**Graphical Authentication for Secure Social Networks**

Contents

[1 Project Description 3](#_Toc355811871)

[2 Problem Statement 3](#_Toc355811872)

[3 Related Work 4](#_Toc355811873)

[3.1 Recall-based systems 4](#_Toc355811874)

[3.2 Cued-Recall-based Systems 4](#_Toc355811875)

[3.3 Recognition-based systems 5](#_Toc355811876)

[4 Procedures and Methods 5](#_Toc355811877)

[4.1 Implementation 5](#_Toc355811878)

[4.1.1 Recall-Based Systems 5](#_Toc355811879)

[4.1.2 Cued-Recall Systems 6](#_Toc355811880)

[4.1.3 Recognition-Based System 6](#_Toc355811881)

[4.2 Testing 6](#_Toc355811882)

[4.2.1 Lab Session 7](#_Toc355811883)

[4.2.2 Field Session 7](#_Toc355811884)

[4.3 Ethical, Professional and Legal Issues 7](#_Toc355811885)

[5 Anticipated Outcomes 8](#_Toc355811886)

[5.1 System 8](#_Toc355811887)

[5.2 Expected Impact 8](#_Toc355811888)

[5.3 Key Success Factors 8](#_Toc355811889)

[6 Project Plan 8](#_Toc355811890)

[6.1 Risks 8](#_Toc355811891)

[6.2 Timeline 9](#_Toc355811892)

[6.3 Resources Required 9](#_Toc355811893)

[6.4 Milestones 10](#_Toc355811894)

[6.5 Deliverables 10](#_Toc355811895)

[7 Work Allocation 11](#_Toc355811896)

[8 Appendix 12](#_Toc355811897)

[9 References 13](#_Toc355811898)

# Project Description

Graphical password schemes have been proposed as an alternative to text-based password authentication. The goal of this project is two-tiered: First we will be implementing three graphical password schemes based on the principles of recall, recognition, and cued-recall. Second, these schemes will be compared to each other and to text-based password schemes to evaluate usability in terms of password initialization, login and password recovery; and robustness to guessing and capture attacks. All testing and implementation will be done on a prototype social networking platform ([http://h](http://hackmi2)[ackmi2](http://www.google.com/url?q=http%3A%2F%2Fhackmi2&sa=D&sntz=1&usg=AFQjCNGmNZxcRZCN6FUy3LG7qeO8d59xqQ)).

# Problem Statement

Text-based password schemes are ubiquitous due to ease of use, inexpensive implementation, and user familiarity. However, they have the security and usability drawback of being typically difficult to remember, and they suffer from predictability if user-choice is allowed. This is because users tend to select weak passwords [1].

Graphical passwords have been proposed on the premise that humans are better at retaining visual information. However, it is a relatively young area of research and the studies conducted have several limitations. First, there is a lack of comparison between the different types of graphical password schemes; and similarly, there have only been a limited number of studies comparing graphical and text-based schemes. Secondly, there have been few studies conducted in the environment of use which is necessary to enable realistic evaluations of the use of graphical passwords [3]. Lastly, none of the existing studies have been conducted in the context of social networks. This is important because performance constraints and goals differ depending on the intended environment of use [1]. For example, in lower risk domains, like social networking it would be acceptable to have lower security schemes that provide high usability. While in a high risk domain like a banking scenario, it would be acceptable for the system to be less usable but providing high level security.

Our focus will be on evaluating these authentication methods for secure social networks, with all testing and comparisons done in this context.

Under this subheading we will be looking at the following questions:

1. **Which category of graphical password schemes is best suited for social networks: schemes based on recall, recognition or cued-recall?**
2. **Are graphical password schemes a viable alternative to text-based schemes as a means of providing authentication for secure social networks?**

# Related Work

Graphical passwords have been gaining in popularity as alternatives to text-based passwords. As a result there are a number of studies that have been conducted on their implementation. In this project we will be implementing three of the most widely researched graphical password schemes.

## Recall-based systems

Graphical password schemes based on recall require users to reproduce something that was created earlier during registration. DAS [4] was the first such system proposed. The authentication process consists of an N x N grid on which the user draws their password using a stylus or a mouse. Dunphy and Yan [2] considered DAS to be a system worthy of extensive study for a couple of reasons. First, DAS has a theoretical password space which is larger than that of text passwords. Second, it is not restricted to user authentication but can be used for key generation as well.

Various studies have been conducted on this system; however, to date DAS has only been tested through paper prototypes. As such, little can be said on its usability or practical security due to this lack of implementation and suitable user studies [1].

## Cued-Recall-based Systems

Cued-Recall based graphical password schemes are systems where the user is provided with a visual cue to aid them in remembering the password. The most extensively studied cued-recall based password scheme is PassPoints [1]. The user is required to select five points on the image to comprise their password. During authentication the user is required to re-enter these points. An important consideration in the implementation of PassPoints is the type of discretization that will be used [1]. This is important as it determines the range in which a click point would be acceptable for the password.

