Password Memorability and Security: Empirical Results

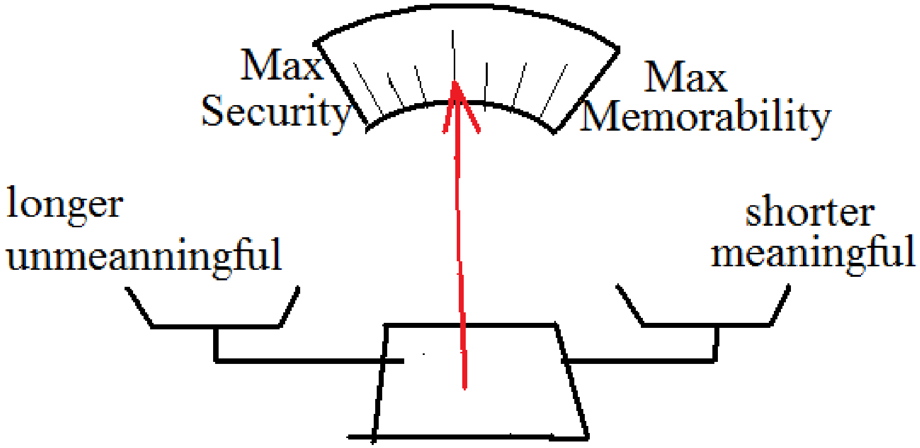
Jeff Yan, Alan Blackwell , Ross Anderson, Alasdair Grant

IEEE Security & Privacy 2(5) Sept.-Oct. 2004

Presented by Yuan Qian

Summary of the article

- In order to investigate the trade-off between password memorability and security, the authors did an experiment.
- The authors tentatively recommended some techniques for choosing passwords.



Appreciate

- Focused properties are critical to the password security and memorability
  - Focused properties in experiment: meaningful, non-letter characters, length

- Good Recommendation
  - Easy to flow
    - No extra work after the passwords are set up

  - Phase based technique increase the memorabitliy and security at the same time (No trade-off)

Criticism

Lack of detailed description about how the passwords cracked

- Factors controlled in the experiment
  - Students in each group is randomly allocated
  - Passwords memorability are reviewed at the same time

- Factors need to be mentioned in the experiment
  - Time taken for cracking the password
    - Will a hacker give up if it takes so much time to crack a password in reality?
    - Should a cracked password still be considered secure enough if it takes so much time to crack?

Criticism (continued)

- Attempt times on passwords cracking
  - Should an individual user’s cracked password still be considered secure enough if a hacker attempted so many times to crack it manually?
- Brute–force attack efficiency
  - What is the efficiency of the Brute-force attack used in the experiment?
  - If the brute-force attack used for the experiment is efficient enough, does that mean none of the password is securable.

  (“Bruce-force attack: Try all possible combinations of keys.”)

Will the experiment results be affected significantly if we take theses factors into count?

Question

- If you are going to do the same experiment, what factors will you consider into the experiment?