STUDY AND DEVELOP A NEW GRAPHICAL PASSWORD SYSTEM

ALI MOHAMED ELJETLAWI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science
(*Information Security)*

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

NOVEMBER
2008

ABSTRACT

Graphical password have been proposed as a possible alternative solution to text- based password, motivated particularly by the fact that humans can remember pictures better than text. The main aim of this project is to study the usability features of the recognition base graphical password methods regarding to general usability features and ISO standard usability features then a comparison study between the usability features and sub features of these methods has been done and finally map all that features and sub features to the existing graphical password methods to get the new usability features can be implemented in the new usable graphical password prototype.

A graphical password system framework has been built and divided into two stages, new user and existing user stage, then the system implemented as prototype and an evaluation of the prototype usability features has been conducted by questionnaire survey in the UTM (CASE) and Computer Science Faculty students (Johor), then the user's feedback about the whole system and the usability features of the graphical password prototype results collected and analyzed and all the results percentages are very good which mean that the new graphical password system is acceptable from the usability point view..

ABSTRAK

Kata Laluan grafik sudah dicadangkan sebagai pilihan untuk menyelesaikan perkataan berteraskan kata laluan, galakkan sebegini adalah kerana manusia lebih mengingati gambar daripada perkataan. Tujuan utama dalam projek ini adalah untuk mengkaji pengenaln atas dasar kata laluan untuk pengunaan dan ISO pengunaan biasa, daripada di banding kan penelitian antara cara cara pengunaan paparan dan sebahagian paparan untuk diteraskan telah pun di buat dan akhirnya semua peta paparan dan sebahgian paparan kepada kewujutan grafik kata laluan untuk mendapatkan penggunaan paparan baru untuk kata laluan grafik prototaip.

Kata laluan grafik system kotak kerja telah di tubuhkan and telah dibahagikan ke dua peringkat, penguna baru dan pengguna tetap, kepada system sebagai prototaip dan prototaip penilaian pengguna biasa telah di lalukan oleh tinjauan soal di UTM (CASE) dan Pelajar di Fakulti Komputer Sains (Johor), maka semua penguna memberi sambutan yang mengalakan bahawa semua system dan paparan pengguna untuk kata laluan grafik prototaip dan di analisiskan keputusan and peratusan yang amat bagus untuk kata laluan grafik system boleh di terima daripada pengguna.

TABLE OF CONTENT

6 DATA COLLECTION AND ANALYSIS

CHAPTER-1

INTRODUCTION

1.1 Introduction

A password is a form of secret authentication data that is used to control access to a resource. The password is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly.

The use of passwords goes back to ancient times. Sentries guarding a location would challenge for a password. They would only allow a person in if they knew the password. In modern times, passwords are used to control access to protected computer operating systems, mobile phones, ATMs machines, etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online (Wikipedia, 2007).

The password is a very good and strong authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of

conventional password appears like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security and avoid the weakness of conventional password.

Graphical password have been proposed as a possible alternative to text-based, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text (R.N Shepard 1967). Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures (Xiaoyuav Suo 2006).

1.2 Problem Background

Because of increasing threats to computer systems, there is great need for security requirements. Security practitioners and researchers have made studies in protecting systems, individual users and digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem, and the system user was not factored into the equation. Users interact with security technologies either passively or actively. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions and usability solutions such as: ease of use, memorability, usability, efficiency, effectiveness and satisfaction. Nowadays there is an increasing recognition that security problems are also fundamentally human-computer interaction issues (Dourish, P 2004 and Patrick *et al* 2004).

Authentication is the process of determining whether a user should be allowed access to a particular system or resource. Conventional passwords are used widely

for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue toremain so for some time as an authentication process (Coventry *et al* 2003, Jain *et al* 2000 and Brostoff *et al* 2000).

Conventional passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit Brown *et al.* 2004, Dhamija *et al* 2000, Feldmeier *et al*. 1990, Klein *et al* 1990, Morris *et al*.1979 and Sasse *et al*. 2001)The "password problem," as formulated by Birget (2005), arises because passwords are expected to comply with two conflicting requirements, which is passwords should be usable and ease to remember, and the user authentication protocol should be executable quickly and easily by humans and passwords should be also secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

1.3 Problem Statement

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Breakdown and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall (Wixted *et al* 2004). If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing conventional passwords (Wixted *et al* 2004).

