2009 33rd Annual IEEE International Computer Software and Applications Conference

Towards Usable Solutions to Graphical Password Hotspot Problem*

Kemal Bicakci*, Nart Bedin Atalay+, Mustafa Yuceel*, Hakan Gurbaslar#, Burak Erdeniz#

*TOBB University of Economics and Technology, Ankara, TURKEY
{bicakci,myuceel}@etu.edu.tr
+Selcuk University, Konya, TURKEY
nartbedin@gmail.com
#Middle East Technical University, Ankara, TURKEY
{gurbaslar,burakerdeniz}@gmail.com

* This research is supported by TUBITAK (The Scientific and Technological Research Council of Turkey) under project number 107E227.

Abstract— **Click based graphical passwords that use background images suffer from hot-spot problem. Previous graphical password schemes based on recognition of images do not have a sufficiently large password space suited for most Internet applications. In this paper, we propose two novel graphical password methods based on recognition of icons to solve the hotspot problem without decreasing the password space. The experiment we have conducted that compares the security and usability of proposed methods with earlier work (i.e. Passpoints) shows that hotspot problem can be eliminated if a small increase in password entrance and confirmation times is tolerable.**

Keywords-graphical password; password security; usable security; authentication

I. Introduction

Authentication is the process to establish the identity of a communication partner. It is an essential security component of today's many Internet applications. The security weaknesses of using text based passwords for user authentication are well known but most systems still rely heavily on this simple and low cost solution (a recent study shows that 93 % of large businesses in UK still use passwords to authenticate users [11]).

There is a significant body of recent research exploring the feasibility of alternative approaches to provide a more secure and usable authentication solution. One promising alternative is graphical passwords. Based on studies showing that human brain is better at recalling images than text [13], these unconventional methods aim to solve memory burden and low entropy problems of classical passwords.

Among graphical password schemes click-based graphical passwords has gained popularity [24, 12, 3, 17, 20]. In click-based graphical password schemes, users click a sequence of points on a pictorial background to create and use passwords. In-depth examination of click-based graphical passwords shows that these systems are vulnerable to predictability [22]. Certain points (hotspots) on the pictorial background are more likely to be selected by users, which makes passwords predictable. Different attack strategies are quite successful to guess click-based graphical passwords [22, 19, 7]. Some images generate more and definite hotspots than others but the hotspot problem persists even when abstract shapes or the same type of objects (such as cars, paper clips) fill the pictorial background. These results call practicality of click-based passwords into question [22].

In this paper, we report implementation and evaluation of two new graphical password schemes (GPI and GPIS) which have a potential to overcome the hotspot problem while keeping the system usable. These schemes use icons as the clicking points of the graphical password interface (see Figure 1) and provide a password space comparable to earlier systems (i.e. 2^{43} as in Passpoints [23]).

GPI (**G**raphical **P**assword with **I**cons) is the first graphical password scheme we propose in this paper. In GPI, to mitigate the hot spot problem users may click on a subset of displayed icons as their passwords instead of selecting specific locations on a background image. Experimental results show that the use of icons in GPI makes possible to evenly distribute possible click-points to a certain extent.

To eliminate the hot spot problem completely, we design a second scheme GPIS (**G**raphical **P**assword with **I**cons suggested by the **S**ystem) in which the system randomly chooses a subset of icons and presents them to user as a password candidate. If the user is not content with the password suggested, he can request a new password from the system.

With a lab study, we also compared usability of GPI, GPIS and Passpoints [23]. Experimental results have shown that there is no significant difference in the ratios of participants who forgot their passwords in all three systems. Though password entrance time with Passpoints interface is the shortest of all, reasonable usability measures were obtained both with GPI and GPIS. Based on these results, we argue that our proposed methods can be considered as a step towards more secure and usable graphical password solutions.

0730-3157/09 $25.00 © 2009 IEEE
DOI 10.1109/COMPSAC.2009.153

The rest of our paper is organized as follows: A detailed discussion of related work and the formal definition of the research problem we address in this paper are presented in section 2. GPI and GPIS schemes we have implemented and the procedure and the design of the experiment we have conducted are introduced in Section 3. Section 4 provides the analysis of the data collected in the experiment. Section 5 gives concluding remarks.

