Software Engineering
at the
University of Oxford

Advanced vulnerabilities: [Ryan, Schneider]

<u>Reflection</u>

Bounce messages back to an agent
- perhaps fool into revealing answer to own question
  e.g. what is p/w?

⇒ Ensure that sentries authenticate themselves with the same password as everyone else.

<u>Oracle</u>

Induce honest agent to perform protocol step that introduces otherwise unobtainable information to the client.

Attack may be across protocols or protocol runs.
+ protocol esp. where key material shared across protocols.

⇒ Explicitness of ~~terms~~ atomic of protocols.

- Abadi, Needham, Prudent eng. practice for crypto. protocols. IEEE Tx on Soft Eng, 22(1), <u>196</u>.

<u>Interleave</u>

Protocol runs overlap.
e.g. <u>Interleave</u> + Oracle: -- Needham-Schroeder Public-Key.

Failure of forward secrecy; Algebraic.

<u>Basic</u>: Man-in-the-middle, Replay