Kerberos

De Wikipedia, la enciclopedia libre

Kerberos es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores 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. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

Índice

Etimología

El nombre se deriva del Cerbero (griego antiguo Κέρβερος *Kérberos*, 'demonio del pozo'), el perro guardando la puerta del reino de Hades en la mitología griega.

Descripción

Kerberos se basa en el Protocolo de Needham-Schroeder. Usa un tercero de confianza, denominado "centro de distribución de claves" (KDC, por sus siglas en inglés: *Key Distribution Center*), el cual consiste de dos partes lógicas separadas: un "servidor de autenticación" (AS o *Authentication Server*) y un "servidor emisor de tiquets" (TGS o *Ticket Granting Server*). Kerberos trabaja sobre la base de "tickets", los cuales sirven para demostrar la identidad de los usuarios.

Kerberos mantiene una base de datos de claves secretas; cada entidad en la red —sea cliente o servidor— comparte una clave secreta conocida únicamente por él y Kerberos. El conocimiento de esta clave sirve para probar la identidad de la entidad. Para una comunicación entre dos entidades, Kerberos genera una clave de sesión, la cual pueden usar para asegurar sus problemas.

Motivación

Internet no es un lugar seguro. Muchos de los protocolos usados en Internet no proporcionan características de seguridad. Es habitual que piratas informáticos maliciosos empleen herramientas para rastrear y conseguir contraseñas de la red. Por lo tanto, las aplicaciones que envían una contraseña no cifrada por la red son sumamente vulnerables. Peor aún, algunas aplicaciones de cliente/servidor dependen de la honestidad del usuario que las está usando acerca de su identidad.

Algunos sitios intentan solucionar los problemas de seguridad de la red con cortafuegos. Desafortunadamente, el uso exclusivo de cortafuegos se basa en la suposición de que los "villanos" están en el exterior, lo que es a menudo una suposición incorrecta y peligrosa. Un buen número de los más graves delitos informáticos son ejecutados desde dentro de la propia corporación atacada. Los cortafuegos también adolecen de una desventaja importante, ya que restringen cómo pueden usar Internet los usuarios de la red por ellos protegida. Después de todo, los cortafuegos son sólo un ejemplo menos extremista del dictamen de que no hay nada más seguro que una computadora que está desconectada de la red. Pero en muchos casos, estas restricciones son simplemente imposibles de asumir.

Kerberos fue creado por el MIT como una solución para estos problemas de seguridad de la red. El protocolo de Kerberos usa una criptografía fuerte con el propósito de que un cliente pueda demostrar su identidad a un servidor (y viceversa) a través de una conexión de red insegura. Después de que un cliente/servidor han conseguido a través de Kerberos demostrar su identidad, también pueden cifrar todas sus comunicaciones para garantizar la privacidad y la integridad de los datos intercambiados.

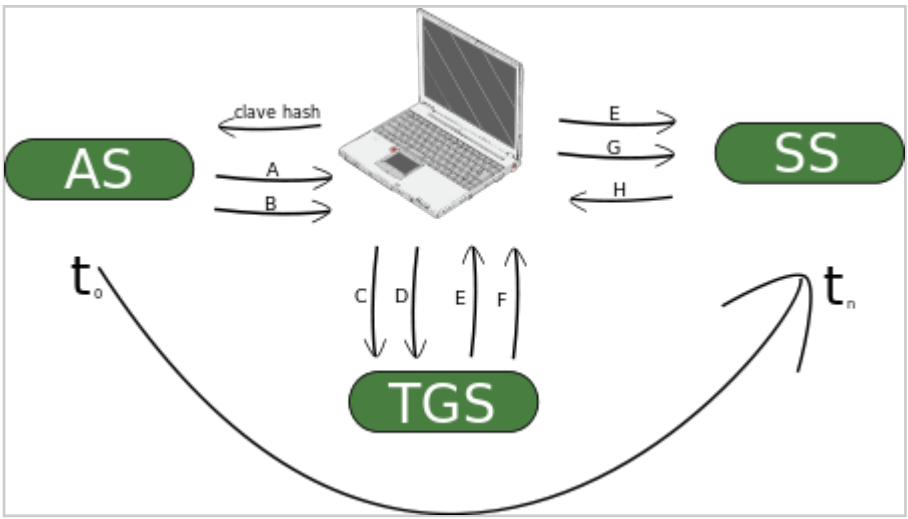
Kerberos está disponible gratuitamente en el MIT, bajo permisos de derechos de autor muy similares a aquellos que usaron para el sistema operativo de BSD y el X Window System. El MIT provee el código fuente de Kerberos con el propósito de que quienquiera que desee usarlo pueda estudiar el código y así asegurarse de que el código es digno de confianza. Además, para aquellos que prefieren depender de un producto con un soporte profesional, Kerberos está disponible a través de muchos distribuidores diferentes como producto comercial.

