Nombre de alumno:

Teresa Méndez Pérez

Nombre del profesor:

Mireya del Carmen García Alfonzo

Nombre del trabajo:

Súper nota

Materia:

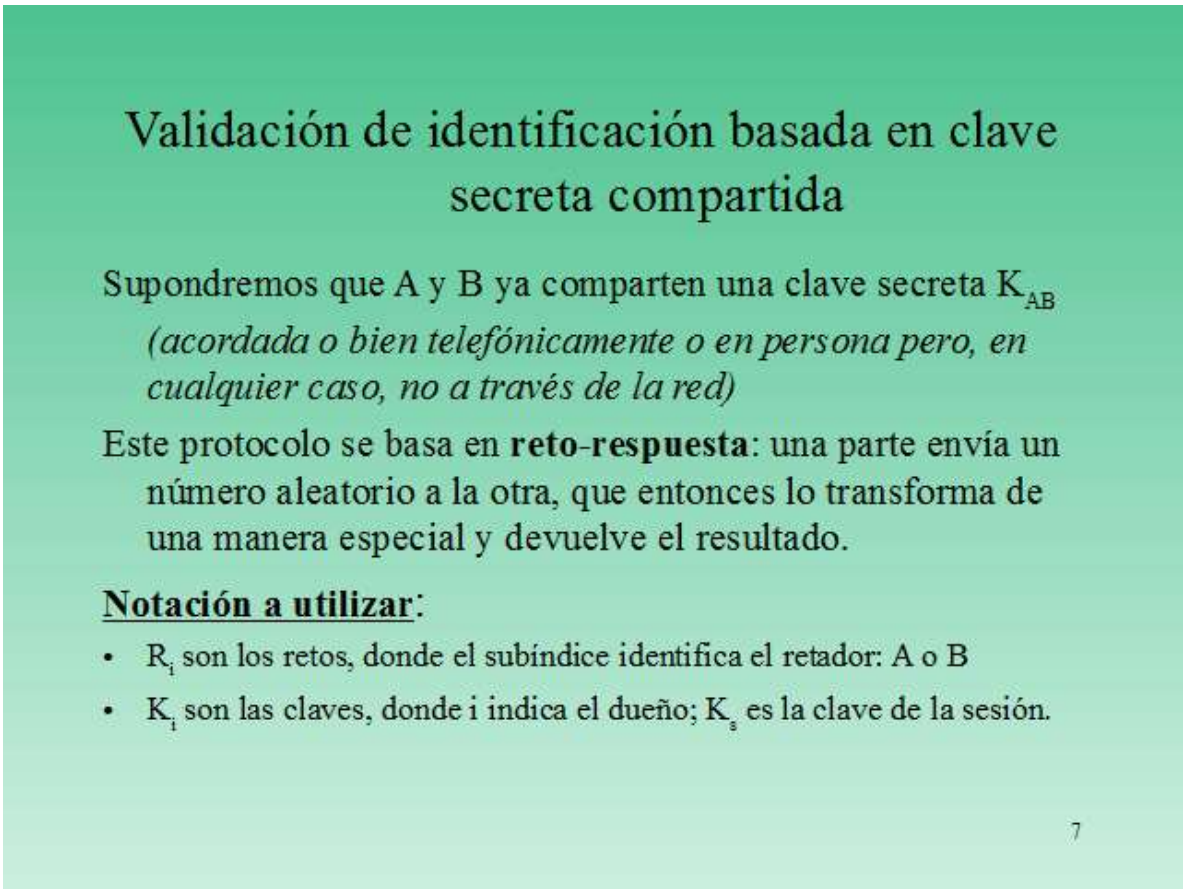
Redes de computadoras III

Grado: 7 cuatrimestre

Comitán de Domínguez Chiapas a 15 de octubre de 2021.

