Curso avanzado de GNU/Linux

Introducción a Kerberos

Rafael Varela Pet

Unidad de Sistemas
Área de Tecnologías de la Información y Comunicaciones
Universidad de Santiago de Compostela

¿Qué es Kerberos?

- Es un protocolo de autenticación de red
- Usa criptografía de clave privada
- Permite:
  - Al cliente probar su identidad ante un servidor
  - Al servidor probar su identidad frente a los clientes
  - Una vez autenticados, cifrar la comunicación
- Versión actual: Kerberos v5

Autenticación

- Cliente y servidor comparten una clave (secreto compartido)
  - El secreto nunca viaja por la red
  - Se usa para cifrar mensajes
- Se emplea un servicio dedicado a la autenticación (AS-*Authentication Server*)
- Los clientes, los servicios y el AS comparten unas claves de larga duración para poder comunicarse

Autenticación

- El usuario pide al AS autenticarse frente a un servicio
- El AS genera un nuevo secreto aleatorio (**clave de sesión**) y envía al usuario un mensaje con 2 partes:
  - [clave aleatoria + nombre servicio] (CREDENCIALES) cifrado con la clave de usuario
  - [clave aleatoria + nombre de usuario] (TICKET) cifrado con la clave del servicio
- El cliente envía al servicio el **autenticador** (una estampa de tiempo cifrada con la clave aleatoria) y el **ticket**
- El servicio descifra el ticket para obtener la clave aleatoria, con la que puede descifrar el autenticador

Ticket Granting Server (TGS)

- Permite usar claves desechables de corta duración
- El cliente pide un ticket al AS para hablar con el TGS
  - Las respuestas se cifran con la clave de larga duración
  - Se le conoce con el nombre de TGT (*Ticket Granting Ticket*)
- Cada vez que el cliente quiere acceder a un servicio, emplea el TGT para pedir un nuevo ticket al TGS
- Las respuestas se cifran con la clave de sesión del TGT
- AS + TGS = *Key Distribution Center* (KDC)

Principals

- Entidades a las que se les puede asignar tickets
- Formato
  - kerberos v4: nombre.instancia@realm
  - kerberos v5:
    componente/componente/componente@realm
- Los *realms* Kerberos tienen una estructura similar a los dominios DNS, pero no son lo mismo
- Lo normal es que coincida nuestro dominio DNS con el *realm* Kerberos
- Los *realm* se denotan en mayúsculas

Principals

- Ejemplos:
  - principal sin instancia. Usado con usuarios:
    - rafael.varela@USC.ES
  - principal con instancia:
    - host/foo.bar.org@BAR.ORG
    - rafael.varela/administrador@USC.ES
  - principal con una instancia que no es un host
    - krbtgt/USC.ES@USC.ES

Referencias

- http://web.mit.edu/kerberos/www/