USER AUTHENTICATION ON SMARTPHONES USING ALPHANUMERICAL AND GRAPHICAL PASSWORD

SITI NUR AINI BINTI AHAMAD

BACHELOR OF COMPUTER SCIENCE (COMPUTER NETWORK SECURITY) WITH HONOURS
USER AUTHENTICATION ON SMARTPHONES USING ALPHANUMERICAL AND GRAPHICAL PASSWORD

SITI NUR AINI BINTI AHAMAD

Bachelor of Computer Science (Computer Network Security) With Honours

Faculty of Informatics and Computing

Universiti Sultan Zainal Abidin

SEPTEMBER 2017
APPROVAL

I have read this report, and in my point of view, this project fulfills conditions to be awarded a Bachelor of Computer Science (Computer Network Security) With Honours.

Signature: ..................................................

Supervisor: Puan Roslinda bt. Muda

Date:
DECLARATION OF ORIGINALITY

I at this moment declare that this project and the work reported herein was composed by and originated entirely from me. Information derived from the published and unpublished work of others has acknowledged in the given list of references and citation.

Signature: .............................................

Name: Siti Nur Aini Binti Ahamad

Date:
All praise is due to Allah who has given me this opportunity to conduct this report “User Authentication On Smartphones Using Alphanumerical and Graphical Password” for my final year project.

My greatest appreciation goes to my family and my friends who supported and encourage me throughout the process. For my parents, thank you for moral support and my fellow friends especially KRK students for semester 6, thanks for the support and all the brainstorming session in this six months.

I would like to express my sincere appreciation and gratitude to my supervisor Mdm. Roslinda binti Muda for the encouragement, guidance, critics, advice, motivation and support. Without this continued support, this project would not be the same as presented here.
ABSTRACT

Authentication is the process to identify someone, usually using username and password, which is used to grant someone’s access to the system object based on their identity. Graphical password is the authentication system that use graphical image as the password on their smart phones or tablet PCs. This project is focusing on the usage of the images that represents the alphanumeric password. As you know, alphanumeric password is vulnerable because it is easy to guess. Users tend to use easy passwords. To secure their smartphones, they must to use difficult password, but it is useless since human’s brain doesn’t quite remember something textual. So, this project will secure the smart phone from any possible attacks with the idea of the combination of alphanumerical character and images. The smart phone will be secure from the server attack since only the alphanumeric password will be saved on the system’s database, not the images. As for the techniques, this application will use the image based password authentication on the random image and the alpha numerical password authentication that will be hidden behind selected images. As it mentions above, the characters will likely be being hiding on the picture that is on the system’s database. The user will choose the pictures for the characters that the user wants. The password will be saved on the database but not the pictures. Then, the system will randomly swap the pictures for every login. This application will focus on the user that wanting to secure their smart phones or tablet PCs from other persons. The outcome for this project is the user will have a secure smart phones or tablet PCs. As to conclude, this will give the user a secured and safe with easy-to-use application and it will be at the users satisfactory.
ABSTRAK

# TABLE OF CONTENTS

APPROVAL ........................................................................................................................................... i
DECLARATION OF ORIGINALITY ........................................................................................................ ii
ACKNOWLEDGEMENTS ....................................................................................................................... iii
ABSTRAK ............................................................................................................................................. iv
ABSTRACT ........................................................................................................................................... v
LIST OF FIGURES ................................................................................................................................ ix
LIST OF TABLES ................................................................................................................................... x
LIST OF ABBREVIATION ..................................................................................................................... xi
LIST OF APPENDICES ........................................................................................................................ xii

## CHAPTER 1: INTRODUCTION

1.1 Introduction ................................................................................................................................ 1
1.2 System Background .................................................................................................................... 2-3
1.3 Problem Statement .................................................................................................................... 3
1.4 Objectives .................................................................................................................................... 3
CHAPTER 2: LITERATURE REVIEW