II. Related work and problem definition

Previous work on click-based graphical password schemes can be studied in two groups. In the first group, there are recognition based schemes in which a number of different images (e.g., faces [14], random art images [6], images clustered into semantic categories [1]) are displayed on user's screen and the user selects among these images to generate his password. This procedure can be repeated for a number of rounds to increase the password space. Second group consists of numerous schemes in which users are free to click any location(s) on background image(s) as his password (e.g. multiple clicks on a single image as in Passpoints [3] or single click on multiple images as in Cued Click Points [4]). These schemes are sometimes called cued recall based schemes since the background image can be regarded as a cue to recall the location of clicks chosen as the password.

Besides their user interfaces, cued recall based schemes differ from earlier recognition based schemes in one important aspect. Their password space (e.g. 2^{43} [3,4]) is significantly larger than the space in recognition based schemes (e.g. 10000 [6]). Hence recognition based schemes are generally regarded as not well suited to Internet applications where brute force attacks (either online or offline) are possible. These schemes are intended for applications where the user account can be locked once a number of false login attempts are detected (e.g. to replace PINs used in ATM machines).

For instance in [3], it is conjectured that *"the drawback of all such passwords based on image recognition is that only a small number of images can be displayed, e.g., nine images, one of which is a chosen image*". Since then, several successful attacks on cued recall based schemes exploiting popular click locations called hotspots have been shown [22,19,7] that call into question the security of these schemes. Therefore we think it is time to question the above conjecture and revisit recognition based schemes and explore the possibility to increase their password spaces. More precisely, the research problem we aim to investigate in this paper is whether it is possible to design a recognition-based graphical password scheme that offers a password space comparable to cued recall based schemes and that has security and/or usability advantages over them.

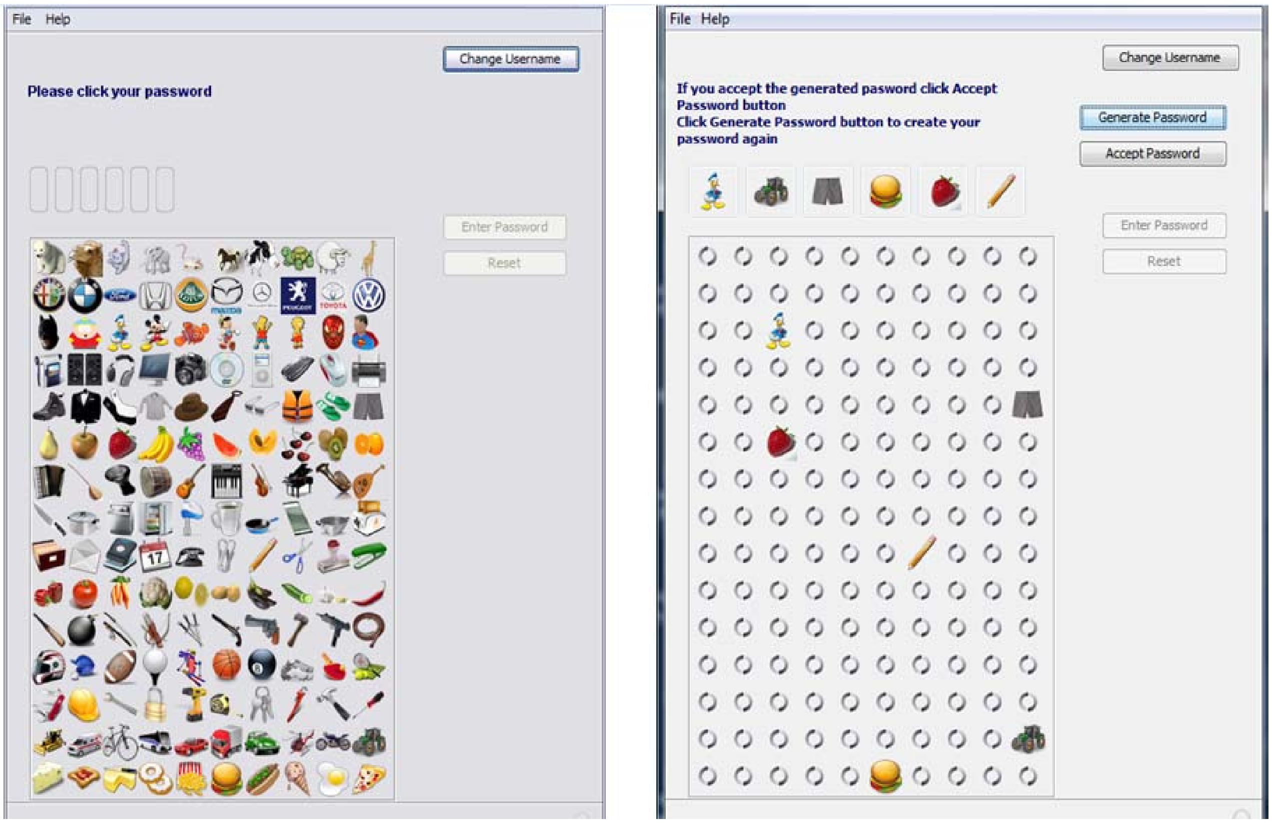
In both schemes (GPI and GPIS) we propose in this paper, we use icons collected from open source libraries available on the Internet (e.g. [10]). Using icons in graphical password schemes is not a new idea. However rather than achieving a large password space, the objective of earlier work that use icons [21, 9] is to safeguard against shoulder surfing attacks. Although shoulder surfing attacks are an important issue for graphical password schemes especially when the password is entered in public places, we do not address this concern in this paper and leave it as a future work. We also note that although the password space in our proposals and previous click based schemes [3] are significantly large (i.e. 2^{43}), this space is still considered to be insufficient for offline attacks [22]. However with some password stretching techniques [8, 18], tolerable levels of password security can be implemented on top of these schemes.

