Last time

- Secure comm channel
- Authorization
  - ACLs
  - Tickets
Example: Web

Guard

Auth.

Service

B

W

Sec. comm channel
authenticated confidential
Authentication Protocol

CA

Cert_B
Cert_W

B

W
Authentication Logic (BAN logic)

msg: \( m, \text{sign}(m, k_A) \); \( m = \) "give A your cc#"

Trust that \( k_A \) speaks for A?

msg \( m_2: m_2, \text{sign}(m_2, k_B) \); \( m_2 = \) "\( k_A \) is A’s key"

“Web of trust”
Make Assumptions Explicit

\[ \text{sign}(m, k_A) \Rightarrow A \text{ says } m \]

\( k_A \text{ speaks for } A \)

- Assume signature is not forgeable

- Assuming private keys are actually private
Establishing initial trust

0) Web of trust ➔ PGP

1) Does W know/trust P?
   How does it decide?
   cc# is good, verified.

2) How does P trust W?
Issues:

CA authenticate W?

User got CA Pub key?

What if priv. keys stolen?