Internet Authentication

Seperation of Concern
- Specialized network
- Specialized hardware

Least Privilege
- Only gain access to each system you need
- Require infrastructure to stop you from always authenticating
- Automate authentication

Kerberos: Most use Internet Authentication System

User sends ticket for AS (Authenticating server)

Ticket returned to user that is encrypted using actual password.
If you can open the ticket with your password you were authentic.

How do you verify the AS
- Shared secret. Also used to encrypt ticket
  some secret ticket
Wendell Reifs

- SSS
- number of registered clients
- number of application servers, shape they withdraw

Multiple Parties
- some trust secrets by
- some trust one another

X.509 Digital Certificate

Use 2-way system to prove I am who I say I am

Use a public and private key communication
- how do you get the public key certificate, only who you trust

Certifying authority
- some one I trust
- how do I trust them - well whom
- how do I know it is them
- use their public key

What happens is CA's private key is compromised
- must revoke it
Public Key Infrastructure
hardware, software, people policies, procedures for digital certificates