Universidad Tecnológica de Puebla

Tecnologías de la información

Alumno: Leonardo Saínos Pérez.

Matricula: UTP0143830

5to Grupo: F

Profesor: JENNY ORTEGA GARCIA.

Materia: APLICAICONES WEB PARA I 4.0

Tarea: Avances de investigación.

Fecha de entrega: 20/01/2021.

¿Qué es un protocolo?

El usuario de una computadora se convierte en un cliente al intentar tener acceso a una página WEB, así como, a través de una línea telefónica, podría solicitar información sobre un servicio o un producto a un proveedor, a quien identificaría como un servidor. A la forma de ponerse de acuerdo en cuanto al modo de envío y recepción de un artículo adquirido telefónicamente, se le llama protocolo. Así, en términos informáticos, un protocolo es un “conjunto de normas y procedimientos útiles para la transmisión de datos, conocido por el emisor y el receptor”. Según la Real Academia Española, protocolo es un “acta o cuaderno de actas relativas a un acuerdo, conferencia o congreso diplomático”. Aunque Internet es producto del enlace entre miles de redes con tecnología distinta, en apariencia esta tecnología es uniforme, pues el “acuerdo” entre la diversidad de redes de que está conformada la Internet para transmitir información, lo ofrece el lenguaje común denominado protocolo TCP/IP (Transmisión Control Protocol/Internet Protocol).

PROTOCOLOS DE SEGURIDAD.

HTTPS.

HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. Dado que los usuarios esperan que su experiencia online sea segura y privada, te recomendamos que adoptes HTTPS para proteger sus conexiones con tu sitio web, independientemente de lo que este contenga.

El envío de datos mediante el protocolo HTTPS está protegido con el protocolo *Seguridad en la capa de transporte* (Transport Layer Security, TLS), que proporciona estas tres capas de seguridad principales:

1. Cifrado: se cifran los datos intercambiados para mantenerlos a salvo de miradas indiscretas. Eso significa que cuando un usuario está navegando por un sitio web, nadie puede "escuchar" sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas ni robarle información.
2. Integridad de los datos: los datos no pueden modificarse ni dañarse durante las transferencias, ni de forma intencionada ni de otros modos, sin que esto se detecte.
3. Autenticación: demuestra que tus usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques de intermediario y fomenta la confianza de los usuarios, lo que se traduce en otros beneficios empresariales.

SCP.

Con el protocolo SCP los datos son cifrados durante su transferencia, para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos. Sin embargo, el protocolo mismo no provee autenticación y seguridad; sino que espera que el protocolo subyacente,SSH, lo asegure.

El modo SCP o simple communication protocol, es un protocolo simple que deja al servidor y al cliente tener múltiples conversaciones sobre una TCP normal. Este protocolo está diseñado para ser simple de implementar.

El servicio principal de este protocolo es el control del dialogo entre el servidor y el cliente, administrando sus conversaciones y agilizadas en un alto porcentaje, este protocolo le permite a cualquiera de los dos establecer una sesión virtual sobre la normal.

SCP implementa la transferencia de archivos únicamente. Para ello se conecta al host usando Tunel SSH y allí ejecuta un servidor SCP. Generalmente el programa SCP del servidor es el mismo que el del cliente.

SET.

El Protocolo SET (Secure Electronic Transaction o Transacción Electrónica Segura) es un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red. Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL. Precisamente esa fue la razón que dio origen a su nacimiento.

Cuando se realiza una transacción segura por medio de SET, los datos del cliente son enviados al servidor del vendedor, pero dicho vendedor sólo recibe la orden. Los números de la tarjeta del banco se envían directamente al banco del vendedor, quien podrá leer los detalles de la cuenta bancaria del comprador y contactar con el banco para verificarlos en tiempo real.

IMAPS

SERVICIOS DE SEGURIDAD.

Los servicios de seguridad lo ayudan a aprovechar al máximo sus inversiones en tecnología. Las organizaciones que usan servicios de seguridad tienen acceso a consultores y expertos técnicos para brindar soporte a su personal con el conocimiento y las capacidades más actuales. También pueden mejorar el tiempo de detección y respuesta ante amenazas. Además, al reducir la complejidad, podrá adaptarse mejor a las cambiantes prioridades organizacionales.

