Kerberos

COMP750 Distributed Systems

Authentication Service

- Kerberos allow users and services to *authenticate* themselves to each other
- Kerberos was created at MIT in the early 1980s
- Based on the Needham-Schroeder authentication protocol
- Internet Engineering Task Force RFC 1510
- Used by Microsoft Windows

Encryption for Authentication

- Kerberos bases its authentication on a principle's ability to decrypt a known value.
- If I send you an encrypted value and you send it back to me unencrypted, then I know that you have the decryption key.

Symmetric Key Encryption

- Kerberos uses secret key encryption.
- DES is the default encryption algorithm, although other algorithms can be used.

User Passwords

- User passwords are hashed
- The hash is used as an encryption key.
- The password itself is never transmitted over the network.

Kerberos Servers

- Authentication Servers (AS)
  - Verify a client's identity
  - Provides a ticket to the TGS
- Ticket Granting Servers (TGS)
  - Provides tickets for application servers
  - Knows an encryption key for each server
- Both servers may be in the same machine

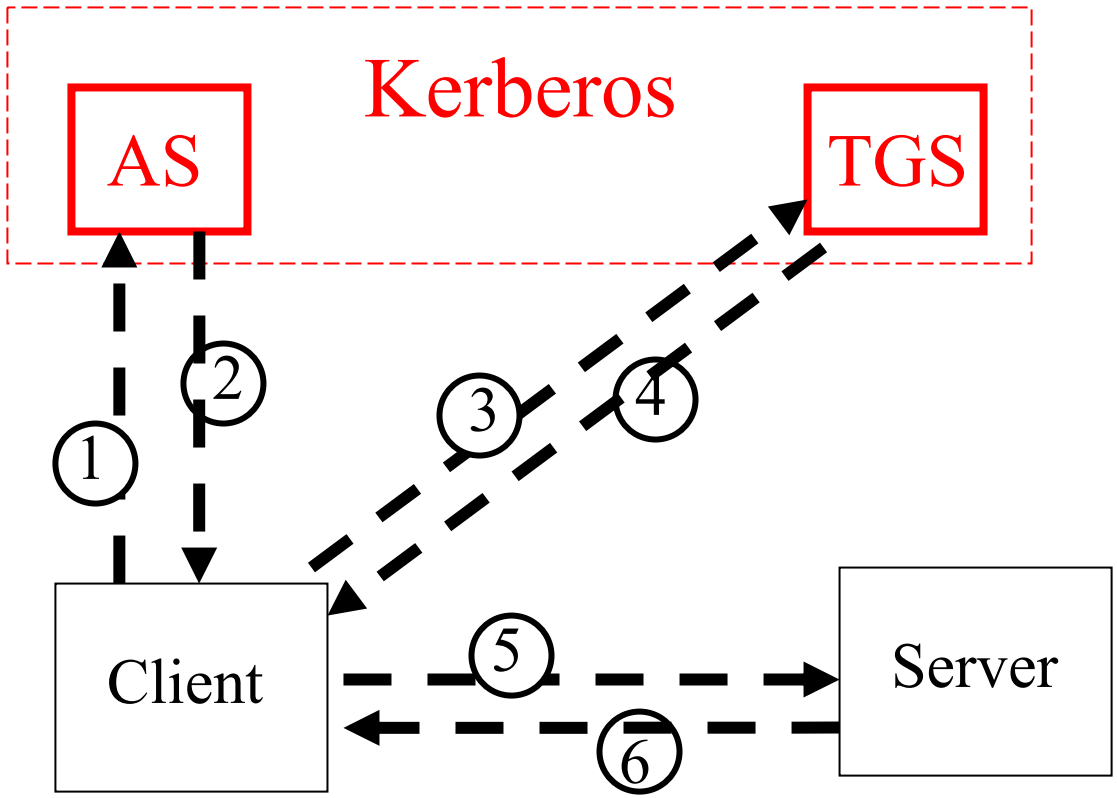
Tickets

- Kerberos passes tickets to verify identity
- Tickets contain a timestamp to avoid future replay.
- Tickets contain a principles name and a key for future communication.
- Tickets are encrypted with the key of the server.

$$\{\text{name}, \text{Key}_{C \rightarrow S}\}\text{Key}_{S \rightarrow TGS}$$

Overview of Kerberos

AS – Authentication Service
TGS – Ticket Granting Service



Authentication Server Exchange

- Client to AS
  - UserID, TGSname, nonce
- AS to Client
  - $Ticket_{C \rightarrow TGS}$, TGT_C
  - $Ticket_{C \rightarrow TGS} = \{U, C, TGS, Key_{C \rightarrow TGS}\} Key_{AS \rightarrow TGS}$
  - $TGT_C = \{TGS, Key_{C \rightarrow TGS}, nonce\} Key_U$

TGS Exchange

- Client to TGS
  - S, nonce2, $\text{Ticket}_{C \rightarrow TGS}$
- TGS to Client
  - U, $\text{Ticket}_{C \rightarrow S}$, Ticket_{C}
  - $\text{Ticket}_{C \rightarrow S}$,= $\{U, C, S, \text{Key}_{C \rightarrow S}\}\text{Key}_{S \rightarrow TGS}$
  - Ticket_{C} = $\{S , \text{Key}_{C \rightarrow S} , \text{nonce2}\}\text{Key}_{C \rightarrow TGS}$

Application Server Exchange

- Client to Application Server
  - $\text{Ticket}_{C \rightarrow S}$, {C,time1} $\text{Key}_{C \rightarrow S}$
- Application Server to Client
  - {time1} $\text{Key}_{C \rightarrow S}$

Triple DES

- Because many people feel that the 56 bit key of DES is too small, Triple DES is frequently used for additional security.
- Triple DES uses two 56 bit keys (112 bits) and executes DES three times.

- cipher = $E_{key1}(D_{key2}(E_{key1}(plaintext)))$