KERBEROS

OVERVIEW...

CONTENT

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

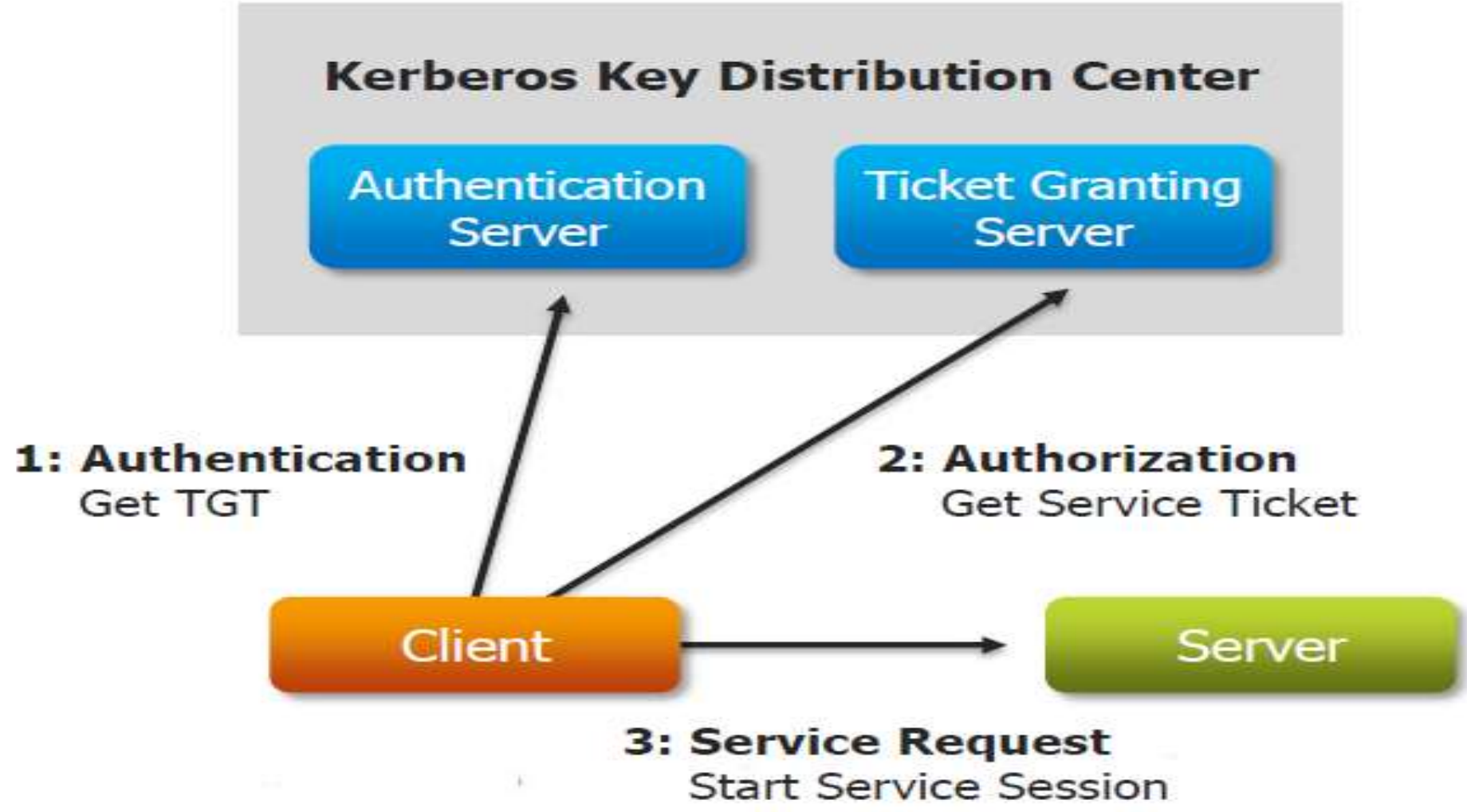
Introduction to Kerberos

- 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

Design

Kerberos consist of three main component

- **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.


Kerberos Key Distribution Center
Authentication Server
Ticket Granting Server
1: Authentication
Get TGT
2: Authorization
Get Service Ticket
Client
Server
3: Service Request
Start Service Session

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.

Working

Kerberos working procedure can be explained in simple steps.

