Seguridad: Ejemplos de aplicación

César Llamas Bello

Sistemas Distribuidos – Curso 2003-2004

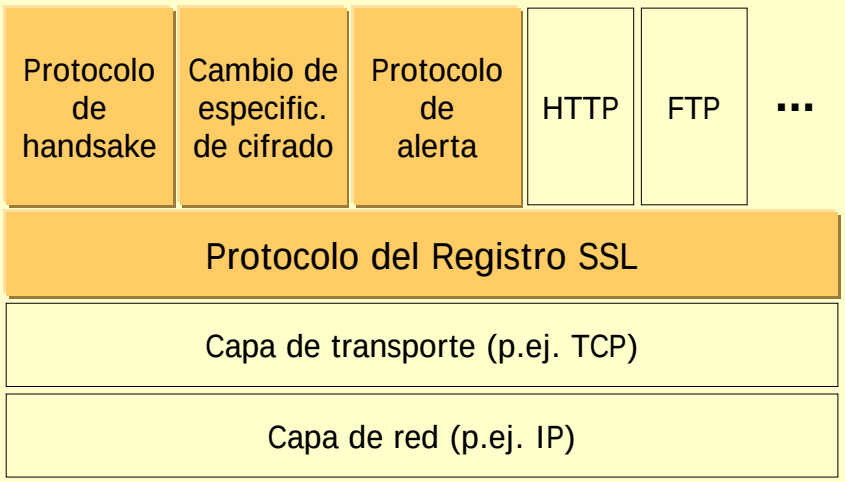
Departamento de Informática de la Universidad de Valladolid

Índice

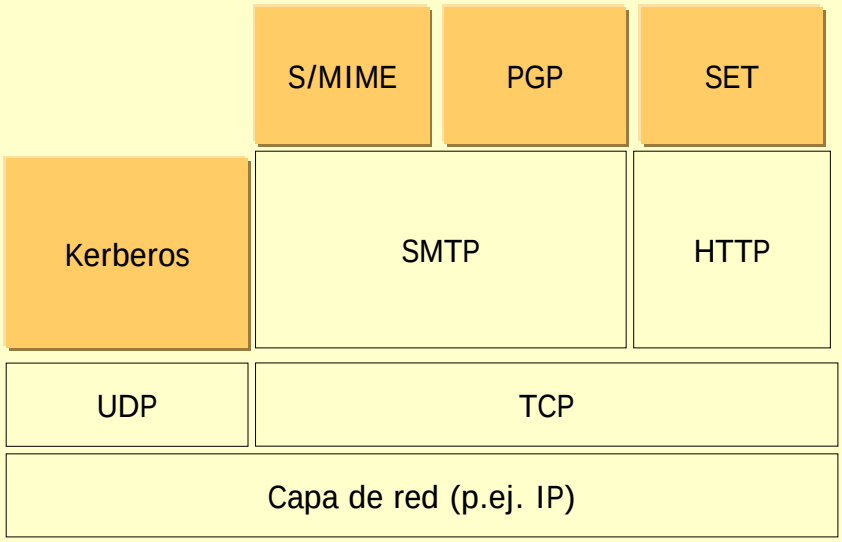
SSL

- Netscape Corporation, 1996.
- Extendida como estándar Internet *TLS* (Transport Layer Security, RFC 2246).
- Da un soporte de transporte
  - Seguro
  - Negociable (para los protocolos)
  - Autoiniciable sin terceraspartes
  - Transparente
- Provee:
  - Autenticación de cliente y servidor
  - Conexión cifrada

