ENHANCING GRAPHICAL PASSWORD AUTHENTICATION ON SMARTPHONES

KHALED GUBRAN YAHYA AL-HASHEDI

UNIVERSITI TEKNOLOGI MALAYSIA

ENHANCING GRAPHICAL PASSWORD AUTHENTICATION ON SMARTPHONES

KHALED GUBRAN YAHYA AL-HASHEDI

A project report submitted in fulfilment of
the requirements for the award of the degree of
Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2017

Dedicated to

my beloved father and mother,

my brothers, sisters, and family members

with thanks for all the

years of caring, love, and support

ACKNOWLEDGEMENTS

All praise is to Allah, the Lord of the Worlds, and may His Blessings and Peace be upon our Prophet Mohammed. I thank Him for the blessings and for honoring me His guidance in order to complete this research.

First and foremost, I would like to express my utmost gratitude and appreciation to my supervisor, Prof. Madya Dr. MOHD SHAHIDAN for his guidance, knowledge, patience, time and support throughout every stage of my MSc and the development of this research.

My completion of this research could not have been accomplished without the support of my parents, my siblings, and my beloved family.

My fellow postgraduate students should also be thankful for their support at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members.

ABSTRACT

Recently, smartphones have emerged into a widely used as an input device for Graphical Password Technique due to the supporting of a touchscreen. Most of the smartphones used for managing a business especially in online trading or storing such an important or sensitive data. However, most of the existing methods of Graphical Password Authentication are suffering from a variety of usability and security issues such as they are more vulnerable to shoulder surfing attack due to the visual interface, difficult to use, and difficult to remember. In this research, a comprehensive study was conducted to determine the issues of usability and security on the existing schemes. A new recognition base graphical password method has been proposed to improve the issues of usability and security by asking the user to select his/her pictures from the mobile's gallery or via camera. The evaluation process was conducted by questionnaire survey and the help of 35 participants from UTM, UM, UPM, and LIMKOWKING university. The finding shows that the participants were completely satisfied with the usability and security which means that the proposed scheme of Graphical Password is acceptable from usability and security points.

ABSTRAK

Baru-baru ini, telefon pintar telah muncul secara meluas sebagai peranti input untuk Password Teknik Grafik dengan menggunakan skrin sentuh. Kebanyakan telefon pintar digunakan untuk menguruskan perniagaan terutama dalam dagangan menerusi talian atau menyimpan apa-apa data penting atau sensitif. Walau bagaimanapun, sebahagian besar daripada kaedah yang sedia ada Password Pengesahan Grafik mengalami pelbagai isu dari segi kebolehgunaan dan keselamatan seperti isu shoulder surfing, sukar untuk digunakan, dan sukar untuk diingati. Dalam projek ini, kajian yang komprehensif telah dijalankan untuk menentukan isu-isu kebolehgunaan dan keselamatan di skim yang sedia ada. Asas pengiktirafan baru kaedah kata laluan grafik telah dicadangkan untuk meningkatkan isu-isu kebolehgunaan dan keselamatan dengan meminta pengguna untuk memilih gambar-gambar mereka dari galeri mudah alih atau melalui kamera. Proses penilaian telah dijalankan melalui kajian soal selidik daripada 35 pelajar dari UTM, UM, UPM, dan LIMKOWKING. Dapatan kajian menunjukkan bahawa para peserta berpuas hati dengan kebolehgunaan dan keselamatan yang bermaksud bahawa cadangan skim Grafik Kata aluan boleh diterima dari segi kebolehgunaan dan keselamatan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	-	AUTOMATED TELLER MACHINE
DAS	-	DRAW A SECRET
BDAS	-	Background Draw A Secret
CCP	-	Cued Click-Points
PCCP	-	Cued Click-Points
CAPTCHA	-	Completely Automated Public Turing tests to tell Computer and Humans Apart
CDS	-	Come from DAS and Story
IPCT	-	Image Pass Code with Tapping
G.P	-	Graphical password
MIBA	-	Multi-touch Image-Based Authentication
TLA	-	THREE-LEVEL AUTHENTICATION
TMD	-	Touchscreen Multi-layered Drawing
GPIP	-	Graphical Password based on Image Portions
GPA	-	Graphical Password Authentication
GPS	-	Graphical Password Scheme

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Modern smartphones have emerged at the present time, to coincide with the developments that have taken place in the world, these devices are operated by sophisticated systems such as Android system ISO and other regulations, and there are a lot of companies that produced many smart as Samsung and Apple phones and other companies, and can do many things with smartphones, they are not limited to the reception and transmission, as in the old mobile phones, but can through these smartphones to do various operations browsing on the Internet, online banking, and social networks. This is very useful for users, but it becomes the main concern when the users have their phones lost or stolen. This poses a problematic to smartphones' users thus users want to protect access to their device (Meng *et al.*, 2017).

