Fundamentos

Capítulo 2

Conceptos sobre seguridad en Internet

Contenido

2.1 Introducción

Una de las bases sobre las que se asienta la federación de sistemas es la seguridad. Aunque es imposible asegurar que la información que se recibe sobre los usuarios sea cierta (esto depende exclusivamente del sistema origen de los datos), si debemos ser

capaces de confirmar que dicha información proviene de la fuente que suponemos, que no es accesible para intermediarios maliciosos y que no ha sido modificada desde su transmisión inicial. Sin una infraestructura segura no es posible la confianza entre servidores.

A lo largo de esta memoria aparecerán con cierta frecuencia determinados conceptos relacionados con la transmisión segura de datos sobre redes de ordenadores. Es posible que dichos conceptos puedan resultar conocidos para la mayoría de las personas familiarizadas con las Tecnologías de la Información pero, a pesar de ello, hemos querido incluir aquí una breve descripción de algunos de ellos.

El texto de este capítulo no pretende más que servir de referencia rápida para el resto de la memoria. Existen numerosos textos, publicados tanto en papel como en Internet, que tratan estos temas con mayor profundidad. Se remite al lector a la bibliografía si desea más información.

En relación con la terminología empleada hay que hacer notar que preferiremos en todo el texto el uso del verbo "cifrar" al de "encriptar", por ser el reconocido oficialmente como palabra de la lengua española (se reconocen también el sustantivo "criptografía" y el adjetivo "criptográfico").

2.2 Objetivos de las técnicas de seguridad

En general, las técnicas y protocolos de seguridad informática existentes se marcan como objetivo proporcionar a los sistemas a los que prestan servicio las siguientes capacidades (o algunas de ellas):

- **Autenticación**

  En el contexto de una transacción electrónica, se define como la capacidad de uno de los participantes en dicha transacción de determinar la identidad de otro de los mismos que participan en ella.

- **Confidencialidad**

  Implica que el contenido de un mensaje pueda ser leído únicamente por el destinatario o destinatarios a los que ha sido enviado y no por cualquier otro individuo a cuyas manos vaya a parar dicha información. En principio, implica algún tipo de cifrado del mensaje.

- **Integridad de datos**

  Consiste en garantizar que el destinatario pueda confirmar que el mensaje que ha recibido no presenta alteraciones con respecto a lo que originalmente se envió desde el origen de datos.

- **No repudio**

  Consiste en que el emisor de un mensaje no pueda negar que fue él quien emitió dicho mensaje.

Para conseguir estos objetivos se emplean diferentes mecanismos criptográficos, como el cifrado digital, que veremos a continuación.

2.3 El cifrado digital

El proceso de cifrado consiste en lo siguiente: dado el mensaje original, le aplicamos una clave criptográfica mediante un algoritmo, obteniendo como resultado un mensaje cifrado. Este mensaje sólo podrá ser descifrado por aquellos que conozcan el algoritmo y la clave que se han empleado. Por ejemplo, podríamos pensar en cifrar una transmisión sustituyendo cada letra del mensaje original por aquella que resulta de retrasar dicha letra 3 posiciones en el abecedario. En vez de enviar una “a”, enviaríamos la “d”, en vez de la “b”, la “e” y así sucesivamente. En este caso el algoritmo sería “retrasar la letra a enviar un número determinado de posiciones” y la clave, “el número de posiciones es igual a 3”.

Los sistemas criptográficos que se emplean hoy en día en Internet son, por supuesto, mucho más complicados, aunque la base es la misma.

Dentro del cifrado digital encontramos dos opciones básicas: el cifrado de clave simétrica y el de clave asimétrica. Vemos a continuación en qué consiste cada uno de ellos.

Cifrado de clave simétrica

Se emplea una sola clave para cifrar y descifrar el mensaje. El remitente cifra la transmisión usando una determinada clave y lo envía al destinatario deseado. Éste aplica la misma clave de manera inversa para descifrar el mensaje recibido. Ya sea de manera previa o junto con el mensaje, el emisor debe hacerle llegar la clave al receptor, para que este pueda llevar a cabo el proceso de descifrado.

El beneficio más importante de la criptografía de clave simétrica es su velocidad, lo cual la hace adecuada para el cifrado de grandes cantidades de datos.

Su inconveniente principal es la necesidad de distribuir la clave que se emplea para el cifrado, por lo que, si alguien consigue hacerse tanto con el mensaje como con la clave, podrá descifrar dicho mensaje. Por esta razón, se plantea el uso de un sistema criptográfico basado en claves asimétricas, el cual describimos a continuación.

