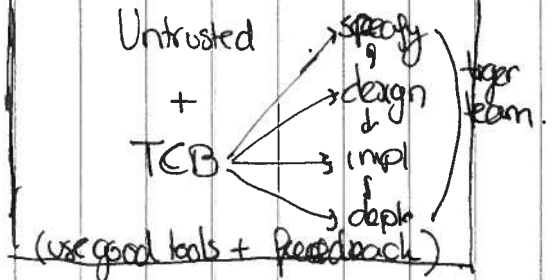
Boardplan (5/9/07)

⓪ Security is hard

- Design? (protocol?) ssl v1.
- Implementation? (buffer overflow)
- Deployment? backdoor (tomorrow's ready) (empty admin password).

(Internet not designed/impl with security in mind).

① Assurance approach



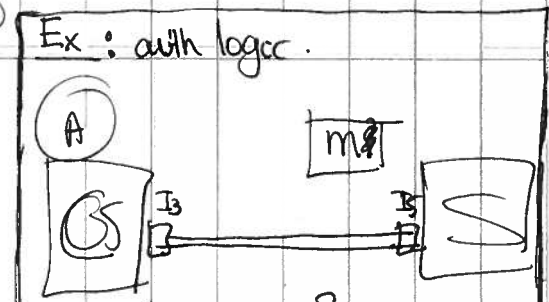
(use good tools + feedback)

② Least privilege

If there is a compromise/failed day

(separate: ssh agent).
okws

③ Ex: auth logic.



A says m ?
I5 says m does I5 speak for A

(logic rule).

④

W I5 speaks for W
W speaks for I3
I3 speaks for OS
OS speaks for A
⇒ A says M

(big TCB).

⑤ Internet

I5 speaks for Internet
Internet speak for I3 ?
X.
{ A→S: M? $k_{A priv}$.

(use sudo).

⑥ Assumptions

- Crypto ok
- ~~A's computer, priv key~~ A is careful w. key
- MIT is " "
- MIT deterred A's ideally careful
-

central PKI ⇒ hard to deploy

⑦ Web of trust

A's { A, $k_{A pub}$} $k_{C priv}$.
{ A, ... { $k_{D priv}$
⋮
~~Social~~ Social nets have
~~six degrees of separation~~
- bob decides who to trust

Next

What is right?
What is wrong?