

Lecture 24

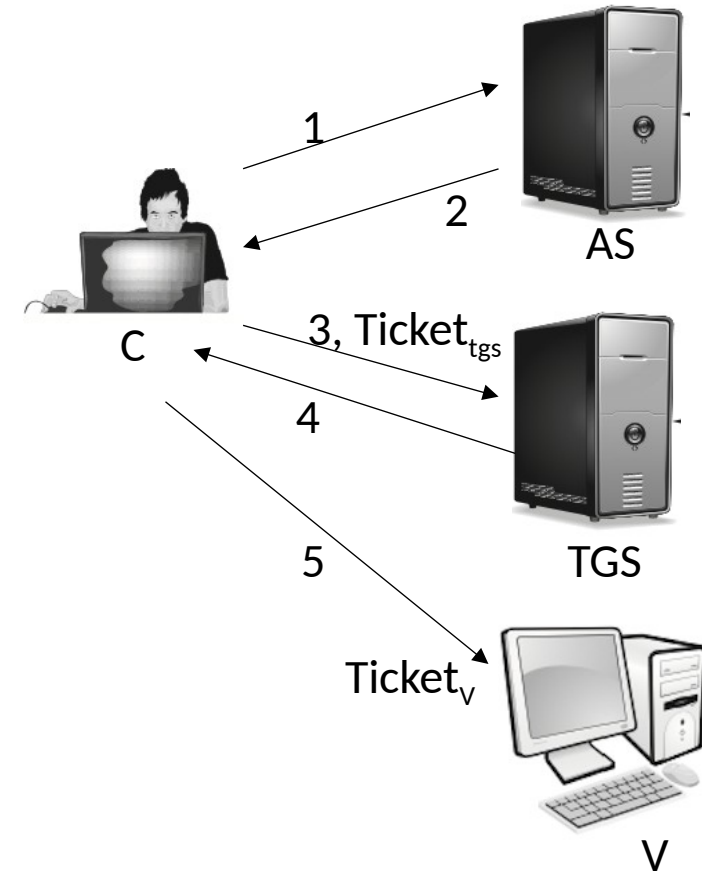
Secure?

- **Insecure**: password is transmitted openly and frequently
- Solution: no password transmitted by involving ticket-granting server (TGS)

1. $C \rightarrow AS: ID_C || P_C || ID_V$
2. $AS \rightarrow C: Ticket = E(K_V, [ID_C || AD_C || ID_V])$
3. $C \rightarrow V: ID_C || Ticket$

A More Secure Authentication Dialogue

- Once per user logon session
 - (1) $C \rightarrow AS: ID_C || ID_{tgs}$
 - (2) $AS \rightarrow C: E(K_C, Ticket_{tgs})$
 - Once per type of service:
 - (3) $C \rightarrow TGS: ID_C || ID_v || Ticket_{tgs}$
 - (4) $TGS \rightarrow C: Ticket_v$
 - Once per service session:
 - (5) $C \rightarrow V: ID_C || Ticket_v$
- $Ticket_{tgs} = E(K_{tgs}, [ID_C || AD_C || ID_{tgs} || TS_1 || Lifetime_1])$
- $Ticket_v = E(K_v, [ID_C || AD_C || ID_v || TS_2 || Lifetime_2])$



1. $C \rightarrow AS: ID_C || P_C || ID_v$
2. $AS \rightarrow C: Ticket = E(K_v, [ID_C || AD_C || ID_v])$
3. $C \rightarrow V: ID_C || Ticket$

Advantage

- No password transmitted in plaintext
- Ticket is reusable. Timestamp is added to prevent reuse of ticket by an attacker

Secure?

no user authentication

- Ticket hijacking
 - Malicious user may **steal the service ticket** of another user on the same workstation and try to use it
 - Network address verification does not help
 - Servers must verify that the user who is presenting the ticket is the same user to whom the ticket was issued
- No server authentication
 - Attacker may misconfigure the network so that he receives messages addressed to a legitimate server – man in the middle attack
 - Capture private information from users and/or deny service
 - Servers must prove their identity to users
- **Solution:** section key
 - Once per user logon session
 - (1) $C \rightarrow AS: ID_C || ID_{tgs}$
 - (2) $AS \rightarrow C: E(K_C, Ticket_{tgs})$
 - Once per type of service:
 - (3) $C \rightarrow TGS: ID_C || ID_v || Ticket_{tgs}$
 - (4) $TGS \rightarrow C: Ticket_v$
 - Once per service session:
 - (5) $C \rightarrow V: ID_C || Ticket_v$