Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience

C Singh[1], L Singh[2]

[1]Chandrashekar Singh
Chandrashekar1990@hotmail.com

[2]Lenandlar Singh
Lecturer, University of Guyana
lenandlar.singh@uog.edu.gy

ABSTRACT

Security has been an issue from the inception of computer systems and experts have related security issues with usability. Secured systems must be usable to maintain intended security. Password Authentication Systems have either been usable and not secure, or secure and not usable. Increasing either tends to complicate the other.

Text passwords are widely used but suffer from poor usability, reducing its security. Graphical Passwords, while usable, does not seem to have the security necessary to replace text passwords. Attempts using text or graphics only have mixed results. A combination password is proposed as a potential solution to the problem.

This paper explores combination as a means of solving this password problem. We implemented three password systems: Text only, Graphics only and a Combination of Text and Graphics. Remote evaluations were conducted with 105 computer science students. Results from our evaluations, though not conclusive, suggest promise for combination passwords.

Keywords: *security, usability, authentication.*

1: INTRODUCTION

1.1 Motivation

The internet has reshaped the way we conduct our daily activities and new tools and models of computing are exclusively based online. With this shift to online-based services and products, computers are fast becoming "thin clients" once again with "cloud computing" beginning to play an increasingly important method for conducting business and other operations online.
With these new developments, the emphasis on building very secure system is paramount since services are not on the client's computer, and the server would need to know who is requesting resources and if that entity / user is authorised to do so. The importance of security was recognised by ACM in their curriculum guideline where they suggested that all graduates should have some awareness of security, by writing safe and secure software. **[1]**

DOI : 10.5121/ijnsa.2011.3207

Though not often mentioned with security, usability is equally important and intimately related. A secured system, to maintain its intended security, must be usable since users normally explore the easiest methods to access a system.

In this thesis we investigate this relationship and further explore a model that is balanced and one where we propose an approach to improving usability and security simultaneously.

2: BACKGROUND

In this section we explore the relationship between usability and security, with respect to authentication. We review the various types of text and graphical authentication systems and provide an analysis of each system as it relates to usability and security.

2.1 The link between usability and security.

The relationship between usability and security in secured systems was first discussed as far back as 1975 when it was suggested that user interfaces be designed with the user in mind. [2]. It was claimed [3] that the industry has lost ground in building secure, but usable systems. The security requirements of computer systems have increased markedly and in trying to address these requirements, usability suffered. In addition, trying to explain security to users is a difficult task primarily because users are reluctant to learn more about security than they already know. Zurko [3] quoted users saying "Why doesn't security just work?"

System designers are perhaps at fault, as they often design a system so that the security decisions are left entirely up to the user. When security is breached, the user is normally blamed, while no blame is on the system design. Bruce Tognazzini, in his book, noted that a security breach is mostly the fault of the system rather than the user.

Chiasson[4] suggested that the easiest way to use a system is often the least secure way. To counter this she proposed using the concept of "safe-path-of-least-resistance" where the most secure path or way of using the system, is also the easiest path. This would, in theory, allow the user to use a system the way he is most comfortable and at the same time; the most secure way.

In the next section, we review and analyse the most commonly used authentication systems.

2.2 Text Only Authentication

Previous work in this area have identified that Alpha-Numeric passwords are widely used to authenticate users. A typical 8 character password created using the standard US keyboard would contain 95 ASCII symbols per character. This could theoretically create a password that has 95^8 possible values. However most people tend to create passwords that utilizes only a small fraction of this space. As a result many passwords are made from dictionary words, names of familiar places and people and familiar dates making it easier for an attacker to guess the password of a user. As of 2010, the largest English dictionary, Oxford English Dictionary contains about only 615, 000 entries (Oxford)[1] and with a bit of information about the user, the possible passwords would be less than 1,000,000.

There have been several proposed improvements to text passwords. Some of these have become usability guidelines, when developing online systems. Some of the more notable ones are:

[1] http://www.askoxford.com/oec/mainpage/oec02/?view=uk

- On-screen advice.
- Mnemonic Passwords. Example ("Georgetown is the garden city of the Caribbean" => "Gitgcotc"). [5].
- Character substitutions ("I love cats" => "I<3c@s"). Instead of using the phrase or word as it would appear in a dictionary, these passwords use symbols and alternative characters in their place. The problem, unique with this technique, is that there are several common substitutions, such as @ for a, that make it not as secure as it should be.
- Passphrases – using phrases instead of words for passwords.
- Persuasive Technology – a method of allowing users to create a secure and memorable password.