In GPIS, the second scheme we propose, a password (a set of icons) is generated randomly and displayed to the user and the user either chooses this password or asks the system to generate a new one. This procedure can be repeated infinitely until the user likes and chooses the password recommended by the system. There are cued recall based graphical password schemes in the literature in which the system helps users to choose a secure password. For instance in [5], the system encourages user to avoid hot spots and select more random hence more secure passwords. The "shuffle" button in [5] to randomly reposition the viewport and the "generate password" button in GPIS to display a new icon set are similar in concept.

III. Experiment

Click-based graphical passwords can come with different user interfaces (different pictorial backgrounds). By changing the user interface it may be possible to mitigate hot spot problem of click-based graphical passwords. It is reported that some images generate more hotspots than others [22]. When we look at a scene or an image, our visual system perceptually organize some regions as figures and others as backgrounds [16]. In addition, our visual system interprets 2-dimensional images as 3-dimensional by analyzing proximal cues [16]. These factors may be the reason of the hotspot problem.

In GPI and GPIS, since icons are located on a grid, neither figure/background nor 3D perception will emerge out of the pictorial background therefore we assume that eliminating the figure/background and 3D perception will reduce the number of hotspots. On the other hand, the use of icons may generate a different kind of hotspot. There is a possibility that some icons draw the attention of users more than others. Some icons may be drawn more attractively, or users may be familiar to some objects that icons represent more than others. Such factors may lead to another kind of hotspot problem, hot-icons.

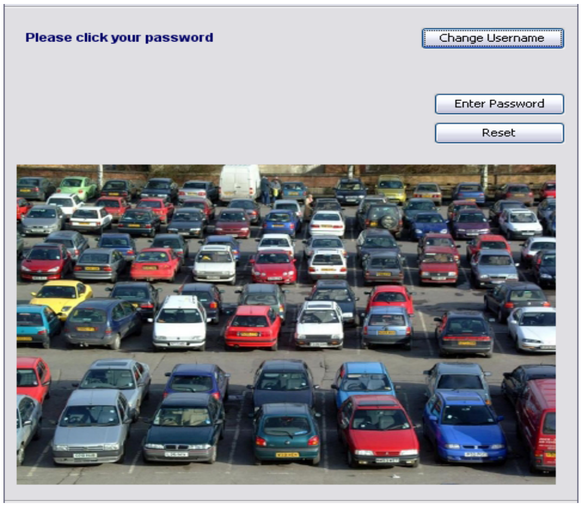


Please click your password

If you accept the generated pasword click Accept Password button
Click Generate Password button to create your password again

