Visual End-User Security

Elizabeth Stobert
Carleton University, Ottawa, Canada
elizabeth_stobert@carleton.ca

Robert Biddle
Carleton University, Ottawa, Canada
robert_biddle@carleton.ca

I. Motivation

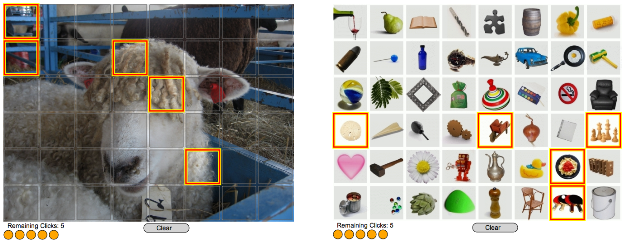
As more transactions (both financial and social) take place online, the importance of computer security grows. One problem that affects many users is remembering and keeping track of passwords. Most users have many different accounts, and are expected to create a password for each account that is secure, memorable, and unique. Users often cope with these demands by choosing passwords that are easily guessed by attackers, re-using the same password across many accounts, or writing their passwords down. Too often, the passwords that are easy to remember are also easily guessed by attackers. This is known as the password problem.

Graphical passwords are one approach to solving the password problem. Graphical passwords [1] are passwords that use images instead of text, and leverage the human ability to remember images better than text (known as the *picture superiority effect* [2]). They have been shown to have good usability and memorability, but have not been widely adopted. Work on graphical passwords has shown that images can be leveraged to help users better remember random assigned passwords (which are less susceptible to guessing attack) [3]. This project involves exploring how these schemes can be deployed effectively to other areas of computer security.

Managing passwords is not programming, but it does involve challenging cognitive tasks where the designer must understand the complex principles that are important for success. We feel that the necessary design task needs to leverage knowledge beyond usability, and requires principles similar to those in notational systems typically used in end-user computing.

II. PassTiles

The psychology literature shows that leveraging recognition memory should lead to more memorable passwords. In our earlier work [3], we investigated the effects of different kinds of memory retrieval (recall, cued-recall, and recognition) on the memorability and usability of random graphical passwords. Random assigned passwords are secure against dictionary attacks, and resistant to brute force attacks, but have typically been very difficult for users to remember. We studied PassTiles (Fig. 1), a graphical password system designed by us to allow direct comparison of different types of retrieval. PassTiles presents the user with a grid of password tiles, and their password consists of a number of those tiles. To log in, the user must click on the correct tiles (in any order). Image PassTiles (Fig. 1(a)) leverages cued-recall and underlays the tile grid with a background image to help the user locate their password tiles. Object PassTiles (Fig. 1(b)) places an object image in each tile of the grid, and the user's password consists of a set of object images. The same set of objects is always displayed, but it is shuffled at every login to force users to rely on recognition memory (rather than recall of the tile positions). Our studies of random assigned PassTiles passwords showed that recognition-based passwords were memorable, but the associated login times were very slow, compromising their usability. We concluded that recognition memory is good for the memorability of graphical passwords, but the system must be carefully designed to avoid usability problems. The work also showed that participants were capable of remembering long random numbers, in the form of graphical passwords. Moving on, we now want to explore practical deployment of this knowledge.



(a) Image PassTiles (b) Object PassTiles

Fig. 1. Password creation interfaces for PassTiles, with the passwords highlighted.

III. Password Managers

Password managers are programs that remember and manage users' passwords to help users better manage their online security. Examples of password managers are LastPass (http://lastpass.com), 1Password (https://agilebits.com/onepassword) and the password managers built into web browsers. Password managers work in two ways [4]: they either generate a password by hashing the user's master password, or the manager stores the user's passwords in a password "wallet", which is protected by a master password. In either case, if the master password is compromised, it becomes a single point of failure for all of the user's passwords.

Our prototype password manager uses PassTiles graphical passwords to help users better remember passwords and manage online accounts. It has several distinctive features:

No stored passwords: Our password manager does not actually store any passwords. Instead it stores the image cues for randomly assigned PassTiles passwords, and allows users to generate their passwords.

Each cue can be used for several accounts: Our password manager separates password management from account management, and passwords and accounts are created independently. Each website account is linked to a password, and multiple accounts can be linked to the same password. The user may choose to use the same password for similar accounts (e.g, using the same password for all e-commerce websites), and may choose to protect more important accounts with a more secure password that isn't used elsewhere.