Cifrado de clave asimétrica

En este caso, cada usuario posee una pareja de claves :

- **Clave privada:** será custodiada por su propietario y no se dará a conocer a ningún otro usuario.
- **Clave pública:** será conocida por todos los usuarios.

Estas dos claves son complementarias: lo que cifra una sólo puede descifrarlo la otra y viceversa. El algoritmo para generar dichas claves hace que sea inviable conocer una a partir de la otra, por razones de tiempo de cómputo.

El proceso para enviar un mensaje cifrado sería el siguiente: el remitente cifra el mensaje utilizando la clave **pública** del destinatario. Éste emplea su clave **privada** descifrar lo que recibe.

Este procedimiento garantiza la confidencialidad puesto que, si algún intermediario no deseado intercepta el mensaje, no será capaz de descifrarlo, ya que la clave privada sólo es conocida por su propietario. A diferencia del método de clave simétrica, se suprime la necesidad de distribución de una clave secreta a los receptores deseados, lo que aumenta la seguridad en la transacción.

Los algoritmos de cifrado de clave asimétrica son más lentos que los de clave simétrica, constituyendo este factor su principal inconveniente.

Con esto se garantiza la confidencialidad e integridad de los datos enviados pero aún nos falta por asegurar la autenticación y el no repudio. Para ello se utiliza la denominada firma digital, concepto que explicamos a continuación.

2.4 La firma digital

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de datos (autenticación), confirmar que dicha información no ha sido modificada desde su generación (integridad) y asegurarse de que el emisor del mensaje no puede negar la responsabilidad de su envío (no repudio). En los párrafos siguientes, y por razones de claridad en la explicación, se obviará la necesidad de confidencialidad, suponiendo que ésta será garantizada por el método expuesto en el apartado anterior o por alguna otra técnica de seguridad.

La firma digital se basa en la clave privada del usuario. A diferencia de la firma manuscrita, la digital es imposible de falsificar, siempre que dicha clave privada sea conocida únicamente por su propietario.

Para firmar digitalmente un mensaje, se procede al cifrado de dicho mensaje usando la clave **privada del remitente**, en vez de la clave **pública del destinatario**. La

criptografía de clave asimétrica nos asegura que lo que se cifra con una clave privada sólo puede descifrarse con su correspondiente clave pública. Así pues, si conseguimos descifrar un mensaje aplicándole la clave pública de un usuario, tendremos la seguridad de que ese mensaje proviene de dicho usuario, al ser éste el único que conoce su clave privada.

Como se ha comentado antes, un inconveniente de los algoritmos asimétricos es su lentitud, la cual, además, crece con el tamaño del mensaje a cifrar. Para superar este problema, se hace uso de funciones *hash*. Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, obteniéndose como resultado otro conjunto de datos denominado hash, resumen o huella. El resumen de los datos tiene una longitud fija sea cual sea la extensión del conjunto original y, además, está unívocamente asociado a él, es decir, no existen dos mensajes distintos que tengan un resumen idéntico. Es este resumen de datos lo que realmente se firma.

El envío de un mensaje firmado digitalmente transcurriría como se describe a continuación:

1. El remitente aplica una función hash al mensaje original, obteniendo el resumen de datos de dicho mensaje.
2. Le aplica su clave **privada** a dicho resumen. El resumen cifrado es la firma digital del mensaje.
3. Se envía el mensaje junto con la firma digital.
4. El destinatario toma la firma digital recibida y le aplica la clave **pública** del remitente, obteniendo el que es, supuestamente, el resumen de datos del mensaje original.
5. Seguidamente toma el mensaje recibido y le aplica la misma función hash del primer paso para calcular el resumen de datos real.
6. Si los resúmenes obtenidos en los pasos 4 y 5 son iguales el mensaje proviene realmente del remitente y, además, no ha sido modificado durante su transporte.

2.5 Certificados digitales

Hemos mencionado anteriormente la importancia que tiene que la clave privada sea conocida únicamente por su propietario. Tan importante como esto, es el hecho de relacionar de manera unívoca la identidad de un usuario con su clave **pública**.

Para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los **certificados digitales** o **certificados de clave pública**. Un certificado digital nos asegura que "la clave pública X pertenece al usuario Y", es decir, es un documento que relaciona una clave pública con la identidad de su propietario.

Además de la identificación del propietario y de su clave pública, el certificado puede contener otros datos, tales como el ámbito de aplicación del certificado, fechas de inicio y fin de validez del mismo, etc.

