Universidad Autónoma del Estado de México
Centro Universitario UAEM Valle de Teotihuacán

CUVT

Programa Educativo:
Licenciatura en informática Administrativa

Unidad de Aprendizaje:
Temas selectos de redes computacionales

Semestre: Octavo

Periodo: 2017 A

Elaboración: Cozobi García Herrera

Criptografía.

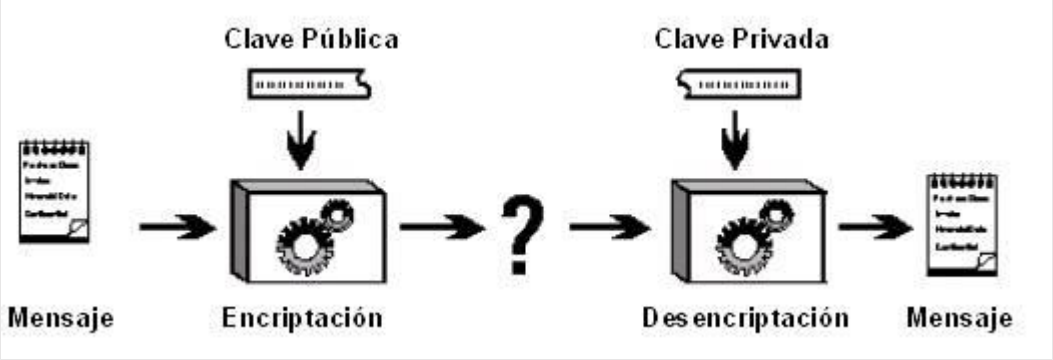
- Es la técnica que protege documentos y datos.
- Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.
- Rama inicial de las Matemáticas y en la actualidad también de la Informática, que hace uso de métodos y técnicas con el objeto principal de hacer ilegible (es decir, cifrar), y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Los sistemas criptográficos se clasifican por:

- El número de claves usadas.
- El tipo de operación utilizado para transformar el texto claro en texto cifrado.
- La forma de procesar el texto claro.

Tipos de criptografía

- Cifradores Simétricos o de Clave Privada.
- Cifradores Asimétricos o de Clave Pública.
- Cifrado de enlace.
- Cifrado de extremo a extremo
- Con la criptografía se intenta garantizar las siguientes propiedades deseables en la comunicación de información de forma segura:
  - Confidencialidad
  - Integridad de la información
  - Autenticación de usuario
  - Autenticación de remitente
  - Autenticación del destinatario

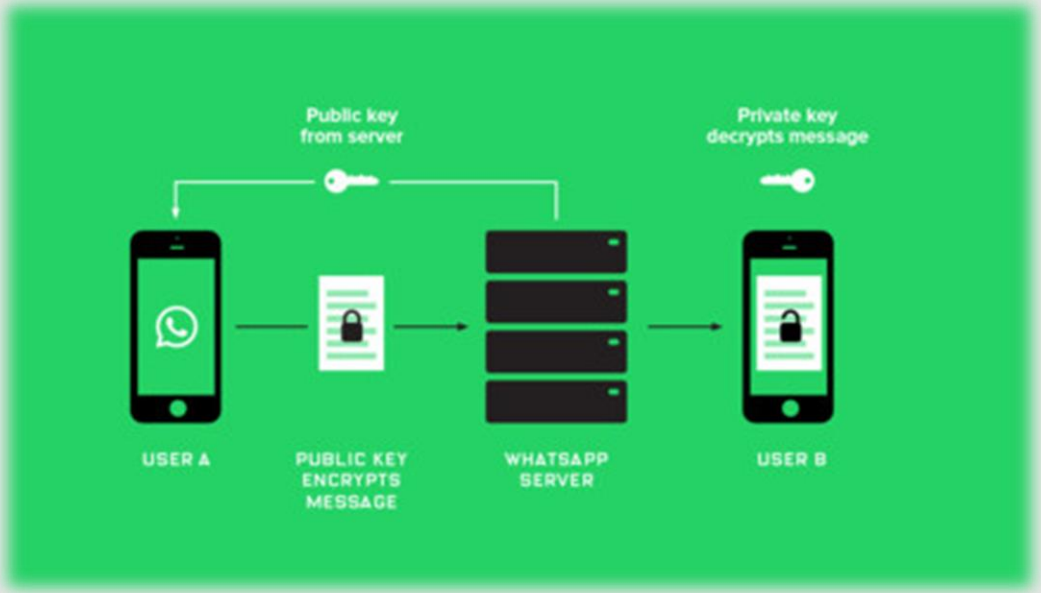


Cifrado de enlace

- La tarea de cifrar la información que sale del ordenador o de descifrar la que entra.
- En el cifrado de enlace se ubica en la capa física.
- Cada bit que sale de la máquina sufre un proceso de cifrado y cada bit que entra en la máquina sufre un proceso de descifrado.
- El encargado de cifrar es el software de red, que es el que se comunica con las aplicaciones y el sistema operativo.