2.1 Introduction ................................................................. 6
2.2 Authentication ............................................................... 6-8
2.3 Graphical Password .......................................................... 8-9
2.4 Existing Works of Graphical Password ..................................... 9
   2.4.1 Déjà Vu ................................................................. 9-10
   2.4.2 Awase-E ................................................................. 10-11
   2.4.3 Story ................................................................. 11-12
   2.4.4 GPI ................................................................. 12
   2.4.5 S3PAS ................................................................. 12-13
2.5 Proposed System Design ...................................................... 13
2.6 Summary ...................................................................... 14
CHAPTER 3: METHODOLOGY

3.1 Introduction ...................................................................................................................... 15

3.2 Project Methodology ....................................................................................................... 15
  3.2.1 Requirement Planning .................................................................................................. 16
  3.2.2 User Design ................................................................................................................. 16
  3.2.3 Construction ................................................................................................................ 16
    3.2.3.1 Framework .................................................................................................................. 17-18
    3.2.3.2 System Flowchart .................................................................................................... 18-19
    3.2.3.3 Entity Relationship Diagram ................................................................................... 19-20
    3.2.3.4 Context Diagram ...................................................................................................... 20-21
    3.2.3.5 Data Flow Diagram .................................................................................................. 21-22
    3.2.3.6 Database .................................................................................................................. 22
  3.2.4 Cutover ....................................................................................................................... 22

3.3 System Requirement ........................................................................................................ 23
  3.3.1 Software ...................................................................................................................... 23
  3.3.2 Hardware .................................................................................................................... 23

3.4 Summary .......................................................................................................................... 23
LIST OF FIGURES

Figure 01: Déjà Vu
Figure 02: Awase-E
Figure 03: Story
Figure 04: GPI
Figure 05: S3PAS
Figure 06: Project Methodology
Figure 07: Framework
Figure 08: System Flowchart
Figure 09: Entity Relationship Diagram
Figure 10: Context Diagram
Figure 11: Data Flow Diagram
LIST OF TABLES

Table 01: User Table
Table 02: Password Table
LIST OF ABBREVIATIONS / TERMS / SYMBOLS

1) FYP: Final Year Project
2) RAD: Rapid Diagram
3) GPI: Graphical Password with Icons
4) S3PAS: Scalable Shoulder Surfing Textual-Graphical Password
LIST OF APPENDICES

Appendix 01: Gantt Chart

Appendix 02: Literature Review (Table version)
CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, technologies like computers, tablet PCs, and smartphones as well as information security are the most significant challenge. Authorized users must log in to the system to get access the information. Authorization cannot do without authentication [9]. Authentication is the process to identify someone, usually using username and password, which is used to grant someone’s access to the system object based on their identity [1]. Current authentication methods divided into three categories; token based, biometric based and knowledge based.
A graphical password is the authentication system that uses the graphical image as the password. It also called as graphical user authentication (GUA). The graphical password divided into three categories which are recognition-based, pure recall-based and cued recall-based graphical techniques. Knowledge-based authentication is the most common authentication method that includes both textual and graphical techniques. The textual password like alphanumeric based method categorized as traditional password method. The alphanumeric password is the method that used alphabets, numbers, and characters.

Two-factor authentication (2FA) refers as two-step authentication, a security process that which user are provided with two authentication factors to verify them. The authentication factors are divided into three types; knowledge, possession and inherence factors. Knowledge factors is what the user know such as PIN numbers, passwords or shared secrets. Possession factors is like what the user have, such as ID card, security keys or smartphone. Lastly, inherence factors that called as biometric. Biometric is the authentication method that using the user physical attributes such as thumbprint, iris reading and many more [3].

1.2 System Background

This project will use both textual and graphical authentication which is a recognition-based authentication that uses the characters and images. The alphanumerical password was vulnerable to use for a password. The psychological study stated that human brain quickly remembers pictures rather than text. Many experts also said that graphical password is resistant from any possible attack such as dictionary attack, shoulder surfing, brute force attack and much more.

