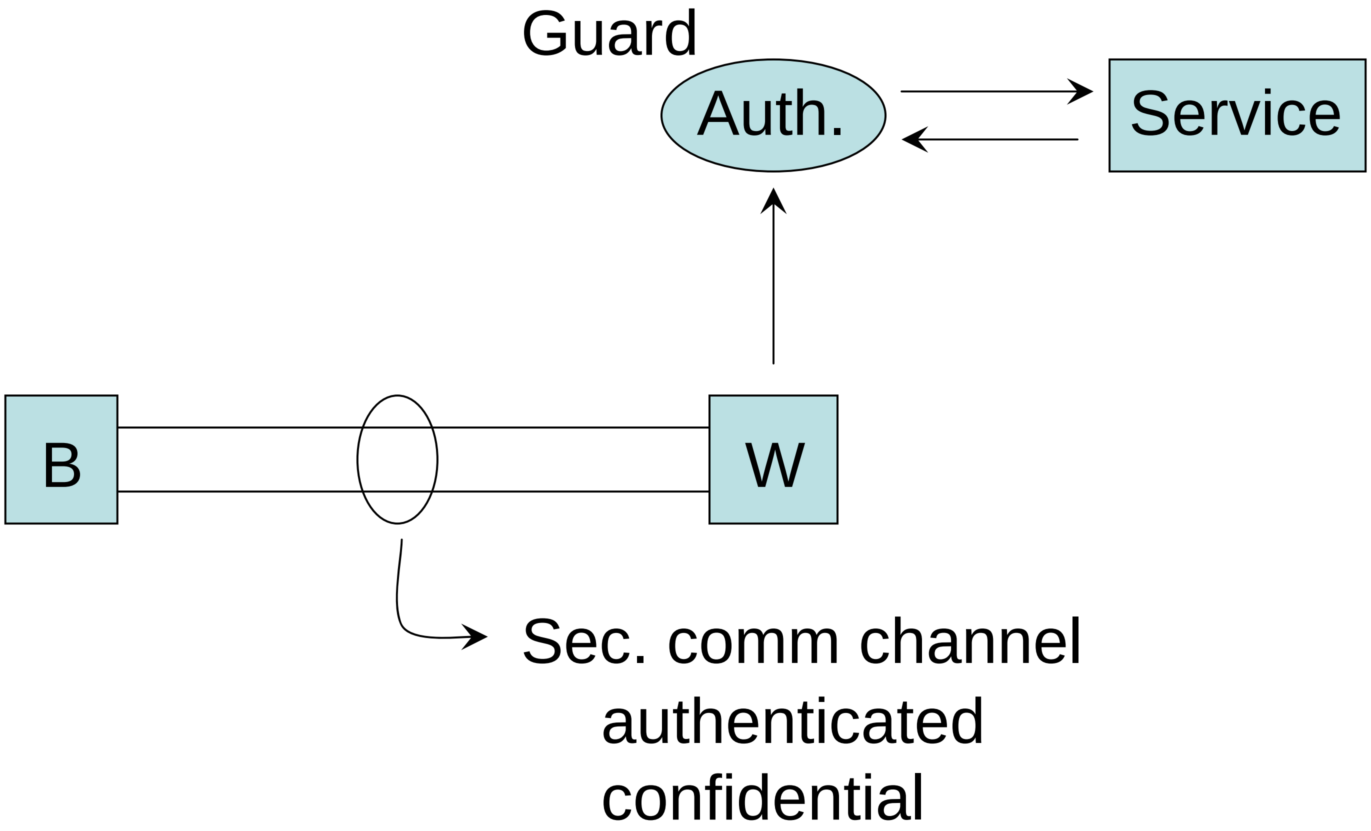
6.033 Computer System Engineering
Spring 2009

Last time

- Secure comm channel
- Authorization
    - ACLs
    - Tickets

Example: Web



Guard

Auth.

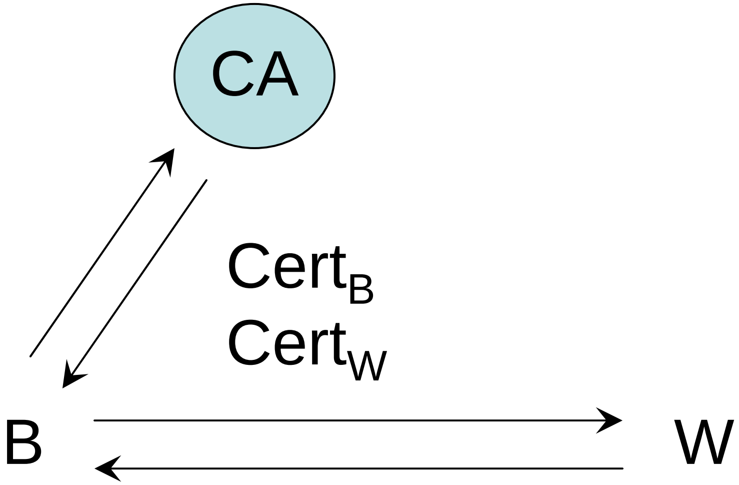
Service

B

W

Sec. comm channel
authenticated
confidential

Authentication Protocol



Authentication Logic (BAN logic)

msg: m, sign(m,kA); m = “give A your cc# **”**

Trust that kA speaks for A?

msg m_2: m_2, sign(m_2,kB); m_2 = “kA is A’s key**”**

“Web of trust”

Make Assumptions Explicit

`sign(m,kA)` ➔ A says m

kA speaks for A

- Assume signature is not forgeable
- Assuming private keys are actually private

Establishing initial trust

0) Web of trust ➔ PGP

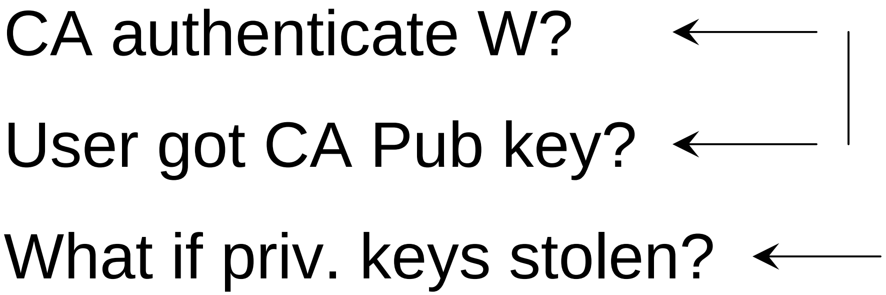
1) Does W know/trust P?

   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?