



KERBEROS

Manuel Pons Martorell
Departament de Telecomunicacions
Escola Universitària Politècnica de Mataró



Índice

1. Introducción	3
2. Características	4
3. Funcionamiento	5
3.1 Conceptos generales	5
3.2 Autenticación de usuario	6
3.3 Autenticación de servicios.	6
4. Instalación de Kerberos.	8
4.1 Obtención del software	8
4.2 Diseño de Kerberos.	8



1. Introducció

Kerberos es un sistema de control de accesos y autenticación completo inventado por el M.I.T. Las primeras versiones se realizaron para el sistema operativo UNIX pero actualmente se están creando nuevas versiones para otros sistemas operativos.

Sus objetivos son:

- **Exigir autenticación a los usuarios para la utilización del sistema y en particular para cada servicio ofrecido.**
- **Exigir autenticación a los servicios** (software de los servidores).

Este sistema identifica usuario y servicios como objetos, por lo tanto, es independiente de las máquinas y su ubicación física. **Es muy eficiente para conexiones remotas a servicios de uso restringido y permite centralizar la gestión de accesos.**

Existen dos versiones:

- Versión 4. Más utilizada.
- Versión 5. Corrige problemas de seguridad encontrados en la anterior, su estándar es el RFC1510.



2. Características

- Utiliza únicamente **clave simétrica**.
- **Los passwords nunca viajan por la red.**
- Se utiliza **control de accesos** individualizado para **cada servicio**, pero sólo **se introduce el password una vez por sesión**.
- Se puede separar la red en **diferentes dominios** físicos de seguridad.
- Basa el control de accesos en un sistema (hardware y software), llamado **Servidor de Autenticación AS**, diferente de los servidores de información.
- En la versión 4 utiliza el algoritmo DES, en la 5 permite **cualquier algoritmo y cualquier longitud de clave**.

3. Funcionamiento

3.1 Conceptos generales

Intervienen los siguientes elementos:

- **Usuario.**
- **Servidor de servicios.**
- **Servidor de autenticación (SA).**
- **Servidor de concesión de tickets (TGS).**

Aunque estos dos últimos pueden estar físicamente en la misma máquina.

Para que los passwords no viajen por la red se utilizan **tickets** para validar el acceso a los servicios. Estos tickets deben estar en posesión del usuario y enviarse a los servidores para conseguir el acceso. Un ticket es información encriptada con un passwords del sistema que permite el acceso al usuario que lo posee. Siempre tienen una fecha de caducidad para que no puedan ser aprovechados por los espías de la red. Tampoco se guardan passwords ni tickets en las máquinas de los usuarios para evitar a los Hackers que tienen accesos a estas máquinas.

El proceso de autenticación se divide en dos fases y 6 mensajes. La Figura 3.1.1 muestra estas fases.

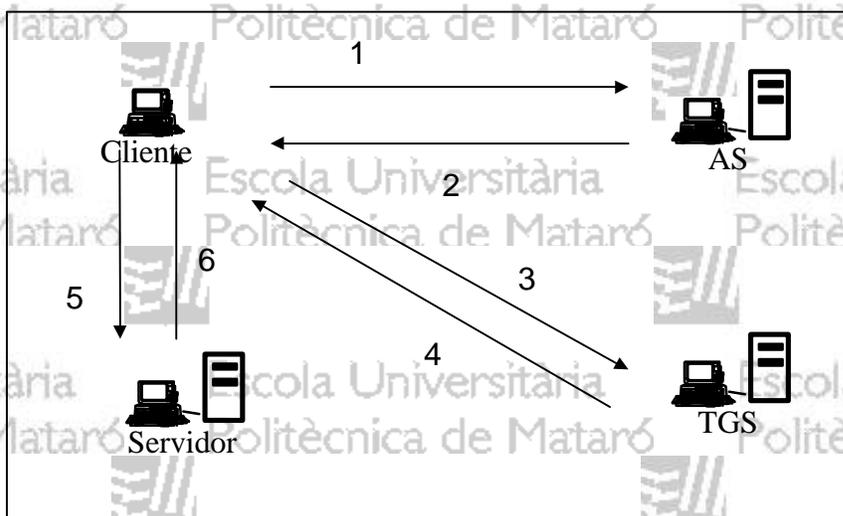


Figura 3.1.1: Proceso de autenticación

Las fases son las siguientes:

1. Autenticación de usuario. Mensajes 1 y 2.



2. Autenticación de servicio. Mensajes 3, 4, 5 y 6.

Al conectarse se debe realizar la autenticación del usuario al sistema Kerberos y después se pueden hacer tantas de servicios como se necesiten conectar, pero sin necesidad de repetir la de usuario.

3.2 Autenticación de usuario

Se autentica el usuario al sistema, **es la única fase del proceso donde se introduce el password**. Esta autenticación sirve para posteriormente acceder al TGS, que concede tickets para los servicios.

