

## Lecture Outline



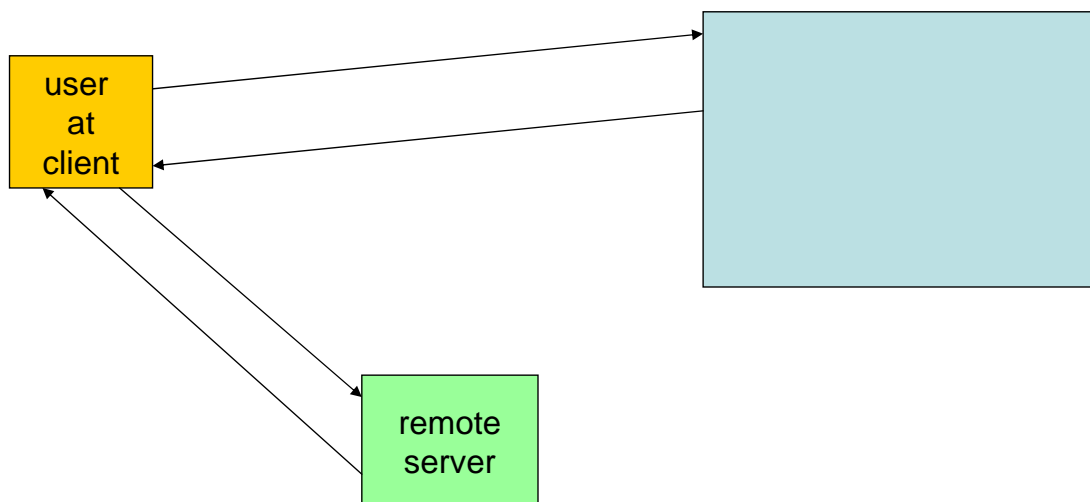
- Internet Authentication Applications
  - **Kerberos (remote log in)**
  - X.509 (Directory Authentication Services – S/MIME) (Friday)
  - PGP (Friday)
  - Computer and Network Forensics (next week)

## Internet Authentication Applications

- Some approaches that organizations use to secure networked servers and hosts (remote log in)
  - Biometric facilities
  - Systems that generate one-time passwords
    - Problem with the above – they require specialized equipment
      - expensive
      - e.g. DES gold card used by banks
  
- Another solutions is to use authentication software tied to a secure authentication server – approach taken by **Kerberos**
  
- MIT
- Available both in the public domain and commercially supported versions
  
- Kerberos is widely used – very popular – defacto standard for remote authentication

## Overall Scheme of Kerberos

- 3<sup>rd</sup> party authentication service
- Clients and servers both trust a Kerberos server to mediate their mutual authentication



## Kerberos Overview

- Authentication Server (AS)
  - user initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket-granting ticket TGT)
  
- Ticket Granting server (TGS)
  - user subsequently request access to other services from TGS on basis of its TGT

## How to do send verification securely

- User at the Client should not have to send password to the AS - over the network
- Kerberos should not have to send a plaintext message to the server to validate the client – over the network
- Some form of \_\_\_\_\_ should be used
- In fact the DES is used
- The AS shares a unique and secret key with each server
  - these keys must be physically – or by some other secure manner – be exchanged beforehand

User and Client interaction with AS

## Ticket Granting Ticket (TGT)

- This ticket contains:
  - indication that AS has accepted this client and its user
  - the user's ID
  - the server's ID
  - a timestamp
  - a TTL
  - copy of the same session key sent in the outer message to the client
  
- The entire ticket is encrypted using a secret DES key shared by the AS and the server – thus no one can tamper with the ticket

## Ticket Granting Server (TGS)

- Recall that the AS served the client the secret session key encrypted by the user's password (it was also buried in the TGT) -  $S_{K_{\text{session}}}$
- Recall that the TGT is encrypted with a secret DES key
- This DES key is shared by the AS and the server

## Server

- The TGT is thus decrypted using the \_\_\_\_\_ by the server
- When the TGT is decrypted, it reveals the \_\_\_\_\_
- Remember the Client also has access to the \_\_\_\_\_