Usability of Graphical Passwords*

Susan Wiedenbeck and Jim Waters, Drexel University
Nasir Memon, Alex Brodskiy, Polytechnic University
Jean-Camille Birget, Rutgers University-Camden

Human users are not good at remembering alpha-numeric passwords, if the passwords are complicated enough to be secure. Graphical passwords may be easier to remember and use over the long run because they are based on recognition of locations in a picture rather than un-cued recall. In a graphical password system, an image is displayed and the user chooses several points in the image as a password. To log in, the user has to click close to these points again. Older systems use preprocessed images with pre-defined click regions, among which a user has to choose. We have designed systems that allow users to choose any points as click points. This increases the flexibility and offers a much larger password space. A major part of this work involves usability evaluation of our graphical password systems.

We are evaluating graphical passwords in terms of five usability goals [1]:

- Learnability – How easy is it for users to learn a graphical password?
- Memorability – Can users remember a graphical password once they have learned it, even when there are gaps in usage?
- Efficiency – How fast can a user log in using a graphical password? User errors are a part of efficiency because they impact the speed of performance.
- Security – Do users develop unsafe practices with graphical passwords that diminish security?
- User satisfaction – Are users subjectively satisfied and would they be willing to use graphical passwords?

We are currently carrying out empirical studies addressing the usability goals above. In one study we are comparing users' performance with graphical passwords and alpha-numeric passwords in a longitudinal study, consisting of a learning session and three retention sessions. In the learning session, participants choose a password and practice it to a criterion. We use trials to the criterion as a measure of learnability. After learning the password, participants answer a questionnaire, which gives us information on security practices and user satisfaction. Following the questionnaire, the participants complete the first retention session by logging in one time with their password. We measure memorability in terms of the number of trials to log in successfully and efficiency in terms of time to log in. The second and third retention sessions take place one week and five weeks later respectively. They are identical to the first retention session. At the end of the third retention session we administer another questionnaire, and we also interview both alpha-numeric and graphical participants about their experience learning and using passwords, particularly their feedback on unsafe practices in using passwords.

Other studies that are underway include:

- A study of how the semantic content of pictures used for graphical passwords affect memorability. This study compares different kinds of pictures, such as everyday objects, people, art and maps.
- A study that varies the tolerance around the click points and measures the effects on efficiency of inputting a graphical password (study based on Fitts' Law).
- A study of the evolution of users' efficiency of inputting graphical passwords in daily use over a period of a month.
- A study of memory interference when a user creates multiple passwords on either the same picture or different pictures.

At the time of the workshop, we will be prepared to report on our first experiment comparing graphical and alpha-numeric passwords, and we expect to have preliminary results on the experiments of semantic content of pictures and the tolerance around click points.

[1] J. Preece, Y. Rogers, H. Sharp, Interaction Design: Beyond Human-Computer Interaction, John Wiley, 2002.

* This work is supported in part by NSF grant CCR-0310490.