HBO

Windows and Kerberos

Gwendal Patat
Univ Rennes, CNRS, IRISA
2025/2026

On today’s schedule

Main points:

- Kerberos Overview
- Kerberos Protocol
- Kerberos messages
- Attacks on Kerberos

Kerberos Overview

Kerberos

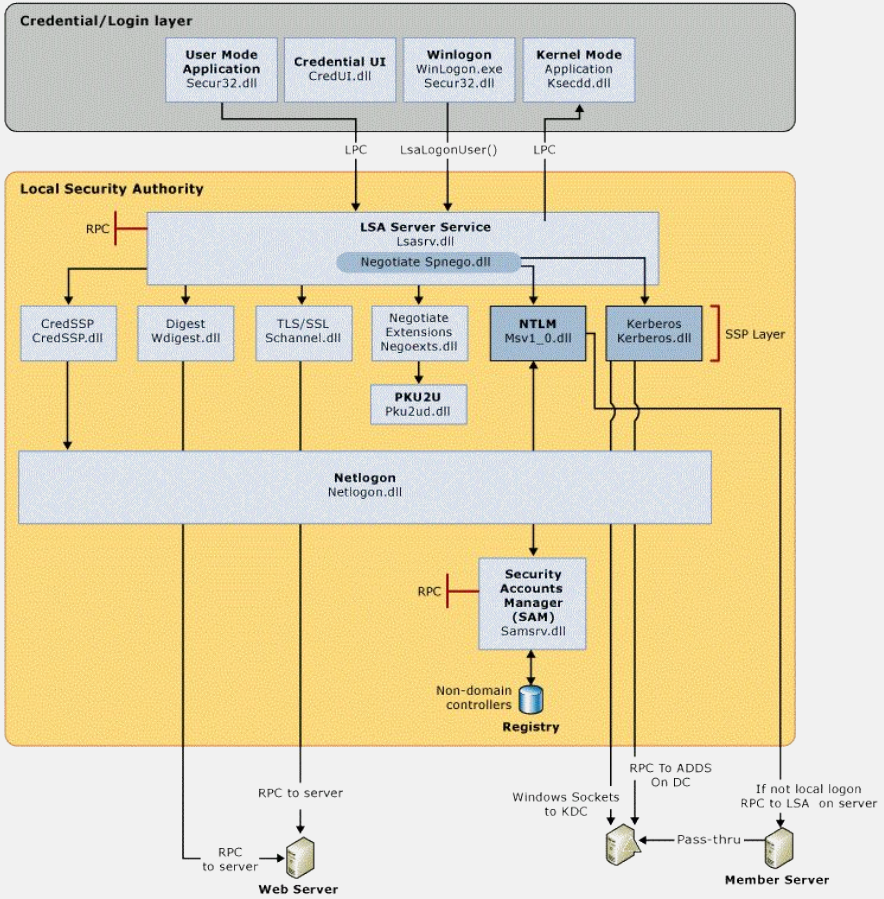
Kerberos is an authentication protocol defined in 1989.

It is used to authenticate a user **across a realm** (domain) in order to provide access to services.

Kerberos is primarily deployed in Windows, where Microsoft uses additional proprietary fields.

- Kerberos is based on a trusted third party model, called the **Key Distribution Center (KDC)**, for *mutual* authentication.
- The KDC issues tickets proving identity.
- Authentication relies on **shared secret keys and encrypted messages**, avoiding sending passwords over the network.
- The protocol uses **tickets** (TGT and service tickets), which allow the user to reuse authentication without repeating password verification.
- In Windows, Kerberos tickets include a **Privilege Attribute Certificate (PAC)** that carries group/SID information for authorization.

Authentication Workflow



Windows Domain

Windows Domain have been around since Windows NT (1993):

- A domain is a logical security boundary used to manage users, computers, and policies.
- All entities in the domain share a central authentication authority.
- Users authenticate once and can access resources across the domain (Single Sign-On).

Domain Controller (DC) is the server responsible for:

- A Domain Controller:
- Storing account credentials and security policies.
- Authenticating users and computers.
- It often the KDC for the Kerberos protocol.

