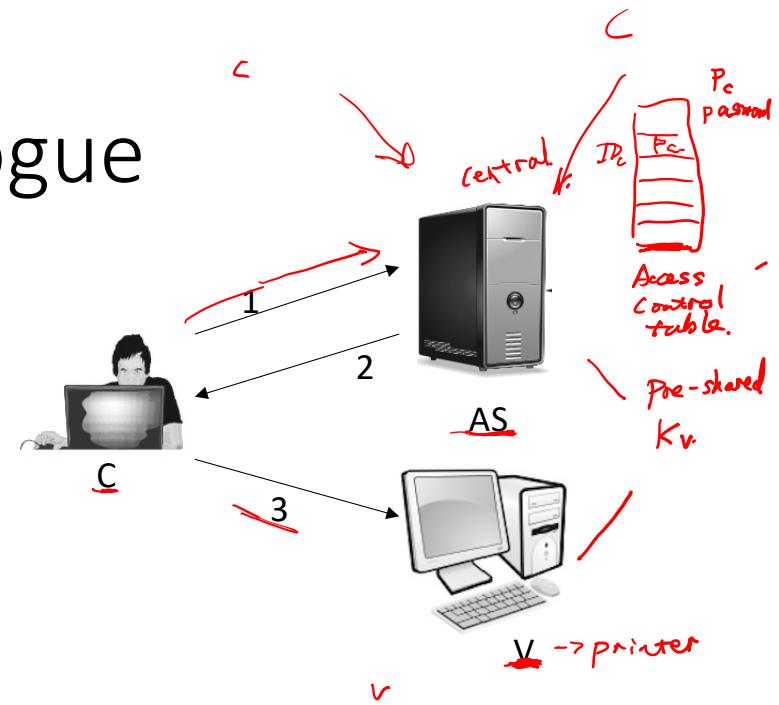


A Simple Authentication Dialogue

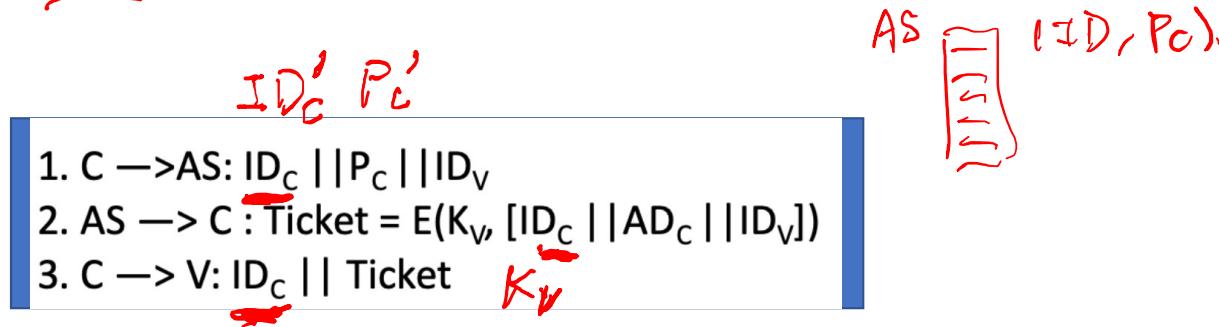
- 1. $C \rightarrow AS: ID_C || P_C || ID_V$ *Symmetric key*
- 2. $AS \rightarrow C: \text{Ticket} = E(K_V, [ID_C || AD_C || ID_V])$
- 3. $C \rightarrow V: ID_C || \text{Ticket}$ *forwarding*

- 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



Secure?