Currently, most of the mobile operating systems are supplied by a display locked which regularly manages authentication process. If the systems are in a locked mode, none of the operations can be performed. In such devices, the most common authentication systems are personal authentication numbers (PINs) and Android unlock pattern. However, most of the existing authentication methods are still suffering from many drawbacks such as usability and Shoulder Surfing Attack especially if a mobile device is unlocked using the existing authentication methods in a public place(Schechter and Bonneau, 2015).

In the world today, authentication technology is the main principle of smartphones components to guarantee data security. Authentication is the process of verifying the identity of the user to gain access to protected resources. Authentication methods can be broken down into three main kinds. The first kind is called Token based authentication (i.e. something that the user has such as bank cards or smart cards). The second kind is called Biometric based authentication (i.e. something that the user him/herself such as a fingerprint or other biometric methods). The third kind is called Knowledge-based authentication (i.e. something the user knows such as a password). Although the main purpose of authentication methods is to confirm one's identity but each method has its own defects and advantages over the other. In addition, many security experts have put the foundation in how to avoid your system from being attacked from all kinds of threats and how to protect your system Alsaiari *et al.* (2015).

In the recent years, smartphones and network security have been defined as a technical problem, particularly when dealing with user authentication due to their great importance in the present time (Lashkari *et al.*, 2010). Nowadays, authentication plays an important role in maintaining data and information security because of the continuing advancement of technology and internet revolution, whether it is an online system or a mobile application. In addition, one of the authentication technique is called "text-based password" which consists of a combination of letters and digits which are the most popular and familiar technique to essentially all users (Togookhuu and Zhang, 2017). Although the widespread of this technique but its limitations are well-known such as dictionary attack, brute force attack, etc. (Murugavalli *et al.*, 2016). For example, when users want to create a strong password, the text-based passwords must be formed and created randomly using a combination of alphabet, and special characters which are difficult to remember. Unlike weak text-based passwords which are short and easy to remember but they are easy to guess by an adversary (Kumar, Arohi and Khan, 2013).

Over the past years of the nineties of the last century, a new authentication scheme called "Graphical Password Authentication" has been proposed to be as an alternative to traditional text-based password authentication to address the shortcomings of the traditional method. Graphical passwords are knowledge-based authentication that has been, and remains to be, the technique by which can be described as memorable and more secure because they are difficult elements to guess. The main purpose of the graphical password is to use pictures as a password instead of the texts. There are different shapes, icons, and digital photos. According to the psychological studies demonstrated that the ability of the human brains to remember lots of pictures are easier than the text (Schechter and Bonneau, 2015). The mechanism of the Graphical Password is composed of a sequence of one or multiple images with the user intervention by clicking, dragging, moving a mouse or touching over the images.

Today, Graphical Passwords have become the area of researchers' interest due to the need of it in order to improve the quality of usability and security of password authentication for smartphones. Presently, Graphical Password Authentication (GPA) is not efficient enough where the existing authentication systems of graphical password contain some drawbacks such they are vulnerable to a variety of attacks and they take a long time to registration phase and login process. One of the vulnerabilities is shoulder-surfing attack where the attacker can easily observe the password during logging process that impacts negatively on the reliability of performance. Currently, graphical passwords have been adopted by an extensive range of many applications such as operating systems, mobile phones, websites, emails, and others.

1.2 Background of the Problem

Due to the increasing of threats on smartphones security, there is an important need of high-level security to secure smartphones components whether they are hardware or software. Recently, many research and study have been undertaken in the field of security in the hope to provide a high level of protection to secure or protect smartphones from any kind of intrusions. However, security was broken down by attackers by which may pose the main problem to security experts and this problem has been defined as a technological trouble. Therefore, security experts must work together with protection technologies to overcome this kind of threats. In the present time, there are a greater than ever admission that defense problems are also fundamentally human-computer dealings issues (Assal, Imran and Chiasson, 2016).