El resultado final es la posesión del **TICKET_{TGS}**. Con este ticket se puede pedir autorización en el TGS a tantos servicios como se necesite.

La seguridad se basa en siguientes claves simétricas:

- El password del usuario genera (con un proceso matemático) una clave para encriptar el mensaje 1. El AS posee la misma clave y con ella comprueba la autenticidad del usuario.
- El **TICKET_{TGS}** está encriptado con una clave conocida solamente por el TGS y el AS. Por lo tanto, el usuario no puede generar ni modificar un ticket de este tipo.
- Una clave de sesión generada aleatoriamente para las transmisiones entre TGS y usuario. Se le envía al usuario encriptada con la del password y al TGS dentro del **TICKET_{TGS}**. Ninguna de las partes la puede modificar.

El resultado final es el Ticket para el usuario, que no se puede modificar y tiene una fecha de caducidad, y posteriormente el TGS lo reconocerá como auténtico. También se recibe la clave de sesión a utilizar con el TGS. Si alguien captura el Ticket en la línea no lo puede utilizar con el TGS ya que no conoce su clave de sesión, está viene para el usuario encriptada con el password.

Al acabar esta fase se destruye el password de usuario. El **TICKET_{TGS}** se puede utilizar para pedir autorización a varios servicios mientras no caduque, sin necesidad de volver a acceder al AS ni introducir el password.

3.3 Autenticación de servicios.

El usuario pide al TGS el **TICKET_{SERVICIO X}** para autenticarse delante del servicio X, también para comprobar la identidad de éste. Este proceso se realiza tantas veces como servicios distintos quiera utilizar el usuario, pero nunca vuelve a introducir el password.



La seguridad se basa en siguientes claves simétricas:

- La clave de sesión mencionada en el capítulo 3.2.
- El $TICKET_{SERVICIO X}$ está encriptado con una clave conocida por el servicio X y el TGS.
- Una clave de sesión para utilizar en las comunicaciones entre el servicio y el usuario. La conoce el usuario porque llega encriptada con la clave de sesión actual y el servicio porque está en el Ticket. Ninguna de las partes la puede modificar.

El resultado es la obtención del $TICKET_{SERVICIO X}$ y una clave para la sesión con el servicio. Si alguien captura el Ticket en la línea no lo puede utilizar ya que desconoce la clave de sesión.

El servicio se identifica utilizando la clave de sesión. Si es falso no podrá desencriptar el Ticket y, por lo tanto, no tendrá la clave de sesión.

4. Instalación de Kerberos.

4.1 Obtención del software

Se puede conseguir gratis por Internet. Estas versiones no disponen de servicio técnico, actualizaciones, instalación, ni formación, por lo tanto, sólo es aconsejable para pequeñas empresas. **Existen muchas versiones comerciales** de Kerberos con soporte técnico y formación a precios muy razonables.

A parte de comprar el software de cliente, el AS y el TGS **se deben adaptar las aplicaciones cliente/servidor (los servicios) al entorno Kerberos.** Esto puede suponer un aumento considerable de los costes de la instalación de este sistema y es muy importante tenerlo en cuenta. Existen herramientas de programación para Kerberos, como GSS-API, útiles para adaptar el software y mantenerlo actualizado a los cambios en sistemas de autenticación.

4.2 Diseño de Kerberos.

Sobre el papel, este sistema **es el mejor entorno actual para seguridad de accesos y autenticación.** Pero antes de instalarlo en una empresa se debe tener en cuenta los siguientes factores:

- 1. Debe formar parte de un plan de seguridad.** Instalar Kerberos no supone resolver los problemas de seguridad. Un sistema Kerberos en una red sin seguridad es como **un muro de papel con una puerta de acero.**
- 2. Como mínimo necesita una máquina adicional para el AS y el TGS** que esté comunicada con todos los servicios **y otra para Backup,** porque la caída de la primera significaría la denegación de todos los servicios de la red. Estas máquinas **deben ser potentes** ya que todos los accesos pasan por ellas.
- 3. La red debe ser rápida** porque el sistema Kerberos genera muchos mensajes adicionales y se puede colapsar.
- Supone **gastos adicionales de personal** para el mantenimiento del sistema.
- Como se comenta en capítulo 4.1, se **debe adaptar a Kerberos todo el software** que presta servicios con seguridad.
- 6. Asegurar la compatibilidad con los nuevos sistemas de autenticación** que surgirán en los próximos años. Si el sistema Kerberos es incompatible con otros servicios pronto se quedará aislado de la red Internet.
- 7. Necesita sincronización de todos los relojes de la red.**



Por lo tanto, la instalación de Kerberos debe salir de un estudio muy cuidadoso del estado de la red y las necesidades de la empresa.