Active Directory

Active Directory (AD) is the directory service that stores and organizes information about:

- Users, groups, computers, organizational units.
- Security settings and group policies.

Relationship Between Domain and AD:

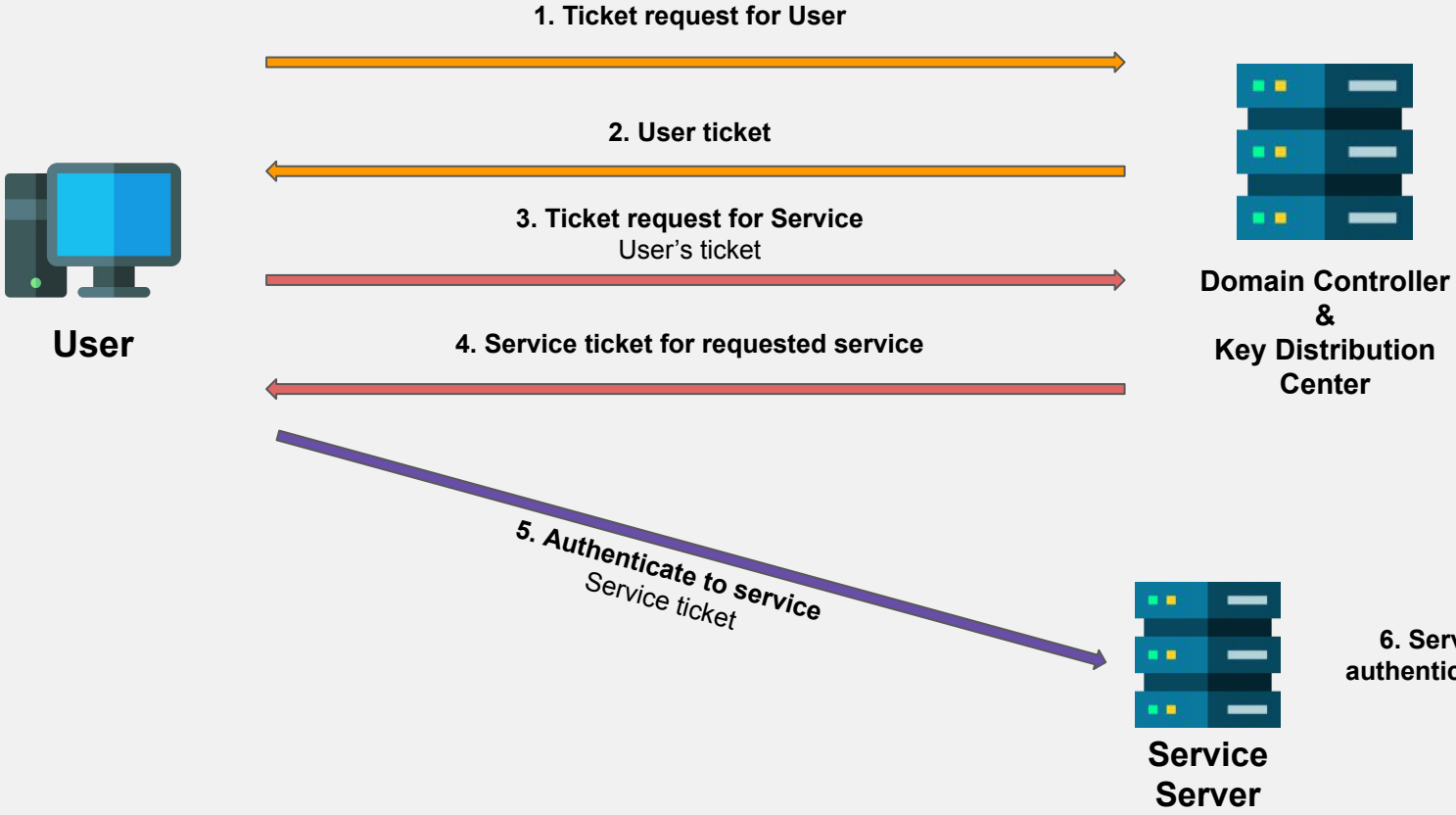
- The domain defines the administrative and authentication scope.
- Active Directory is the underlying database/service that implements the domain.
- Every Domain Controller runs AD and shares the same replicated directory data.