None of these studies have managed to really solve the problem. Most evaluations were inconclusive. It is widely accepted that users choose the minimum requirements they must make in order to use a system. Thus, even with these enhancements, text passwords remain insecure. Alternative approaches are proposed as described in the next section.

2.3 Graphics Only Authentication

Graphical password Systems have been touted as a possible alternative for traditional passwords. Several types of graphical password schemes have been proposed.

Blonder proposed what is usually referred to as the first graphical password scheme in 1996 [6]. It used pre-defined tap regions on one image to form a password. The user entered a password by clicking on these regions in a specific order. This scheme is vulnerable to shoulder surfing and suffers from having a pre-determined and very small password space. However, this scheme formed the basis for some of the best graphical password schemes designed thus.

Passfaces [9] was used to investigate how graphical passwords can be described and how someone can authenticate using the descriptions. They found that users were very likely to choose decoys instead of the original image when given a description of the original image, suggesting increased security.

An earlier study was done on the risks associated with different authentication schemes and their security with respect to shoulder surfing [10]. This study raised some important points; one of which is that complex text passwords were found to [be] just as vulnerable as the common graphical password schemes. One Reason for this was that users take longer to enter a complex password as well as the fact that users have to move their fingers further from the "home keys" making their keystrokes more visible.

Evidence also suggests that the user found it more difficult to remember multiple graphical passwords [7]. Although some studies have shown graphical passwords to be more user-friendly, their usability may in fact be closer to text passwords when looking at retention with multiple passwords.

Wiedenbeck et al [10] investigated the use of Passpoints to authenticate users. This system is similar to Blonder's scheme and requires the user to select a group of points, in any order, from an image. When logging in, five points must be selected in the order that they were entered. It is different from Blonder's scheme, in that the points, selected by the user can be from any part of the image, rather than being pre-defined click regions. Their results were mostly positive for Graphical Passwords, with good success rates and password entry times. They however

indicated that it was more difficult for persons to learn the graphical system, as well as remembering their passwords. In addition, they noted that some persons may have used the trajectory of their click points to help them remember their passwords. This may indicate a possible security problem, where attackers use this trajectory to guess a password. Participants were given a "show my password" button, which revealed their password. While this may have been helpful in a lab trial, this is not a practical feature in the real world and could have affected the usability results of this study. It is also important to note, that the worst performing 20% of participants in this test, did not use this feature very much.

Feedback from user evaluation on the above graphical authentication systems, has been inconclusive. While users found graphical passwords easier to remember, there are security concerns with shoulder surfing and the effective password space of these systems. There is also evidence of users trying to choose the least complex passwords that meets security requirements.

Further research was done on Passpoints by doing both a lab test and a field test [11]. A field test revealed some usability issues for the user. This was because the field study did not have any practice sessions and the user did not have any question and answer session with the researcher. As a result the success rates were below the lab tests, but for reasons suggested, the field tests had lower login time. The field tests also showed users entering into common patterns thus creating security risks. This is because an attacker may be able to guess a user's password by trying common patterns. They also investigated the usability and security of both Text passwords and Graphical passwords, however this was done to compare the two, not test them as a combination.

Cued Click Points (abbreviated CCP) was proposed as an improvement to Passpoints [12]. Being an improvement, it is similar to Passpoints with the major difference being that each point is selected on a different image. At both password creation and login, each point the user clicks opens a different image, while the number of clicks remain the same, at 5. This improves usability by providing a cue to the user if he/she is on the right path to login. It also improves security by having more than one image per password because the user only has to remember one point on each image. However this system suffered from the same hotspots and patterns seen in Passpoints. Hotspots are points or areas on an image, where persons are more likely to select as their click point.

To improve security, a further improvement on Cued Click Points was proposed, called Persuasive Cued Click Points [13]. This system maintains all the features found in CCP, with the improvements at the create login phase. Each of the 5 images is shown shaded, except for a small, randomly selected viewport. The user has to select his/her point on this image from that viewport. If the user is not satisfied with the viewport, a shuffle button is available that randomly positions the viewport on the image. Results from this research showed marked improvements in security by encouraging more random click points and discouraging the phenomenon of "Hotspots". However usability appeared so suffer, according to the author, in a statistically insignificant manner. This study is significant because it focussed on improving security and at the same time trying to maintain usability.

Most of the existing graphical password systems suffer from the risk of Shoulder surfing. Another major issue is that they try to replace text passwords completely which goes directly against a common usability guideline of consistency. The majority of computer users are already familiar with text passwords.