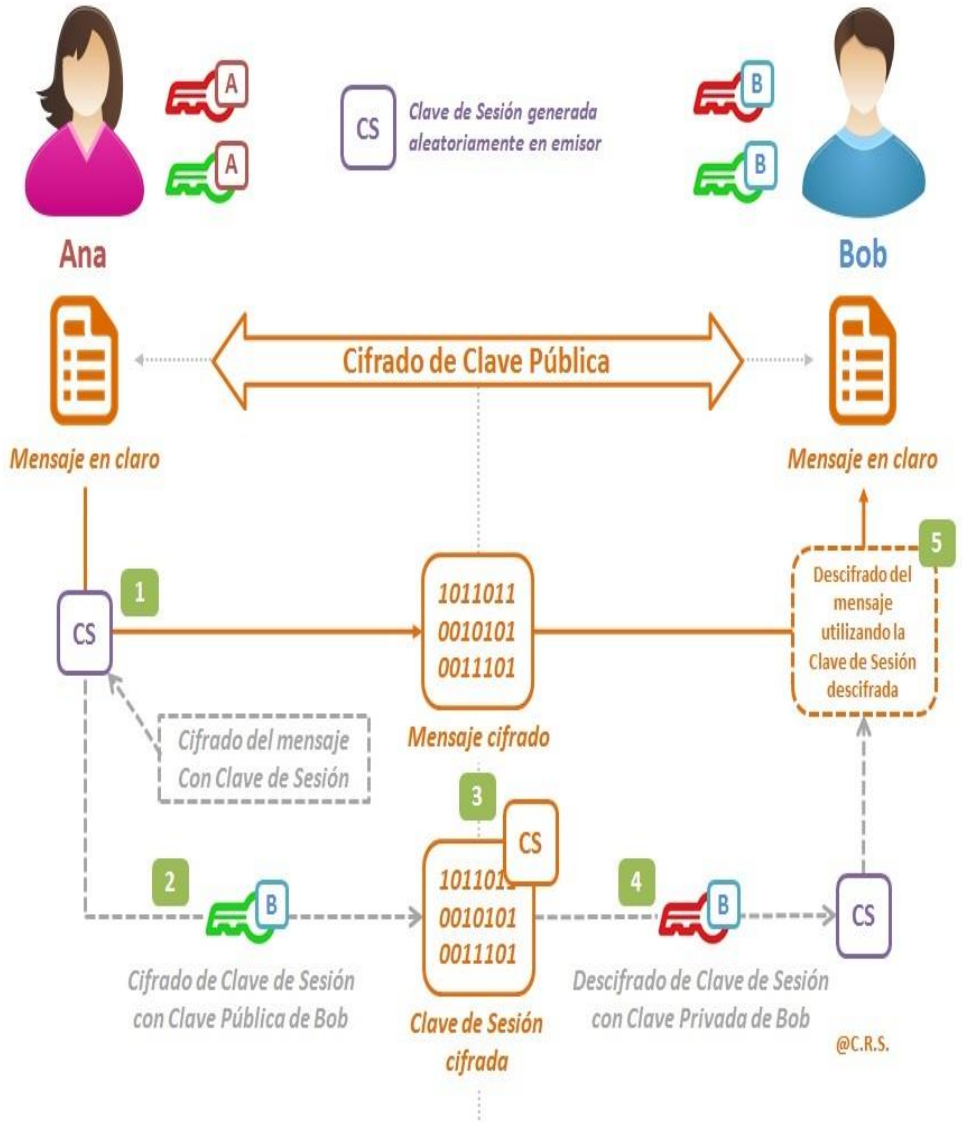
Cifrado de extremo a extremo

- Se realiza en el nivel 4, de aplicación.
- La aplicación es la que cifra los datos antes de mandarlos al sistema operativo y este a la capa de red, y la que los descifra una vez recibidos.
- SSL, SSL2, SSL3, TLS. Son protocolos de CEE para comunicaciones con sesión, se usan mayoritariamente para web.