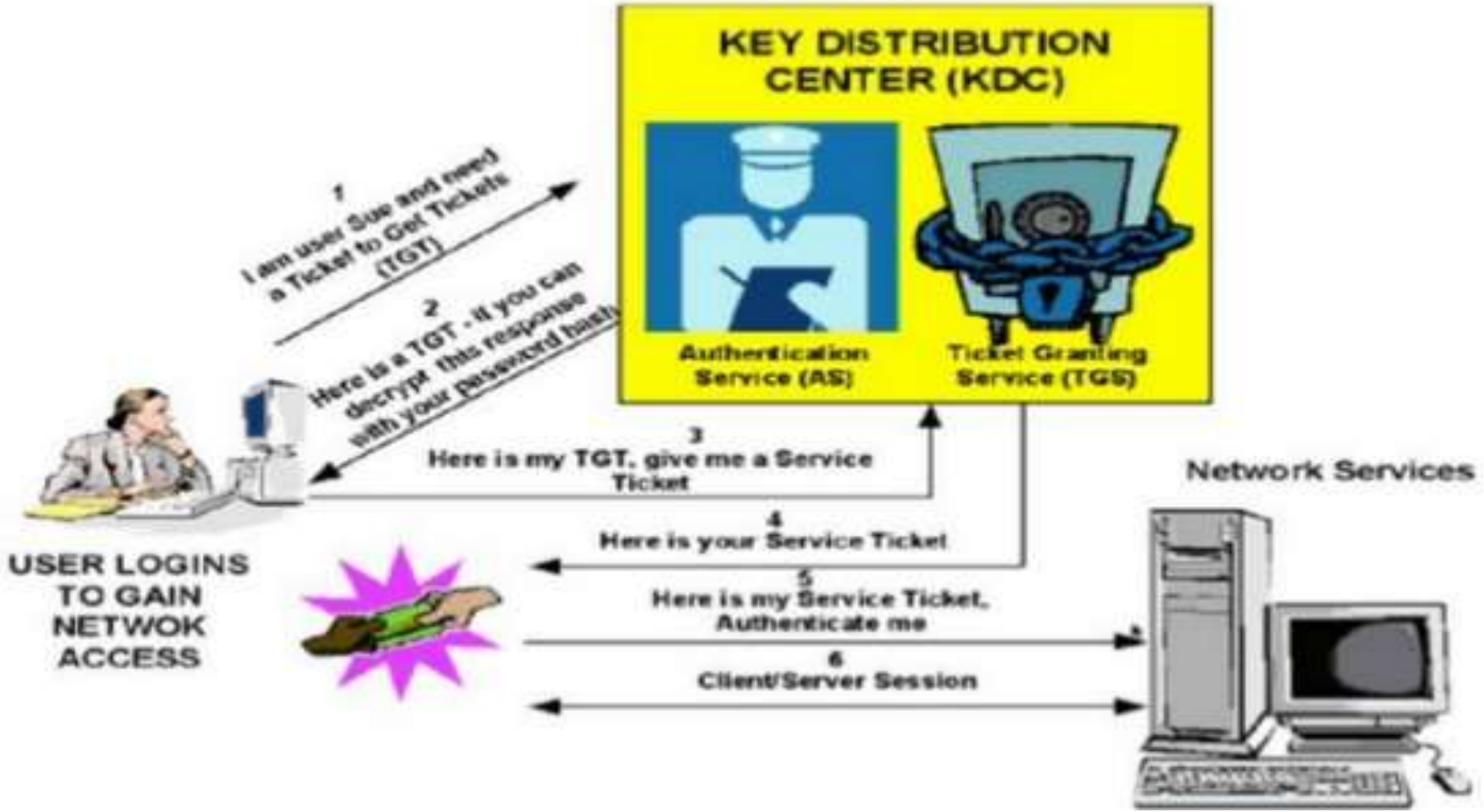
- When the user logins to his or her machine. The principal, is sent to KDC server for login, and the KDC server will provide TGT in return.

- Kdc server searches the principal name in the database, on finding the principal a TGT is generated by the KDC, which will be encrypted by the user's key, and send back to the user.

- When the user gets the TGT, the user decrypts the TGT with the help of user's key.

- Now the client has got TGT in hand. If suppose the client needs to communicate with some service on that network, the client will ask the KDC server, for a ticket for that specific service with the help of TGT and connect with the server.

KERBEROS TICKET EXCHANGE



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.

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.

THANK YOU...