Shoulder surfing refers to someone that using direct observation techniques to capture other person’s password. For example, Girl A watching over Girl B that unlock her smartphone to know her screen lock password. A dictionary attack is a technique that used to breach the computer security of password-protected machine or server. Brute force search is a trial-and-error method used to obtain
information such as a password or personal identification number (PIN). It used automated software to generate a large number of consecutive guesses as for the value of desired data.

This application is using user authentication as the program protocol. It will authorize human-to-machine interaction. This system will protect the 8-characters alphanumeric passwords and images that the user chooses from the system’s library. This project will use a two-factor authentication which is using both textual and graphical authentication. Two-factor authentication provides additional security to the system. It is already being used commercially to prevent user’s data being accessed without authorization from the user him/herself.

1.3 Problem Statement

As we know, the alphanumeric password widely used everywhere. The main problem of this kind of authentication is the vulnerability of the system. The alphanumeric password is the most vulnerable since the hacker can make a guess of the user’s password and username using brute force search attack. Although it will be safe to the user that registered their account using a complicated password since it cannot easily guess by the hacker, it will be useless as the user himself forgot the password or writing it on a piece of paper. It is same to who that like having a simple password on the system. It would be easy to remember but it also easily guessed by the hacker.

Besides that, alphanumeric password authentication is vulnerable because the user tends to use their first and last name and other standard information that can easily guess such as birthdays, son or daughter names, and much more.
1.4 **Objectives**

1. To study about graphical user authentication that can apply to the application system.
2. To design a simple, user-friendly application system that will authenticate the authorized user.
3. To implement the authentication system based on the research about the textual and graphical password.

1.5 **Project Scope**

For this system, there are two scopes in this project which are user and system. In the user scope, there are two phases; registration phase and login phase.

In registration phase, the user needs to create at least eight characters of the alphanumeric and graphical password based on the images that are in the system’s database. The user must retype and reselect both alphanumeric and graphical password that have been created again to authenticate. After that, the application will verify the authentication of the user. In login phase, the user will select those images that user picked earlier on the screen lock.

On the system scope, the system will have to verify the password by comparing the password that user selected on the login process to the ones that the user selected in the registration process.
1.6 Limitation of works

This system has their requirements that user must follow. The password that created by the user must be a combination of 8 characters and images. For this project, the user has to choose a group of images that fixed in the system’s database to create their password. The password cannot be least of six images and characters since the purpose of this project is to prevent possible attacks.

But since the screen were small, the picture may be the common images and icons that did not have much complexity and abstraction.

1.7 Summary

In the Chapter 1, we can conclude about background of the system, problem statement, objective, scope and limitation of work of the authentication system. Therefore, to overcome the problem, this project will use the combination of numbers and image as password.
CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

As you know, many researchers are taking their interest on this innovation. So, for this chapter, I will analyze a few journals that those researchers had researching about the graphical and alphanumerical password.
2.2 Authentication

Authentication is a process in which the credentials provided are being compared from the files in a database of authorized users’ information on a local operating system or to an authentication server. If the credentials match, the process is completed, and the user is granted authorization for access [1]. It is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity [2].

Current authentication methods can be divided into three main areas: (1) token-based authentication, (2) biometric-based authentication and (3) knowledge-based authentication [5]. Token-based techniques are based on “something you possess”. For example, Smart Cards, a driver’s license, credit card, and a university ID card. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource, without using their username and password. Biometric-based techniques are based on “something you are”. It uses physiological or behavioural characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user’s biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. Knowledge-based technique is based on “something you know” to identify the user. For example, a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question [6].

