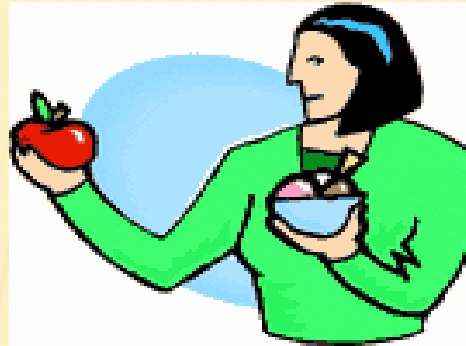


PASSWORD MEMORABILITY AND SECURITY: EMPIRICAL RESULTS

J. Yan, A. Blackwell, R. Anderson, A. Grant
IEEE Security & Privacy 2(5), pp. 25-31, 2004

Presenter: Luwei Zhang

SUMMARY



- Description of the **trade-off** between password memorability and security;
- Empirical investigation of this trade-off in password users;
- Comparison between pass phrase and random password;
- Tentative recommendation & Suggestion of looking for compliance enforcement mechanism that work well with mnemonic password choice.

PARTIAL DEFINITION OF EXPERIMENTAL DESIGN

- Treatment: something that researchers administer to experimental units.
 - ❑ E.g. pass phrase, etc.
- Variable
 - ❑ Input variable: controlled independent factor, e.g. length;
 - ❑ Output variable: dependent result of experiment, e.g. crack rate;
- Experiment bias: the favoring of certain outcomes over others.

APPRECIATION

- A valuable and contributing experiment study against the trade-off.
 - ❑ Correct choose of treatments
 - Traditional password, random password and passphrase
 - Representativeness
 - ❑ Output variables are supportive
 - Time to memorize (memorability)
 - Password difficulty level (memorability)
 - Crack rate (security)
 - ❑ Detailed analysis and comparison among the three password types
 - ❑ Suggestion are constructive

CRITICISM (1)

➤ One experiment bias

- ❑ Experiment bias: the flavouring of certain outcomes over others.

- ❑ Where was the bias?

- Comparison between random password & pass phrase;
- Random password group was **not** instructed using special character, however pass phrase group was given;
- The author neglected to **control** for the effect of the differences in special character.
- Crack rate of random password could be much lower if using special character.

CRITICISM (2)

- Dictionary files were neither clarified nor briefly discussed.
 - ❑ Deduction of credibility of the crack rates in table 1.
 - Dictionary size and variety are unclear
 - Passphrase dictionary files are unclear
 - Attackers are studying phrases and building large passphrase dictionary.
 - ❑ Implicit experiment bias

QUESTION

- What other good experimental designs would you suggest? Or what other good element could be taken into account to improve the current design model?