In short:

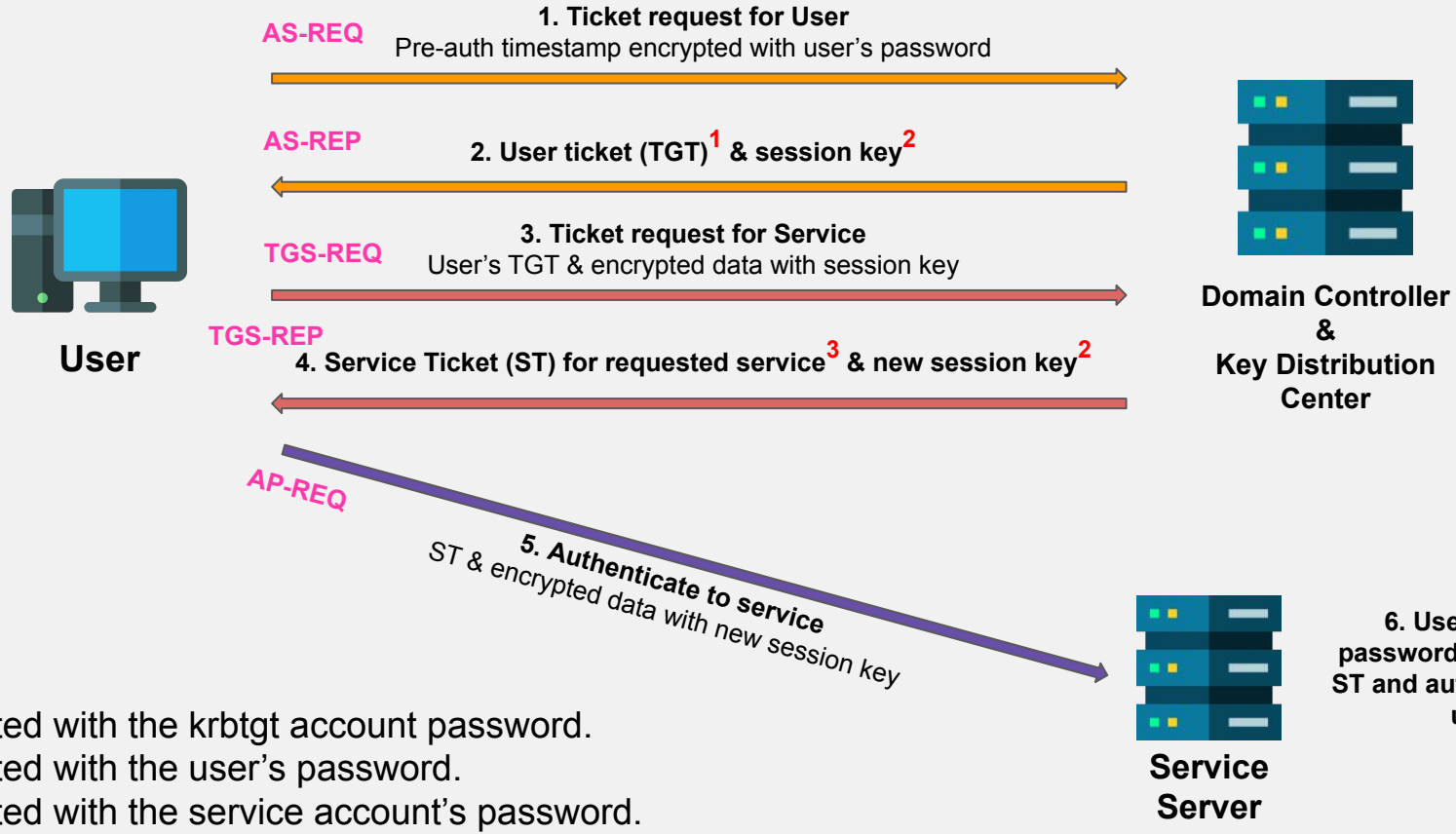
- Domain = Security boundary + Identity namespace.
- AD = Directory + Data + Policy framework that supports the domain.

