Kerberos

Kerberos lets the client prove its identity on the network without ever sending its password in the clear, by using encrypted tickets and session keys.

Made By
MOHAMED G.

The Main Actors

Client (User)

The one trying to access a service on the network

KDC (Key Distribution Center)

The KDC is the trusted authority that stores the secrets tied to accounts (including the keys derived from passwords) and uses them to verify your identity and encrypt tickets.

Service Server

It hosts the application or service being used.
It can be a file server, a web server, a database server, etc...

Client

KDC

Service

1 — AS - REQ

Authentication Service Request

The client asks the AS to send it a TGT ticket !
If pre-authentication is enabled, the client must add the current timestamp to the request, encrypted with the key derived from its password !

2 — AS - REP

Authentication Service Response

The client decrypts the AS-REP and retrieves its content :
- TGT : encrypted with the krbtgt account's secret key, unreadable to the client.
- Session Key client-kdc : encrypted with the key derived from the client's password, this is the only part the client actually decrypts in the response.

AS
Authentication Server

3 — TGS - REQ

Ticket Granting Service Request

The client wants to access a specific service, it sends the TGS :
- The TGT
- An Authenticator encrypted with the Session key from step 2, to show the TGT really is ours
- The name of the server it wants to access

4 — TGS - REP

Ticket Granting Service Response

If everything is valid, the TGS sends :
- a Service Ticket, encrypted with the service's Long Term Key, itself derived from the secret (password or machine key) of the service in question
- a Session Key client-service, encrypted with the session Key client-kdc from step 2

TGS
Ticket Granting Server

AP - REQ

Application Request

The client sends the service server :
- The Service Ticket
- An authenticator proving you really are the one who holds the ticket, and that the ticket is recent !

AP - REP

Application Response

The server verifies the ticket with its Long Term Key, if everything checks out, access is granted ! If Mutual Authentication is enabled, the AP-REP is encrypted with the Session Key from step 4, to show the client that the server is legitimate too !

By time !

For pre-authentication to be accepted, the timestamp sent by the client must fall within a tolerance window around the KDC's clock, in order to limit replay attacks.

Tickets (TGT, ST) also have a validity period to prevent abuse in case of theft.

Uniqueness !

A unique Session Key is created for each authentication session between the parties.