It was suggested that rather than replace text passwords, combining graphical password with text password might prove useful. Several security advantages of the combination over regular text passwords were given to support this idea [14]. These include better password strength (space), better protection from key logging attacks, protection from phishing and man in the middle attacks. This system, called TwoStep, consists of a regular text login followed by a graphical component. The graphical component consists of the user choosing one image from a grid of images. This is similar in concept to Passfaces, with the exception that any kind of images are used and the size of the grid can be changed by the system administrator at anytime. We believe that usability issues can arise if the grids are changed after the system is deployed, because it would remove the consistency that is needed to maintain good usability. Another usability issue could arise since the user might be faced with over two dozen images to select from and be overwhelmed.

However TwoStep was not evaluated, therefore we have no idea how this would perform. The concept appeals to us, because it seems to [theoretically] have a good combination of security and usability strengths. In addition it appears closer to that ideal security/usability ratio. It was also suggested that TwoStep's concept be evaluated, first in a lab, then a field evaluation. In this study, we explore this idea.

3: METHODOLOGY

3.1 Numeric Comparison

In order to compare existing authentication schemes and choose the most suitable system to represent each authentication scheme, we represent numeric values to each metric to develop a new method that could be used to evaluate password systems. This process was done fairly subjectively since there are no available quantification models or methods. An example of this is that password space is normally measured in a bit value and a numeric value can be assigned to this metric for a system using the password space measured in this bit value. However social engineering risk (described in the next section) are not as easily measured numerically because of the nature of this metric.

The metrics that were used to conduct this evaluation are divided into two categories, namely usability and security metrics.

3.1.1 Security Metrics

- Total Password Space – total number of possible values in a password system.
- Effective Space – subset of the total password space, which forms most passwords. Research into the security of password systems seeks to maximise this.
- Shoulder Surfing – The extent to which someone can look over the shoulder of a person entering his / her password and guess his / her password.
- Social Engineering – Practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection.
- Malware – Extent to which the password system resists malware attacks.

3.1.2 Usability Metrics

- Memorability – Extent to which a user can remember his / her password after a period of time. (Usually 1-4 weeks).

- Login time – Time taken to login using a particular authentication system. Shorter login times mean a higher score.
- Creation Time – Time taken to create a password using an authentication system. The lower the time taken, the higher the score in this metric.
- Login Success Rate – Percentage of users that are able to successfully login at least once after creating their passwords using a particular system. Memorability is different since it caters for successful login over an extended period.

Each metric is given a score out of ten, with ten being the highest possible score. Numeric values on this scale were chosen, since we believe it makes comparison of different authentication systems more practical. The numbers are assigned for metrics based on the evidence we found in the literature on each metric for a particular system [12] [13] [15] [16] [10] [17]. For example, a system where participants consistently remember their passwords would have a high score on the usability metric.

Table 1

Metrics	Password Systems								
	Arm Chair	Passfaces	DAS	PCCP	CCP	Passpoints	Blonder	Text Passwords	MAX
Security									
Password Space	5	4	7	10	10	7	2	10	10
Effective password space	3	2	3	8	5	4	1	3	10
Shoulder Surfing	9	1	3	2	1	1	1	8	10
Social Engineering	9	4	9	9	9	9	9	4	10
Malware	8	8	8	8	8	8	8	5	10
TOTAL	34	19	30	37	33	29	21	30	50
Usability									
Memorability	7	9		8	8	8	9	4	10
Login time		3		7	7	8		8	10
Creation time		2		6	7	5		8	10
Login Success Rate*		9		9	9	8		5	10
	8.75	28.75	0	37.5	38.75	36.25	11.25	31.25	40
Ratio	3.10857143	0.52869565	0	0.789	0.68	0.64	1.49333333	0.768	1

