

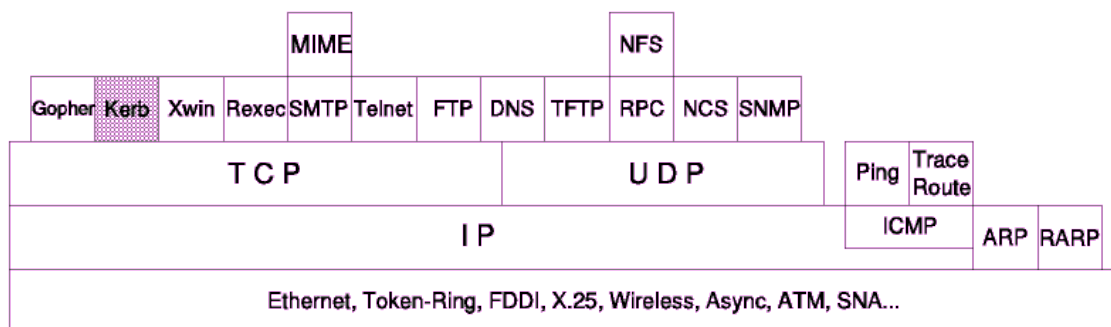
Autenticación Kerberos

Tabla de Contenidos

5. Accesos autenticación. Kerberos.....	2
Supuestos.....	3
Nombres.....	3
Proceso de autenticación en Kerberos.....	4
Resumamos los puntos centrales de este esquema:	8
Administración de la base de datos de Kerberos	8
Modelo de autorización de Kerberos	9
Mejoras de la versión 5 de Kerberos.....	9



5. Accesos autenticación. Kerberos.



El sistema de autenticación y autorización Kerberos.

Según el Gran Diccionario del Diablo("Enlarged Devil's Dictionary(Ambrose Bierce)"), Cerbero es "el perro guardián del Hades, cuyo deber era guardar la entrada del infierno; se sabe que Cerbero tenía tres cabezas".

El sistema de autenticación y autorización Kerberos es un sistema de seguridad basado en la encriptación que proporcionar autenticación mutua entre usuarios y servidores en un entorno de red. Las metas asumidas por este sistema son:

Autenticación para evitar solicitudes/respuestas fraudulentas entre servidores y usuarios que deben tener índole confidencial y en grupos de al menos un usuario y un servicio.

Cada servicio que desee proporcionar su propio sistema de autorización puede implementarlo independientemente de la autenticación. El sistema de autorización puede asumir que el sistema de autenticación usuario/cliente es fiable.

Permitir la implementación de un sistema de contabilidad que esté integrado y sea seguro y fiable, con estructura modular y soporte para facturación

El sistema Kerberos se usa principalmente con propósitos de autenticación, aunque también aporta la flexibilidad necesaria para añadir información de auto.

Las versiones actual del protocolo Kerberos son las 4 y 5. La versión 4 tiene un amplio uso y es la que se suele implementar en productos comerciales. La versión 5 está propuesta actualmente como borrador de Internet. Se basa

en la versión 4 e incorpora cierto número de mejoras y nuevas características.

Supuestos

Kerberos da por hecho lo siguiente:

- El entorno que lo usará incluirá: estaciones de trabajo públicas y privadas que estarán localizadas en áreas con seguridad física mínima; una red universitaria sin encriptación de los enlaces que puede estar compuesta de redes locales dispersas conectadas por troncales o pasarelas; servidores operados de modo centralizado en habitaciones cerradas con seguridad física moderada o alta.
- Los datos confidenciales o las operaciones de alto riesgo tales como transacciones bancarias no pueden formar parte de este entorno sin seguridad adicional, ya que una vez que tienes una estación de trabajo como terminal puedes emular ciertas condiciones y los datos normales fluirán sin ningún tipo de protección por encriptación.
- Uno de los sistemas de encriptación utilizados es el DES("Data Encryption Standard"), que está disponible en el mercado de U.S pero no puede ser exportado sin una licencia oficial de exportación, por lo que los diseñadores de Kerberos lo han desarrollado para que sea modular y admita recambios o sustituciones.
- Kerberos asume la existencia de un reloj débilmente sincronizado en todo el sistema así que la estación de trabajo dispone de una herramienta de sincronización como la que le suministre el servidor de sincronización ("Time server").

