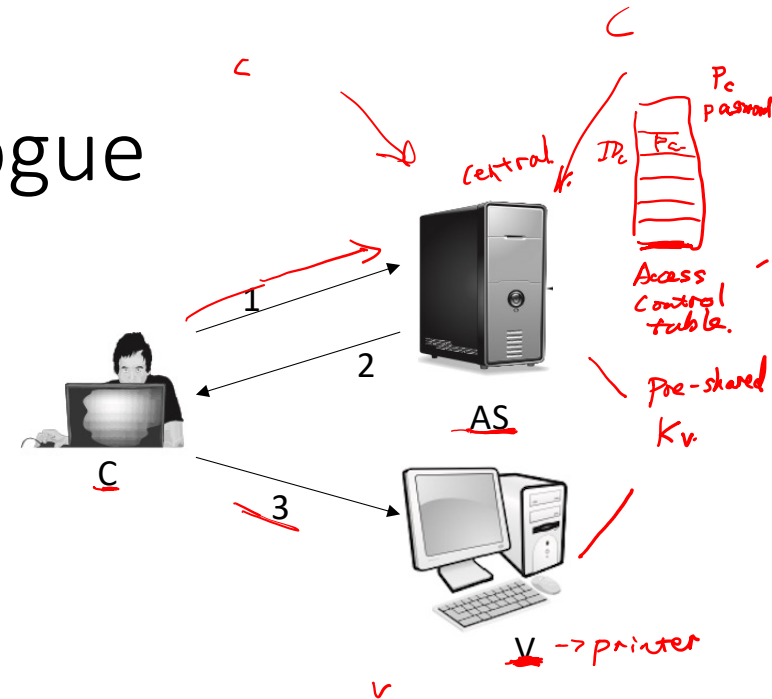


A Simple Authentication Dialogue

- 1. $C \rightarrow AS: \underline{ID_C} || \underline{P_C} || \underline{ID_V}$ *Symmetric Key*
- 2. $AS \rightarrow C: \underline{Ticket} = E(K_V, [\underline{ID_C} || \underline{AD_C} || \underline{ID_V}])$
- 3. $C \rightarrow V: \underline{ID_C} || \underline{Ticket}$ *forwarding*

- AS – authentication server
- ID* - identifier
- P_C - password of user
- AD_C - network address of C
- K_V - secret encryption key shared by AS and V



Advantage

- Client and malicious attacker cannot alter ID_C (impersonate), AD_C (change of address), ID_V
- server V can verify the user is authenticated through ID_C , and grants service to C K_V AS K_V
- guarantee the ticket is valid only if it is transmitted from the same client that initially requested the ticket

$ID'_C \quad P'_C$

AS (ID, Po).

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. $C \rightarrow V: ID_C || Ticket$

Secure?

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

*replay → time stamp
nonce
IV
seq #*

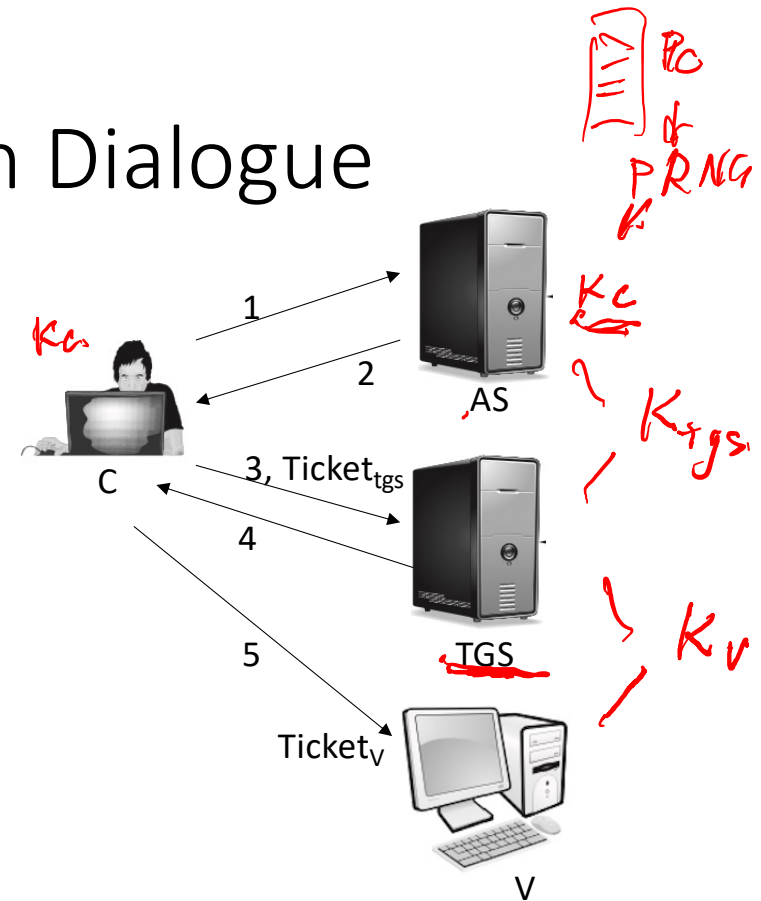
1. $C \rightarrow AS: ID_C || P_C || ID_V$
2. $AS \rightarrow C: \text{Ticket} = E(K_V, [ID_C || AD_C || ID_V])$
3. $C \rightarrow V: ID_C || \text{Ticket}$

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: $C \rightarrow TGS$
 - (3) $C \rightarrow TGS: ID_C || ID_v || Ticket_{tgs}$
 - (4) $TGS \rightarrow C: Ticket_v$
- Once per service session: $C \rightarrow V$
 - (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
- Timestamp is added to prevent reuse of ticket by an attacker

Review and Quiz 2

- Time: Nov. 3, 2025 (Monday) in class
- Content: Chapter 3