Kerberos: Overview, Communication and Authentication

Kerberos Components:

- **Transport layer**

  Kerberos uses either UDP or TCP as transport protocol, which sends data in cleartext. Due to this Kerberos is responsible for providing encryption. Generally protocols/ports used are TCP/88 and UDP/88

- **Agents**

  * **Client or user** who wants to access the service.
  * **AP** (Application Server) which offers the service required by the user.
  * **KDC** (Key Distribution Center), the main service of Kerberos, responsible for issuing the tickets, installed on the DC (Domain Controller). It is supported by the **AS** (Authentication Service), which issues the TGTs.

- **Encryption keys**

  * **KDC or krbtgt key** which is derivative from krbtgt account NTLM hash.
  * **Service key** which is derived from the NTLM hash of the service owner, which can be an user or computer account.
  * **User key** which is derivative from user NTLM hash.
  * **Session key** which is negotiated between the user and KDC.
  * **Service session key** to be used between user and service.

- **Tickets**

  * The **TGS** (Ticket Granting Service) is the ticket which users can use to authenticate against a service. It is encrypted with the service key.
  * The **TGT** (Ticket Granting Ticket) is the ticket presented to the KDC to request for TGSs. It is encrypted with the KDC key.

Kerberos improvement over NTLM:

Active Directory supports two primary authentication protocols, NTLM and **Kerberos**. Generally whenever a client connects to a resource via domain name authentication is done via kerberos but whenever raw IP address Modern Windows versions default to Kerberos authentication.NTLM suffers from two main weaknesses:
1) the NTLM password hash only changes when the password changes, so exposure of this hash provides access to the account until the password is changed, and
2) the server hosting the resource needs to check with the Domain Controller to verify the challenge response data sent from the client is valid

Kerberos improves on these issues by
1) limiting the Kerberos ticket lifetime so if the ticket is stolen, can only be used for a set amount of time, and
2) The authentication flow involves the user getting a service ticket (from a DC) for the service on a server which the server checks without requiring communication with a DC.

Kerberos Authentication Example:

User logs on with username & password.

1a. Password converted to NTLM hash, a timestamp is encrypted with the hash and sent to the KDC as an authenticator in the authentication ticket (TGT) request (AS-REQ).

1b. The Domain Controller (KDC) checks user information (logon restrictions, group membership, etc) & creates Ticket- Granting Ticket (TGT).

2. The TGT is encrypted, signed, & delivered to the user (AS-REP).
Only the Kerberos service (KRBTGT) in the domain can open and read TGT data.

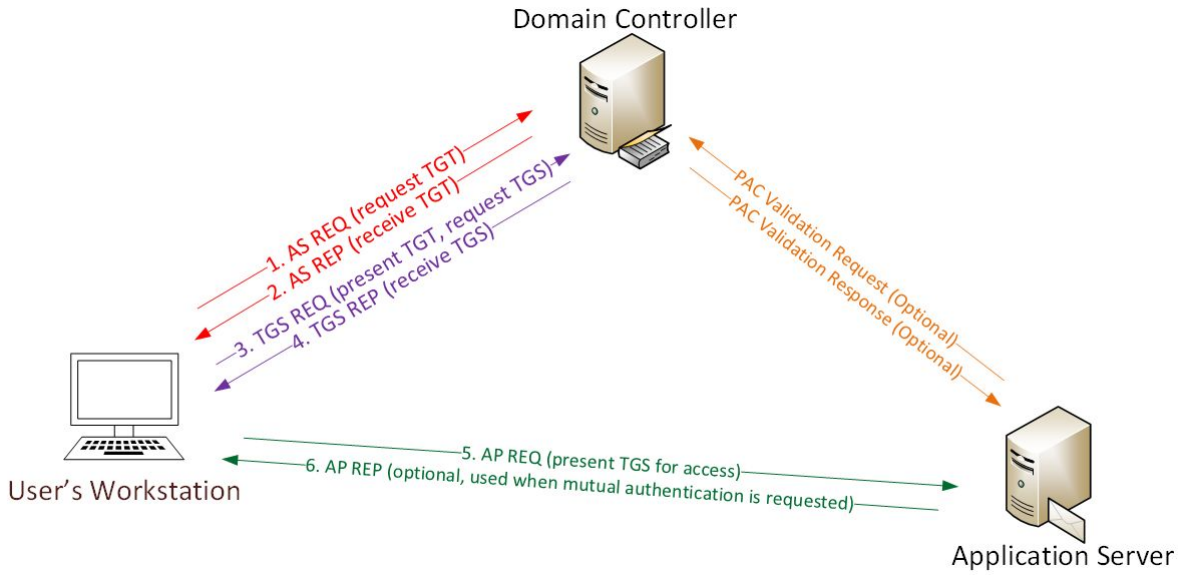
3. The User presents the TGT to the DC when requesting a Ticket
Granting Service (TGS) ticket (TGS-REQ). The DC opens the TGT & validates PAC checksum–If the DC can open the ticket & the checksum
check out, TGT = valid. The data in the TGT is effectively copied to create the TGS ticket.