Nombres

Un Identificador Principal es el nombre que define un cliente o un servicio en el sistema Kerberos.

En la versión 4, el identificador consta de tres componentes:

- El nombre principal es único para cada cliente y servicio asignado por el Manager o Administrados de Kerberos.
- El nombre de instancia, usado para la autenticación es una etiqueta añadida para clientes y servicios que existe bajo diversas formas. Para usuarios, una instancia puede proporcionar diferentes instancias para máquinas diferentes. Para servicios, una instancia suele especificar el nombre del host en la máquina que proporciona el servicio.
- El nombre de reino, usado para permitir sitios administrados independientemente con Kerberos. El nombre principal y el de instancia son calificados por el del reino al que pertenecen, y son únicos sólo dentro de ese reino. El reino es habitualmente el nombre del dominio.

En la versión 4, cada uno de estos componentes tiene un límite de longitud de 39 caracteres. Debido a convenios, (.) no es un carácter aceptado.

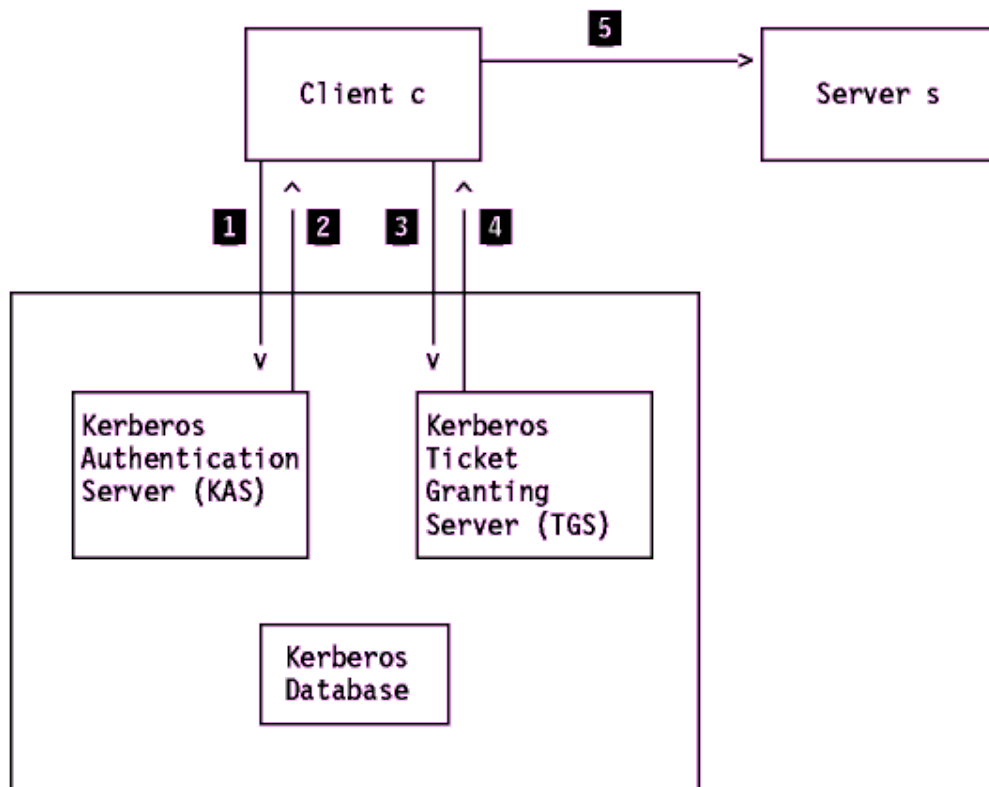
En la versión 5, el identificador consta sólo de dos partes, el reino y el resto, que es una secuencia de cuantos componentes sean necesarios para determinar al principal. Tanto el reino como cada componente del resto se definen como Ristras Genéricas("GeneralStrings") de ASN.1("Abstract Syntax Notation One", estándar ISO 8824), lo que supone pocas restricciones para los caracteres disponibles para los identificadores principales.