Same password, different encoding: For each account, the system stores a password "sugar" to be hashed with the generated password string. The password sugars are modelled on password salts, which are random strings hashed with passwords to make them less vulnerable to guessing attacks on the hashed password. The sugar is a user-chosen string that is encoded with the string generated by the password system to create the password that is sent to the website. If a user assigns the same password to multiple accounts, but chooses different password sugars, the passwords saved by the websites will be different (even though the cue and response are the same).

Accommodating different password rulesets: Different websites have different requirements for the lengths and character sets used in their passwords. These rulesets can conflict, and some websites have mutually exclusive rulesets. Our password manager allows the user to define and select an appropriate ruleset for each website.

After passwords are set up in the password manager, they are accessed from a bookmarklet saved in the user's browser. The bookmarklet is a short javascript program that takes the url and username and pops up the appropriate password cue. Once the user has entered their password, the appropriate ruleset and sugar are used to generate the password, which is automatically pasted into the appropriate field. This frees the user from having to install web browser extensions.

By only storing password cues, our prototype password manager avoids becoming a single point of failure. It also provides a safe way for users to reuse the same password across different accounts. Our earlier work has indicated that users should be able to more easily remember PassTiles random assigned passwords than text passwords, and we leverage that in our password manager for increased security.

In our future work, we are interested in further development and user testing of our password manager. One challenge is to develop an easy way for users to define password rules about character set and length. We think that a visual language may allow users to better understand password rulesets. In addition, we would like to conduct detailed user testing of the password manager. When studying security products, ecological validity is very important, and we would like to study use of the password manager in a real life situation. This requires instrumented data collection, and balancing data collection against privacy concerns.

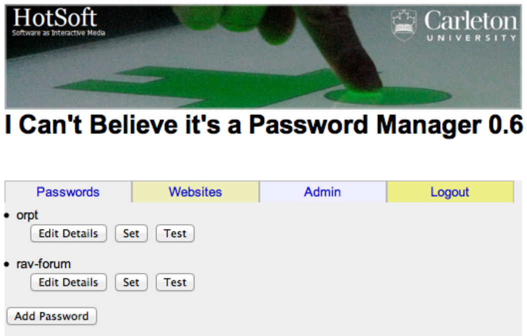


Fig. 2. Screenshot of our prototype password manager, showing the passwords tab.

IV. Applications of Random Numbers

As well as the password manager, we are also interested in other applications of human-memorable large random numbers. An important related area in computer security is encryption of email messages. Even the most usable solutions for email encryption have been shown to have problems [5]. These problems typically relate to difficulties with the concept of asymmetric encryption, where a public and private key are required to sign and open encrypted emails. The key metaphor does not accurately reflect the way these keys are used in encryption. We believe that graphical passwords can be leveraged to not only help users remember keys, but also to better understand the security model. An issue related to email encryption is public-key infrastructure and the certificate model for web security. We speculate that it may be possible to leverage graphical passwords to help users check the validity of security certificates. We also suggest that the development of a model similar to the Cognitive Dimensions of Notations framework [6] could help designers to understand the issues present in designing security tools for end users.

V. Conclusion

In our work, we examine ways to apply work on graphical passwords to password management and other aspects of web security. We hope that applying knowledge from end-user computing will help to design more secure and usable systems.

References

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," *ACM Computing Surveys*, vol. 44, no. 4, to appear.

[2] A. Paivio, T. B. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?" *Psychonomic Science*, vol. 11, no. 4, pp. 137–138, 1968.

[3] E. Stobert, "Memorability of Assigned Random Graphical Passwords," Master's thesis, Carleton University, Department of Psychology, Aug. 2011.

[4] S. Chiasson, P. Van Oorschot, and R. Biddle, "A usability study and critique of two password managers," *15th USENIX Security Symposium*, pp. 1–16, 2006.

[5] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *USENIX Security Symposium*. Carnegie Mellon University, Aug. 1999, pp. 169–183.

[6] A. Blackwell and T. Green, "Notational systems–the cognitive dimensions of notations framework," *HCI Models, Theories, and Frameworks: Toward an Interdisciplinary Science. Morgan Kaufmann*, 2003.