

MIT OpenCourseWare
<http://ocw.mit.edu>

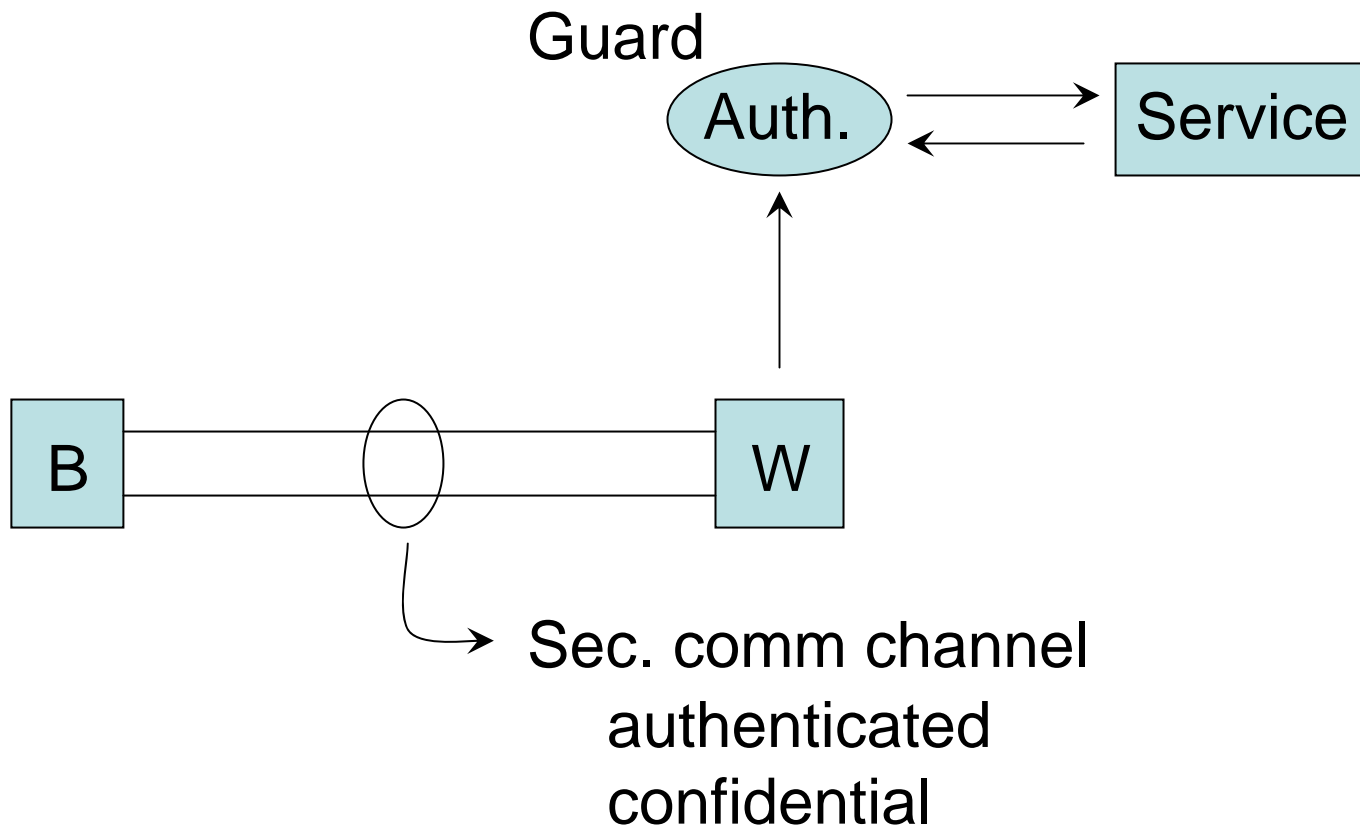
6.033 Computer System Engineering
Spring 2009

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.

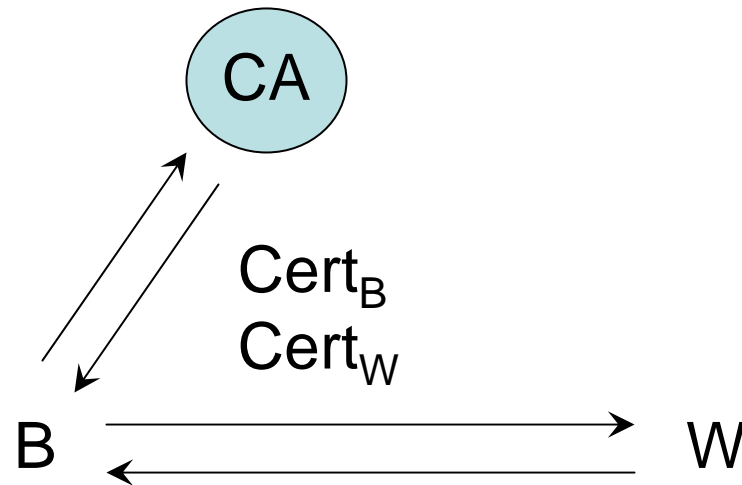
Last time

- Secure comm channel
- Authorization
 - ACLs
 - Tickets

Example: Web



Authentication Protocol



Authentication Logic (BAN logic)

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

Trust that kA speaks for A?

$\text{msg } m_2: m_2, \text{sign}(m_2, kB)$; $m_2 = \text{"kA is A's key"}$

“Web of trust”

Make Assumptions Explicit

$\text{sign}(m, k_A)$ \rightarrow A says m

k_A speaks for A

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



Establishing initial trust

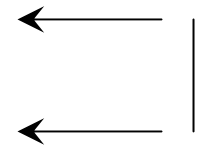
- 0) Web of trust → PGP
- 1) Does W know/trust P?
How does it decide?
cc# is good, verified.
- 2) How does P trust W?

Issues:

CA authenticate W? ←

User got CA Pub key? ←

What if priv. keys stolen? ←

A vertical line is positioned to the right of the first two questions. Two horizontal arrows point from this line to the left, one to the first question and one to the second question. A third horizontal arrow points from the left to the third question.