Proceso de autenticación en Kerberos

En el sistema Kerberos, el cliente que desea contactar con un servidor para que le dé un servicio, debe pedir primero un ticket de una tercera parte de mutua confianza, el KAS("Kerberos Authentication Server"). Este ticket se obtiene como una función en la que uno de los componentes es una llave privada conocida sólo por el servicio y el KAS, de modo que el servicio puede estar seguro de que el ticket procede sólo de Kerberos. El KAS conoce al cliente por su nombre principal(c). La llave privada(K(c)) es la llave de autenticación conocida sólo por el usuario y el KAS.

En este capítulo, el símbolo {X,Y} indica un aje que contiene información o datos X e Y. {X,Y}K(z) indica que un mensaje que contiene los datos X e Y ha sido cifrado usando la llave k(z).





```

1 Client → KAS: c, tgs, n
2 KAS → Client: {Kc,tgs, n}Kc, {Tc,tgs}Ktgs
3 Client → TGS: {Ac}Kc,tgs, {Tc,tgs}Ktgs, s, n
4 TGS → Client: {Kc,s, n}Kc,tgs, {Tc,s}Ks
5 Client → Server: {Acn}Kc,s, {Tc,s}Ks

```

In Kerberos Version 4:

```

message 2 was: KAS → Client: {Kc,tgs, n, {Tc,tgs}Ktgs}Kc
message 4 was: TGS → Client: {Kc,s, n, {Tc,s}Ks}Kc,tgs

```

Esquema de autenticación de Kerberos.

1 Cliente -> KAS

El cliente envía un mensaje {c, tgs, n}, al KAS, que contiene su identidad(c), un una palabra temporal o "nonce"(un sello de tiempo u otro forma de identificar su solicitud), y solicita un ticket para usarlo con el servidor de tickets(TGS).

2 KAS -> Cliente

El servidor de autenticación busca el nombre del cliente(c) y el nombre del servicio(TGS, el servidor de tickets) en la base de datos de Kerberos, y obtiene una llave de encriptación para cada uno de ellos K(c) y K(TGS).

El KAS crea a continuación una respuesta para enviársela al cliente. Esta respuesta contiene un ticket inicial T(c, TGS) que garantiza al cliente acceso al servidor solicitado(el TGS). T(c, TGS) contiene k(c.TGS), c, TGS, el "nonce", el tiempo de vida y otra información. El KAS también genera una llave aleatoria de encriptación K(c, TGS), llamada llave de sesión. Luego encripta este ticket usando la llave de encriptación del TGS(K(TGS)). Este procedimiento es lo que se denomina un ticket sellado $\{T(c, tgs)\}K(tgs)$. Inmediatamente se crea un mensaje consistente en el ticket sellado y la llave de sesión de TGS K(c, TGS).

Nota: En la versión 4 de Kerberos, el mensaje es:

$\{K(c, tgs), n, \{T(c, tgs)\}K(tgs)\}K(c)$

, mientras que en la 5 el mensaje tiene una forma más simple:

$\{K(c, tgs), n\}K(c), \{T(c, tgs)\}K(tgs)$

Esto simplifica la doble encriptación(innecesaria) del ticket.

3 Cliente -> TGS

A la recepción del mensaje, el cliente lo desencripta usando su llave secreta K(c) que es la única que él y el KAS conocen. Comprueba que el "nonce" (n) coincide con la solicitud específica, y entonces guarda la llave de sesión K(c, tgs) para futuras comunicaciones con el TGS.