Pila de protocolos SSL



Seguridad en el nivel de aplicación



Protocolo de Registro

Datos de la aplicación

stream-block

Unidades de protocolo de registro

compresión

Unidades comprimidas

hash

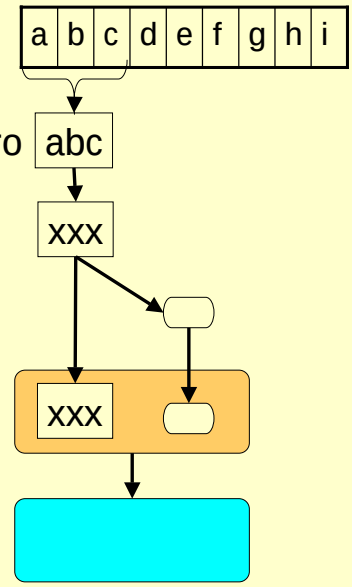
MAC

encriptar

Bloque cifrado

transmitir

Paquete TCP



Protocolo de handsake (saludo)

- Permite:
  - Autenticarse mutuamente entre el cliente y el servidor
  - Acordar los algoritmos de Cifrado y MAC
  - Intercambiar las claves públicas y privadas necesarias

Protocolo de handsake (saludo)

- Fases del protocolo:
  1. Acuerdo sobre: versión del protocolo, suite de cifrado, método de compresión e intercambio de valores aleatorios
  2. Autenticación del servidor (envío del certificado de servidor y petición del de cliente)
  3. Autenticación del cliente (envío de certificado del cliente) e intercambio de clave de sesión
  4. Cierre del saludo: Cambia la suite de cifrado y cierre.
- Suite de cifrado: (RSA, DH ...), (IDEA, 3DES, ...) y (SHA, MD5 ...)

Kerberos

- MIT en los años 80
  - Origen: Autenticación y seguridad de la red de un campus universitario (Athena)
  - Destino: Estándar Internet (además se ofrece en el DCE de OSF, y en Windows 2000)
  - Entorno:
    - Muy heterogéneo: Variedad de plataformas, necesidades de seguridad, administraciones
    - Disperso (administración compleja)
    - Inseguro

Ticket

- Un **ticket** es un testigo que da entrada a un servicio concreto,
  - Durante un tiempo prefijado (sesión)
  - Para un cliente concreto
  - Contiene una clave de sesión para las comunicaciones
  - Y que se encuentra encriptado en estado natural.
- Se emplea con los servicios normales y con los servicios de seguridad.

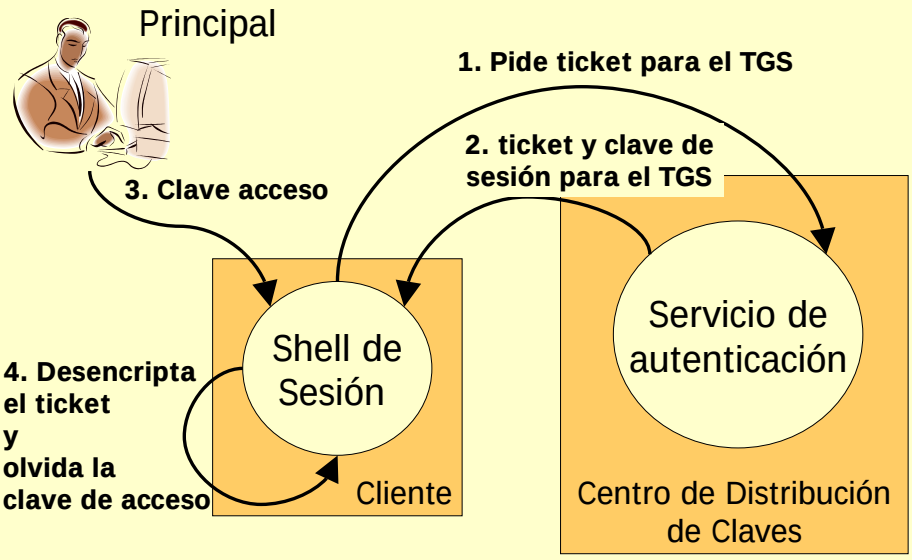
Ocasiones en los tickets

- Una **ocasión** (nounce) es un dato (una especie de número mágico) generado sobre la marcha.
- Demuestra la vigencia del dato al que acompaña.
- En Kerberos se generan ocasiones a partir de la fecha y la hora.