Fig.1. GPI interface (left) and GPIS interface (right). In GPI user selects the click-points whereas in GPIS the system selects and displays them (sizes are scaled down to fit into the page, best viewed in color)

To overcome these problems, first we used colored-icons that were drawn stylistically similar. Second, we refer to a category norm study to select the objects that icons represent [15]. This study reports the word lists that are generated by participants as category instances given a category. For each word and for each category, they gave the probability of the word to be included in the category list. Using this measure, we selected popular instances of categories and use icons of them. By this way, we aimed to normalize the familiarity of each object and each icon to minimize the hotspot problem.



Please click your password

Fig.2. The PassPoints [24] interface

In GPI and GPIS interfaces (Figure 1) there are 150 icons selected from 15 categories (animals, car brands, cartoon characters, electronic devices, clothes, fruits, music instruments, kitchen utensils, office equipment, vegetables, weapons, sports, hand tools, vehicles, and fast food). Icons that belong to the same category are presented on the same line. The order of each category and instances of it are randomized for each user. In Passpoints interface (Figure 2), the background image is 451x331 pixels in size and users are asked to select and mouse-click a sequence of five points as their passwords, and confirm it by clicking inside a tolerance circle of 19 pixels centered on the original click-points. There are 391 such circles in total and the password space is calculated as $P(391,5) \approx 2^{43}$ when points should be clicked in the correct order (P denotes permutation).

To keep the password space as same as in Passpoints, GPI users are asked to select and mouse-click a sequence of six icons as their passwords, and confirm it by clicking on the same sequence again ($P(150,6) \approx 2^{43}$). In GPI and GPIS systems, the size of each icon is chosen as 32 x 32 pixels. This makes the total area icons cover approximately equal to the size of the background image in Passpoints.

To completely eliminate the hotspot problem, in GPIS system we use computer generated click-points as passwords. In this scheme computer selects a sequence of six icons. Icons and their sequence were presented with a flash animation (not shown in Figure 1). Then user mouse-clicks to learn and applies the password. GPIS uses the same interface as GPI except for the password generation phase.

We conducted a laboratory experiment to compare the usability and security of GPI and GPIS with the classical click-based graphical password scheme (PassPoints) that use image as a pictorial background. We evaluated whether using icons as click-points changes the effectiveness, efficiency, user satisfaction and security of click-based graphical passwords. This experiment was approved by the ethics committee of Middle East Technical University.

Performance memory and data entry speed were compared for different user interfaces. Each participant either used GPI, GPIS (Figure 1) or PassPoints (Figure 2) interface. In all cases, participants were required to click in the correct order and confirm their password by clicking on icons for a second time. Participants were invited one week later to enter their passwords again. Sixty-nine participants (students or employees of TOBB University of Economics and Technology or Middle East Technical University) were employed. They were randomly allocated to one of the three experimental conditions: GPI (n=23), GPIS (n=23), and PassPoints (n=23). They were informed about click-based graphical passwords and they were introduced to the stand alone version of the graphical password software[2].

IV. Results and Discussion of the Experiment

Efficiency of click-based graphical password interfaces is measured with the time that user confirms his/her password (Figure 3). Confirmation is the longest with GPI, the shortest with PassPoints and in between for GPIS. Difference between conditions is marginally significant [$F(2,65)=2.828$, $p<0.06$]. A planned comparison reveals a significant difference between GPI and PassPoints interfaces ($p<0.05$).

