KERBEROS

OVERVIEW...

CONTENT

* Introduction
* Kerberos Design
* Common terms used in Kerberos
* How does Kerberos work
* Kerberos features
* Some Limitations

Introduction to Kerberos

- Is a computer network authentication protocol which works on the basis of tickets
- Part of project Athena(MIT)
- Provides a strong security on a non-secure network
- Uses trusted 3rd party authentication scheme
- Assumes that hosts are not trustworthy
- Based on Needham-Schroeder Protocol

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

- **Authentication Server (AS):**
The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

- **Database:**
The Authentication Server verifies the access rights of users in the database.

- **Ticket Granting Server (TGS):**
The Ticket Granting Server issues the ticket for the Server

Design

- **Client** are applications acting on behalf of users who need access to a resource or service.
- **Key Distribution Center** its the authentication server in a Kerberos environment,KDC consist of Database, Authentication server and Ticket granting server.
- **Server** its the server user want to connect with or the app user want to use in the server.

Terms Used In Kerberos

- **KDC** Key distribution Centre, this will be the server which we call the middle man server or the central server arbitrator, which issues the keys for the communication.
- **REALM** a kerberos network identified by a name, mostly this is the domain name in all caps.
- **Principal**: this is the name used by the kerberos central server to call users, service name etc.

- **TGS** Ticket Granting Server, this is mostly the same central server (KDC server), it grants the tickets for a service.
- **TGT** A special ticket which contains the session key for communication between the client machine and the central KDC server.

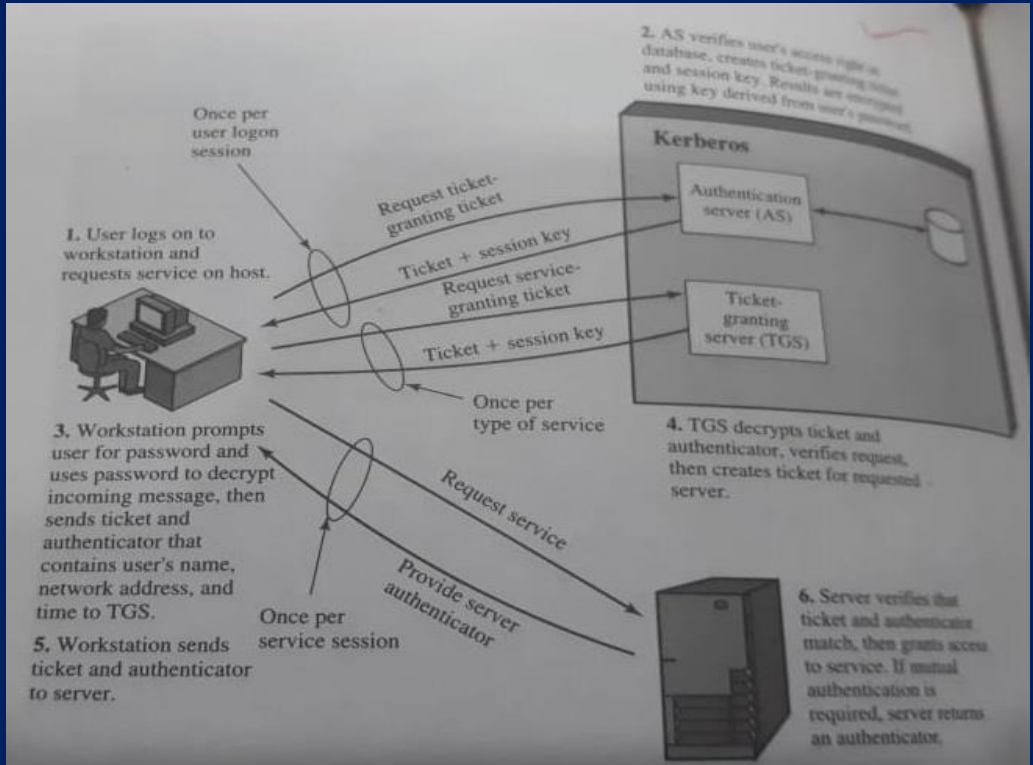

Figure 14.1 Overview of Kerberos

Kerberos working:

Step-1:
User login and request services on the host. Thus user requests for ticket-granting service.

Step-2:
Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

Step-3:
The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

Step-4:
Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

Step-5:
The user sends the Ticket and Authenticator to the Server.

Step-6:
The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Limitations

- If some attacker gets access to the central server, the entire infrastructure will be under threat.
- The applications that can be protected using kerberos must have kerberos functionality inbuilt into them.

Limitations

- Each network service must be modified individually for use with Kerberos
- It doesn’t work well in a timeshare environment
- Requires an always-on Kerberos server
- Assumes workstations are secure
- May result in cascading loss of trust.
- Scalability

Features

- Password and login credential is centralized in kerberos infrastructure, which prevents clients from storing passwords on their machines.
- Protocol weaknesses due to unencrypted data transfer on some network services can be reduced with the help of kerberos.

Features

- Password and login credential is centralized in kerberos infrastructure, which prevents clients from storing passwords on their machines.
- Protocol weaknesses due to unencrypted data transfer on some network services can be reduced with the help of kerberos.