The first idea for graphical passwords was described by Blonder (1996). His approach was to let the user click, with a mouse or stylus, on a few chosen regions in an image that appeared on the screen. If the correct regions were clicked in, the user as authenticated, otherwise the user was rejected. There are some points to be discussed about the graphical password idea that is the creation and learning of the graphical password because from a human viewpoint, the problem of creating a password is making it memorable so that the user can retrieve it later. In a graphical password system, a user choosing click locations in an image needs to choose memorable locations since there are two issues in memorability: the nature of the image itself and the sequence of click locations, the memory because most existing graphical password systems can be classified as being based on either recognition or cued recall. Recognition involves identifying whether one has encountered an item before. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images. By contrast, pure recall is retrieval without external cues to aid memory, e.g. remembering a textual password that one has not written down and the efficiency and perception of efficiency are important in password systems because users want quick access to systems. Time to input a highly practiced graphical password can be predicted by Fitts' Law, which states that the time to point to a target depends on the distance and size of the target.

1.4 The Project Objective

The objective of this project to develop and implement a new graphical password scheme to improve the usability features of graphical password.

1- Identify and explore the characteristics, schemes, methods of the graphical password and the conventional password as well as existing usability features.

2- Design and develop a new graphical password scheme by using selected Graphical Password usability features.

3- Implement and test the new scheme by simulating a prototype of the new scheme.

1.5 The Project Scope

The scope of this project

1- Study an existing graphical password schemes and concern on recognition base type.

2- Study the usability features of the existing graphical password methods from the general and ISO features.

3- Mapping between the recognition base graphical password methods and the usability features and extract a collection of usability features to be built in the new prototype.

4- Design and Develop a graphical password prototype which carries the most usability features to give a usable graphical password system by using Delphi programming language.

5- Implement the usability features in Graphical Password Prototype System.

1.6 Summary

This chapter has presented an overview of the password problem background, problem statement, and objective of the project which lead to develop and implement new Graphical Password scheme.

LIST OF REFERENCES

A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptography Techniques and E-Commerce*, 1999.

A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In *People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000)*. Springer Verlag, 405-424.

Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. Generating and remembering passwords. *Applied Cognitive Psychology 18* (2004), 641-651.

Berger, M.A., (2003), "Password Security is a Must for Any Organisation", *Computers in Libraries* 23(5), May2003, p41.6- Coventry, L., De Angeli, A. and Johnson, G. Usability and biometric verification at the ATM interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'03)* (Fort Lauderdale, FL, USA, April 5-10, 2003). ACM Press, New York, NY, 153-160.

Bailey, R. 2001. How reliable is usability performance testing? UI design update newsletter.http://www.webusability.com/article_reliability_of_usability_testing_10-2001.htm [14 Jan 2008].

Dourish, P. Security as experience and practice: Supporting everyday security. Talk given at the *DIMACS Workshop on Usable Privacy and Security Software*, July 7, 2004.

Dhamija, R. and Perrig, A. Déjà Vu: User study using images for authentication. In *Ninth Usenix Security Symposium* (Denver, CO, USA, Aug. 14-17, 2000).

http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html, accessed: Feb. 20, 2005.

D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Usenix Security Symposium*. San Diego, CA, 2004.

Feldmeier, D.C. and Karn, P.R. UNIX password security – ten years later. In *Advances in Cryptology – CRYPTO'89*, Lecture Notes in Computer Science 435, Springer Verlag (1990), 44-63.

Faulkner, L. 2003. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behaviour Research Methods, Instruments, & Computers, 35(3)*, pp. 379-383.

G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

Google (2007) http://www.usabilitypartners.se/usability/what.shtml.

Google (2007) http://www.usabilitypartners.se/usability/standards.shtml

Google(2007)http://www.baychi.org/calendar/files/ISO-Standards-for-Usability/ISO- Standards-for-Usability.pdf

I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

Jain, A., Hong, L. and Pankanti, S. Biometric identification. *CACM 43*, 2 (2000), 91-98 28- J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," Cryptology ePrint archive 2003.

J. Rumbaugh, I. Jacobson, G. Booch: The Unified Modeling Language Reference Manual. Reading MA: Addison-Wesley 199945- Wikipedia. The free encyclopedia,"Usabilitylastaccess15.3.2007.URL:http://en.wikipedia.org/wiki/Usability

Klein, D. A survey of, and improvement to, password security. In *UNIX Security Workshop II Proceedings, Tenth Usenix Security Symposium* (Portland, OR, USA, Aug. 27-28, 1990), 83-86.