Authentication can be said as a foundation to ensure data security for every system providing a secure access (Zizzi, 2015). The reliable system must provide a sufficient security in different aspects of its meant environment. Otherwise, it will not achieve its primary goal (Biddle, Chiasson and P.C. Van Oorschot, 2012). Currently, most of the modern systems depend on authentication to verify the user identity in order to gain access to a secure data. Therefore, numerous techniques have been proposed to provide a secure data access such as Text-based authentication, Biometric models authentication, and Smart cards. Some of these techniques have advantages and disadvantages over another. For instance, there is a PIN used with smart cards which can be damaged or lost over the time because they are made from plastic but this type of technique is not used in smartphones. In Biometrics schemes, there is a problem of cost where the majority of smartphones do not support Biometrics schemes. However, text-based authentications are still the most widely dominant, but they are still suffering from some drawbacks such as brute for attacks and Dictionary attacks. For example, users tend to select a password that can be easily guessed. In contrast, complicated passwords are difficult to remember thus users tend to write them down in a piece of paper (Purushothaman G R & Ashwini 2016).

Usually, forgetting passwords are the main issue to users. This problem largely emerges from limitations of the human memory's ability to remember things on the long run. For instance, once the password has been selected and memorized, the users should be able to recall in order to access their personal data. But, most of the people continuously forget their own passwords. In fact, there are many items existed in human's memory. Studies have shown the reason people forget their passwords is due to the interference of the items previously stored in the memory with the passwords. Thus, posing difficulty to recall them accurately (Sadeh *et al.* 2016). According to report has revealed that the average user has to remember more than 20 passwords in many accounts whether online or offline such as smartphones locks, emails, online banking, internet shopping, social media, and websites. This huge amount password increases the possibilities to forget passwords (Zhang-Kennedy *et al.* 2016).

In the fact, an authentication system is evaluated based on its ease of use and its availability. Thus, difficult or complicated passwords are not easy to remember due to the weakness of human brain to memorize passwords. However, users tend to pick short and easy passwords that are easy for attackers to break because of their fear of forgetting them (Bhawani, Lawate and Chaudhary, 2016), if the passwords are too long thus most users write them down on pieces of papers or save them into a smartphone file which may result from increasing the chances of penetration by attackers. Despite the widespread of textual passwords, but it still contains some drawbacks and vulnerabilities. Moreover, text-based passwords are vulnerable to many powerful software and techniques such as spyware attack, and others social engineering attacks (Gao, Jia *et al*. 2013).

Furthermore, there are many threats that affect the function of text-based passwords through the using of numeric powerful software that help to steal passwords. Recently, survey report shows that the normal user has nearly 25 online accounts that ask for passwords, and every user must input 7 passwords a day (Zhang-Kennedy, Chiasson and van Oorschot, 2016). Hence, most of the users tend to use the same passwords on several accounts. However, most passwords commonly used for authentication are related to their personal life such as personal names, dictionary words, birth date, or phone numbers. Thus, they are more vulnerable to several attacks such as dictionary attack and brute force attack. Accordingly, in order to overcome authentication of alphanumeric passwords problems, many solutions have been proposed as an alternative solution to address these issues and one of them is through using of graphical password systems.

According to the above statement by (Zhang-Kennedy, Chiasson and van Oorschot, 2016), we can notice that why most of people are looking for a secure authentication password system using images as a replacement of text-based password.

Graphical Password Authentication (GPA) schemes on smartphones are a replacement of Text-based password but they are still suffering from some shortcomings (Chiasson *et al.*, 2012). One of the potential drawbacks of GPA on smartphones is that their security vulnerabilities. Thus , they are more vulnerable to shoulder surfing attack than traditional text-based passwords due to the visual interface that is supported by the system where attackers can easily observe the password during login process especially in public place, unlike text-based passwords which they are defended of this type of attack by replacing asterisks of password characters in the display during login process (Zakaria *et al.* 2011). Despite the large number of proposed methods against Shoulder- Surfing Attacks but they are difficult to implement on smartphones due to the complexity in design which requires a large screen size and more steps that must be remembered (Park *et al.*, 2014).