Table 2

Metrics	Password Systems								
	MAX	Text Passwords	Blonder	Passpoints	CCP	PCCP	DAS	Passfaces	Arm Chair
Security	**The maximum for each metric is 10**								
Password Space	10 points is for maximum protection against brute force attack.	Text Passwords have a maximum of 95 values for each character, giving a very large password space that would take years to crack using current technology.	Only predefined tab regions can be selected as passwords and these are very few / image.	This system contained enough clickable points to make the total password space similar	This system improved little over the passpoints system in this regard, because in essence, we're still looking at points on a rectangular grid	Same as CCP	Password space is big because of the amount of different shapes and drawings possible with this system.	Total password space is limited by the number of rounds a user has to choose an image. Typical 9x9 grid, with 5 rounds would only give 9^5	Total password space is limited by the number of images on each grid
Effective password space	This is the password space that results as a result of users typically forming patterns and using some combinations more often than others. 10 means that effective space is as large as the maximum.	However most users only select a small portion of this, the 26 English letters, numbers and more importantly dictionary words. (common combinations)	Even with such a small password space, based on results from improvements to this system and perceptions, users would have still have hotspots with this system.	Research has found hotspots on passwords created using this scheme	Hotspots were found in this scheme as well	This is where the major improvement over CPP happened, and is one of the more important security metrics.	Users tend to choose simple and symmetric patterns when creating passwords	Effective password space is even smaller, because users tend to choose faces of people within the same ethnic and cultural backgound	It was found that users may still find "hotspots" when creating passwords
Shoulder Surfing	A score of 10 here means that it is nearly impossible to crack a password using this scheme	It is difficult to really get someone's password by looking at them typing it. However seasoned shoulder surfers can effectively use this method.	It is almost guaranteen to get someone's password by watching them login.	While more difficult than blonder's scheme, it is still easy to guess someone's password by watching them login	The author made note that shoulder surfing isn't considered. However it is assumed that passwords can still be guessed	Login phase is almost the same as CCP, so risks remain, but the additional security measures at creation time may make for more resistance	Because of the simplicity of some of the drawings, they can be guessed by watching someone login.	Since each screen only has 9 faces it is quite easy to see when someone uses the mouse to login. This can be improved using keyboard password entry	This system was designed from the ground up to be resistant to shoulder surfing
Social Engineering	This is a measure of how resistant a scheme is against social engineering. 10 means there is no chance a password can be cracked by having information about the user	A significant number of sample text passwords have been words of things related to the user	It is highly unlikely that knowing information about a user would let an attacker guess their click regions	Same as Blonder	Same as Blonder	Same as Blonder	It is a bit likely that information about the user might aid an attacker into guessing the secret	Since users choose faces of people with similar and familiar phisical characteristics then social engineering is a major issue	We believe it is difficult to guess a password with this system and information about a user.
Malware	How resistant a system is to malware attacks	Keyloggers can be used to acquire user's text passwords.	Unless screen grabbers and mouse loggers are more readilbly available, this is a relatively low risk	Same as Blonder	Same as Blonder	Same as Blonder	Same as Blonder	Keyloggin possible when keyboard is used as input	Does not appear to be vulnerable to malware.
Usability									
Memorability	How easy it is for users to remember their passwords	It is easier to remember simple text passwords than some graphical passwords. Complex passwords (secure) are not very memorable however	The tap regions are not difficult to remember	Because humans remember images easily and the points are based on location on image, passwords are memorable	Same	Same		In user studies, only 1/2 of participants were, on average, able to remember their passwords.	Passwords from this scheme were quite memorable
Login time	Less time taken to login, means a higher score in this metric	Providing that users remember their passwords, login time for text passwords are very small	Not enough information	Typically, after users are familiar, login times are good	Same	Same		Based on the procedure described, participants may have taken a long time to login using this system	
Creation time	Less time taken to create a login means a higher score in this metric.	Simple text passwords take minimal time to create. Secure passwords however takes a much longer time	Not enough information	Users took a long time to create a password with this system	Users reported that differnent images allowed them to create password with more ease and in less time	Improvements allowed better effective password space, but creation time suffered		Based on the procedure described, participants may have taken a long time to create login using this system.	
Login Success Rate*	The percentage of users than can successfully login using a created login. Higher percentage means a better score in this metric.	There is evidence that many users have difficultties remembering their passwords, and this affects the score in this metric	Not enough information	Most users were able to successfully login using this system	Most users were able to successfully login using this system	Most users were able to successfully login using this system		Only 1/2 of participants were able to remember passwords using this system.	

Table 1 gives the numeric values that were assigned to each system for the individual metrics. Tables 2 give explanations for each corresponding numeric value in the first table. It should be noted that blank spaces in the first table indicates that enough information was not available on that system to give a numeric value for that metric.

3.2 Choice of Systems

We used the results of this comparison to select the system that best suites the three types of password we would be evaluating. The following systems were chosen:

- 3.2.1 Text Only Authentication – We decided to use the regular text password interface. The main reasons for choosing this system; (1) users are already familiar with it; (2) there does not appear to be a significant difference between the different parts of text passwords.