Un certificado será auténtico si la clave pública que aparece en él pertenece realmente al propietario indicado. ¿Cómo podemos asegurar que un certificado no es falso? La respuesta es utilizar una tercera parte en la comunicación, en la que confían tanto remitente como destinatario. Esta tercera parte de confianza actúa como autoridad que asegura que la información contenida en el certificado digital es cierta. La forma en que esa autoridad avala la autenticidad del certificado es firmar dicho certificado con su firma digital. Por tanto, podremos confiar en la veracidad de la información de un certificado digital si confiamos en la autoridad que lo firma. Las entidades dedicadas a la firma de certificados digitales se denominan autoridades de certificación o CA (por las siglas en inglés de *Certification Authority*). Algunos ejemplos son CAcert.org, Thawte, Verisign, Firmaprofesional y la Fábrica Nacional de Moneda y Timbre.

Queda aún por comentar un detalle relacionado con este tema. Para plantearlo de la forma más clara posible, vamos a recapitular lo expuesto hasta ahora sobre firma digital y certificados.

Nuestro objetivo inicial era poder asegurar la identidad del remitente de un mensaje recibido. Para ello, hacíamos que el emisor lo firmara, empleando su firma digital. Para realizar la autenticación requeríamos de la clave **pública** del remitente, por lo que

necesitábamos un documento que relacionara, de forma confiable, el nombre del remitente con su clave pública. Dicho documento es el certificado digital del emisor. Finalmente, para saber si dicho certificado es realmente confiable, hacíamos que una autoridad de certificación lo firmara digitalmente. De nuevo nos encontramos con una firma digital a autenticar, con la particularidad de que esta firma proviene de una autoridad de certificación.

La pregunta es entonces: ¿quién certifica a la autoridad certificadora? Pues bien, se emplea un certificado que está firmado por la propia autoridad de certificación. En este punto habríamos llegado al último eslabón de la cadena de certificación. Si queremos comprobar la autenticidad de este último certificado, necesitaríamos otro, donde se relacione de forma fiable la clave pública del firmante (autoridad de certificación) con su nombre. Ese certificado es precisamente el que ya tenemos en nuestro poder, es decir, este certificado no puede autenticarse contra ningún otro.

¿Cómo podemos, entonces, asegurar que es válido? En el caso particular de los navegadores web, el código del navegador trae "de fábrica" una serie de **certificados raíz**, en los que se confía por defecto, con un período de validez "eterno". Debido al poder que poseen para certificar la veracidad de datos sensibles en Internet, las claves privadas correspondientes a estos certificados se cuentan entre las mejor guardadas.

2.6 Infraestructura de clave pública

Una infraestructura de clave pública o PKI (Public Key Infraestructure) es un conjunto de protocolos, servicios y estándares que dan soporte a aplicaciones basadas en criptografía de clave pública. Algunos de los servicios que presta una PKI son: emisión de un nuevo certificado para una clave pública, cancelación de un certificado previamente emitido, publicación de la clave pública de los usuarios, etc.

El Sector de Normalización de la Unión Internacional de Telecomunicaciones (UIT-T) ha definido un estándar para una infraestructura de clave pública, que se denomina X.509. X.509 define, entre otras cosas, un formato estándar para los certificados de clave pública. Los dos protocolos criptográficos más empleados actualmente en Internet

y que hacen uso de este formato estándar, se denominan ***Secure Sockets Layer*** (SSL) y ***Transport Layer Security*** (TLS). Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0 pero el protocolo es básicamente el mismo. En muchas ocasiones se utiliza el término "SSL" para referirse a ambos indistintamente.

Como se ha comentado anteriormente, un certificado puede provenir de una autoridad "oficial" de certificación, pero una institución, tal como una universidad o una empresa, podría crear también su propia infraestructura de clave pública, con su propia fuente de certificados. No serían válidos fuera de dicha universidad o empresa, pero se podrían instalar en todos los ordenadores usados por los miembros de la empresa o comunidad universitaria, añadiéndolos a la base de datos raíz de los navegadores usados por dichos miembros.

2.7 Los certificados en Java

Java contiene su propia base de datos de certificados raíz. Se aplica en los casos en los que la validación del certificado la realiza Java en primer lugar, sin dejar que ninguna otra aplicación lo compruebe antes. Esta base de datos se encuentra por defecto en el directorio del Java Runtime Environment, en concreto en el archivo lib/security/cacerts. Tomcat posee, asimismo, la suya propia.

Para certificados no provenientes de autoridades "oficiales" de certificación, es decir, aquellos que cualquier usuario puede generar en su propio ordenador empleando el software apropiado, Java provee el soporte de los **archivos JKS** (Java Key Store). Un fichero JKS es una base de datos que puede contener muchos certificados y claves públicas.