Cifrado con clave asimétrica

- Si una persona con una pareja de claves cifra un mensaje con la llave privada, ese mensaje sólo podrá ser descifrado con la llave pública asociada.
- Si se cifra con la pública, se descifra con la privada.
- Si “ciframos” un mensaje con la clave privada, no podremos descifrarlo con la propia llave privada, deberemos usar la pública.
- La ventaja del cifrado asimétrico sobre el simétrico radica en que la clave pública puede ser conocida por todo el mundo.



Cifrado con clave de sesión

- Ralentiza el proceso de cifrado.
- La solución a esto es usar el cifrado asimétrico como el simétrico (como hace IPSec o SSL).
- En las VPN como OpenVPN TLS/SSL la clave de sesión, que es conocida por los usuarios, se regenera cada cierto tiempo para incrementar la seguridad.

Firmas digitales

- Es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales.
- Es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
- No implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.
- Es un instrumento con características técnicas y normativas.

Funcionamiento

- Funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados.

- El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital.

- Cada participante tiene un par de claves, una se usa para encriptar y la otra para desencriptar.

- Cada participante mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).

- El emisor calcula un resumen del mensaje a firmar con una función hash. El resumen es un conjunto de datos de pequeño tamaño que tiene la propiedad de cambiar si se modifica el mensaje.

- El emisor encripta el resumen del mensaje con una clave privada y ésta es la firma digital que se añade al mensaje original.

Firma digital con árbitro

- Donde dos usuarios con desconfianza mutua confían en un tercero.
- Se utilizan criptosistemas de clave única (una sola clave para cifrar y descifrar).
- El emisor y el receptor tienen sus propias claves por lo que es el árbitro el encargado de recibir el mensaje del emisor, desencriptarlo con la clave del emisor. De esta forma el emisor y el receptor no necesitan compartir claves.

Firma digital ordinaria

- En la cual el usuario firmante envía directamente la firma al destinatario, y este debe poder comprobar la validez de la firma sin necesidad de un árbitro.
- A este método pertenecen los sistemas de firmas actuales que se basan en criptosistemas de clave pública.

Administración de claves públicas

- En 1976, Whitfield Diffe y Martin Hellman crearon la criptografía mediante claves públicas. La criptografía mediante claves públicas representa una gran innovación ya que altera fundamentalmente el proceso de cifrado y descifrado.
- los usuarios eligen una clave aleatoria que sólo ellos conocen.
- A partir de esta clave, automáticamente se deduce un algoritmo (la clave pública). Los usuarios intercambian esta clave pública mediante un canal no seguro.
- Cuando un usuario desea enviar un mensaje a otro usuario, sólo debe cifrar el mensaje que desea enviar utilizando la clave pública del receptor (que puede encontrar, por ejemplo, en un servidor de claves como un directorio LDAP). El receptor podrá descifrar el mensaje con su clave privada (que sólo él conoce).

- Emplean una doble clave (kp,kP). kp se la conoce como clave privada y kP se la conoce como clave pública.
- Una de ellas sirve para la transformación o función E de cifrado y la otra para la transformación D de descifrado.
- En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa.
- Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros.
- Se usan dos claves diferentes para cifrar y descifrar la información.

Ventajas y desventajas

El problema de la comunicación de la clave de descifrado ya no existe, ya que las claves públicas se pueden enviar libremente. Por lo tanto, el cifrado con clave pública permite a las personas intercambiar mensajes de cifrado sin tener que compartir un secreto.

Seguridad en comunicación

- Proteger host ("anfitrión" o computadoras conectadas a una red)y los servicios que se proporcionan en la red.
- Autenticación (password) y autenticación mutua (emisor y receptor).
- Confidencialidad, Integridad y Disponibilidad.
- Medidas de encriptación para aumentar CIA (confidentiality ”confidencialidad”, integrity “integridad” and availability “disponibilidad”).

- Confidencialidad de los datos: Impide la divulgación no autorizada de los datos.
- Control de acceso: Protege contra la utilización de recursos de la red.
- Autenticación: Permite comprobar la identidad de entidades comunicante.
- No repudio: Impide que una persona o una identidad nieguen haber realizado una acción concreta en relación con los datos presentando las pruebas de esas acciones en la red
- Garantiza que los flujos de información sólo tienen lugar entre puntos extremos autorizados Integridad de los datos

- Garantiza que los datos son correctos y exactos.

- Disponibilidad: Garantiza que ningún evento que pueda ocurrir en la red impedirá el acceso autorizado a los elementos, la información almacenada, los flujos de información, los servicios y las aplicaciones de la red.