4. The TGS is encrypted using the target service accounts' NTLM password hash and sent to the user (TGS-REP).

5.The user connects to the server hosting the service on the appropriate port & presents the TGS (AP-REQ). The service opens the TGS ticket using its NTLM password hash.

6. If mutual authentication is required by the client (think MS15-011: the Group Policy patch from February that added UNC hardening).

Unless PAC validation is required (rare), the service accepts all data in the TGS ticket with no communication to the DC.



Kerberos Authentication Summary

Kerberos Key points:

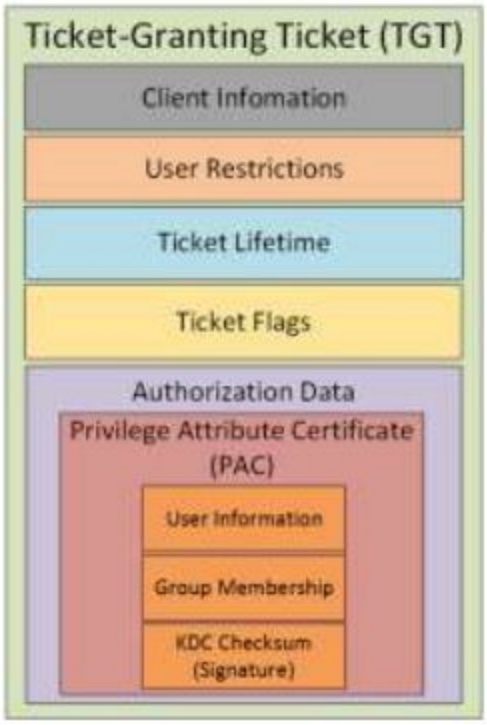
- Microsoft uses the NTLM password hash for Kerberos RC4 encryption.
  Kerberos policy is only checked when the TGT is created & the TGT is the user authenticator to the DC.
- The DC only checks the user account after the TGT is 20 minutes old to verify the account is valid or enabled. TGS PAC Validation only occurs in specific circumstances.
- If it runs as a service, PAC validation is optional (disabled). If a service
  runs as System, it performs server signature verification on the PAC (computer account long-term key).

Kerberos Ticket Format:

In Kerberos a user has a ticket which is used to gain access to a resource. The Ticket-Granting-Ticket,TGT, is the authentication ticket and the Ticket-Granting-Service, TGS ticket is the service ticket which provides access to Kerberos enabled services.

The format of these tickets are:

- Client information – workstation FQDN & IP address
- User Restrictions – logon schedule, workstation restrictions, etc.
- Domain Kerberos Policy - Ticket Lifetime (Default: 10 hour lifetime & 7 day max)
- Ticket Flags – Encryption, ticket type (impersonation, can it be delegated, etc)
- Auth Data - PAC
- User Info: User name, user SID , profile info, etc
- Group Membership: Group RIDs
- PAC Signature
- A TGS has a server component & user component


Ticket-Granting Ticket (TGT)
Client Infomation
User Restrictions
Ticket Lifetime
Ticket Flags
Authorization Data
Privilege Attribute Certificate (PAC)
User Information
Group Membership
KDC Checksum (Signature)

Trust