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

replay \rightarrow time stamp
nonce
IV
seq #

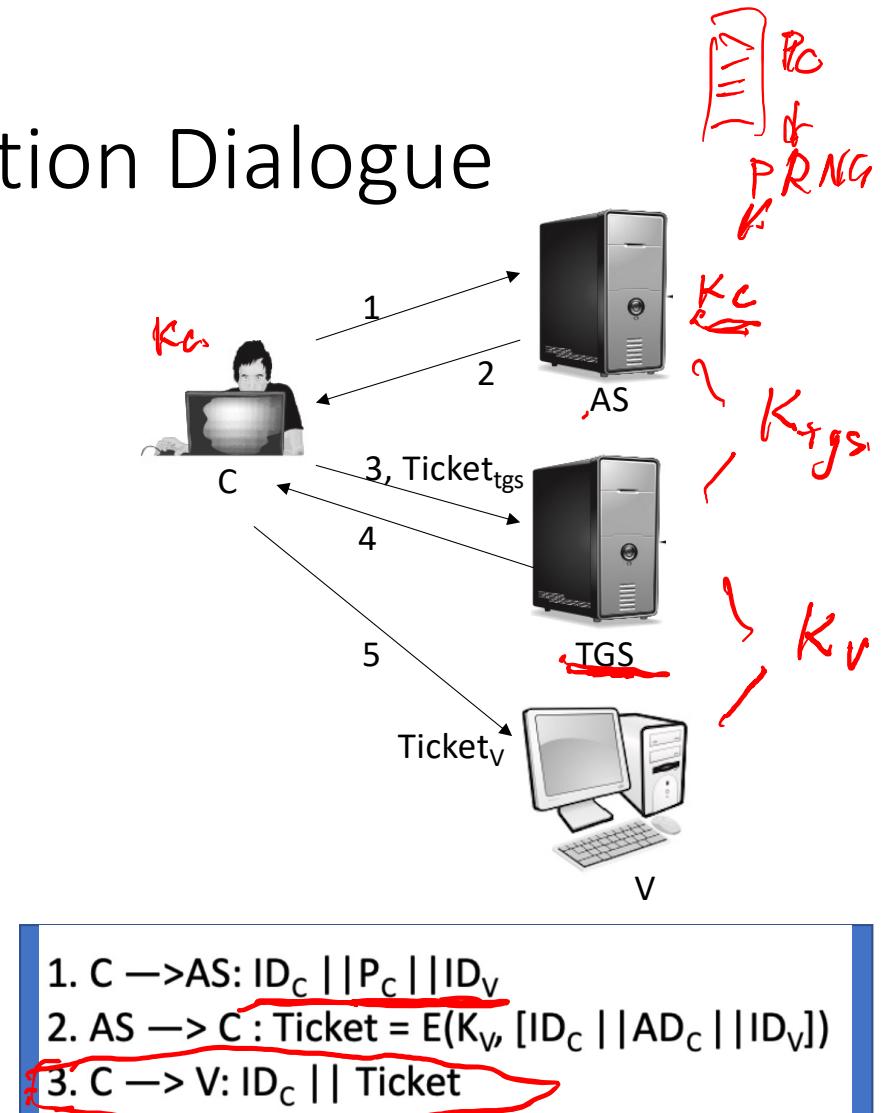
1. $C \rightarrow AS: ID_C || P_C || ID_V$
2. $AS \rightarrow C : \text{Ticket} = E(K_V, [ID_C || AD_C || ID_V])$
3. $C \rightarrow V: ID_C || \text{Ticket}$

A More Secure Authentication Dialogue

- Once per user logon session
 - (1) $C \rightarrow AS: ID_C \parallel ID_{tgs}$
 - (2) $AS \rightarrow C: E(K_C, Ticket_{tgs})$
- Once per type of service: $C \rightarrow TGS$
 - (3) $C \rightarrow TGS: ID_C \parallel ID_v \parallel Ticket_{tgs}$
 - (4) $TGS \rightarrow C: Ticket_v$
- Once per service session: $C \rightarrow V$
 - (5) $C \rightarrow V: ID_C \parallel Ticket_v$

$$Ticket_{tgs} = E(K_{tgs}, [ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_1 \parallel Lifetime_1])$$

$$Ticket_v = E(K_v, [ID_C \parallel AD_C \parallel ID_v \parallel TS_2 \parallel Lifetime_2])$$



1. $C \rightarrow AS: ID_C \parallel P_C \parallel ID_{tgs}$
2. $AS \rightarrow C: Ticket = E(K_v, [ID_C \parallel AD_C \parallel ID_v \parallel TS_2 \parallel Lifetime_2])$
3. $C \rightarrow V: ID_C \parallel Ticket$

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