PROTOCOLOS DE AUTENTICIDAD

4.1 AUTENTICACION BASADA EN UNA CLAVE SECRETA COMPARTIDA



Protocolos de autenticación¨

>PAP (protocolo de autenticación de contraseña)

El nombre del usuario y la contraseña se envían por medio de escritorio remoto

No es muy útil utilizar el PAP ya que es fácil de leer

Se utiliza únicamente en servidores UNIX

>SPAP (protocolo de autenticación de contraseña de shiva)

Se envía una contraseña cifrada al servidor

Algoritmo de cifrado bidireccional

El servidor descifra la contraseña

>MS-CHAP Y MS-CHAP v2

MS-CHAP se creó para autentificar trabajos de Windows

Utiliza un mecanismo de desafío y respuesta sin contraseña

El autentificador envía un desafío por un identificador de sesión

MS-CHAPv2 proporciona autentificación mutua

No se admiten métodos más antiguos

>claves secretas compartidas

Se conoce como protocolo de desafio-respuesta

De uso sencillo y no requiere que un cliente lo ejecute

4.2 ESTABLECIMIENTO DE UNA CLAVE COMPARTIDA, EL INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN

>definir dos números primos muy grandes

>cada equipo/entidad debe definir una clave privada

>cada equipo/entidad debe definir una clave publica

>cada equipo/entidad debe intercambiar una clave publica

>las claves de verificación deben de ser iguales entre si

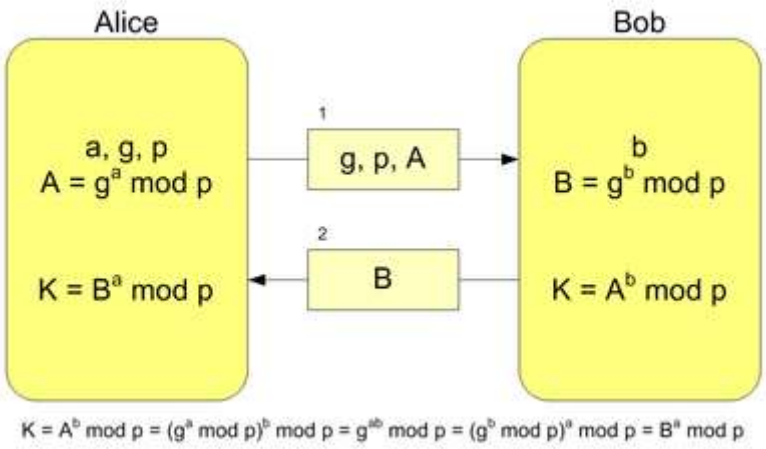
>programación con Socker

Interface de programación de aplicaciones de entorno de red

La programación sincrónica se enfoca en el tiempo

La programación asincrónica en la demanda del servicio

Se aplica en un esquema cliente/servidor



4.3 AUTENTICACION QUE UTILIZA UN CENTRO DE DISTRIBUCIÓN DE CLAVES

En una red con usuarios hay tres enfoques básicos que se pueden utilizar para dar control de acceso;

*no hacer nada

*requerir que el host apruebe su identidad

*requerir que el usuario apruebe su identidad

¿QUE ES Y QUE HACE KERBEROS?

Kerberos es un protocolo que ofrece un servicio de autentificación en arquitecturas cliente-servidor.

Kerberos sabe todas las clavles privadas que se pueden crear

Kerberos provee tres distintos niveles de protección;

*autenticación

*integridad de datos

*privacidad de datos

FUNCIONAMIENTO DE KERBEROS

Todas las claves se generan en el KDC, el cual también genera los billetes asociados y se los envía al cliente y al servidor de recursos a través del cliente.

La secuencia de funcionamiento es la siguiente;

