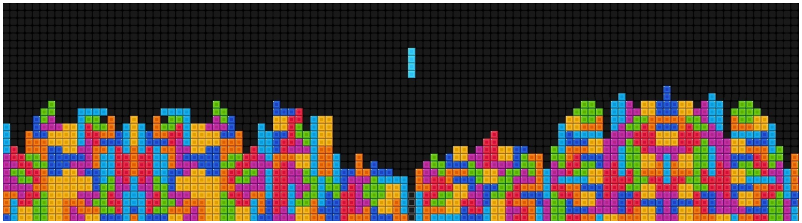
Generation T – The Gamification of Password Generation

Henry Li, Matthew Kuo, Anson Wong, Kevin Lim

University of British Columbia



wallpaperscraft.com/image/background_texture_tetris_figures_29901_3840x2160.jpg

October 27, 2015

Computer Security

Introduction

The usual problems...

- Users do not in general choose good passwords
- Memorability of passwords is still a pervasive problem
- Memorable passwords become predictable

The use of *gamification*

- Entice users to perform important task seen as secondary
- leverage a specially designed *enjoyable* task

Use Case

Password managers already respected as good solution.

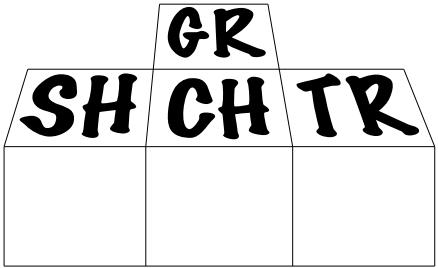
- We do not propose to replace these solutions
  - unique passwords per account is still recommended
  - untenable to expect users to memorize unique passwords for every account (usability issue)
- Complement managers
  - Password managers still need to be authenticated
  - We want a secure yet memorable password to fit this use

Related Work

- Shing-hon Lau, Stephen Siena, Ashutosh Pandey, Sroaj Sosothikul, Lorrie Cranor, Blase Ur and Richard Shay. **Exploring the Usability of Pronounceable Passwords.**
  - Lead us to the idea of using phonemes as *atomic* pieces with which to construct passwords. They present some sets of useful phonemes and compares them to alphanumeric character sets.
- Sundararaman Jeyaraman and Umut Topkara. **Have the cake and eat it too – Infusing usability into text-password based authentication systems.**
  - Gives a study on the use of mnemonics techniques in password generation
- Andrew M. White, Fabian Monrose, Katherine Shaw and Elliott Moreton. **Isnt that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens.**
  - Presents some heuristics and ratings for pronouncability of *word-like strings*

Proposed Approach

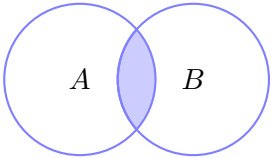
- Use tetris to test hypothesis
- Put phonemes (distinct units of sound) on blocks since they lead to prounounceable passwords—more memorable (ref related works)
- Cleared lines construct strings to be potentially used as passwords
- Hopefully see if user's interaction in password generation will affect memorability of password



Evaluation of Our Method

A-B Testing

- One group will be aware of the phonemes represented as blocks
- Second group will not have transparent blocks
- Both groups will be subject to memorization of fully automated random generation of phoneme based passwords



- Password entry will be timed to evaluate usability of the generated passwords

Users will be invited for follow up evaluations to test password recall.

Brief Security Analysis

Empirical study on security of passwords generated

- Will use a GPU to try and crack collected passwords
- We choose a representative hash function
- Gives a realistic strength metric given an offline scenario

Timeline

- Prototype (~2 weeks)
- Conduct experiment and analysis (~1-2 weeks)
- Prepare film, final report and presentation (~1 week)

Conclusion

- We explore the correlation between memorability and interaction in the generation of prounounceable passwords
- Limited time and scope
- Invite further study on tasks focussing on interaction and memorability