Additionally, one of the main challenges in graphical password authentication (GPA) on a smartphone is usability in terms of user's satisfaction such as easy to use, easy to remember the password, easy to create, and easy to learn. Thus, difficult or complicated passwords are not easy to remember due to the weakness of human brain to memorize complicated steps. However, users tend to pick short and easy passwords that are easy for attackers to break because of their fear of forgetting them(Bhawani, Lawate and Chaudhary, 2016). For instance, when users need to use the advantage of the graphical password system, the first thing that comes to their mind is how long it is going to take to perform login or registration process because of a complex design of the system which is known as a time-consuming. Therefore, time- consuming is one of the main factors that users face in the graphical password which may affect the usability of the system (Lashkari, 2014).

Operation system security of smartphones depends largely on user's password authentication thus long passwords are better than short in terms of security. Therefore, alphanumeric passwords have the ability to use a large password space comparing to the Graphical Password Authentication on smartphones due to the restricted size of the mobile screen (Zakaria *et al.*, 2011) However, in a conventional password, the possibilities of brute force attacks are more than in Graphical Passwords. In order to avoid an easy attack of Graphical Password Authentication (GPA) on smartphones, computer security scientists suggest to use a large password space to make it more strong against any potential attack (Swapnil Sunil, Prakash and Ramesh Shivaji, 2014).

1.3 Problem Statement

Human behavior is influenced by the rapid advancement in technology that keeps on changing. The recent security threats demand to have a secure system, especially for those individuals who have interests in the use of mobile phones to run their business or keep their privacy. For mobile devices users, the main concerns of graphical password authentication are security and usability. In terms of usability, creating and logging a password takes a long time comparing to text password because of a complex design of the system especially if users have a large password space where the main concern security is vulnerable to shoulder surfing attack more than text password due to the visual interface of the system supported by the fact the human's brain is better to memorize pictures than texts. Lastly, a strong graphical password is evaluated by the password space where the current systems have small password space.

1.4 Aim of the Study

The purpose of this research is to enhance the usability and security of Graphical Password Authentication (GPA) and to get a better graphical password authentication scheme that is applicable for smartphones.

1.5 Research Questions

This research would answer several questions regarding to Graphical Password Authentication (GPA).

i. What are the available graphical password schemes?
ii. How to enhance the usability and security of graphical password for smartphone?
iii. How to evaluate the proposed the graphical password scheme?

1.6 Research Objectives

Based on aforementioned questions, we came up with the following objectives to be able to answer research questions:

i. To review various graphical password schemes and methods.
ii. To design a usable and secure graphical password scheme on Android platform.
iii. To evaluate the proposed graphical password scheme.

1.7 Research Scope

The scope of this research as the following:

i. The research will only focus on password authentication, specifically on Graphical Password Authentication (GPA) on smartphone.

ii. The implementation of the proposed scheme will be developed on emulator such as SDK with target version 24.

iii. The proposed scheme will be only limited for smartphone specifically in Android Platform.

iv. The design and the development of the graphical password prototype for android smartphone will focus on usability and security features to give a usable and secure graphical password system by using Java Android programming language.

1.8 Significant of Research

The importance of this research is to facilitate the use of the advanced technologies that are based on touch devices. This research helps Graphical Password Authentication (GPA) to identify factors that influence both security and usability. Android smartphones are the widespread devices that contain personal information or businesses that are need to be secured at all the time. The proposed scheme will address the issue of password space by increasing the password size through the use of image portions as well as it will solve the problem of Shoulder-Surfing Attack. For usability, the proposed scheme will provide a user with more than one option of selecting image during registration phase. The user can whether select a password from the provided images or taking a picture via camera or import a picture from the smartphone library. Thus, the usability of the proposed scheme will play a role of improving the security of the scheme where the user will not be restricted to the given pictures by the system.

1.9 Thesis Outline

This thesis consists of seven chapters starting from the introduction, literature review, research methodology, design and development, implementation and testing, data result and analysis, and conclusion. The content of each chapter can be summarized as the following:

Chapter 1 provides a general information of the research that includes a background of the problem, problem statement, research questions, objectives, scope and importance of the study.

Chapter 2 describes previous studies as a literature review of Graphical Password that includes various of authentication systems, various types of graphical password techniques, related works, and a comparison of the related works.