There are three categories of knowledge-based graphical user authentication algorithm, Recognition-based, Recall-based and Hybrid. Using Recognition-based, the user clicks a correct image in a particular order from a group of images shown to the user. Some of the examples to be explained further in the next section include: Déjà Vu, Awase-E, Story, GPI (Graphical Password with Icons) and S3PAS (Scalable Shoulder Surfing Textual-Graphical Password Authentication). In Recall-based, the user is asked to reproduce the password that was created during registration. There are two types of recall-based algorithm, pure recall-based (the user is not
given hints to help with reproducing their password) and cued recall-based (the user is given hints and clues implicitly to help with reproducing their password) [7]. Hybrid scheme are the combination of two or more graphical schemes. These schemes are introducing to overcome the limitations of single scheme, such as hotspot problems, shoulder surfing spyware and many more [8].

The most common authentication is using a username and password. Generally, user authentication is based on three factors: what user knows, what user has and what user is [16]. Major problems of the textual password are the difficulty of remembering passwords [5]. A survey has shown that most of the users tend to select short passwords or passwords that are easy to remember which unfortunately, can be easily guessed or broken by attackers [14]. On the other hand, if the passwords are hard enough to guess, the user cannot remember the password, so they tend to use the same password on various accounts or write down the passwords [16].

2.3 Graphical Password

Text-based username-password system have been traditionally in authenticating users before allowing them to access the services [13]. Alphanumerical password is called a recall-based password since the user must enter the exact characters that the user entered on the registration phase. Alphanumerical password is known as the traditional password scheme but they are also known to have security and usability issues. It becase users tend to choose a short, simple password that are easy to guess [18]. Surveys shows that frequent passwords are personal names of family members, birth date, or dictionary words [10]. One way to overcome this problem is to assign a random password to the user [13]. On the other hand, password that hard to guess and break are hard to remember. Thus a large portion of customer services calls are related to one’s forgetting his or her passwords. Studies showed that since user can only remember a limited number of password, they tend to write them or will use the same password for different accounts [5].
Graphical password provides a promising alternative to traditional alphanumerical passwords [17]. The birth of the graphical password idea was from Blonder in 1996. He proposed that a user required to click on the predetermined areas of the predetermined images in the predetermined sequences to enter the password [10]. His method was later being an inspiration idea for graphical password scheme development [12]. As time flows, many researchers that are taking their interests on graphical password and it results of many authentication schemes were born in this era.

Graphical password mainly operates when the user must recognize previously chosen images from a larger group of distractor images. The decision is binary: either the image is known or not. Many researcher agreed that graphical password is relatively better than alphanumeric ones. Studies of recall also confirm that pictures are recalled better than words and this has led to the tag “picture superiority effect” [24].

There are the three ways of associating people with images: (1) let them supply the images themselves, or (2) allow them to choose from a range of images, or (3) assign images randomly to them. Unfortunately, the first two options can cause severe security concern since user are allowed to choose their own images and they tend to choose predictable images. So, it would be better if the images should be assign to users randomly [11].
2.4 Existing Works of Graphical Password

2.4.1 Déjà Vu

This Déjà Vu system is proposed by Dhamija et al. in year 2000. This system is mainly with selecting a random art pictures from a set of pictures by a program. Dhamija et. al. aim to satisfy the following requirements:

- The system should not rely on precise recall. Instead, it should be based on recognition, to make the authentication task more reliable and easier for the user.
- The system should prevent users from choosing weak passwords.
• The system should make it difficult to write passwords down and to share them with others [21].

Déjà Vu has three phases: portfolio creation, training and authentication. At the time of authentication, system shows a set of images that contains both password images and decoys. During an authentication session, the user is required to identify the selected images upon which the user is then authenticated. Each image is abstract in nature and the collection is generated using a mathematical formula, the output is depending on an initial seed [11].

