# Lecture 22

# Network Security

Chapter 4

# Key Distribution

# Symmetric Key Distribution and User Authentication

4.2

# Ways to achieve symmetric key distribution

- A key could be selected by A and physically delivered to B
- A third party could select the key and physically deliver it to A and B
- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key
- If A and B each have an encrypted connection to a third-party C, C could deliver a key on the encrypted links to A and B
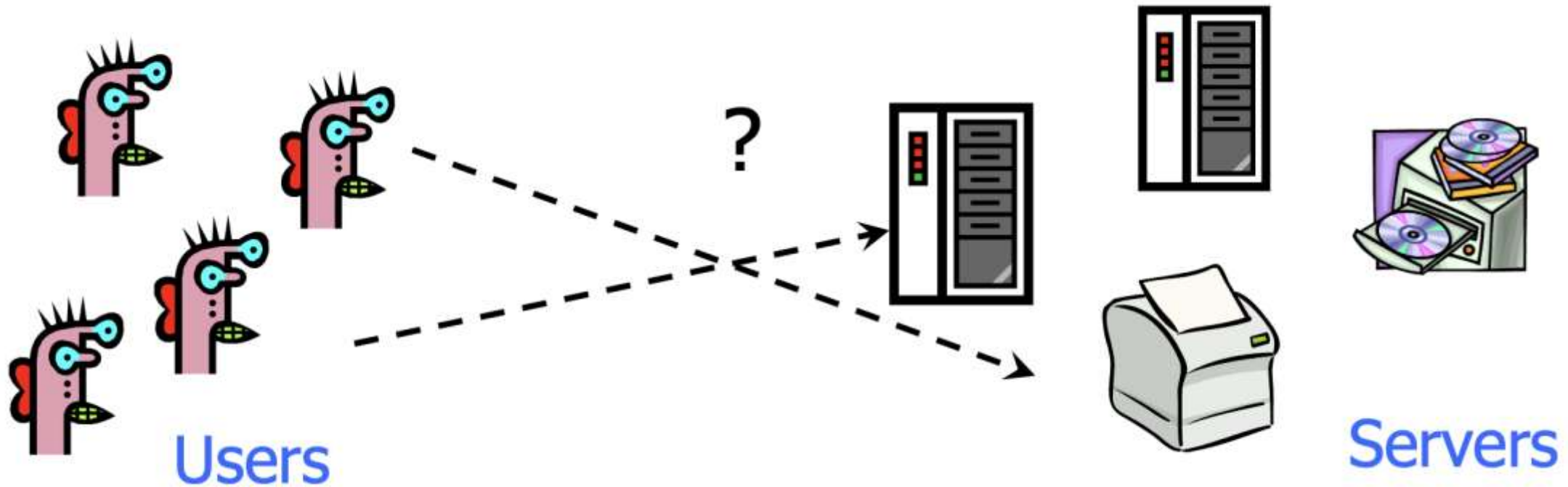
# Terminologies

- Session key

- Permanent key

- key distribution center (KDC)
  - third party authority, centralized infrastructure
  - give permissions for two parties to communicate

# Kerberos

## 4.3

# Many-to Many Authentication



How do users prove their identities when requesting services from machines on the network?

# Threats

- User impersonation
  - Malicious user with access to a workstation pretends to be another user from the same workstation
- Network address impersonation
  - Malicious user changes network address of his workstation to impersonate another workstation
- Eavesdropping, tampering, replay
  - Malicious user eavesdrops, tampers, or replays other users' conversations to gain unauthorized access

# Requirements

- Security
  - against attacks by eavesdroppers and malicious users

- Transparency
  - users shouldn't notice authentication taking place
  - entering password is ok, if done rarely

- Scalability
  - Large number of users and servers

# Kerberos

- scenario: users at workstations wish to access services on servers distributed throughout the network – many to many authentication

# Kerberos

- a centralized authentication server provides mutual authentication between users and servers

    - a key distribution and user authentication service developed at MIT
    - works in an open distributed environment

- client-service model

- Kerberos protocol messages are protected against eavesdropping and replay attacks

- Kerberos v4 and v5 [RFC 4120]

# A Simple Authentication Dialogue

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



- 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
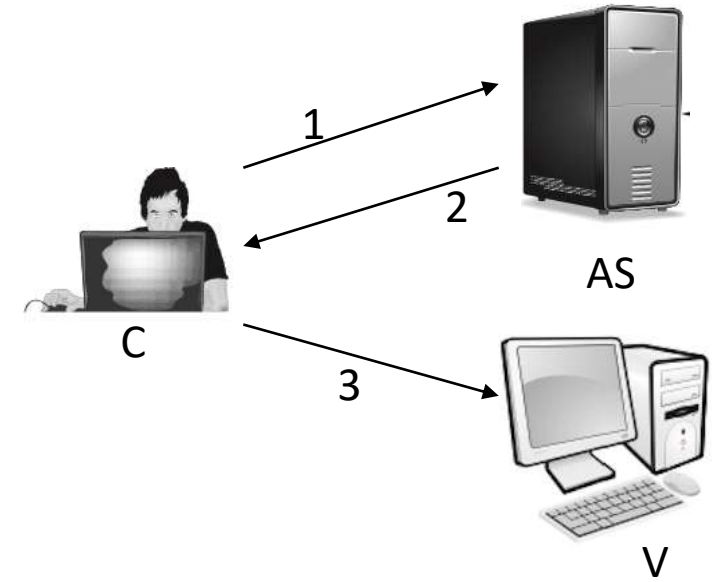
# Cheat sheet

- Allow for half of an A4 paper