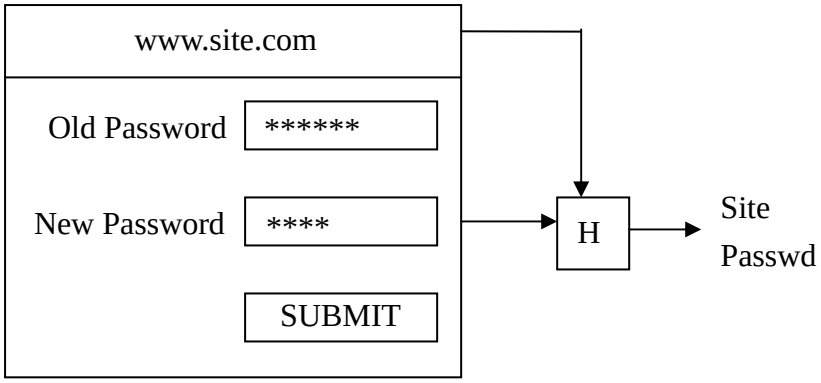
Class Note: 4/24/2007

Human Fallibility in Security

- "Why Johnnie can't Encrypt"
- Web password managers
- Ad-hoc networks
- Site Key

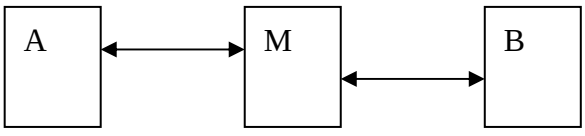
Web password managers



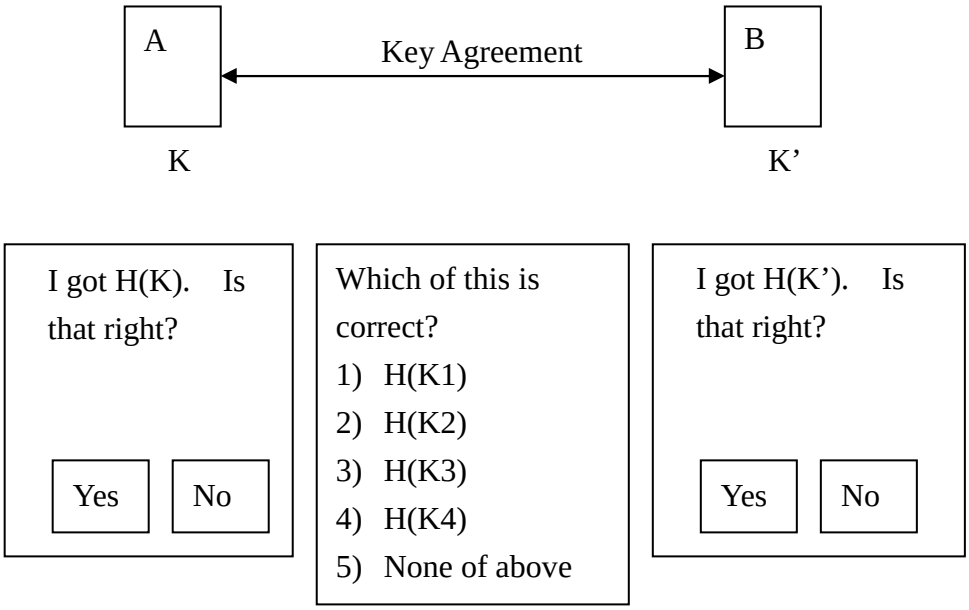
- User needs to be able to control whether hashing occurs
- Web browsers, such as IE & Firefox, plug-in: Standford Pwdhash
- Enable hashing in two ways
  1. Hashing defaults to off
  2. Enable via F2 or @@ prefix

- Remember password?
- Some kind of feedback will help indicating hashing is either on/off

Ad-Hoc Networks



Man in the middle
Attack



This kind of questions helps users, like A & B, to answer the questions seriously; instead of carelessly choosing Yes.

Seeing is Believing

- Piggyback security actions onto other user actions.
- Example: take a picture of the barcode of the communicating device

Site-Key Paper

- Users are lazy, unreliable
- Users take different actions based on perceived risk
  - User studies benefit when subjects face real risks

In the paper: the study

Group A	Group B	Group C
Role-playing	Role-playing	no Role-playing
No security	security	no security

Result:

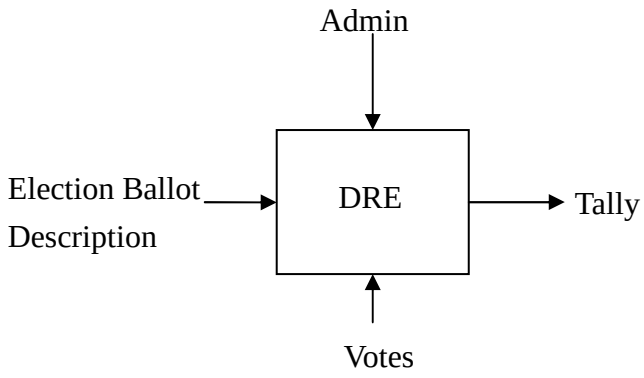
A – C: no difference

B – C: no difference

(A + B) – C: difference because number of participants increased

Electronic Voting System

- A touchpad with
  - Many voting screens
  - Review screen
  - Cast vote (final step)
  - Voters have private access to the machine



Security Goals:

- Voter anonymity
- Correctness of Ballots
- Correct tally
- One vote-per-voter
- Availability