En resumen, Kerberos es una solución para ciertos problemas de seguridad de la red. Provee las herramientas de autenticación y criptografía reforzada a través de la red para ayudar a asegurar que los sistemas de información de una empresa o corporación estén bien resguardados.

Cómo funciona

A continuación se describe someramente el protocolo. Se usaran las siguientes abreviaturas:

- AS = Authentication Server
- TGS = Ticket Granting Server
- SS = Service Server



Funcionamiento de Kerberos.

En resumen el funcionamiento es el siguiente: el cliente se autentica a sí mismo contra el AS, así demuestra al TGS que está autorizado para recibir un ticket de servicio (y lo recibe) y ya puede demostrar al SS que ha sido aprobado para hacer uso del servicio kerberizado.

En más detalle:

1. Un usuario introduce su nombre de usuario y password en el cliente
2. El cliente genera una clave hash a partir del password y la usará como la clave secreta del cliente.
3. El cliente envía un mensaje en texto plano al AS solicitando servicio en nombre del usuario. Nota: ni la clave secreta ni el password son enviados, solo la petición del servicio.
4. El AS comprueba si el cliente está en su base de datos. Si es así, el AS genera la clave secreta utilizando la función hash con la password del cliente encontrada en su base de datos. Entonces envía dos mensajes al cliente:
    1. Mensaje A: Client/TGS session key cifrada usando la clave secreta del usuario
    2. Mensaje B: Ticket-Granting Ticket (que incluye el ID de cliente, la dirección de red del cliente, el período de validez y el Client/TGS session key) cifrado en primer lugar con la clave secreta del TGS y después con la clave secreta del usuario.
5. Una vez que el cliente ha recibido los mensajes, descifra el mensaje A para obtener el client/TGS session key. Esta session key se usa para las posteriores comunicaciones con el TGS. (El cliente descifra parcialmente el mensaje B con su clave secreta para obtener el TGT, pero no puede descifrar el TGT en sí puesto que se encuentra cifrado con la clave secreta del TGS). En este momento el cliente ya se puede autenticar contra el TGS.
6. Entonces el cliente envía los siguientes mensajes al TGS:
    1. Mensaje C: Compuesto del Ticket-Granting Ticket del mensaje B y el ID del servicio solicitado.
    2. Mensaje D: Autenticador (compuesto por el ID de cliente y una marca de tiempo), cifrado usando el client/TGS session key.

7. Cuando recibe los mensajes anteriores, el TGS descifra el mensaje D (autenticador) usando el client/TGS session key y envía los siguientes mensajes al cliente:
    1. Mensaje E: Client-to-server ticket (que incluye el ID de cliente, la dirección de red del cliente, el período de validez y una Client/Server session key) cifrado usando la clave secreta del servicio.
    2. Mensaje F: Client/server session key cifrada usando el client/TGS session key.
8. Cuando el cliente recibe los mensajes E y F, ya tiene suficiente información para autenticarse contra el SS. El cliente se conecta al SS y envía los siguientes mensajes:
    1. Mensaje E del paso anterior.
    2. Mensaje G: un nuevo Autenticador que incluye el ID de cliente, una marca de tiempo y que está cifrado usando el client/server session key.
9. El SS descifra el ticket usando su propia clave secreta y envía el siguiente mensaje al cliente para confirmar su identidad:
    1. Mensaje H: la marca de tiempo encontrada en el último Autenticador recibido del cliente más uno, cifrado el client/server session key.
10. El cliente descifra la confirmación usando el client/server session key y chequea si la marca de tiempo está correctamente actualizada. Si esto es así, el cliente confiará en el servidor y podrá comenzar a usar el servicio que este ofrece.
11. El servidor provee del servicio al cliente.

Véase también

- Proyecto Athena

Enlaces externos

- Página del proyecto Kerberos en el MIT (http://web.mit.edu/kerberos/) (en inglés)
- Heimdal Kerberos (http://www.pdc.kth.se/heimdal/) (en inglés)