Kerberos Protocol

Kerberos Protocol Simplified



Kerberos Protocol



1: Encrypted with the krbtgt account password.
2: Encrypted with the user's password.
3: Encrypted with the service account's password.

AS-REQ (Authentication Service Request)

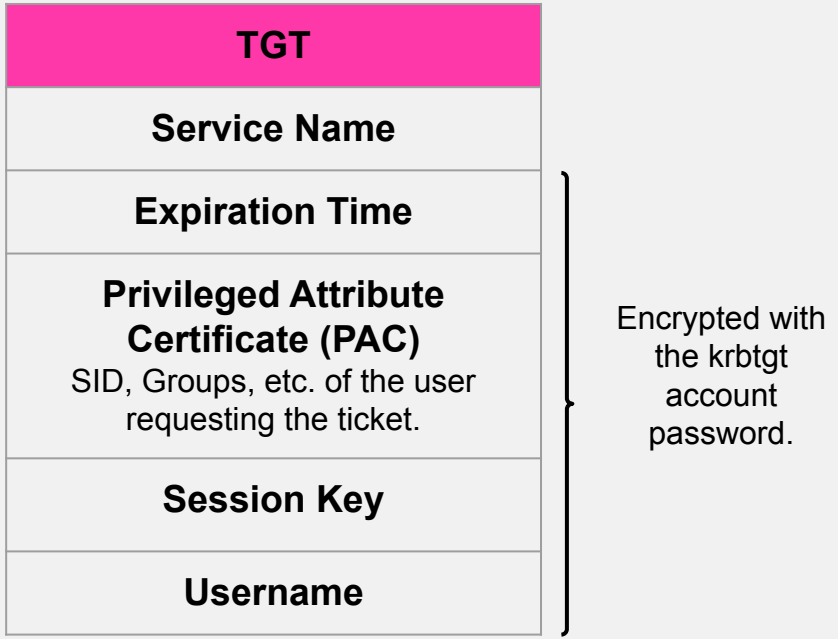
User request a TGT:

- **Pre auth Data**
  - Timestamp encrypted by the user’s password.
- **Username**
- **Service Name**
  - Here “*krbtgt*”

AS-REP (Authentication Service Reply)

Ticket Granting Ticket (TGT) and Session Key:

- **User's TGT**
- **Session Key**
  - Encrypted with the user's password.



TGS-REQ (Ticket Granting Server Request)

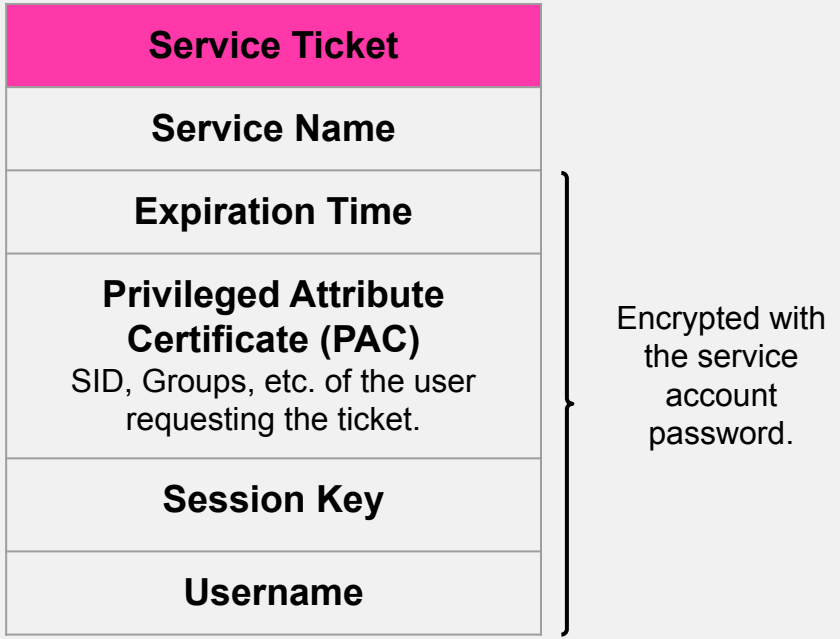
User request a ST:

- **Service Name**
- **Ticket-Granting Ticket**
  - User’s TGT with the krbtgt encrypted session key.
- **Authenticator**
  - Encrypted by the session key.
  - Proves that the user knows the session key.
  - Contains the user name, client realm, timestamp, etc.