El cliente envía a continuación un mensaje al YGS. Este mensaje contiene el ticket inicial $\{T(c, tgs)\}K(tgs)$, el nombre del servidor(s), un "nonce", y un nuevo autenticador A(c) que lleva un sello de tiempo. A(c) es {c, nonce}. El mensaje es:

$\{A(c)\}K(c, tgs), \{T(c, TGS)\}K(TGS), s, n$

4 TGS -> Cliente

El TGS recibe el mensaje anterior del cliente(c), y descifra primero el ticket sellado usando su llave de encriptación TGS(este ticket fue sellado originalmente por el KAS en el paso 2 usando la misma llave). El TGS obtiene la llave de sesión para TGS de del ticket descifrado, y la emplea a su vez para descifrar el autenticador sellado (la validez se chequea comparando el nombre del cliente tanto en el ticket como en el autenticador, el nombre del servidor TGS que figura en el ticket, la dirección de red que debe ser igual en el ticket, en el autenticador y en el mensaje recibido). Finalmente, chequea la hora actual en el autenticador para cerciorarse de que el mensaje es

reciente. Esto requiere que todos los clientes y servidores matengan sus relojes dentro de cierto margen prescrito de tolerancia. Ahora el TGS busca el nombre del servidor que aparece en el mensaje en la base de datos de Kerberos, y obtiene la llave de encriptación($K(s)$) para el servicio especificado.

El TGS crea una nueva llave aleatoria de sesión $K(c,s)$ para el cliente(c) y el servidor, para generar a continuación un nuevo ticket. $T(c,s)$ que contiene:

$K(c,s)$, n , "nonce", tiempo de vida

Luego ensambla un mensaje y lo envía al cliente.

Nota: En la versión 4 de Kerberos Version, el mensaje es:

$\{K(c,s), n, \{T(c,s)\}K(s)\}K(c, tgs)$

En la versión 5 el mensaje tiene una forma más simple:

$\{K(c,s), n\}K(c, tgs), \{T(c,s)\}K(s)$

Esto simplifica la doble encriptación(innecesaria) del ticket.

5 Cliente -> Servidor

El cliente recibe este mensaje y lo descifra usando la llave de sesión para el TGS que sólo comparten él y el TGS. De este mensaje calcula una nueva llave de sesión $K(c,s)$ que comparte con el servidor(s) y un ticket sellado que no puede descifrar porque está cifrado con la llave secreta del servidor $K(s)$.

El cliente construye un autenticador y lo sella con la nueva llave de sesión $K(c,s)$. Por último, envía un mensaje que contiene el ticket sellado y el autenticador al servidor(s) para solicitar su servicio.

El servidor(s) recibe este mensaje y descifra primero el ticket sellado con su llave de encriptación, conocida sólo por él y el KAS. Luego usa la nueva llave de sesión contenida en el ticket para descifrar el autenticador y realiza el mismo proceso de validación que el descrito en el paso 4.

Una vez que el servidor ha validado a un cliente, el cliente tiene la opción de validar a su vez al servidor. Esto evita que un intruso suplante al servidor. El cliente requiere que el servidor le devuelva un mensaje con el sello de tiempo(procedente del autenticador del cliente, incrementado en uno). Este mensaje se cifra con la llave de sesión que pasó del cliente al servidor.

Resumamos los puntos centrales de este esquema:

1. Con el fin de que la estación de trabajo emplee cualquier servidor, se requiere un ticket. Todos los tickets, a excepción del primero(también llamado ticket inicial) se obtienen del TGS. El primer ticket es especial: es un ticket para el propio TGS y se obtiene del KAS.
2. Cada ticket está asociado con una llave de sesión que se asigna cada vez que se concede un ticket.
3. Los tickets son reutilizables. Cada ticket tiene un tiempo de vida, típicamente de ocho horas. Después de que un ticket ha expirado, el usuario ha de identificarse de nuevo al Kerberos, introduciendo el nombre de usuario y el password.
4. A diferencia de un ticket, que puede ser reutilizado, hace falta un nuevo autenticador cada vez que el cliente inicia una conexión con el servidor. El autenticador contiene un sello de tiempo que expira a los pocos minutos de haber sido expedido(esta es la razón por la que los relojes de clientes y servidores deben estar sincronizados).