Several improvements to PassPoints have been proposed and implemented. One of these systems is Cued-Click Points [1]. This system makes use of different images for each of the five required click points. As a result the system is more robust than PassPoints.

## Recognition-based systems

Passfaces [1] is the recognition-based scheme most extensively studied. This is because the task of recognizing visual data is easier than recalling something from memory. In addition, human faces can be recognized more easily than other image types. However, the task of having to scan many images in order to identify a few pre-selected images takes time, thereby making the login process slower than that of text passwords.

Everitt et al. [3] conducted a study on multiple graphical passwords to examine the effects of frequency of access, and memory interference resulting from the use of multiple graphical passwords. The study used email-based prompts where users were required log on to four different accounts according to different schedules.

# Procedures and Methods

## Implementation

The HackMi2 social networking site was developed using Elgg, an open source social networking engine. It is a cross platform system written in PHP. Our implementation of the graphical password schemes will be conducted using Java. This is mainly because Elgg provides functionality to embed Java applets into its pages through the use of Plugins. This will enable the graphical password schemes to be used on HackMi2.

We will be implementing three graphical password schemes based on the principles of recall, recognition and cued-recall.

### Recall-Based Systems

The recall-based password scheme that will be implemented will be based on a proposed system called Draw-a-Secret (DAS) [4]. It consists of an N x N grid on which users draw their passwords. A drawing consists of a single or several pen strokes separated by “pen ups”. The system encodes the user-drawn password as a sequence of coordinates of the grid cells passed through in the drawing. This yields an encoded DAS password.

An important design feature will be determining how the implementation of DAS will enforce grid restrictions that aim to prevent illegal crossings made by tracing grid lines, or crossing through cell corners.

### Cued-Recall Systems

The cued-recall graphical password scheme that we will be implementing will be based on PassPoints. PassPoints is a graphical password system that uses pre-selected points on an image as the user password [5].

A key implementation feature will be determining the appropriate discretization algorithm to use [5]. The discretization algorithm will determine whether each selected point is within an acceptable range to the original click point [5]. This will have a direct impact on both the usability and the security of the password. The images that will be used for cued-recall based password scheme will be obtained from an open source database of images.

### Recognition-Based System

The recognition-based password scheme that we will implement will be based on the PassFaces password system [1]. PassFaces requires that the user selects a number of human portraits to make up their password. During authentication the user should select images from their password set in order to gain access to the system. A key implementation feature for this scheme will be ensuring for efficient managing of the image database. For example ensuring that only one image from the user’s pre-selected set appears in each round.

## Testing

We will conduct a four stage study to compare the four implementations of password schemes: a text-based password scheme and three graphical schemes based on recall, recognition, and cued-recall.

First, we will carry out a pre-study questionnaire to elicit the participants’ current strategies when using text passwords. For example we will be exploring issues such as how often the users forgot their passwords and whether they made use of coping strategies such as writing down the passwords in order to aid their memory. Second, a lab study to evaluate and compare robustness to guessing and capture attacks. Thirdly, a 4-week web-based study to evaluate and compare usability across the four implemented schemes. Lastly, a post-study questionnaire regarding the participants' experience and preferences. The questionnaire will examine how the users interacted and managed their graphical passwords.

### Lab Session

The lab session will be divided into two sections. The first section will involve assisting the participants with creating their graphical passwords and with the initial login to the system. This will allow us to measure metrics including time taken to create a new password and the memorability of the passwords after a short time. The second section of the lab session will involve testing the system for robustness against attacks. The following attacks will be tested on the system.

Guessing attacks

- Dictionary attacks

Capture attacks

- Shoulder surfing

- Social engineering

### Field Session

The online study will allow users to access and authenticate the social network under realistic settings. Email-based prompts will be sent to participants 3 times a week. This will allow us to evaluate the usability of the system and the memorability of the passwords by monitoring specific metrics including, how often a password was reset, the number of login attempts and the login time. This will require continued participation from the participants. To this end we will offer incentives to encourage high participation.

The four part study will span four weeks and will be tested on 30-40 participants, who will be randomly divided into four groups. Each group will then authenticate on a different authentication system.

## Ethical, Professional and Legal Issues

The second phase of this project will require participation from users in order to test the functioning of this system. As a result, ethical clearance will need to be obtained from the Ethics Committee. The users will also be requested to fill out a consent form before they take part in the study. The users will be provided with all the necessary information required to successfully participate in the study.

During this project we will adhere to any legal requirements pertaining to the implementation and the testing of the various graphical password schemes.

