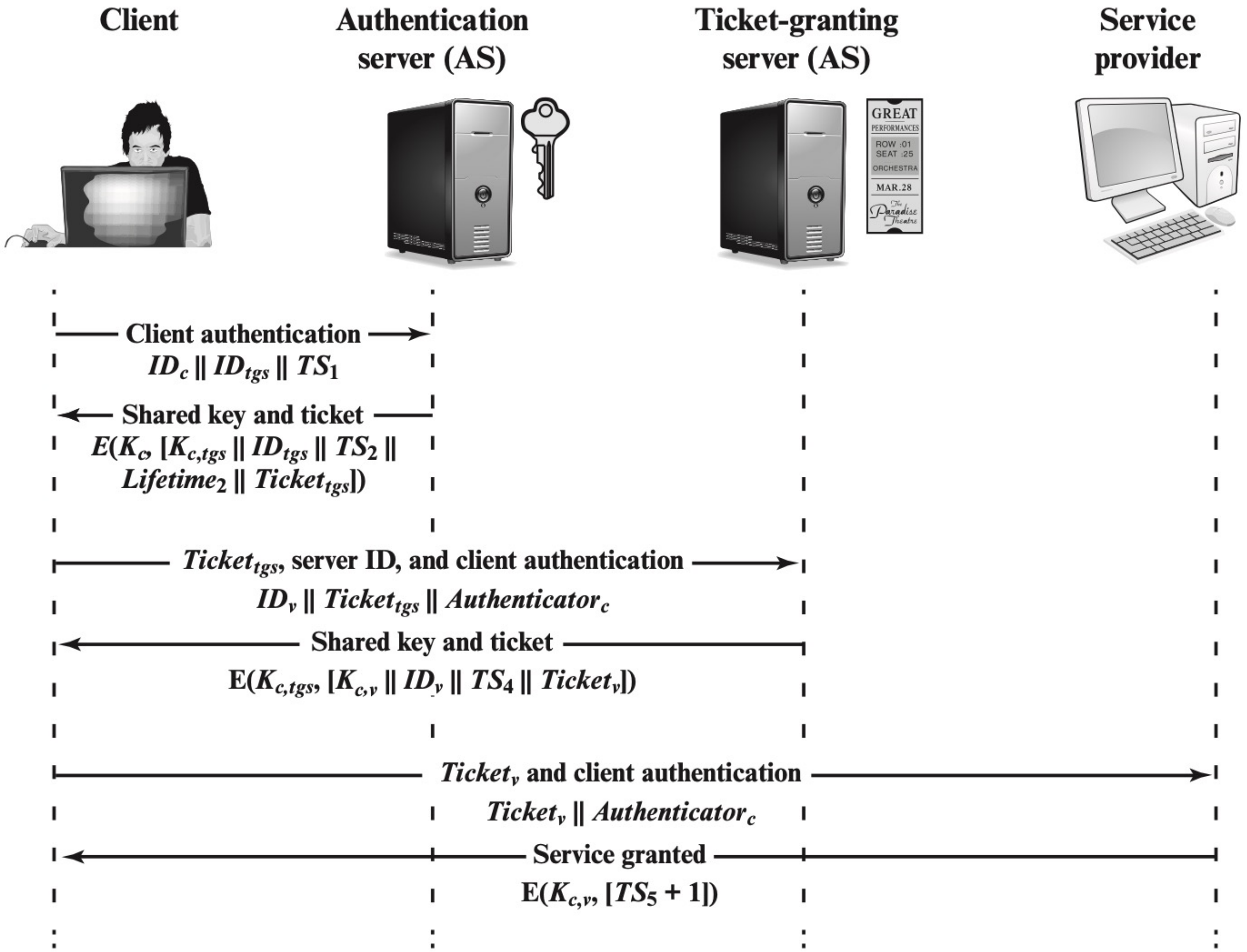
Lecture 26

Overview of Kerberos



Client

Authentication server (AS)

Ticket-granting server (AS)

Service provider

Client authentication

$ID_c \,||\, ID_{tgs} \,||\, TS_1$

Shared key and ticket

$E(K_c, [K_{c,tgs} \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2 \,||\, Ticket_{tgs}])$

$Ticket_{tgs}$, server ID, and client authentication

$ID_v \,||\, Ticket_{tgs} \,||\, Authenticator_c$

Shared key and ticket

$\mathrm{E}(K_{c,tgs}, [K_{c,v} \,||\, ID_v \,||\, TS_4 \,||\, Ticket_v])$

$Ticket_v$ and client authentication

$Ticket_v \,||\, Authenticator_c$

Service granted

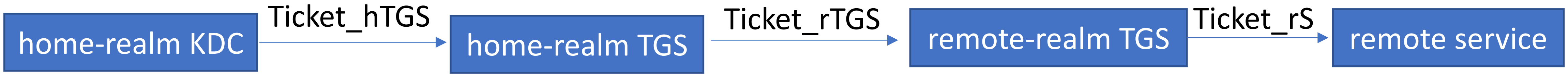
$\mathrm{E}(K_{c,v}, [TS_5 + 1])$

Important Ideas in Kerberos

- Short-term session keys
  - Long-term secrets used only to derive short-term keys
  - Separate session key for each user-server pair
    - Re-used by multiple sessions between same user and server
- Proofs of identity based on authenticators
  - Client encrypts his identity, addr, time with session key; knowledge of key proves client has authenticated to KDC/AS
    - Also prevents replays (if clocks are globally synchronized)
  - Server learns this key separately (via encrypted ticket that client can't decrypt), then verifies client's authenticator
- Symmetric cryptography only

Kerberos in Large Networks

- One KDC isn't enough for large networks
- Network is divided into realms
  - KDCs in different realms have different key databases
- To access a service in another realm, users must...
  - Get ticket for home-realm TGS from home-realm KDC
  - Get ticket for remote-realm TGS from home-realm TGS
    - As if remote-realm TGS were just another network service
  - Get ticket for remote service from that realm's TGS
  - Use remote-realm ticket to access service



Practical Uses of Kerberos

- Microsoft Windows – Active Directory
- Email, FTP, network file systems, many other applications have been kerberized
    - Use of Kerberos is transparent for the end user
    - Transparency is important for usability!
- Local authentication
    - login and su in OpenBSD
- Authentication for network protocols
    - rsh
- Secure windowing systems

Readings

- Kerberos: The Network Authentication Protocol
  https://web.mit.edu/kerberos/

Practice

- William Stallings, “Network Security Essentials”, 6 Edition, 2017
    - Chapter 4’s problems: 4.8, 4.9, 4.10