*solicitud de credenciales

*generación de tickets y clave de sesión

*verificador de ticket y generador de autenticado

*concesión de la autorización

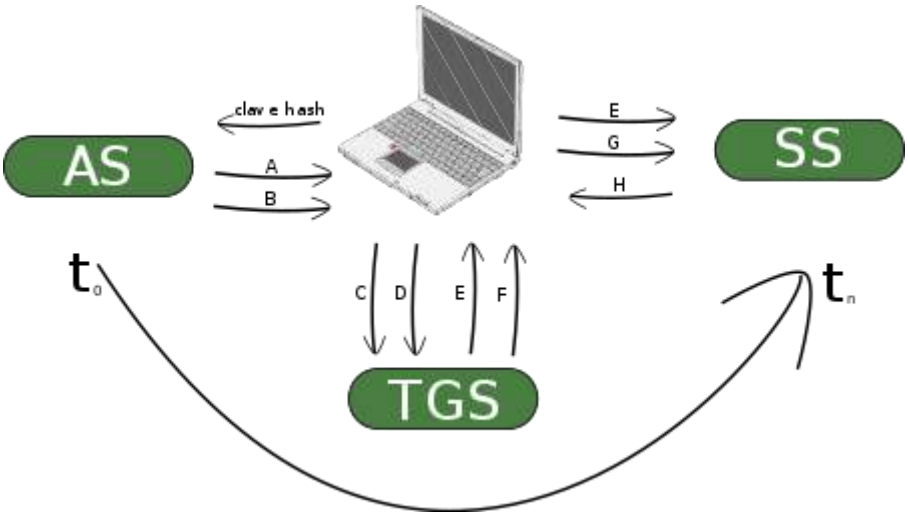
CONCLUSIONES Y FUTURO DE KERBEROS

La consecución de la interoperabilidad en la autentificación no es una tarea sencilla y complica la administración.

El kerberos estándar utiliza claves de 128 bits y no puede exportarse

Kerberos no produce firmas digitales

Se considera que kerberos es un sistema de dominio administrativo y es muy fiable en los sistemas de seguridad basados en la criptografía de clave pública.



4.4 AUTENTICACION UTILIZANDO KERBEROS

Un servidor independiente denominado KDc emite en ticket tras verificar la valides de un inicio de sesión del usuario.

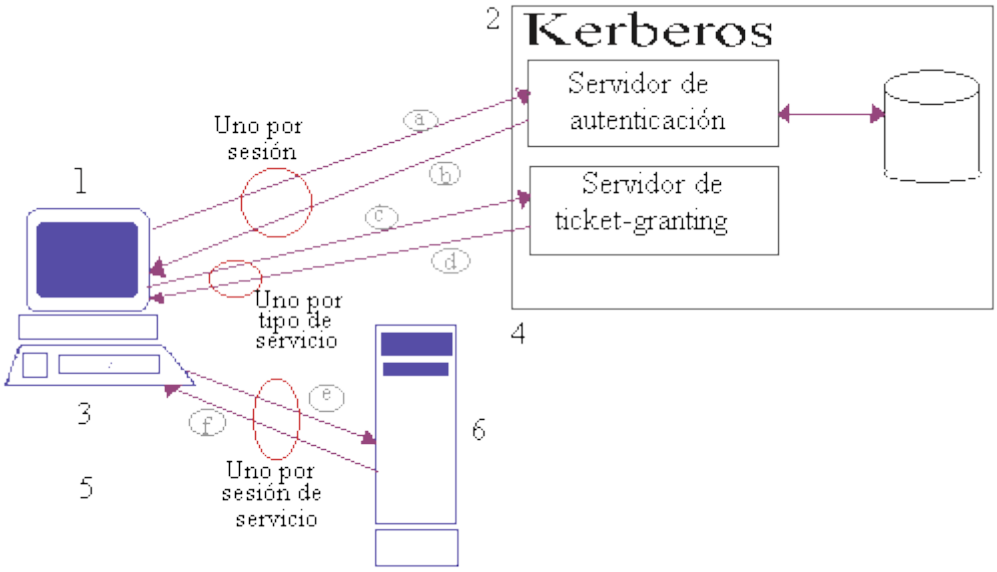
El protocolo kerberos tiene las siguientes características;

*los tickets de servidor existen en la red durante un periodo limitado

*solo el cliente y el servidor pueden descifrar estos tickets

*la entrada del nombre del usuario y contraseña esta limitada a la sesión de inicio de sesión inicial.

La desventaja de esta descentralización es que crea un solo punto de ataque a los piratas informáticos.



4.5 AUTENTICACION UTILIZANDO CRIPTOGRAFIA DE CLAVE PUBLICA

El cifrado de clave pública utiliza un algoritmo matemático con un par de claves pública/privada para cifrar y descifrar datos. Una de estas claves es una clave pública, que puede distribuirse libremente entre los participantes de la comunicación, y la otra es una clave privada, que el propietario de la clave debe guardar en un lugar seguro. Los datos cifrados con la clave privada sólo pueden descifrarse con la clave pública, mientras que los datos cifrados con la clave pública sólo pueden descifrarse con la clave privada.

Cuando se utilizan claves para la autenticación, la parte que se está autenticando crea una firma digital utilizando la clave privada de un par de claves pública/privada. El receptor deberá utilizar la clave pública correspondiente para comprobar la autenticidad de la firma digital. Es decir, el receptor deberá tener una copia de la clave pública de la otra parte y confiar en la autenticidad de dicha clave.

Autenticación SSH
con clave publica y privada