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
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

<table>
<thead>
<tr>
<th>Group A</th>
<th>Group B</th>
<th>Group C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-playing</td>
<td>Role-playing</td>
<td>no Role-playing</td>
</tr>
<tr>
<td>No security</td>
<td>security</td>
<td>no security</td>
</tr>
</tbody>
</table>

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