Chapter 3 describes the methodology that will be used for this research. This includes all the procedures that will be used to make the proposed Graphical Password Scheme as well as it will cover all the tools and materials that are required for this research such as software.

Chapter 4 describes the design and development of the proposed system. This includes functional and non-functional requirements, system design using UML that covers User Case Diagram, Sequence Diagram, and Activity Diagram, and finally System Architecture Diagram.

Chapter 5 discusses the implementation and testing of the proposed system. This covers the interface testing where it will mainly focus on the interface design and functions. This chapter also includes two types of technique testing namely: Black Box Testing and White Box Testing.

Chapter 6 discusses the evaluation and testing of the proposed system by recruiting 35 participants from different universities. The data result and analysis will be collected after the participants answered the given questionnaire that mainly focus on the overall evaluation of the proposed system in terms of usability and security.

Chapter 7 is the final chapter that discusses the conclusion of the research, limitation of this research, and recommendation for future work. The two appendices will be included at the end of this thesis. Appendix A presents the questionnaire questions while Appendix B presents the source code of the proposed system and Appendix C presents the pictures used for evaluation.

.

1.10 Summary

This chapter presents a brief introduction of the study. An overview of authentication passwords problems, the background of the problem was discussed as well and the problem statement was demonstrated. On the other hand, to research questions on this research. A certain group of objectives is being set by the researcher, which includes investigation and exploration the existing Graphical Passwords Authentication (GPA) schemes, investigate and identify the usability of the existing graphical schemes, design and improve graphical password authentication scheme. Also, the aim, the scope and the significant of research were introduced.

REFERENCES

Alsaiari, H., Papadaki, M., Dowland, P. S. and Furnell, S. M. (2015) 'A Review of Graphical Authentication Utilising a Keypad Input Method', in Proceedings of the Eighth Saudi Students Conference in the UK. World Scientific, p. 359.

Aman Kumar, E. and Bilandi, E. N. (2014) 'A GRAPHICAL PASSWORD BASED AUTHENTICATION BASED SYSTEM FOR MOBILE DEVICES', International Journal of Computer Science and Mobile Computing, 34(4), pp. 744–754.

Android (2016) Otaku, Cedric's weblog: Android's locking pattern, site accessed in Nov.

Assal, H., Imran, A. and Chiasson, S. (2016) 'An Exploration of Graphical Password Authentication for Children'.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M. and Smith, J. M. (2010) 'Smudge Attacks on Smartphone Touch Screens', WOOT, Berkeley,CA,USA, 10, pp. 1–7.

Bhawani, V., Lawate, P. and Chaudhary, V. (2016) 'GENERIC AUTHENTICATION SYSTEM', International Research Journal of Engineering and Technology, 3(5), pp. 2395–56.

Biddle, R., Chiasson, S. and Van Oorschot, P. C. (2012) 'Graphical passwords : Learning from the First Twelve Years', ACM Computing Surveys. ACM, 44(4), pp. 1–41.

Biddle, R., Chiasson, S. and Van Oorschot, P. C. (2012) 'Graphical Passwords: Learning from the First Twelve Years', ACM Computing Surveys (CSUR), 44(4), p. 19.

Blonder, G. (1996) '"Graphical passwords"', United States Patent, 5, p. 559,961.

BRADI, J. M. H. (2010) IMPROVING A MULTI-FACTOR AUTHENTICATION USING MULTIPLE GRAPHICAL PASSWORD AND PDA. UNIVERSITI TEKNOLOGI MALAYSIA.

Brostoff, S. and Angela Sasse, M. (2000) '"Are Passfaces More Usable Than Passwords?&quot';, A Field Trial Investigation ,.

Brostoff, S., Inglesant, P. and Sasse, M. A. (2010) 'Evaluating the usability and security of a graphical one-time PIN system', 24th BCS Conference on Human Computer Interaction ., pp. 1–8.

Chiang, H.-Y. (2013) A GRAPHICAL PASSW ORD SCHEME FOR MOBILE DEVICES.

Chiang, H.-Y. and Chiasson, S. (2013) 'Improving user authentication on mobile devices: A touchscreen graphical password', in Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. ACM, pp. 251–260.