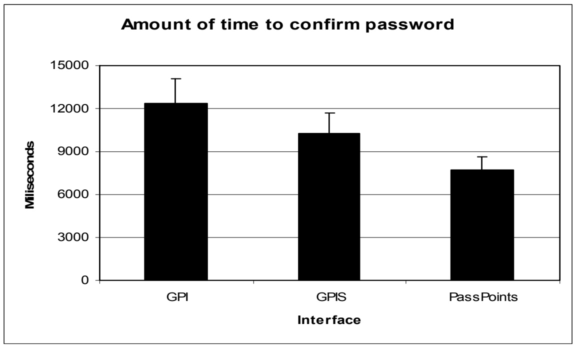


Fig. 3. Amount of time to confirm a click-based graphical password for GPI, GPIS and PassPoints interfaces.

Effectiveness of click-based graphical password interfaces is measured with the number of participants who forget their passwords, number of attempts to remember the password, and the amount of time to enter the correctly remembered password. Four participants of the GPI group, six participants of the GPIS group, and five participants of the PassPoints group forget their passwords. There is no significant difference between groups ($X^2(2) = 0.5$, n.s.).

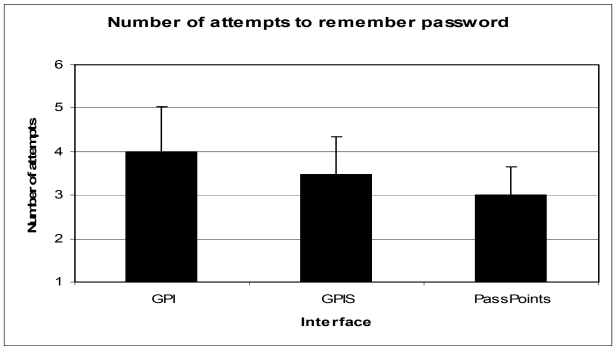


Fig. 4. Number of attempts to remember a click-based graphical password for GPI, GPIS and PassPoints interfaces.

Number of attempts to remember the correct password is presented in Figure 4. The results are not significantly different between groups [$F(2,65)=0.34$, n.s.]. Amount of time to enter the correctly remembered password is presented in Figure 5. PassPoints interface provides the

[2] It is also possible to implement GPI and GPIS as a browser extension. For more information, see [2].

fastest entry time. But there is no significant difference between groups [F(2,65)=0.34, n.s.].

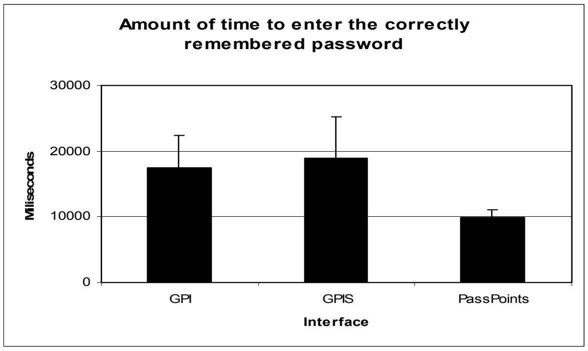


Fig. 5. Amount of time to enter the correctly remembered password for GPI, GPIS and PassPoints interfaces.

In the measurements, we see that there was a difference between PassPoints and our proposed schemes in favor of Passpoints. On the other hand, usability measures of GPI and GPIS interfaces are still in reasonable limits.

Security of graphical passwords with the GPI and PassPoints interfaces are compared with a hot-spot analysis. Passwords of the GPIS interface are generated by the system randomly. Therefore this interface is free from hotspots[3].

For the PassPoints and GPI interfaces users click 115 (five clicks per user) and 138 (six clicks per user) points in total, respectively. Figure 6 presents the number of regions with respect to number of times clicked by users for the PassPoints interface. For instance, there are 32 regions clicked only one time, 10 regions clicked two times and so on. Then, we devise the following formula to calculate the expected number of clicks per region.

$$E_r = \binom{115}{r} \times \left(\frac{390}{391}\right)^{115-r} \times \left(\frac{1}{391}\right)^{r} \times 391$$

E_r denotes the number of regions that are chosen *r* times. Since we have a total of 115 points, the probability of choosing the given region for *r* times is $\left(\frac{1}{391}\right)^{r} \times \left(\frac{390}{391}\right)^{115-r}$.