# Anticipated Outcomes

## System

We anticipate to have implemented three fully functional graphical password systems on the HackMi2 social networking site. These systems will be the recognition, recall and cued-recall based graphical password schemes. One of the key challenges we anticipate to face will be to replace the existing text-based login on HackMi2 with the new graphical password login system.

## Expected Impact

Depending on the results from our implementation and testing, this project has the potential to provide new knowledge on how to implement graphical passwords for social networking sites. Specifically it can aid in the choice of graphical password schemes used. This project will also enable us to determine if using graphical passwords is a viable alternative to text-based passwords.

## Key Success Factors

For this project we have two main factors that we will be observing in order to determine the success of the project. The first measure will be to have fully implemented and integrated the three graphical password schemes on HackMi2. The second measure will be to have conducted user testing that will enable us to compare the efficiency and suitability of graphical passwords to text-based passwords for social networking sites.

# Project Plan

## Risks

**Risk:** The social networking site is poorly documented.

**Impact:** High

**Likelihood:** High

**Mitigation:** Get familiar with the implementation of HackMi2. Also contacting the creators of the system and requesting documentation from them

**Risk:** Challenges in integrating the graphical password schemes with the HackMi2 site

**Impact:** High

**Likelihood:** Medium

**Mitigation:** Ensure that the implementation of HackMi2 is understood to allow for the creation of graphical password schemes that can merge with the system. Integrating the code in iterations will allow for early identification and resolving of any merging issues.

**Risk:** Loss of project data

**Impact:** High

**Likelihood:** Medium

**Mitigation:** Ensure that there are daily backups of each iteration stored both online and offline

**Risk:** Challenges in getting the required number of users for testing

**Impact:** High

**Likelihood:** Medium

**Mitigation:** Recruit potential users for the system early. Also, provide incentives to the users to encourage them to fully participate in the study.

**Risk:** One group member is forced to leave the project due to unforeseen circumstances

**Impact:** High

**Likelihood:** Low

**Mitigation:** Ensure that the project tasks are clearly separated into two distinct projects. This will enable each member to have an individual mini project

**Risk:** Implementation phase running over-time

**Impact:** High

**Likelihood:** Medium

**Mitigation:** Get familiar with the implementation of HackMi2. Also contacting the creators of the system and requesting documentation from them

## Timeline

The project timeline highlights our implementation plan and schedule for the project. The initial phase will be implementing the three graphical password schemes and integrating them onto the HackMi2 social networking site. The final stage will be comprised of user testing. Strict adherence to this plan will be essential to ensuring that the project is completed on time. The Gantt chart for the project can be found in the appendix section of this paper.

## Resources Required

* Hackmi2 source code and documentation
* Participants
* Money – to provide incentives for user testing
* Lab resources
* Hardware – computers
* Open source password image database

## Milestones

**Milestone Date**

Project Proposal 10 May

Project web presence 11 June

Background theory chapter 19 July

Design chapter 26 August

First Implementation Test+ Write-up 16 September

Final Prototype/Experiment/Performance Test + Write-up 25 September

Chapters on Implementation and Testing 30 September

Coding Complete 30 September

Outline of complete report 7 October

Final Complete Draft of Report 21 October

Project Report Final Hand in 28 October

Poster due 31 October

Web Page 4 November

Project Demonstrations 5 November

Reflection Paper 8 November

## Deliverables

* Project Proposal
* Project web presence
* Background theory chapter
* Design chapter
* Project Report Final Hand in
* Poster Due
* Web Page
* Reflection Paper

# Work Allocation

The project tasks have been split into two in order to allow each group member to have a mini-individual project. Each member will be responsible for implementing one graphical password scheme. The remaining graphical password scheme and the user testing phase will be conducted as a joint collaboration. For the text-based scheme, we will be using the existing implementation on HackMi2.

Lebogang Mametja - Recognition and Recall Implementation

Dorothy Mhlanga - Recognition and Cued-Recall Implementation

# Appendix



# References

[1] Biddle, R., Chiasson, S., and van Oorschot, P. C. 2012. Graphical Passwords: Learning from

the First Twelve Years. *ACM Computing Surveys* (CSUR), vol. 44, 4, Article 19 (August 2012),

41 pages

[2] Dunphy, P. and Yan, J. 2007. Do Background Images Improve “Draw a Secret” Graphical

Passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications*

*Security (CCS)*, ACM Press, New York, pp. 36-47

[3] Everitt, K., Bragin, T., Fogarty, J., and Kohno, T. 2009. A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press, New York, pp. 889-898

[4] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. 1999. The Design and Analysis

of Graphical Passwords. In *Proceedings of the 8th USENIX Security Symposium*, vol. 8, ACM

Press, New York, pp. 1-1

[5] Birget, J., Hong, D. and Memon, N., 2006. Graphical Passwords Based on Robust Discretization. *Information Forensics and Security, IEEE Transactions on,* vol. 1, 3, pp. 395-399.