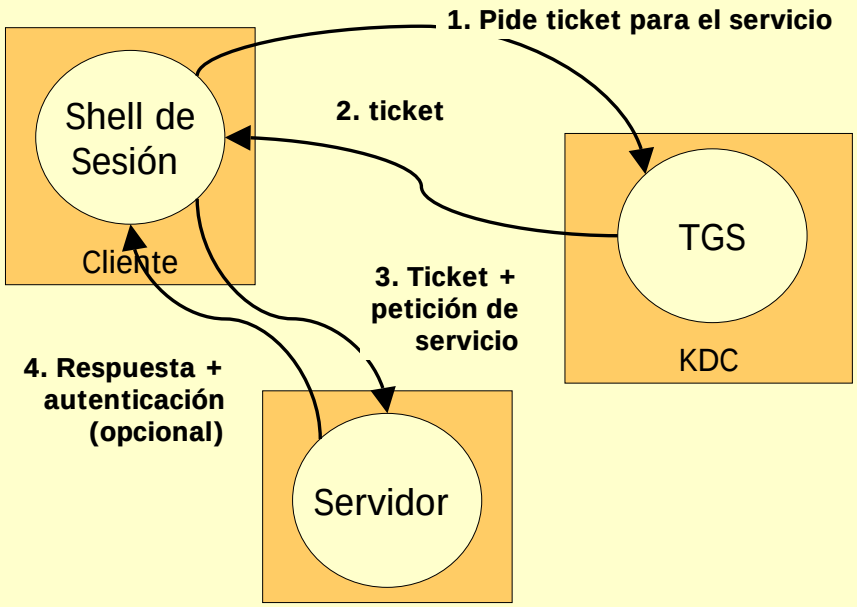
Sistema de Concesión de Tickets

- Los Centros de autenticación de Kerberos contienen:
  - Servicios de autenticación (clientes y servidores)
  - Servicios de concesión de tickets (TGS) que generan tickets para cada sesión de **todo** el sistema
- Pueden organizarse en esferas de seguridad, al modo jerárquico.
  - Existe un único Servicio de Administración de la Base de Datos Kerberos que actúa como maestro.
- Contienen las claves secretas de los clientes y del resto de servidores del sistema que son capaces de autenticar.

Entrada de un cliente en Kerberos



Solicitud de ticketes para servidores



PGP

- Pretty Good Privacy
- Mecanismo para ...
  - La confidencialidad del correo electrónico
  - Firmar y autenticar documentos (con revocación de claves).
  - Almacenar de modo seguro la información.
  - Mantener relaciones de confianza de autenticación entre principales
  - Mantener seguros los conjuntos de claves (keyrings: llaveros o anillos de claves) de un principal.

Versiones de PGP

- Alternativa a PEM (Privacy Enhanced Mail), del IETF
- Primera versión en 1991 (Phillip Zimmerman)
- Aparece la distribución internacional en 1992
- Existen aplicaciones que se integran con la mayoría de los clientes de correo electrónico
- Actualmente existe:
  - Versiones gratuitas y de pago en http://www.philzimmermann.com, www.pgp.com y www.pgpl.com
  - Versiones libres www.gnupg.org
    No usa IDEA pero trae CAST5 y AES
- Vea el estándar OpenPGP (www.openpgp.org)

Algoritmos y suite criptográfica usual de PGP

ZIP	❑ Compresión antes de la transmisión vía Base-64
RSA, DSS, DSA o ElGamal	❑ Generación de claves (diversa longitud) ❑ Intercambio de claves ❑ Firma digital
IDEA, CAST5, AES, 3DES (EDE), Twofish	❑ Cifrado (128 bits) ❑ Transmisión y almacén de datos segura ❑ Almacén de claves.
SHA1, MD5	❑ Firma digital ❑ Clave de almacenamiento de un sentido, Clave=Hash(passfrase)
Conv. Base-64	❑ Armadura ASCII

Mecanismos básicos

- PGP basa su seguridad en la frase de paso (passfrase) que suele ser muy larga y se emplea como clave de un solo sentido junto a MD5
  - Clave inicial = MD5(passfrase) (128 bit)
  - Se usa para la encriptación local y el anillo de claves.
- El anillo de claves almacena las claves y las relaciones de confianza de PGP
  - En dos archivos uno para las claves públicas y otro para las privadas.