A similar formula gives the expected value of number of clicks for GPI interface. Figure 7 represents the number of clicks for each icon. By examining Figure 6 and 7, it can be easily concluded that GPI is superior to Passpoints in terms of security since experimental results are closer to expected values in Figure 7 as compared to values in Figure 6. However, the hot spot problem still exists in GPI to some extent. On the other hand, GPIS is free from any hotspot problem. Since GPIS has usability results comparable to GPI and has the advantage of being hotspot free, we do not think a more extensive security comparison is needed between GPI and Passpoints systems.

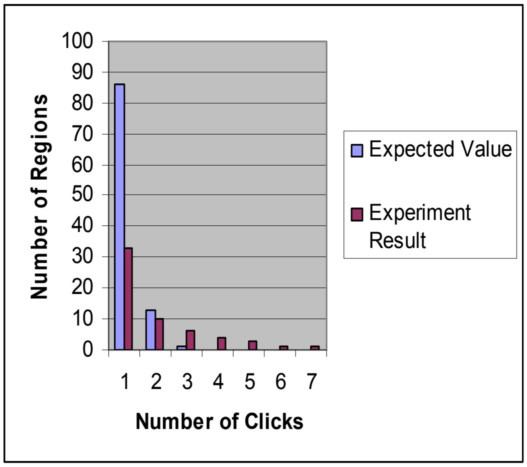


Fig. 6. Number of clicks for each region in PassPoints.

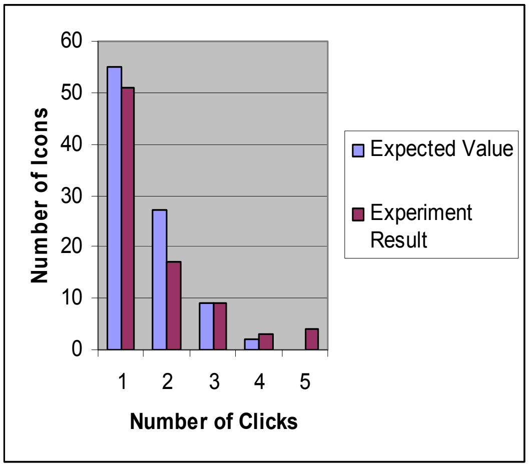


Fig. 7. Number of clicks for each icon in GPI.

V. Conclusion and Future Work

In this study, we developed and tested two click-based graphical password schemes (GPI and GPIS). To the best of our knowledge, these are the first image recognition based schemes that offer comparable password spaces to previous cued recall based schemes. The experimental results for GPI and GPIS justify that hot spot problem of click based graphical passwords can be overcome.

In GPIS scheme, although user is not free to choose any password he likes, experimental results show that this feature has not a significant usability and memorability disadvantage. This is contrast to text based passwords in

[3] We ignore the possibility of bias towards more popular icons by clicking repeatedly on "Generate Password" button. In the experiment, this kind of behavior was not observed. Only 4 out of 23 participants click to generate a new password.

which memorability of system generated password is low unless the system is supported by mnemonics [25] or similar memory enhancement tools. We believe this is one big advantage of graphical passwords in general and GPIS system in particular over text based password systems.

There are some usability concerns for GPI and GPIS. Based on the feedback from users participated in the experiment, we think that most of these are due to small size of icons. We have deliberately miniaturized the icons to make the interfaces equal size for a fair usability comparison with earlier work. In today's technology there is a trend for larger display sizes. As a future work, we are planning to explore whether usability of GPI and GPIS can be improved by using larger icons. A long-term evaluation study of proposed methods is another promising future work. We are optimistic that users will be more comfortable with their passwords in a long-term study and password entrance and confirmation times for GPI and GPIS will start dropping.

ACKNOWLEDGMENT

We thank Orhun Kara for his help on analyzing the experimental results. We also thank anonymous reviewers for their suggestions for improving the paper.