- Privacidad Impide conocer información observando las actividades de la red, por ejemplo los sitios web que un usuario ha visitado, la ubicación geográfica del usuario y las direcciones IP y los nombres DNS.

Fundamentos de la protección

En términos generales será necesario proteger los siguientes elementos:

- Servicios de comunicaciones y de informática.
- Información y datos.
- Los equipos y las instalaciones.

Integridad

- Requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.

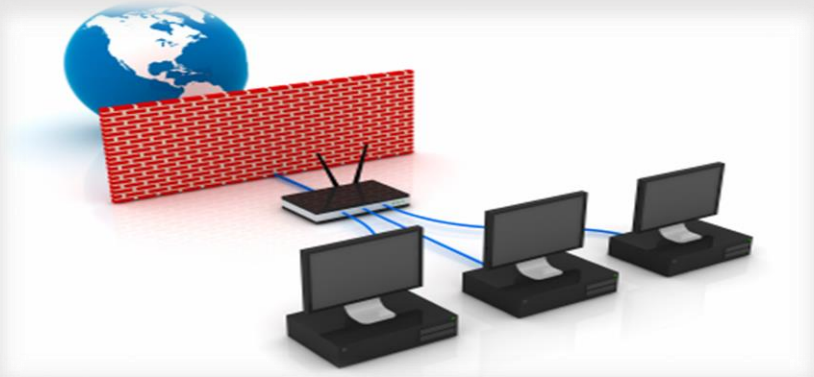
Confidencialidad

- Se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación.

Ataques a la seguridad de la red

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos:

- Ataques pasivos: Son oidores o monitoreos de las transmisiones.
- Divulgación del contenido de un mensaje: Es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida.
- Análisis de Tráfico: Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que esta siendo transmitido aun cuando este protegido por medio de cifrado.



Ataques activos

Suponen modificación de los datos o creación de flujos de datos falsos.

Enmascaramiento

- Es un tipo de ataque activo que tiene lugar cuando una entidad.
- Pretende suplantar a otra para obtener información confidencial.

Repetición

Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.

Modificación de Mensajes

Se modifican los mensajes para producir efectos no autorizados.

Denegación de Servicios

Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin especifico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma.

Herramientas de seguridad

- Existen métodos o herramientas tecnológicas que ayudan a las organizaciones a mantener segura la red. Estos métodos, su utilización, configuración y manejo dependen de los requerimientos que tenga la organización para mantener la red en un funcionamiento óptimo y protegido contra los diferentes riesgos.
  - Autenticación.
  - Autorización.
  - Auditoria.
  - Cifrado
  - Filtros de paquete

Protocolos de autenticación

- Al utilizar el Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol), un mecanismo de autenticación arbitrario valida las conexiones de acceso remoto.
- La autenticación es un aspecto fundamental de la seguridad de un sistema. Confirmar la identidad de cualquier usuario que intenta iniciar la sesión en un dominio o tener acceso a los recursos de la red.
- Es un tipo criptográfico que tiene el propósito de autentificar entidades que desean comunicarse de forma segura.

CHAP (Protocolo de autenticación por desafío mutuo)

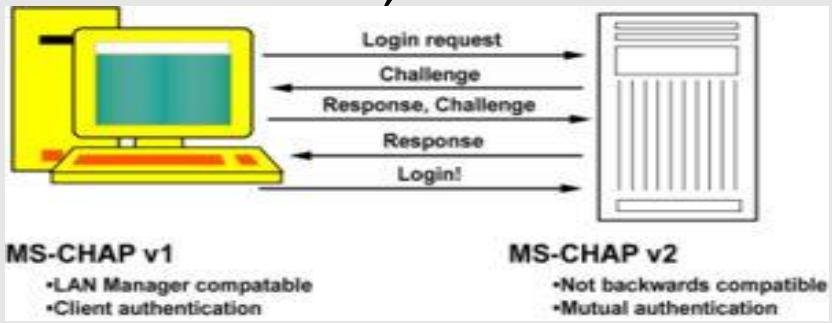
- Es un método de autenticación muy utilizado en el que se envía una representación de la contraseña del usuario, no la propia contraseña.
- El servidor de acceso remoto envía un desafío al cliente de acceso remoto.
- El cliente de acceso remoto utiliza un algoritmo hash (también denominado función hash) para calcular un resultado hash de MessageDigest-5 (MD5) basado en el desafío y un resultado hash calculado con la contraseña del usuario.
- El cliente de acceso remoto envía el resultado hashMD5 al servidor de acceso remoto.
- El servidor de acceso remoto, que también tiene acceso al resultado hash de la contraseña del usuario

SPAP (Protocolo de autenticación de contraseña de shiva)

- Es un protocolo de autenticación simple de contraseña cifrada compatible conservadores de acceso remoto de Shiva.
- El cliente de acceso remoto envía una contraseña cifrada al servidor de acceso remoto.
- Utiliza un algoritmo de cifrado bidireccional.
- El servidor de acceso remoto descifra la contraseña y utiliza el formato sin cifrar para autenticar al cliente de acceso remoto.