Un servidor debería mantener un seguimiento de las solicitudes anteriores de los clientes para las que el sello de tiempo en el identificador es aún válido. De este modo el servidor puede rechazar solicitudes duplicadas que podrían surgir de un ticket y un identificador robados.

Administración de la base de datos de Kerberos

Kerberos necesita un registro para cada usuario y servicio de su reino y cada registro sólo contiene la información necesaria, que es la siguiente:

- Identificador principal(c,s)
- Llave privada para el identificador principal(K(c),K(s))
- Fecha de expiración de la identidad
- Fecha de la última modificación del registro
- Identidad de la persona que modificó por última vez el registro(c,s)
- Tiempo de vida de los tickets concedidos al identificador principal
- Atributos(no usado)
- Implementación de datos(no visible externamente)

El campo de llave privada se cifra con una llave maestra de forma que la eliminación de la base de datos no causará ningún problema puesto que la llave maestra no está en ella.

La entidad responsable de gestionar la base de datos es el KDBM("Kerberos Database Manager"). Sólo hay un KDBM en un reino, pero es posible tener más de un KKDS("Kerberos Key Distribution Server"), cada uno con una copia de la base de datos de Kerberos. Esto se hace para mejorar la disponibilidad y el rendimiento de modo que el usuario pueda elegir de entre un grupo de KKDSs a cuál enviar su petición. El KKDS efectúa sólo operaciones de lectura, dejando la actualización al KDBM, que copia toda la base de datos unas cuantas veces al día. Así se simplifica la operación al usar

un protocolo protegido de Kerberos. Este protocolo es básicamente una autenticación mutua entre el KDBM Y EL KDDS seguida de una operación de transferencia de dichos con campos de checksum y checkpoint.

Modelo de autorización de Kerberos

El modelo de autenticación de Kerberos sólo permite al servicio verificar la identidad del solicitante pero no da información de si éste puede usar o no el servicio. El lema de autorización de Kerberos se basa en el principio de que cada servicio conoce al usuario de modo que puede mantener su propia información de autorización. Sin embargo, el sistema de autenticación de Kerberos se podría extender con información y algoritmos que servirían para propósitos de autorización. (Esto es más fácil en la versión 5. Ver la siguiente sección). El Kerberos podría chequear entonces si un usuario/cliente está autorizado a usar cierto servicio.

Obviamente, tanto la aplicación del cliente como la del servidor deben ser capaces de manejar el proceso de autenticación de Kerberos. Es decir, cliente y servidor deben estar kerberizados.

Mejoras de la versión 5 de Kerberos

La versión 5 de Kerberos tiene una serie de mejoras sobre la versión 4. Algunas de las importantes son:

El uso de la encriptación se ha separado en distintos módulos de programa que permiten soportar múltiples sistemas de encriptado.

Las direcciones de red que aparecen en mensajes de protocolo se marcan con campos de longitud y tipo. Esto permite la compatibilidad con múltiples protocolos de red.

La codificación de mensajes se describe con la sintaxis ASN.1("Abstract Syntax Notation 1") de acuerdo con los estándares ISO 8824 y 8825.

El ticket en la versión 5 de Kerberos tiene un formato expandido para soportar nuevas características(por ejemplo, la cooperación entre reinos).

Como se menciona en Nombres, el identificador principal ha cambiado.

Se ha mejorado el soporte a operaciones entre reinos.

La información de autorización y contabilidad ya se puede encriptar y transmitir en un ticket con el campo de autorización de datos. Esto facilita la extensión del esquema de autenticación para que incluya también un esquema de autorización.

La implementación e la versión 5 de Kerberos proporcionar una liga con el GSSAPI("Generic Security Service API").