Boardplan: principal authentication (5/7/07)

1

Today: authentication of principals.

"give me quiz 3"

A

who is A?
who is S?

- slide w. CA

2

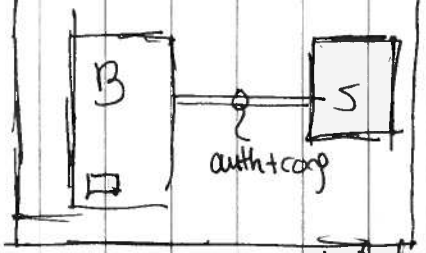
Attacks:

1) ~~attacks on~~ crypto + known key
2) replay
3) impersonation
4) reflection ⇒ cryptographic protocols.

- denning-sacco slides + fix.

3

User Authentication in Web



(SSL slide + ~~certificate~~ cert slide)

4

User authentication

1) render-vous
2) verification.

3a

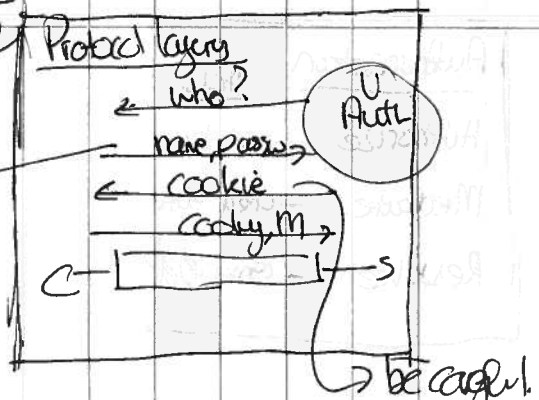
Issues:

- ~~Verisign~~ Verisign's public
- What if private key is compromised
- What if DNS names differ?
- Trust CA?

→ Verisign slide → ease of use versus security.

5

Protocol layers



weak but popular. dictionary attack.

→ be careful.

6

Questions.

- passwd?
- what does S know? does it know identity of U No
- when transaction? No

7

Authorization

1) access control list
   - authorization
   - revocation
2) capabilities
   - revocation
   - cookies

(often both)

AFS

2.08.