REFERENCES

[1] A. De Angeli, L. M. Coventry, G. Johnson, K. Renaud: *Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems*. International Journal of Man-Machine Studies 63(1-2): 128-152 (2005)

[2] K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, N. B. Atalay, *Graphical Passwords as Browser Extension: Implementation and Usability Study*, Third IFIP WG 11.11 International Conference on Trust Management June 15-19, 2009, Purdue University, West Lafayette, USA.

[3] G. Blonder. Graphical Passwords. United States Patent 5,559,961, 1996.

[4] S. Chiasson, P.C. van Oorschot, R. Biddle, *Graphical Password Authentication Using Cued Click Points.* ESORICS, Sept.24-27 2007, Dresden, Germany. Springer-Verlag, LNCS 4734 (2007).

[5] S. Chiasson, A. Forget, R. Biddle, P.C. van Oorschot, *Influencing Users Towards Better Passwords: Persuasive Cued Click-Points.* HCI 2008, September 1-5 2008.

[6] R. Dhamija, A. Perrig, 2000. *De′ja` vu: a User Study Using Images for Authentication.* Proceedings of USENIX Security Symposium, August 2000.

[7] A. Dirik, N. Memon, and J.-C. Birget. *Modeling User Choice in the PassPoints Graphical Password Scheme*. In *SOUPS*, 2007.

[8] J. A. Halderman, B. Waters, and E. W. Felten. *A Convenient Method for Securely Managing Passwords*. In Proceedings of the 14th International WorldWideWeb Conference, pages 471–479. ACM Press, 2005.

[9] D. Hong, S. Man, B. Hawes, and M. Mathews, *"A password scheme strongly resistant to spyware,"* in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[10] Icon archive, www.iconarchive.com, *accessed on March 11, 2009.*

[11] Information Security Breaches Survey 2006, PriceWaterhouseCoopers, April 2006.

[12] W. Jansen, S. Gavrilla, V. Korolev, R. Ayers, and R. Swanstrom. *Picture Password: A Visual Login Technique for Mobile Devices*. NIST Report: NISTIR 7030, 2003.

[13] S. Madigan, Picture Memory, In John C. Yuille, editor, *Imagery, Memory and Cognition*, pages 65–89. Lawrence Erlbaum Associates, N.J., U.S.A., 1983.

[14] D. Davis, F. Monrose, and M.K. Reiter, *On User Choice in Graphical Password Schemes.* In Proceedings of the 13th USENIX SecuritySymposium, San Diego, 2004.

[15] J. P. Van Overschelde, K. A. Rawson, and J. Dunlosky, *Category norms: An updated and expanded version of the Battig and Montague* (1969) norms Journal of Memory and Language 50 (2004) 289–335

[16] S.E. Palmer, (1999). *Vision Science: Photons to Phenomenology*. Cambridge, MA: MIT Press.

[17] Passlogix. http://www.passlogix.com, accessed on March 12, 2009.

[18] N. Provos and D. Mazieres. *A Future-Adaptable Password Scheme.* In Proceedings of the USENIX Annual Technical Conference, 1999.

[19] A. Salehi-Abari, J. Thorpe, P.C. van Oorschot. *On Purely Automated Attacks and Click-Based Graphical Passwords*. 24th ACSAC, Dec.8-12, 2008, Anaheim, California.

[20] The Grafical Login Solution For your PocketPC – visKey. *www.sfr-software.de/cms/EN/pocketpc/viskey/index.html, accessed on March 11, 2009.*

[21] L. Sobrado and J.-C. Birget, *"Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.*

[22] J. Thorpe, P.C van Oorschot, *Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords*, pages 103-118. In 16th Usenix Security Symposium, Boston, USA, 2007.

[23] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, *PassPoints: Design and longitudinal evaluation of a graphical password system'*, International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005).

[24] S.Wiedenbeck, J.Waters, J.C. Birget, A. Brodskiy, and N. Memon. *PassPoints: Design and Longitudinal Evaluation of a Graphical Password System*. International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63:102–127, 2005.

[25] S. Jeyaraman and U. Topkara. *Have the Cake and Eat it too - Infusing Usability into Text-Password Based Authentication Systems.* In 21st ACSAC, pages 473–482, 2005.