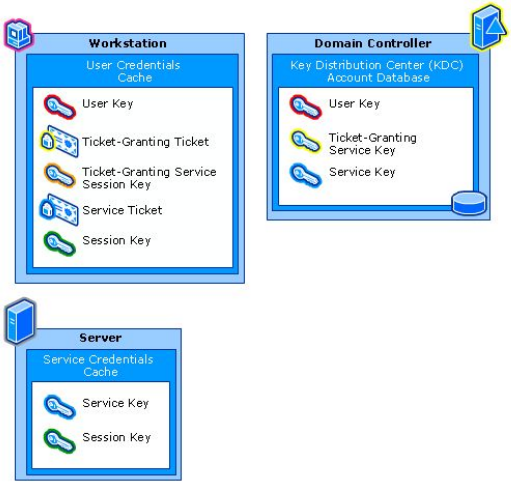
Network Security 2018/Spring

Amir Arbel
302726310

Kerboros Protocol

A widely used protocol [default protocol for Windows Server 2003] to securely confirm identities between parties over non-secure communication channel. It uses symmetric keys and in some cases public keys.

It has several components:



(taken from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772815(v%3dws.10))

Definitions -

A “ticket” is a data structure containing login and authentication information. Tickets are not readable by clients - only the KDC server holds keys to decrypt them. To protect against theft of tickets, they have expiration time handled by the KDC.

TGT (ticket granting ticket) - the first ticket that a client gets, used to request services from the server.

TGS (ticket granting service) - for access to any service, a client must request a ticket from the KDC by sending the TGT to the TGS.

Process - login and authenticate

1. Client wants to authenticate against a server, needs to create an encryption scheme:
   - Inputs a username/password combo.
   - The password is salted and hashed (one way encryption) and then used as the symmetric key.
   - Other options to the password scheme includes scheduled keys or public-key authentication.
2. Username / ID is sent in plaintext (or encrypted with a public key) from the client to the server.
   - Server checks if the user exists. If it doesn’t, stops the authentication process.
   - Generates a secret key by salting and hashing the user’s password from it’s database.

- Sends back two messages: (A) client session key message encrypted with the secret key of the user, and a (B) ticket-granting-ticket* encrypted with the server's own secret key.
- Client should have the same secret key if it inputted the correct password.

3. When requesting a service from the server, the client will send the TGT in combination with the ID of the service required (encrypted in either the password-based secret key shared between the client and the server or in a public key). The KDC will respond with a service ticket that allows the user to use the service for a configured amount of time.