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

Morris, R. and Thompson, K. Password security; A case study. *CACM 22* (1979), 594-597.

Nielsen, J., & Landauer, T. 1993. A mathematical model of the finding of usability problems. Proceedings of *ACM INTERCHI'93 Conference* (Amsterdam, The Netherlands, pp. 206-213.

Nielsen, J. 2000. Why you only need to test with 5 users: Alertbox. http://www.useit.com/alertbox/20000319.html [14 Jan 2008].

Patrick, A.S. Long, A.C. and Flinn, S. HCI and security systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'04)* (Vienna, Austria, April 24-29, 2004). ACM Press, New York, NY, 1056-1057.

Page, J., Zaslavsky, A., Indrawan, M., (2003) "Security Aspects of Software Agents In Pervasive InformationSystems", in Proceedings of The 14th Australasian Conference on Information Systems, 26-8 November 2003, Perth, Western Australia.

Passlogix, "www.passlogix.com," last accessed in March 2007.

Perfetti, C. & Landesman, L. 2002. *Eight is not enough*. http://www.uie.com/articles/eight_is_not_enough/ [14 Jan 2008].

R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

RealUser, "www.realuser.com," last accessed in March 2007

Sasse, M.A., Brostoff, S. and Weirich, D. Transforming the 'weakest link'–ahuman/computer interaction approach to usable and effective security. *BT Technical Journal 19* (2001), 122-131.

S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV, 2005.

S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Symposium on Usable Privacy and Security (SOUPS)*. Carnegie-Mellon University, Pittsburgh, 2005.

S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in *People and Computers XIV - Usability or Else: Proceedings of HCI*. Sunderland, UK: Springer-Verlag, 2000.

Spool, J, & Schroeder, W. 2001. Test web sites: five users are nowhere near enough. In J. Jacko and A. Sears (Eds.), *Conference on Human Factors in Computing Systems: CHI 2001* Extended Abstracts (pp. 285-286). Traditional AuthenticationMethod.URL http://www.oit.duke.edu/~rob/kerberos/dumbauth.html

T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

Van Der Putte, T., and Keuning, J., (2000), "Biometric Fingerprint Recognition: Don't Get Your Fingers Burned", *IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, pp289-303.

Virzi, R. A. 1992. *Refining the test phase of usability evaluation: How many subjects is enough?*. Human Factors, 34, 457-468. Wikipedia. The free encyclopedia "Authentication"2007-03-12- URL: http://en.wikipedia.org/wiki/Authentication

Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A. and Memon, N. PassPoints: Design and evaluation of a graphical password system. Submitted, (2005).

Wixted, J. T. (2004). The psychology and neuroscience of forgetting. *Annual Review of Psychology*, 55, 235-269.

Wikipedia. The free encyclopedia, "authentication" last access 4.4.2007- URL: http://en.wikipedia.org/wiki/authentication

Wikipedia. The free encyclopedia, "authentication factor "last access 10.4.2007- URL: http://en.wikipedia.org/wiki/authentication_factor

Wikipedia. The free encyclopedia, “Password strength “last access 13.3.2007- URL http://en.wikipedia.org/wiki/Password_strength

W. Jansen, "Authenticating Mobile Device Users through Image Selection," in *Data Security*, 2004.

Wikipedia. The free encyclopedia, “Qualitative _research” 20.3.2007- URL: http://en.wikipedia.org/wiki/Quantitive_resarch

Wikipedia. The free encyclopedia, “Qualitative _method” 20.3.2007- URL: http://en.wikipedia.org/wiki/Quantitive_method

Wikipedia. The free encyclopedia, “Quantitive _research” 20.3.2007- URL: http://en.wikipedia.org/wiki/Qualtitive_resarch

Wikipedia. The free encyclopedia, “Quantitive_research” 20.3.2007- URL: http://en.wikipedia.org/wiki/Quantitive_resarch

Wikipedia. The free encyclopedia, “Comparative method” 21.3.2007- URL: http://en.wikipedia.org/wiki/Comparative_method

XIAOYUAN SUO (2006) DESIGN *AND ANALYSIS OF GRAPHICAL PASSWORD*.College of Arts and Sciences, Georgia State University: Master of Science.OnLineURL:http://scissec.scis.ecu.edu.au/conference_proceedings/2004/aism/Pierce-Warren-Mackay-Wells.pdf