Mecanismos básicos

- El anillo de claves públicas guarda las claves públicas de otros usuarios y sobre las que se fija cierto grado de confianza...
  - dado que estas claves nos permiten autenticar al remitente que encripta sus mensajes con su clave privada.
- Existen autoridades que actúan como repositorios de claves (generalmente LDAP), como
  - ldap://certserver.pgp.com
  - http://pgpkeys.mit.edu
- Y autoridades de certificado (CA) (VeriSign, ...)

Anillo de confianza

- Cada clave del anillo es válida
- Podemos importar claves de otros, si vienen firmadas por principales de nuestro anillo,
  - Debemos depositar cierto nivel de confianza en el firmante:
    - Desconocido: no sabemos si es de fiar
    - Ninguno: el firmante no es de fiar
    - Marginal: el firmante merece cierta confianza
    - Completa: el firmante es de toda confianza

Anillo de confianza

- Una clave se considerará válida si:
  - Viene firmada convenientemente:
    - La hemos firmado nosotros, o
    - Ha sido firmada por un firmante de completa confianza
    - Ha sido firmada por tres firmantes de confianza marginal

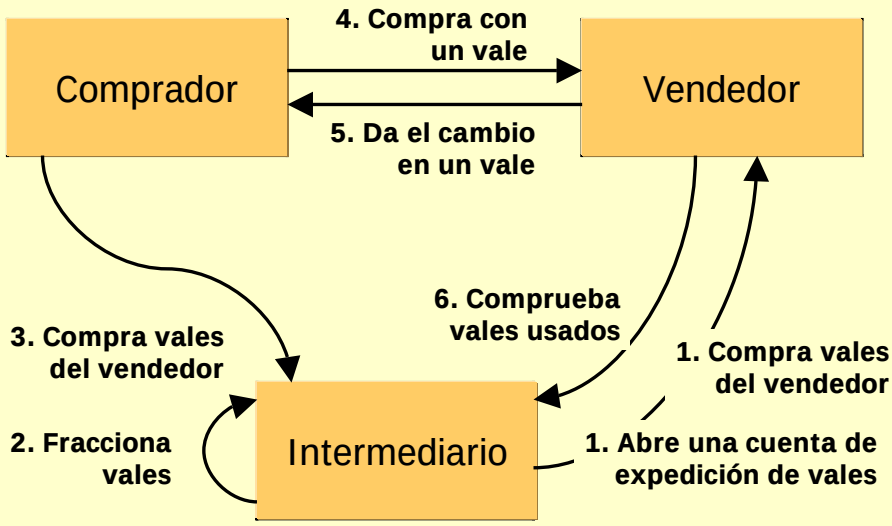
Y

  - La máxima cantidad de relaciones a emplear para establecer la confianza no de más de 5 (pasos)

Millicent (motivación)

- Para pequeñas transacciones ...
  - Debe costar menos que las transferencias y las tarjetas, que tienen un coste muy alto.
  - Sería deseable no tener que abrir cuentas con los proveedores.
  - Debe ser local, sin tener que acumular las transacciones.
  - Caso de generar dinero digital, debe ser infalsificable y eficiente.

Pagos con dinero digital en Millicent



Detalles de Millicent

- El vendedor (o el intermediario) mantienen una clave maestra de generación de firma para cada vale original.
  - Con esta clave se generan las firmas de los vales generados por fraccionamiento.
- El vendedor comprueba la firma de cada vale que se gasta.
- El vendedor cancela los vales:
  - Comprobando que ya han sido gastados.
  - Comprobando la fecha de expiración.
- Al comprar un vale el comprador se autentica frente al vendedor, y puede crear sesiones seguras con él.