Drawbacks of this scheme are it is hard to remember obscure pictures and the corpus size is much smaller than that of the text based password. [8].
2.4.2 Awase-E

In this scheme, users can use their favourite pictures as a password. The user has to select or register some images which are tagged as “pass images” with the system. Upon authentication, a sequence of images is shown to the user, if the user’s image is shown in the grid of images, the user has to select the correct pass-image. If the user’s image doesn’t show up on the grid of images shown, the user has to select “no pass-image” which is used for decoy images [7]. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration [5]. It will give another function-notification which gives user a trigger to handle malicious attempts. Shows P images with N rounds, every round includes one or zero pass images. With it, usability and security will be a higher level [10].

![Figure 02](image)
2.4.3 Story

This scheme is proposed by Davis et al. [7]. This authentication scheme is said to be similar to PassFaces authentication scheme. This scheme is need only one rounds of authentication, but password images are in the sequence of several unique images that creates a story to enhance memorability. It is like the user is telling a story based on the picture password. It also requires user to remember the sequence of images [8]. The user must select from a given number of images, the selected images chosen during the registration period. Only when the sequences of images are correct, then the user is authenticated. The drawback of this algorithm is that some users found it hard to remember the sequence of images in comparison to PassFaces algorithm [7].
2.4.4 GPI

Graphical Password with Icons, initialized as GPI is a graphical password that designed to solve hotspot problem. The user must select 6 from 150 icons as a password in one panel. Main drawbacks of this scheme is the unacceptable login time and small size of icons [8].
2.4.5 S3PAS

Scalable Shoulder Surfing Textual-Graphical Password Authentication, initialized as S3PAS, is a system that was proposed by Zhou and Li to resist the shoulder surfing attacks. It is the hybrid scheme that using a combination of textual and graphical passwords [8]. S3PAS has the following salient features:

1. Shoulder-surfing, hidden-camera and spyware resistant. The secret cannot be stolen even when an attacker watches or camera-records the victim enter the password.

2. Exactly match the conventional password and can go beyond. S3PAS can coexist with
text passwords without changing the existing user profiles. Further, it can add more graphical pass-icons and sophisticated rules to further enhance the security level.

(3) It is robust against brute-force attacks.

(4) It supports both keyboard and mouse as input devices [22].

S3PAS can accommodate various lengths of textual passwords, which requires zero-efforts for users to migrate their existing passwords to S3PAS [23]. S3PAS system generates the login image locally and transmits the image specification (e.g., the coordinates of every character or icon in the image) instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time [22]. This model seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder surfing, hidden-camera and spyware attacks [23].

2.5 Proposed System Design

In this project, I am going to implement the graphical-based authentication system algorithm that based on the validating authentication. The system will be using textual and graphical password. The general idea of this project are typing at least 8-character password image password that will be used to hide the numbers. Although alphanumeric password has many drawbacks based on security, the usability factor can be the advantage for these password. On the other hand, graphical password can be good in terms on security, but it is still a big question on the usability.

On registration phase, the user will enter the username, password and existing email. Next, the user will enter 8-character password and images. For authentication process, the user will re-enter and reselect those password and images. On login phase, the user will enter characters and images password that the user entered on the registration phase.
2.6 Summary

Based on this chapter can be concluding about previous research to know the existing method that use by another researcher. Moreover, every technique that has been proposed in the research has their strength and weakness.
CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter will be discussing about how to develop the project. There are some requirements that we must be fulfilled and considered as a researcher. In methodology term, it can be simply the method that the researcher intends to use to collect data. Methodology is a set of practices regarding to develop the project.
3.2 Project Methodology

3.2.1 Requirement Planning

There are initial research and studied has been made to highly understanding about authentication and their type. In this requirement planning, we need to determine and understand clearly the objective of this project before develop the system. Besides that, analyse the problem in authentication then we know the existing technique that have been proposed. Basically, in this phase also can be prepare the requirement and specification for this project.
3.2.2 User Design

In this phase, the user interacts with systems to analyse and develop model that represent all the system processes, input and output from the system. As general design, there are two groups of image and characters. The group of images that consist of 30 images on an interface where it can swap position in every login session while group of textual characters by creating the password.

