Jonder Hernández Gutiérrez

1. Administración de claves públicas

La criptografía de llave pública permite que dos personas se comuniquen de forma segura aun sin compartir una clave común. Por último, gracias a los resúmenes de mensajes firmados, el receptor puede verificar de una manera fácil y segura la integridad de los mensajes recibidos.

Aunque dejamos de lado un problema muy importante, el cual es como obtiene cada uno la llave pública del otro. Una posible solución es que obtenga la llave desde la web del otro, pero esto no funciona, ya que un tercero podría interceptar esta solicitud y cambiarla por una llave de él o incluso hacer phishing, es evidente que se necesita un mecanismo para asegurar que las claves públicas se puedan intercambiar de manera segura.

Certificados

Un acercamiento para solucionar el problema de intercambio de llave pública puede ser que un centro de distribución de claves este siempre disponible y proporcione claves públicas bajo demanda, sin embargo, esto no es realista, ya que si alguna vez fallara la seguridad seria penetrada.

Por estas razones se desarrolló una solución diferente, una que no requiere que el centro de distribución de claves esté en línea todo el tiempo. De hecho, ni siquiera tiene que estar en línea. En su lugar, lo que hace es certificar las claves públicas que pertenecen a las personas, empresas y otras organizaciones.

Ahora, a una organización que certifica claves públicas se le conoce como **CA (Autoridad de Certificación**, del inglés Certification Authority).

X.509

Si todas las personas que quisieran algo firmado fueran a la CA con un tipo diferente de certificado, la administración de todos los distintos formatos de certificados pronto se volvería un problema. Para resolverlo se ha diseñado un estándar para certificados, aprobado por la ITU. Dicho estándar se conoce como X.509 y se utiliza mucho en Internet.

En esencia, el X.509 es una forma de describir certificados. Las descripciones que se establecen en esa figura deben proporcionar una idea general de lo que hacen los campos.

Los certificados están codificados mediante la **ASN.1 (Notación de Sintaxis Abstracta 1**, del inglés Abstract Syntax Notation 1) de la OSI, que puede considerarse como si fuera una estructura de C, pero con una notación muy diferente.

Infraestructuras de clave pública

El hecho de que una sola CA emitiera todos los certificados del mundo obviamente no funcionaría. Una posible solución sería tener múltiples autoridades CA que fueran operadas por la misma organización y que usaran la misma clave privada para firmar los certificados. Si bien esto podría solucionar los problemas de carga y de fallas, introduciría un nuevo problema: la fuga de claves. Si hubiera docenas de servidores

esparcidos por todo el mundo, todos con la misma clave privada de la CA, la probabilidad de que esta clave fuera robada o se filtrara de algún otro modo se incrementaría de manera considerable. Puesto que la situación comprometida de esta clave arruinaría la infraestructura de la seguridad electrónica mundial, tener una sola CA central es muy peligroso.

Por estas razones se ha desarrollado una forma diferente para certificar claves públicas. Su nombre general es **PKI (Infraestructura de Clave Pública)**

Una PKI tiene varios componentes: usuarios, autoridades de certificación (CA), certificados y directorios. Lo que la PKI hace es proporcionar una manera de estructurar estos componentes y definir estándares para los diversos documentos y protocolos. Una forma particularmente simple de PKI es una jerarquía de autoridades CA.

Directorios

Otro problema de cualquier PKI es en dónde están almacenados los certificados (y sus cadenas de vuelta hacia un ancla de confianza conocida. Una posibilidad es hacer que cada usuario almacene sus propios certificados. Si bien esto es seguro, a la vez es inconveniente.

Una alternativa que se ha propuesto es utilizar el DNS como un directorio de certificados. Antes de contactar a Bob, es probable que Alice tenga que buscar la dirección IP de Bob mediante DNS.

Algunas personas piensan que esta es la forma de hacer las cosas, pero tal vez otras prefieran servidores de directorios dedicados cuyo único trabajo sea manejar los certificados X.509. Tales directorios podrían proporcionar servicios de búsqueda mediante el uso de las propiedades de los nombres X.500.

2. SSL – La Capa de Sockets Seguros

Cuando la web entro en la vista pública, en un principio se utilizó para distribuir páginas estáticas, sin embargo, pronto algunas compañías tuvieron la idea de usar la web para actividades financieras, como para comprar mercancía, operaciones bancarias y comercio de acciones. Estos usos crearon una gran demanda de conexiones seguras. En 1995, Netscape Communications Corp., que entonces dominaba el mercado de los navegadores, respondió a esta demanda mediante la introducción de un paquete de seguridad llamado **SSL (Capa de Sockets Seguros)**. Actualmente se utiliza globalmente para asegurar una conexión segura.

El llamado SSL es una nueva capa de seguridad puesta entre la capa de aplicación y la capa de transporte en donde acepta solicitudes del navegador y envía a TCP para transmitirlas al servidor. Cuando se haya establecido una conexión segura el trabajo del SSL es la compresión y encriptación. El uso de SSL sobre HTTP se conoce como **HTTPS (HTTP Seguro)**

Como se mencionó antes, SSL soporta múltiples algoritmos criptográficos. El más robusto utiliza triple DES con tres claves separadas para encriptación y SHA-1 para la integridad de los mensajes. Esta combinación es relativamente lenta, por lo que se utiliza principalmente para operaciones bancarias y otras aplicaciones en las que se requiere la seguridad de mayor nivel. Para las aplicaciones comunes de comercio electrónico, se utiliza RC4 con una clave de 128 bits para encriptación y MD5 para la autentificación de mensajes.

Para un transporte real se utiliza un segundo subprotocolo. Los mensajes que provengan del navegador primero se dividen en unidades de hasta 16 KB. Después de eso, se obtiene una clave secreta a partir de los dos nonces y la clave premaestra se concatena con el texto comprimido; después, al resultado se le aplica un

hash con el algoritmo de hash acordado (por lo general MD5). Este hash se adjunta a cada fragmento como el MAC. Después, el fragmento comprimido y el MAC se encriptan con el algoritmo de encriptación simétrico acordado. Por último, se adjunta un encabezado de fragmento y el fragmento se transmite a través de la conexión TCP.

Sin embargo es necesario precaución ya que se ha mostrado que el RC4, que es el algoritmo más usado para encriptación simétrica, tiene claves débiles que se pueden analizar con facilidad.

En 1996, Netscape Communications Corp. entregó el SSL a la IETF para su estandarización. El resultado fue TLS (Seguridad de la Capa de Transporte).

TLS se basa en la versión 3 de SSL, aunque los cambios fueron pequeños son suficientes como para hacer que SSL versión 3 y TLS no puedan interoperar.