Chiasson, S., Forget, A., Biddle, R. and Van Oorschot, P. C. (2008) 'Influencing Users Towards Better Passwords: Persuasive Cued Click-Points', In Human Computer Interaction (HCI) , The British Computer Society, September.

Chiasson, S., Van Oorschot, P. C. and Biddle, R. (2007) 'Graphical Password Authentication Using Cued Click Points', In European Symposium On Research In Computer Security (ESORICS) , LNCS 4734, September, pp. 359–374.

Chiasson, S., Stobert, E., Forget, A., Biddle, R. and Van Oorschot, P. C. (2012) 'Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism', IEEE Transactions on Dependable and Secure Computing, 9(2), pp. 222–235.

Citty, J. and Ralph Hutchings, D. (2010) TAPI: Touch-screen Authentication using Partitioned Images.

Dhamija, R. and Perrig, A. (2000) 'Dé a Vu: A User Study Using Images for Authentication £', in Proceedings of 9th USENIX Security Symposium.

Dorage, N. and Sawant, B. (2016) 'Authentication Schemes for Session Passwords using Colors', IJCSNS International Journal of Computer Science and Network Security, 16(4).

Eljetlawi, A. M. and Ithnin, N. (2008) 'Graphical Password: Prototype Usability Survey', in 2008 International Conference on Advanced Computer Theory and

Engineering. IEEE, pp. 351–355.

Gao, H., Jia, W., Ye, F. and Ma, L. (2013) ‘A Survey on the Use of Graphical Passwords in Security’, JOURNAL OF SOFTWARE, 8(7).

Gao, H., Liu, X., Wang, S. and Dai, R. (2009) ‘A new graphical password scheme against spyware by using CAPTCHA’, Proceedings of the symposium on usable privacy and security, pp. 15–17.

Gao, H., Ren, Z., Chang, X., Liu, X. and Aickelin, U. (2010) ‘A New Graphical Password Scheme Resistant to Shoulder-Surfing’, International Confer-ence on CyberWorlds, Singapore.

Ghori, F. and Abbasi, K. (2013) ‘Secure User Authentication Using Graphical Passwords’, Journal of Independent Studies and Research, 11(2), p. 34.

Ghorsad, T. N., Pippal, R. S., Prasad Patel, B. and Bhopal, R. (2015) ‘A REVIEW ONSCHEMES FOR USER AUTHENTICATION’, Patel Research Cell An International Journal of Engineering Sciences, pp. 2229–6913.

Gokhale, A. and Waghmare, V. (2013) ‘Graphical Password Authentication Techniques: A Review’, International Journal of Science and Research (IJSR) ISSN (Online Index Copernicus Value Impact Factor, 14(7), pp. 2319–7064. Available at: www.ijsr.net (Accessed: 8 October 2016).

Hayashi, E., Dhamija, R., Christin, N. and Perrig, A. (2008) ‘Use your illusion: secure authentication usable anywhere’, in Proceedings of the 4th symposium on Usable privacy and security. ACM, pp. 35–45.

Herrera, L. A. (2015) ‘AUTHENTICATION METHOD USING MULTI-FACTOR EYE GAZE’. US Patent 20,150,302,252.

Hong, D., Man, S., Hawes, B. and Matthews, M. M. (2004) ‘A Graphical Password Scheme Strongly Resistant to Spyware.’, In Proceedings of International conference on security and management . Las Vergas, NV, pp. 94–100.

Istyaq, S. (2016) ‘A New Technique For User Authentication Using Numeric One Time Password Scheme’, International Journal of Computer Sciences and Engineering, 4(5).

Jakob, N. (2000) ‘Why you only need to test with 5 users’, Alertbox.

Jansen, W., Gavrila, S., Korolev, V., Ayers, R. and Swanstrom, R. (2003) ‘Picture password: a visual login technique for mobile devices’.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. and Rubin, A. D. (1999) ‘The Design and Analysis of Graphical Passwords’, Proceedings of the 8th USENIX Security Symposium, 8, p. 1.

Jesudoss, A. and N.P, S. (2014) ‘A SURVEY ON AUTHENTICATION ATTACKS AND COUNTERMEASURES IN A DISTRIBUTED ENVIRONMENT’, Indian Journal of Computer Science and Engineering (IJCSE), 5(2).

