un entorno controlado de su propiedad o que se haya obtenido autorización de los propietarios legítimos de los sistemas bajo análisis.

David Ramírez Morán
Analista del IEEE