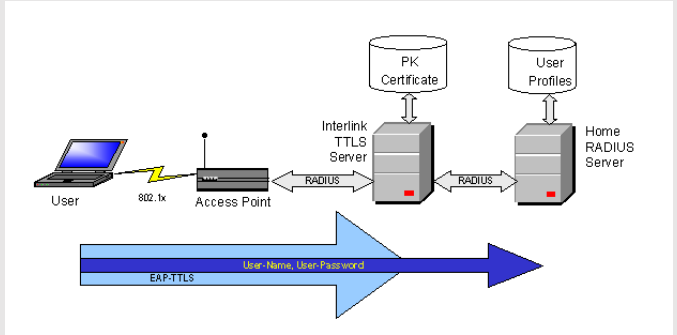
MS-CHAP y MS-CHAP v2

- Protocolo de autenticación por desafío mutuo de Microsoft.
- Microsoft creó MS-CHAP para autenticar estaciones de trabajo Windows remotas, integrando la funcionalidad a la que los usuarios de redes LAN están habituados con los algoritmos de has utilizados en las redes Windows.
- Utiliza un mecanismo de desafío y respuesta para autenticar conexiones sin enviar contraseñas.
- El autenticador (el servidor de acceso remoto o el servidor IAS) envía al cliente de acceso remoto un desafío formado por un identificador de sesión y una cadena de desafío arbitraria.
- El cliente de acceso remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.



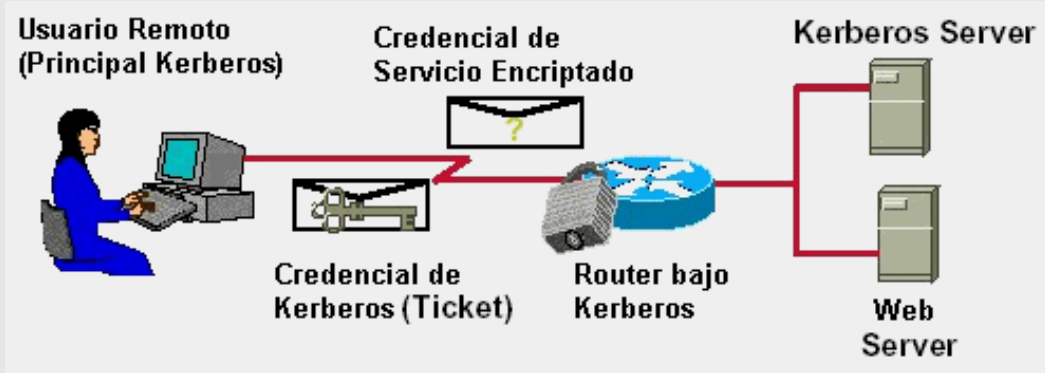
EAP (Protocolo de autenticación extensible)

- Es una extensión del Protocolo punto a punto (PPP) que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias.
- EAP se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado.
- Se pueden admitir esquemas de autenticación adicionales, conocidos como tipos EAP.
- Incluyen las tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados.



Kerberos

- Es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.
- Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro.
- Los mensajes de autenticación están protegidos para evitar eavesdropping y ataques de Replay .
- Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza.



Referencias

- Bandom LTD. (2003). Guía completa de Protocolos y Telecomunicaciones. España. McGraw Hill.
- Black, U. (1997). Redes de Computadoras, protocolos normas e interfaces. Segunda Edición. México. Alfaomega.
- Fine, L. (1990). Seguridad en centros de cómputo, Trillas.
- Gratton, P. (2004). Administración de la Seguridad Informática, Trillas.
- Halsall, F (1998). Comunicación de datos, redes de computadores y sistemas abiertos. Cuarta Edición. México. Addison Wesley Longman.
- Kuhlmann, F. (2002). Información y Telecomunicaciones. México. Fondo de Cultura Económica.