TGS-REP (Ticket Granting Server Reply)

ST and Session Key:

- **Service Ticket**
- **Session Key**
  - Encrypted with the user's password.



AP-REQ (Application Request)

Service defined protocol.

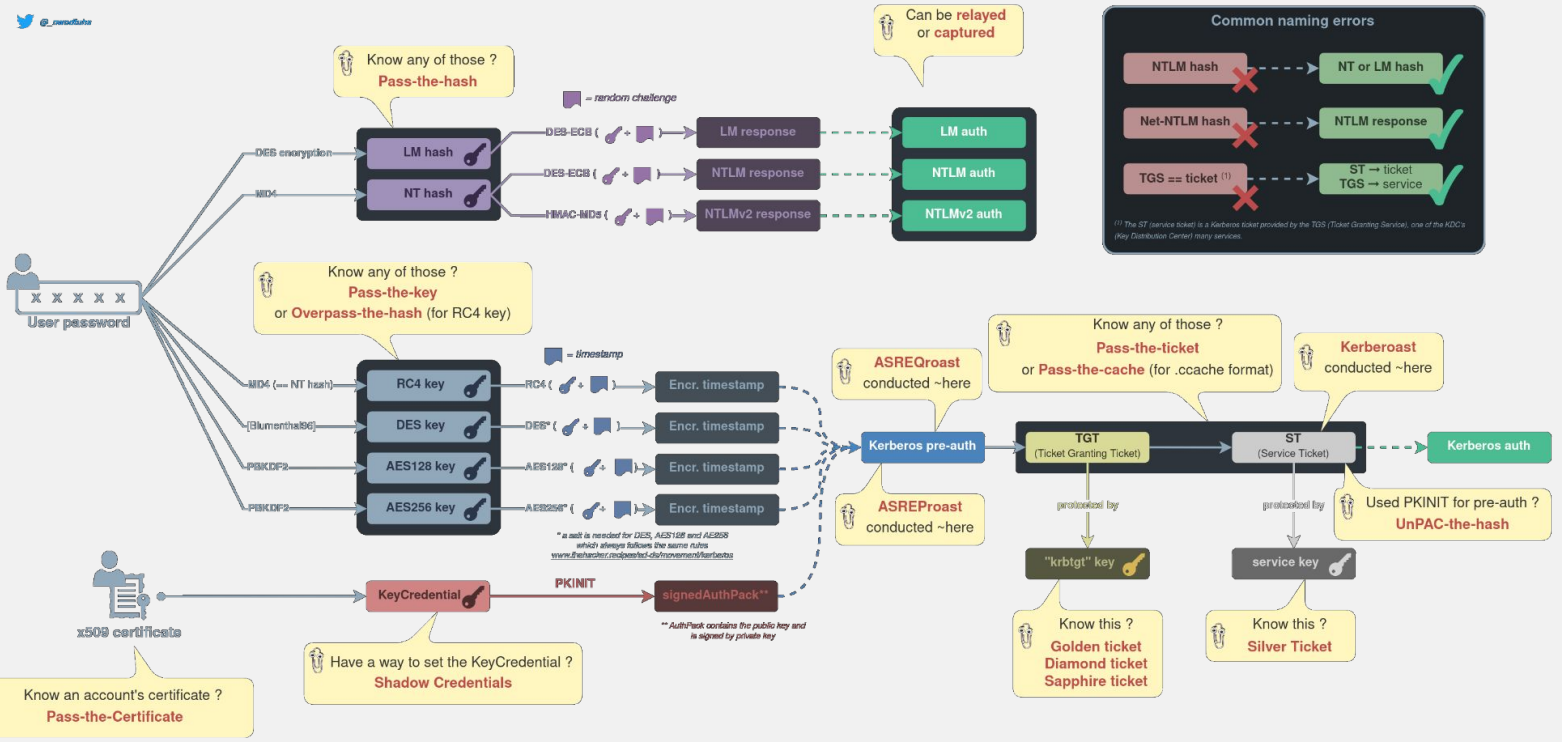
Kerberos Security

An old protocol (1989), with old ciphersuites...