Kaur, S. (2016) ‘Three Level Authentications Using Graphical Password With Pass Point Scheme’, International Journal of Advanced Research in Computer Science and Software Engineering, 6(6), pp. 2277–128.

Khan, W. Z., Aalsalem, M. Y. and Xiang, Y. (2011) ‘A Graphical Password Based System for Small Mobile Devices’, IJCSI International Journal of Computer Science Issues, 8(5).

Kumar, H., Arohi, S. and Khan, F. U. (2013) ‘Graphical Password Authentication Schemes: Current Status and Key Issues’, nt. J. Eng. Innovative Technol.(IJEIT), 10(2).

Kuseler, T. and Lami, I. A. (2012) ‘Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones’, Torben Kuseler & Ihsan Alshahib Lami International Journal of Computer Science and Security, (64), pp. 2012–277.

Lashkari, A. H. (2014) ‘GPIP: A new Graphical Password based on Image Portions’, Advances in Information Science and Applications , 1.

Lashkari, A. H., Gani, A., Sabet, L. G. and Farmand, S. (2010) ‘A new algorithm on Graphical User Authentication (GUA) based on multi-line grids’, Scientific Research and Essays, 5(24), pp. 3865–3875.

Liu, X., Qiu, J., Ma, L., Gao, H. and Ren, Z. (2011) ‘A Novel Cued-recall Graphical Password Scheme’, in 2011 Sixth International Conference on Image and Graphics. IEEE, pp. 949–956.

Malek, B., Carmen, P. Del, Orozco, M., Eid, M. and Saddik, A. El (2006) ‘Proceedings of Virtual Concept 2006 Haptic-Based Sensible Graphical Password’, In Proceedings of Virtual Concept.

Man, S., Hong, D. and Matthews, M. (2003) ‘A Shoulder-Sur_ng Resistant Graphical Password Scheme’, in Proceedings of International conference on security and management . Las Vergas, NV,.

Meng, W., Li, W., Kwok, L.-F. and Choo, K.-K. R. (2017) ‘Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones’, Computers & Security, 65, pp. 213–229.

Murugavalli, S., Jainulabudeen, S., Senthil Kumar, G. and Anuradha, D. (2016) ‘Enhancing security against hard AI problems in user authentication using CAPTCHA as graphical passwords’, International Journal of Advanced Computer Research, 6(24).

Nali, D. and Thorpe, J. (2004) ‘Analyzing User Choice in Graphical Passwords’, Technical Report TR-04-01, School of Computer Science, Carleton University.

Nielsen, J. and Jakob (1993) Usability engineering. Academic Press. Available at: http://dl.acm.org/citation.cfm?id=529793 (Accessed: 14 May 2017).

Park, M., Kita, Y., Aburada, K. and Okazaki, N. (2014) ‘Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance’, in 2014 17Th International Conference On Network-Based Information Systems. IEEE, pp. 495–500.

Passlogix (2013) ‘Http://www.passlogix.com’, last accessed in Oct 2013.

Patel, J. and Patel, A. (2015) ‘A Survey on Different Authentication Schemes for Session Passwords’, International Journal of Scientific Research in Science, Engineering and Technology, 6(6), pp. 190–192.

Paul, D. and Jeff, Y. (2007) ‘“Do background images improve Draw a secret graphical passwords?’, In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS) , pp. 36–47.

Pering, T., Sundar, M., Light, J. and Want, R. (2003) ‘Photographic Authentication Through Untrusted Terminals’, Pervasive Computing, pp. 30–36.

Purushothaman G R and Ashwini, M. (2016) ‘A Novel Two Step Random Colored Grid Process: Graphical Password Authentication System’, International Journal of Computer Networks and Communications Security, 4(2), pp. 52–55.

Ramanan, S. and S, B. J. (2014) ‘A Survey on Different Graphical Password Authentication Techniques’, International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization), 3297(12).

Renaud, K. and Smith, E. (2001) ‘Jiminy: “Helping user to remember their passwords”’, Technical report, School of Computing, Univ. of South Africa ,.

Rittenhouse, R. G. and Chaudhry, J. A. (2016) ‘A Survey of Alternative Authentication Methods’.

Ritter, D., Schaub, F., Walch, M. and Weber, M. (2013) ‘MIBA’, in CHI ’13 Extended Abstracts on Human Factors in Computing Systems on - CHI EA ’13. New York, New York, USA: ACM Press, p. 787.