La seguridad es un concepto considerado clave dentro de los que comprenden el aseguramiento de calidad dentro del servicio Web. Si se realiza una catalogación básica de los servicios de seguridad son la confidencialidad, integridad, autenticidad de origen, no repudio y control de acceso. A continuación se explica brevemente cada uno de ellos:

- **Autenticación de los participantes.** Los servicios Web por definición tienen mucha heterogeneidad, lo que provoca que los sistema de autenticación tengan que ser flexibles. Si imaginamos un servicio Web que necesita comunicarse con otro servicio, este podría solicitar al demandante credenciales junto a una demostración de que es el propietario de las mismas. Resulta necesario conseguir un estandarización de los protocolos y en los formatos a utilizar. Otro problema remanente es definir un modelo de autenticación Single Sign-On de forma que un servicio que necesita comunicarse con otros servicios Web,no tenga la necesidad de estar continuamente autenticándose y logre completar el proceso de negocio en un tiempo de respuesta aceptable.
- **Autorización**. Con frecuencia , es necesario aplicar unos criterios que permitan controlar el acceso a los diferentes recursos. Es necesario definir los usuarios que pueden realizar diversas acciones sobre los diferentes recursos. En combinación con la autenticación, permite a las identidades conocidas realizar las acciones para las que tienen permisos. Con frecuencia se definen políticas de acceso en base a jerarquías.
- **Confidencialidad**. Es necesario asegurar que el contenido incluido en los mensajes que se intercambian se mantiene como información confidencial. Es muy habitual emplear técnicas de cifrado, ya muy extendidas. Obviamente, la confidencialidad del mensaje va más allá que el canal por el que es transmitido.
- **Integridad**. Esta propiedad garantiza que la información que se ha recibido , es exactamente la misma que se envió desde el cliente.
- **No repudio.** En una comunicación que se realizan transacciones, es necesario registrar que las mismas se han producido y registrar el autor que lo ejecutó. En el caso de los servicios Web, trasladamos esta política la uso del servicio. Se comprueba que cierto cliente hizo uso de un servicio a pesar de que éste lo niegue (no repudio del solicitante) así como probar la ejecución se llevó a cabo (no repudio del receptor).
- **Disponibilidad**. Uno de los ataques mas frecuentes a las aplicaciones se basa en la denegación de servicios. Se lanzan múltiples solicitudes falsas para inundar el servicio y provocar su caída. Es necesario contemplar la disponibilidad, como punto muy importante en el diseño de servicio web, ya que permiten cierta redundancia de los sistemas.
- **Auditabilidad**. El registro de las acciones en los servicios Web permite mantener una traza de las mismas de manera que se puedan realizar análisis posteriores de los datos.
- **Seguridad extremo-a-extremo**. Cuando se ejecuta un servicio es necesario garantizar la seguridad durante todo el recorrido que efectúan los mensajes. Dado que normalmente existen routers como intermediarios de la comunicación, esto provoca un aumento de la política de seguridad que garantice que se realiza el transporte de forma segura y confirme la seguridad de los intermediarios. Es importante disponer de un contexto de seguridad único y que incluya el canal de comunicación. Para conseguirlo, es necesario aplicar diversas operaciones de carácter criptográfico sobre la información

en el origen. De esta manera se evita una dependencia con la seguridad que se configure por debajo de la capa de aplicación y se garantiza los servicios de seguridad

Requisitos de Seguridad

Si realizamos una abstracción sobre la problemática, el objetivo principal es conseguir un entorno para las transacciones y los procesos que sea seguro para todo el canal de comunicación. Obviamente, es necesario garantizar la seguridad durante el tránsito de la comunicación, ya sea con intermediarios o sin ellos durante la misma. Pro otra parte, se necesita asegurar la seguridad de la información en los procesos de almacenamiento: A continuación se ofrece una revisión breve de los principales requisitos para asegurar la seguridad en la comunicación.

CERTIFICADOS DE SEGURIDAD.

SSL

SSL (Secure Sockets Layer) es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications

Corporation junto con su primera versión del Navigator. Sin embargo, no fue hasta su tercera versión, conocida como SSL v3.0 que alcanzó su madurez, superando los problemas de seguridad y limitaciones de sus predecesores. No es exclusivo del comercio electrónico sino que sirve para cualquier comunicación vía Internet y, por lo tanto, 58 Industrial/Vol. XXVII/No. 2-3/2006 S. ORTEGA - L. CANINO también para transacciones económicas.

SSL está incorporado a muchos navegadores web además del Navigator de Netscape, y el Internet Explorer de Microsoft. Hoy constituye la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios de comercio electrónico. SSL está basado en la aplicación conjunta de criptografía simétrica (de llave secreta), criptografía asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet.

1 De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación. Estos sistemas adicionan códigos de autenticación de mensajes (MAC por sus siglas en inglés) para garantizar la integridad de los datos. Por su parte, los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la confidencialidad en la transmisión de datos. La identidad de un servidor web seguro (y a veces también del usuario cliente) se consigue mediante el certificado digital correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles, mientras que de la seguridad de la integridad de los datos intercambiados se encarga la firma digital mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos.

Google académico

Freeditorial

Dialnet

Redalyc

Internet archive