3.2.3 Construction

In this RAD, the scheme is going to be as an android based and this project have their database where the pre-selected images and characters are stored. During registration phase, the general idea and design will be interpreted to implement the specification that proposed in the project.
3.2.3.1 Framework

This is the framework of the authentication based application system that using textual and graphical. This framework describes about overview of the system work. The framework can be divided into two phases which are registration and login phase.

In the first phase, the user need to register, so the user must to fill all required information in data form and create the password based on the character and a groups of images. User must choose the combination of image and characters as their password. The password cannot be three image and three numbers in sequence. The user information and password will store in the database.
On the second phase, the user need to login by entering and clicking the characters and images as their password by order. The user need to recognize the password that selected in registration phase. This is known as recognition-based technique. The password that entered during login then is compared in database using recall-based technique. The system will retrieve the password from the database store. Login successfully if the username and password are valid.
3.2.3.2 System Flowchart

Figure 08
This figure shows the flowchart of the authentication system. User need to choose either already register or not then proceed to login phase. If no, user should do registration. In registration, user need to choose their password in password selection based on the group of image and number that appears during registration page. Then user need to login by enter username then select their password that already register. In login phase, user must reselect the images and click button number as their password that user choose early the registration phase. Then, system will verify username and password, if it is incorrect, user need to re-enter their username and password again. Otherwise, verification is successfully.
This figure shows the Entity Relationship Diagram of this system. There are the five entities such as user, password, image and character. For the first relationship, user needed to login the system. User entity has four attributes which are Username, Password and Email. Username as the primary key that used to connected with the entities. Second relationship such as user must create the password. In password entity have attributes like Username, Character and Image. One password can contain many character and image but not
by three number or image in sequence order. The values are combination image and number by sequence position that created by user in registration.

3.2.3.4 Context Diagram

Figure 10
The figure explained about the context diagram in this system, the user need to register by entering the information that the system wants and create the password. In login process, the user will enter their password by clicking the selected password that are chosen when in registration phase, then system will verify the user as the password that were saved on the database are correct.

3.2.3.5 Data Flow Diagram

![Data Flow Diagram]

Figure 11
This figure shows the Data Flow Diagram of the system. Firstly, ‘User’ should give the user details in register phase then choose the password with combination of images and characters. ‘User details’ will store into user file while password details store into password file. Next, system need to verify the user by login process. In login process, user must enter the password then it will be retrieved from user and password file.

### 3.2.3.6 Database

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>varchar(50)</td>
<td>Primary key</td>
</tr>
<tr>
<td>Password</td>
<td>varchar(50)</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>varchar(50)</td>
<td></td>
</tr>
</tbody>
</table>

Table 01: User Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>varchar(50)</td>
<td>Primary key</td>
</tr>
<tr>
<td>character</td>
<td>varchar(50)</td>
<td></td>
</tr>
<tr>
<td>image</td>
<td>varchar(50)</td>
<td></td>
</tr>
</tbody>
</table>

Table 02: Password Table
3.2.4 Cutover

According to this phase, the system will be used the prototypes with the real data to test the how far the functionality of system and change over to the new system if needed some changes.

3.3 System Requirement

3.3.1 Software

The system development required by Windows 10 Pro, Microsoft Word 2016, Microsoft Power Point 2016, Android Studio and SQLite.

3.3.2 Hardware

The hardware that been used to develop the authentication system which is Acer Aspire E 15 and a mouse.
3.4 Summary

In this chapter, it can be concluded about the methodology of the authentication system. Methodology that been used for this project is RAD model that explain about requirement planning, user design, construction and cutover. System requirement divide into software and hardware requirements that needed to develop the authentication system.
REFERENCES


APPENDICES

1) Gantt Chart

FYP 1

<table>
<thead>
<tr>
<th>Task</th>
<th>Week 1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic discussion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project title proposal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal writing – Chapter 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal writing – Chapter 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Part 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal writing – Chapter 2 (Part 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal progress presentation &amp; evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discussion &amp; correction of proposal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal solution – Chapter 3 (Part 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposal solution – Chapter 3 (Part 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof of concept</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seminar preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seminar presentation &amp; evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Literature Review