Sayed, S., Mohid Student, A. B., Pal Student, M. B. and Haji Student, M. B. (2016) ‘Graphical Password based Authentication System with Sound Sequence’, International Journal of Computer Applications, 138(12), pp. 975–8887.

Schechter, S. and Bonneau, J. (2015) ‘Learning Assigned Secrets for Unlocking Mobile Devices’, Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).

SFR (2013) www.sfr-software.de/cms/EN/pocketpc/viskey/ index.html, last accessed in Oct 2013.

Shankar, V., Singh, K. and Kumar, A. (2016) ‘IPCT: A scheme for mobile authentication’, Perspectives in Science, 8(C), pp. 522–524. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2213020916301483 (Accessed: 15 November 2016).

Singh Thakur, M. R., Pathak, S., Patil, R., Kate, N. and Badkul, A. (2012) ‘GRAPHICAL PASSWORD (PUZZLES) AUTHENTICATION SYSTEM’, International Journal Of Computer Architecture And Mobility, 1(1).

Six, J. M. and Macefield, R. (2016) ‘How to Determine the Right Number of Participants for Usability Studies’. UXmatters.

Swapnil Sunil, S., Prakash, D. and Ramesh Shivaji, Y. (2014) ‘Cued Click Points: Graphical Password Authentication Technique for Security’, (IJCSIT) International Journal of Computer Science and Information Technologies, 5.

Taiabul Haque, S. M. (2015) HUMAN FACTORS IN TEXTUAL PASSWORD-

BASED AUTHENTICATION.

Takada, T. and Koike, H. (2003) ‘Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images’, in Human-Computer Interaction with Mobile Devices and Services, pp. 347–351.

Tao, H. (2006) ‘Pass-Go, a New Graphical Password Scheme’, MSc., University of Ottawa, Canada.

Thorpe, J. and Van Oorschot, P. C. (2004) ‘Towards Secure Design Choices for Implementing Graphical Passwords’, in proceedings of the 20th Annual Computer Security Applications Conference,Tucson, Arizona.

Togookhuu, B. and Zhang, J. (2017) ‘New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation’, Procedia Computer Science, 107, pp. 148–156.

Ugochukwu, K., Ekeke, E. and Jusoh, Y. Y. (2013) ‘A review on the graphical user authentication algorithm: recognition-based and recall-based’, International Journal of Information Processing & Management, 4(3).

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X. and Aickelin, U. (2010) ‘Against Spyware Using CAPTCHA in Graphical Password Scheme’, in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, pp. 760–767.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N. (2005) ‘PassPoints: Design and longitudinal evaluation of a graphical password system ARTICLE IN PRESS’, Int. J. Human-Computer Studies, 63, pp. 102–127.

Young-Hwa, A. (2015) ‘Security enhancements of smart card-based remote user password authentication scheme with session key agreement’, in 2015 17th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 669–674.

Zakaria, N. H., Griffiths, D., Brostoff, S. and Yan, J. (2011) ‘Shoulder surfing defence for recall-based graphical passwords’, in Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS ’11. New York, New York, USA: ACM Press, p. 1.

Zhang-Kennedy, L., Chiasson, S. and van Oorschot, P. (2016) ‘Revisiting password rules: facilitating human management of passwords’, in Electronic Crime Research (eCrime), 2016 APWG Symposium on. IEEE, pp. 1–10.

Zheng, Z., Liu, X., Yin, L. and Liu, Z. (2010) ‘A Hybrid Password Authentication Scheme Based on Shape and Text’, JOURNAL OF COMPUTERS, 5.

Zhu, B. B., Yan, J., Wei, D. and Yang, M. (2014) ‘Security Analyses of Click-based Graphical Passwords via Image Point Memorability’, in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS ’14. New York, New York, USA: ACM Press, pp. 1217–1231.

Zizzi, S. (2015) ‘User authentication system and method for encryption and decryption’. Google Patents, pp. 203–626.

Zulkarnain Syed Idrus, S., Cherrier, E., Rosenberger, C., Schwartzmann, J.-J. and Schwartz-mann, J.-J. A. (2013) ‘A Review on Authentication Methods’, Review on Authentication Methods. Australian Journal of Basic and Applied Sci-ences, 7(5), pp. 95–107.