Kerberos

Ahmet Burak Can
Hacettepe University
abc@hacettepe.edu.tr

Kerberos

- Advantages:
  - secure authentication
  - single sign-on
  - secure data flow

- Applications benefiting from Kerberos:
  - telnet, ftp
  - BSD rtools (rlogin, rsh, rcp)
  - NFS
  - Others (pine, eudora, etc.)

Overview of Kerberos

Kerberos Keys

- Each principal shares a “master key” with KDC
  - $K_A$: Alice’s master key. Used for initial authentication
  - $K_{TGS}$: The key known by AS and the TGS.
  - $K_{A,TGS}$: The key shared between the TGS and Alice

Ticket Granting Tickets (TGT):

- issued to Alice by AS after login
- encrypted with $K_{TGS}$
- used to obtain session key $K_{A,TGS}$
Logging into the Network

1. Alice → AS: ID_A || ID_Asp || TS_A
2. AS → Alice: E_{K_Asp}[K_{A-S} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A || Ticket_{sp}]

Ticket_{sp} = E_{K_{A-S}}[K_{A-S} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A]

ID_Asp denotes the identifier of the Ticket Granting Server (TGS)
K_{A-S} is the key shared by the TGS and Alice
K_{sp} is the key shared by AS and the TGS

Obtaining a Ticket from TGS

3. Alice → TGS: ID_A || Ticket_{sp} || Authenticator_A
4. TGS → Alice: E_{K_{A-S}}[K_{A-S} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A || Ticket_{sp}]

Authenticator_A = E_{K_{A-S}}[ID_A || AD_A || TS_A]
Ticket_{sp} = E_{K_{A-S}}[K_{A-S} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A]
Ticket_{sp} = E_{K_{A-S}}[K_{A-S} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A]

K_{A-S} is the key shared by the TGS and server B

Client-Server Authentication Exchange

5. Alice → Bob: Ticket_{sp} || Authenticator_A
6. Bob → Alice: E_{K_{B}}[TS_A || 1]

Ticket_{sp} = E_{K_{B}}[K_{B} || ID_A || AD_A || ID_Asp || TS_A || Lifetime_A]
Authenticator_A = E_{K_{A-S}}[ID_A || AD_A || TS_A]

Key Relation in Kerberos

K_A is the key shared by the TGS and server B