- DES-CBC-CRC: deprecated since Windows 7
- DES-CBC-MD5: deprecated since Windows 7
- RC4-HMAC: weak
- AES*-CTS-HMAC-SHA1 (key = PBKDF2(password))
  - 4 096 iterations
  - salt: concatenation of the realm name, and the client’s name (in uppercase)

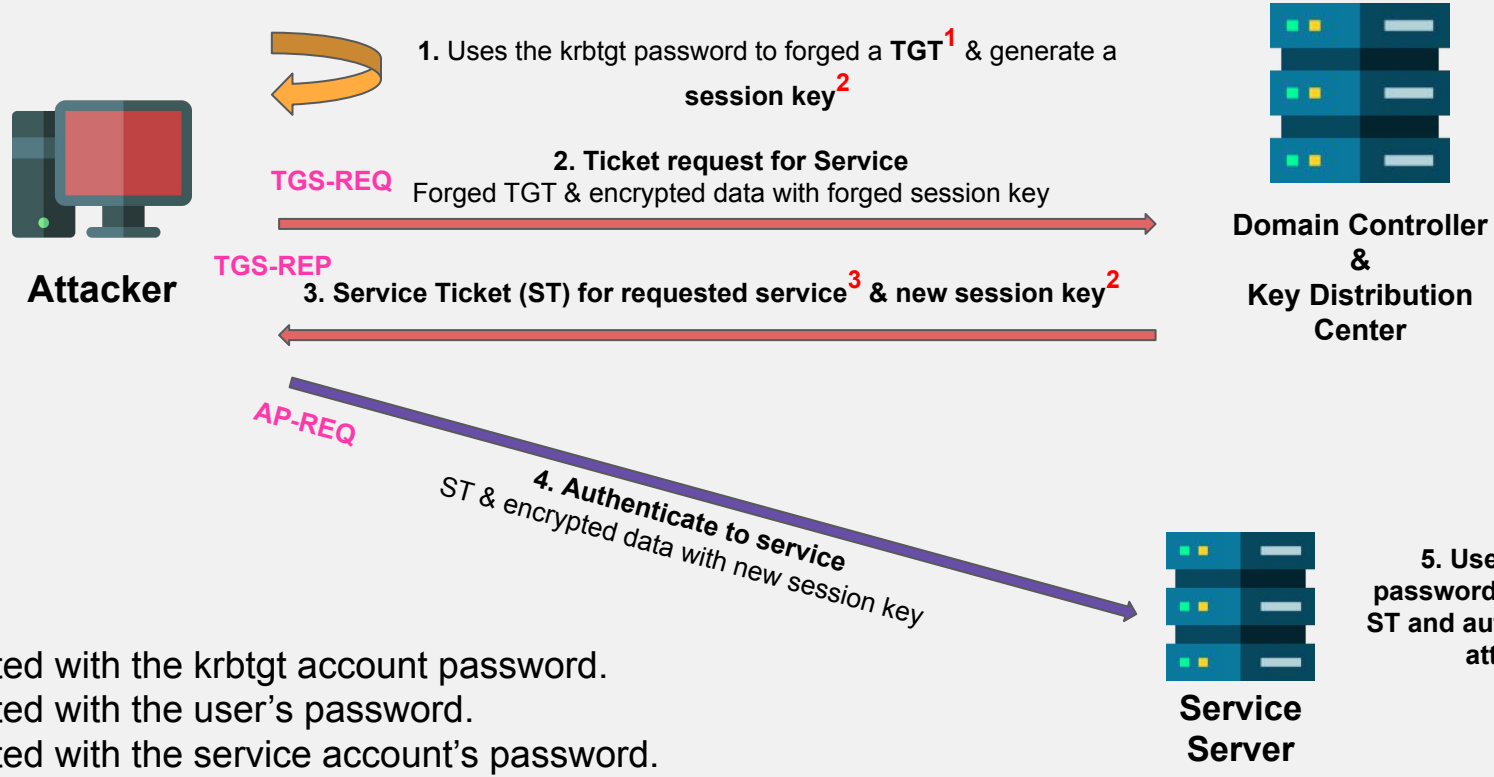
Attacks on Kerberos

Windows authentication Attacks



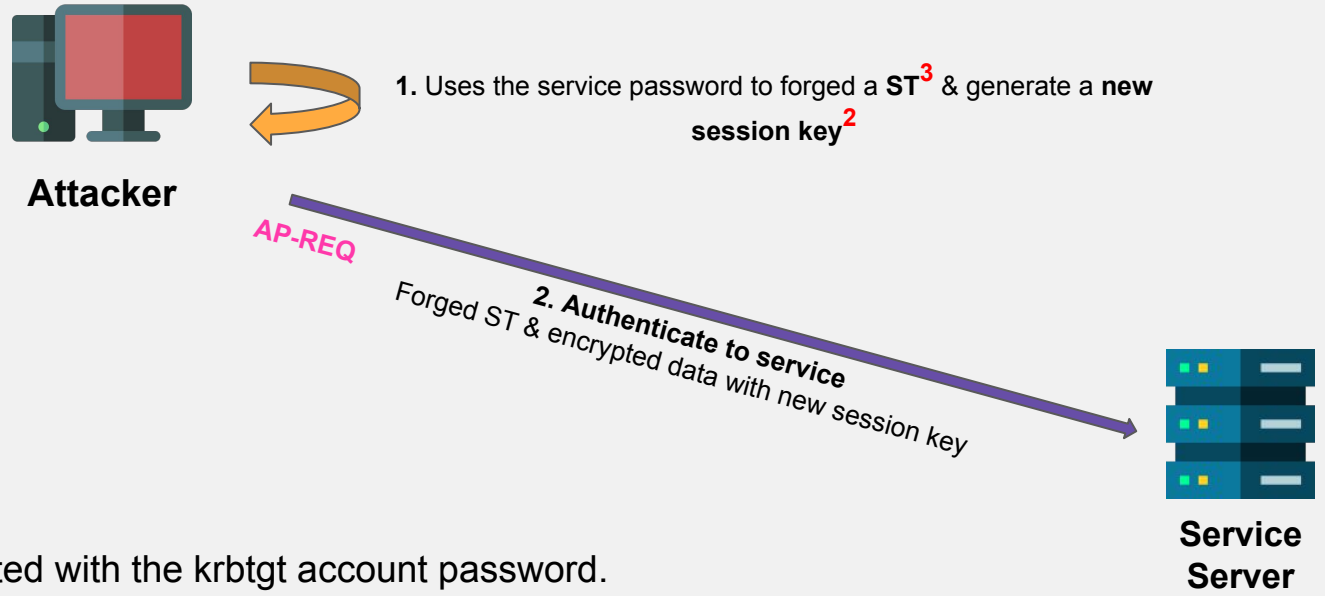