<table>
<thead>
<tr>
<th>AUTHOR/YEAR</th>
<th>PROJECT NAME</th>
<th>OBJECTIVES</th>
<th>TECHNIQUE/METHOD</th>
<th>FINDINGS/DESCRIPTIONS</th>
</tr>
</thead>
</table>
| Blonder, Greg E. | Graphical password   | • To overcome the difficulties of limitation on the conventional alphanumerical passwords. | Cued click-based Graphical Password. | • User seeking access to a resource:  
  ▪ presented with a predetermined image on a visual display  
  ▪ required to point to (e.g. touch) one or more predetermined positions on the displayed image (referred to herein as “tap regions”) in predetermined order as a way of indicating |
his or her authorization to access the resource.

- There is provided a graphical password arrangement and/or method.

- The arrangement comprises means for:
  - displaying a predetermined image,
  - storing a predetermined number of predetermined positions in a predetermined image as a password.
  - responsive to a determination of a lack of correspondence between the determined locations and the predetermined positions for denying the user access to a resource that is protected by a password.
• The method correspondingly comprises:
  ▪ the steps of displaying predetermined image.
  ▪ selecting locations in the displayed image under user control.
  ▪ determining whether the selected locations correspond to a predetermined image that are stored as a password, and
  ▪ denying the user access to the resources in response to a determination that correspondence is lacking between the selected locations and the predetermined positions.

• Advantages:
  ▪ people generally finds images to be easy to recall than alphanumeric sequences, particularly
images with personal meaning.

- even a very coarse matrix of tap regions yields great security.
- graphical password arrangement is substantially no more difficult or expensive to implement than a conventional password arrangement.

To discuss security threats for mobile devices.  
To determine the performances of pattern and PIN with Alphanumeric (PIN) and Recall-based Graphical password (Pattern). | Screen size affects login performances on creation time, login time and login success rate.  
On creation time, the pattern on the tablet takes the highest time among other comparison.  
The pattern takes slightly less time to log in on phone, and PIN takes slightly less time to log in on tablet.  
Pattern is easier to use on tablet rather than on phone. |
| Saharkar, Mr Chetan, and S. V. Dhopte (2014) | Graphical Region Based and Alphanumeric Password for Authentication System |  • To conduct comprehensive survey of the existing graphical password techniques.  
• To implement graphical based authentication system algorithm. |  • Shoulder surfing attack has 43% chance to be threat on PIN  
• Smudge attacks has 50% chance for pattern.  

