UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE ELECTRÓNICA

Seguridad en la Web

Nombre: Luis Vera Alvarado
Rol: 2621020-8

Valparaiso 14 de Julio de 2010

Introducción

La masificación del uso de internet y las aplicaciones web en diferentes aspectos de la vida (transacciones comerciales, relaciones personales, comunicaciones, etc), imponen la necesidad de generar métodos de seguridad como realizar conexiones seguras, autenticar usuarios, enviar información encriptada, manejar mensajes íntegros etc.

La seguridad se puede implementar en las diferentes capas de la red, éste documento comienza con las ideas primitivas de seguridad luego se centra en la capa de aplicación y una breve mirada a la capa de transporte.

Seguridad Propósitos

Los propósitos de la seguridad en la web se pueden clasificar en cuatro categorias detalladas a continuación:

Autenticación: El usuario debe saber con certeza con quién realmente se está comunicando. De lo contrario se podría creer cómo vlida información falsa proveniente de una suplantación de usuario.

Confidencialidad: El mensaje no puede er leido por una persona no autorizada, para prevenir robo de información o datos o información de de la configuración de la red.

Integridad: El mensaje no puede ser cambiado. En una transacción comercial por ejemplo es de suma importancia que los datos no se modifiquen.

No Repudio: La operación no puede ser negada por la contraparte. El proceso no se puede interruptir.

Segurida Capas

La segurida se puede implementar en las diferentes capas de la red como son:

Capa de Enlace: Sólo se asegura un enlace pero no la conexión completa.

Capa de Red: Asegura toda la conexión, afecta a todas las aplicaciones.

Capa de Transporte: Asegura todas las conexiones que usen dicho transporte. Ejemplo: SSL, TLS.

Capa Aplicación: Criptografía, Firma , Certificado digital.

Encriptar Datos

El concepto más primitivo para seguridad es encriptar datos, es decir cifrar y descifrar información mediante técnicas especiales con el fin de que los mensajes puedan ser leídos por quienes pueden descifrarlos. Podemos encontrar dos tipos Criptografía Simétrica y Criptografía Asimétrica.

Criptografía Simétrica: En este método se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunicandeben ponerse de acuerdo de antemano sobre

la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma. La encriptacón puede ser por sustitución (cambiar un mensaje por otro) o por transposición (desordenar el mensaje).

Criptografía Asimétrica: En éste método cada usuario posee una llave privada y una pública. Lo que se encripta con una se puede desencriptar con la otra. La llave privada es mantenida en secreto por el usuario. La llave pública es conocida por el resto. Una llave no puede deducirse de la otra. En otras palabras el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce.

Pero cómo se comprueba que la llave pública usada es la correcta, por otra parte se puede querer autenticar un mensaje pero no necesariamente cifrarlo, finalmente ¿Qué pasa con el no repudio?.

Firma Digital

El mensaje se somete a un algoritmo HASH (SHA-1 u otro), que arroja un string de tamaño fijo. La encriptación de este string con la llave privada es la firma digital. Quien recibe le mensaje lo somete al mismo algoritmo HASH, decripta la firma y compara los strings. Si los strings son iguales implica autentificación, integridad y una respuesta implicaría un no repudio.

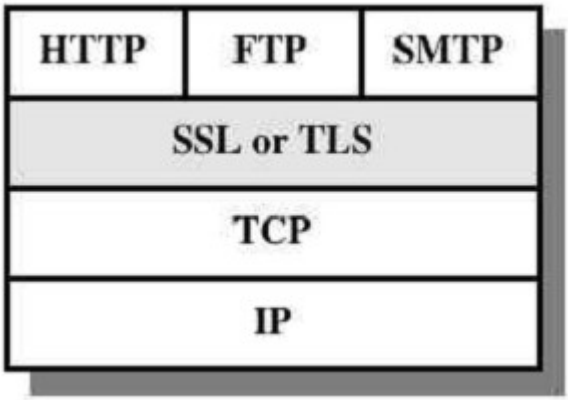
Certificado Digital

¿Cómo sabe el receptor que la llave pública es realmente del emisor?. Para garantizar que una llave pública le pertenece a cierta entidad, una AC (Autoridad Certificadora) emite un documento electrónico denominado "certificado digital" en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el período de validez de dicho certificado, más otros datos como el e-mail, restricciones de uso, etc.

En Chile las Entidades de Certificación están listadas en www.entidadacreditadora.cl y están reguladas por el Ministerio de Economía.

Seguridad en la Capa de Transporte

En la capa de transporte se asegura toda la conexión. En realidad los protocoloes de seguridad se incorporan en una capa intermedia entre la capa de aplicqación y la capa de transporte.



Protocolo SSL

El protocolo SSL (Secure Sockets Layer) es un sistema diseñado y propuesto por Netscape Communications Corporation, luego sirvió como base para TLS un estandard IETF (RFC2246). Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico. El protocolo handshake es la parte mas compleja de SSL, permite al servidor y al cliente autenticarse mutuamente y se usa antes qye cualquier cinjunto de datos de aplicaciones sea transmitido.

Conclusiones

En la actualidad es de vital importancia que se cumplan ciertos requisitos mínimos de seguridad y confiabilidad al momento de uasr internet, ya sea para evitar usos maliciosos o simplemente porque no es algo que el usuario común deba preocuparse cada vez que trabaje en la web.

Para cumplir con los requerimientos de seguridad se ha implementado primero tecnicas de encriptación de datos, firmas digitales, certificados digitales; además en la capa de transporte se utilizan protocolos de encriptación el mas importante es el estandar TLS derivado de SSL.

Sin duda esto basta para los usuarios, pero siempre hay que tener en cuenta los ataques maliciosos que están presentes y para los que estas medidas no son suficientes por lo que siempre se seguirá trabajando para mejorar estos sistemas de seguridad.

Referencias

William Stallings, “Fundamentos de Seguridad en Redes Aplicaciones y Estándares”, Prentice Hall, 2° Edición.

http://es.wikipedia.org/wiki/Transport_Layer_Security

Rodolfo Sumoza, Carlos Figueira, “Criptografía y Seguridad de Datos”

http://es.wikipedia.org/wiki/Criptograf%C3%ADa

http://www.entidadacreditadora.cl/