https://www.thehacker.recipes/ad/movement/kerberos/

Golden Ticket Attack



1: Encrypted with the krbtgt account password.
2: Encrypted with the user's password.
3: Encrypted with the service account's password.

Silver Ticket Attack



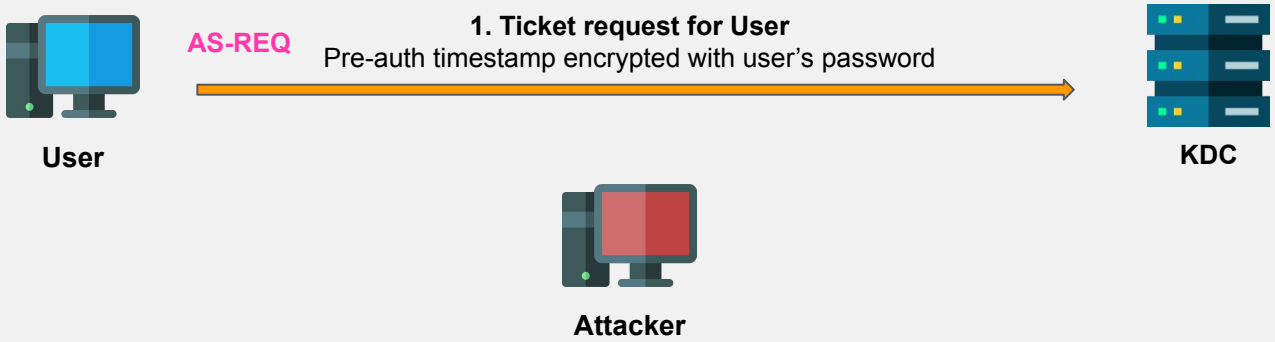
1: Encrypted with the krbtgt account password.
2: Encrypted with the user's password.
3: Encrypted with the service account's password.