|  |  | Recall-based Graphical password. |  • This proposed system is using recall-based graphical authentication.  
• It checks user ID and pictures if both are current, then it will check if it presents on database.  
• If it is present it will grant access to the user.  
• They should be more resistant to brute force attack since the search space is infinite practically.  
• In this proposed system, user will select picture, POIs and corresponding words.  
• The order and number of POIs can be enforced for stronger authentication. |
<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Contributions</th>
</tr>
</thead>
</table>
| Gokhale, Mrs Aakansha S., and Vijaya S. Waghmare (2016) | The Shoulder Surfing Resistant Graphical Password Authentication Technique. | - To reduce the shortcomings of textual passwords with introducing new technique.  
- To provide a strong security against attacks like brute force and guessing.  
Combination of Recognition and Recall-based Graphical password.  
- The proposed system is using both recognition and recall-based approach.  
- As password space is very large, it provides security against brute force search attacks.  
- Randomization of passwords in both steps.  
- Using registered e-mail to provide authenticity of user.  
- Have ROAs (Region-of answers) as secret question if forget the password.  
- Have a very large password space. |
- To provide in-depth analysis with specific Graphical passwords  
- The current passwords can be classified into four group: drawmetric, locimetric, cognometric and hybrid schemes.  
- Déjà vu:  
  - In registration phase, user selected a certain number of art pictures. |
<p>| Schemes of attack methods | | | |
|---------------------------|------------------|------------------|
| ▪ Advantage: art images makes it difficult to record or share with others. |
| ▪ Disadvantage: obscure picture is hard to remember and password space is smaller than alphanumerical password. |
| ▪ Passfaces: |
| ▪ User need to click on faces image preselected on several rounds. |
| ▪ It is reported to be vulnerable to shoulder surfing and spyware. |
| ▪ There are some predictable images users are more inclined to select on gender, race and complexion. |
| ▪ GPI or GPIS: |
| ▪ Designed aimed at solving hotspot problem. |
| ▪ Selecting 6 icons from 150 icons in a panel as password. |</p>
<table>
<thead>
<tr>
<th>Almulhem, Ahmad (2011)</th>
<th>A Graphical Password Authentication System</th>
<th>- To propose graphical password authentication system that using both graphical and text-based password.</th>
<th>Graphical passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- The proposed system that combines graphical and text-based passwords trying to achieve the best of both worlds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In registration, user create a graphical password by first entering a picture that the user chooses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using Point-of Interest (POI) region on the picture.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- User types a word or phrase that would be associated with that POI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For login, user first enters username and password. And then, system will display the registered pictures and has to correctly pick the POIs and type the associated words.</td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Title</td>
<td>Methods</td>
<td>Results</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Ramanan, Saranya, and J. S. Bindhu (2014)</td>
<td>A Survey on Different Graphical Password Authentication Techniques</td>
<td>To conduct comprehensive survey of the existing graphical password techniques. To analyze the strengths and weaknesses.</td>
<td>Graphical passwords Guessing the correct gesture set based on smudging is very difficult, but attacks like hotspots and shoulder surfing is still a matter to concern. Commercial products that using pure recall-based graphical password clearly demonstrate that the product must be simple to use.</td>
</tr>
</tbody>
</table>
drawbacks of the method.

- Click-based graphical password is vulnerable to shoulder surfing since the position of the image is remain same in each login.
- Screen scraper can find exact location and it will be sufficient to hacking as attacker knows when the user clicked the mouse.
- To resist the attack, the graphical password should use a shield to hide the entering of password.

<table>
<thead>
<tr>
<th>Suo, Xiaoyuan (2006)</th>
<th>A Design And Analysis of Graphical Password</th>
<th>Graphical passwords</th>
<th>The proposed system is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>- RAF, or recall a formation which allow user to choose from a set of images to be placed into 8x8 grid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Neural network based approach that authenticate user by user’s daily mouse motion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Shoulder surfing resistant passpoint.</td>
</tr>
</tbody>
</table>
and point out future research directions.

- RAF using recall based technique.
- Have a simple interface, which is two 8x8 tables, an input table and data table.
- Data table contains possible choices of icons, there are four different themes and “singleObject” which there only one kind of icon.
- In registration, user can choose any of these themes and the data table will show the icons.
- User can choose among the icons appeared on the data table and place them to corresponding place on the input table.
- The data will be saved with user’s name as the actual graphical password.
- In login phase, user have to put the exact icons on the exact input table cell. System will determine whether user has been authenticated.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• To design a new and more secure graphical password system</td>
<td>• The proposed design, Passpoints is based on Blonder’s original idea.</td>
<td></td>
</tr>
<tr>
<td>• To compare the use of the graphical passwords system to alphanumeric passwords in a longitudinal study</td>
<td>• It will overcome the limitations of needing simple, artificial images, predefined regions and consequently many clicks in a password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scheme:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Allows any images to be used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does not need artificial predefined click regions with well-marked boundaries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To login, user has to click close to the chosen click points, within some tolerance distance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• the advantage of the scheme is the password space is larger than alphanumeric scheme.</td>
<td></td>
</tr>
</tbody>
</table>