Diamond/Sapphire Ticket Attacks

Variant of the Golden and silver ticket attacks.

- Golden and Silver ticket attacks can easily be detected due to the lack of REQ before the forged REP.
- In addition since 2021, the username in the PAC needs to match an existing user in the Active Directory.
- Now, we first request a legitimate ticket and modify its content to make a stealthy forgery:
  - ***Diamond***: we modify the PAC of the ticket to match what we want.
  - ***Sapphire***: The PAC is replaced by a legitimate PAC with more privilege, retrieved before.

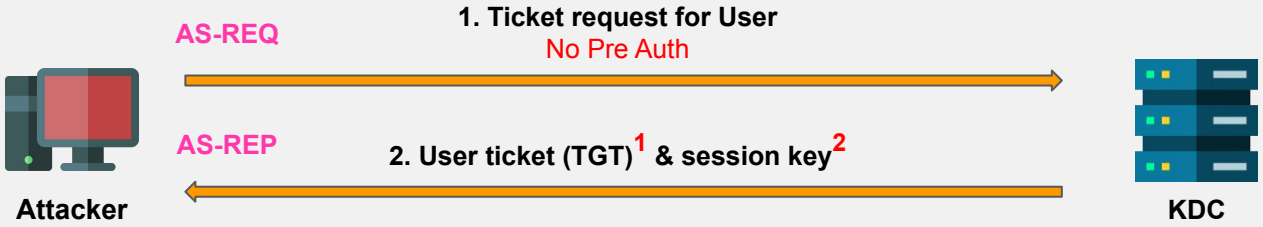
ASREQroast



An attacker with network sniffing capabilities (APR poisoning, DHCP spoofing, etc.) can either intercept the AS-REQ to perform an offline attack:

- Attackers can try to crack those encrypted timestamps to retrieve the user's password.
  - Mainly depend on the algorithm being used (RC4 vs AES).

ASREProast

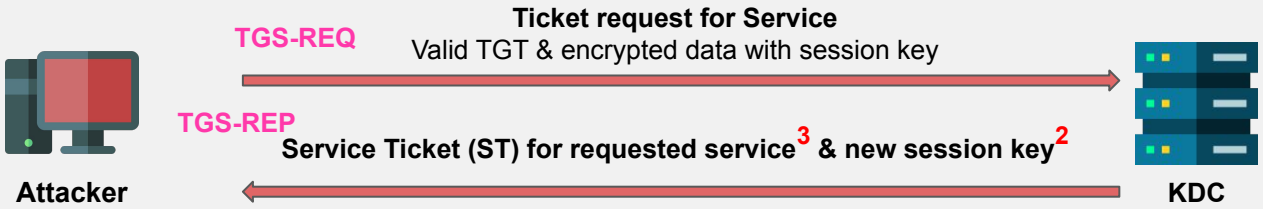


1: Encrypted with the krbtgt account password.
2: Encrypted with the user's password.

Because some applications don't support Kerberos preauthentication, it is common to find users with Kerberos preauthentication disabled:

- An attackers can request TGTs for these users and crack the session keys offline.
  - Why the session key? Because it is encrypted using the hash of the user.

Kerberoast



2: Encrypted with the user's password.
3: Encrypted with the service account's password.

If an attacker knows service names to request a ST to the KDC:

- An attackers can request STs for services and try to crack the service password offline.
  - Most service accounts have strong passwords making this attack less practical.
    - However, some user accounts are also service accounts: meaning with user defined password…

Resources and Acknowledgements

- https://book.hacktricks.wiki/en/
- https://learn.microsoft.com/en-us/
- https://www.thehacker.recipes/ad/movement/kerberos/
- *Windows Internals, Part 1, 7th Edition*
- External materials from Daniel De Almeida Braga.