- 3.2.2 Graphics Only Authentication – We use Persuasive Cued Click Points. This is because, through our comparisons (see Table 3.1 above); we believe that Persuasive Cued Click Points is the best graphical password system developed so far.

- 3.3.3 Combination –We choose to use Cued Click Points. This is because cued click points offers reasonable security and high usability. Though we believe that PCCP is a better graphical password system, it is our opinion that the combination should have a system with better usability. We believe that when combined with text passwords, this may help to bridge the gap between security and usability.

3.3 Authentication Scenarios

While there is literature on authentication systems for different scenarios, we have not found any that describes authentication scenarios and which authentication mechanisms would be more suitable for any scenarios [18], [19]. We believe that this would help to guide our future research on the usability and security needs of various systems and the appropriate authentication requirements. We attempted to do this placing the scenarios into three categories. These categories are:

- High Security and Low Usability – Systems where security is paramount and usability is not a major concern.
- Equal Balance of Usability and Security –Authentication where usability and security are of equal importance.
- High Usability and Low Security – this is defined as scenarios where it is very important that the system be usable. Whereas security may be a concern of the scenario but not authentication by itself. An example of this is smartphones which need good usability these days (Iphone), but they are with the owner most of the time. This in fact increases security, since attackers would need physical access to the device.

After defining the authentication scenarios, we provided examples of systems that fall under the various categories. The systems were placed in categories based on usability and security scores received in comparison done in section 3.1. For example; Passfaces scored highly on usability, and not so high with security. As a result, it was placed in the HI-Usability, Low Security category.

The following table indicates authentication system and categories they fit into. Listed are examples of common scenarios for each category.

Table 3 - Security scenarios and Examples

	High Security	**Balanced**	**High Usability**
Security	*High*	*Medium*	*Low*
Usability	*Low*	*Medium*	*High*
Examples			
	Banking and Financial systems	Personal Email	Chat Rooms
	Business Email	Personal Computer	Online Gaming
	Enterprise Computer Systems		Mobile Devices
	Authentication Systems		
	Strong Text Password	Text Password	PassPoints, CCP, PCCP
	Combination	Combination	Passfaces (mobile devices)
		PCCP	

The following table explains why each scenario was placed in its respective category. In bold, it has the examples of scenarios where authentication is used. Below these scenarios, are texts explaining why each scenario was placed under that column.

Table 4

High Security	**Balanced**	**High Usability**
High	*Medium*	*Low*
Low	*Medium*	*High*
Banking and Financial Systems	**Personal Email**	**Chat Rooms**
These systems protect huge amounts of financial information and as a result need maximum security.	These Systems generally need a balance, because many online systems rely on email to restore their passwords, etc. In addition they are usually available for a big part of society who demands systems with high usability.	The trend seems to be that chat should be more user friendly. Common IM programs are constantly adding more features to make them more user friendly.
Business Email	**Personal Computer**	**Online Gaming**
Many business emails, in addition to the fact mention in personal email about other systems, also have confidential information.	The PC has many uses in the home, and as a result must have reasonable security. In addition, the pc usually needs to have good usability for people to want to use it over other means of doing things.	The focus here is on entertainment, so it must be highly usable.
Enterprise Computer Systems		**Mobile Devices**
These huge, expensive Systems are usually used to store and		As was suggested

process data for large organisations. In addition, recently the concept of "Cloud" computing makes these systems and their resources a service for many organisations. Security is paramount when dealing with data storage as a service.		earlier, mobile devices such as cell phones are almost always on the user, so there is less need for high security authentication.

The above exercises allowed us to identify the systems and scenarios more suitable for the category of authentication systems we were focusing on. We chose the balanced category. We wanted to advance, a method that appears to weigh equally in favour of improving security and usability simultaneously.

3.4 Proposed solution

We propose a combination of text and graphical passwords. We believe this would improve resistance to shoulder-surfing and at the same time provide some measure of consistency with the text component of the combination. At the same time, we believe the combination would preserve most of the enhanced usability found in graphical passwords.

3.5 Design of proposed system

3.5.1 Implementation Details

Three systems were implemented for our evaluation. Each system was implemented as PHP web applications together with AJAX technology. All text passwords were stored in plain text. Since we wanted to perform security analysis on the passwords and that would only be possible if the passwords are plain text. This evaluation focused solely on the authentication systems.

3.5.1.1 Text Only Authentication -

This utilised the built-in HTML form elements for text and password fields.

3.4.1.2 Graphics Only Authentication

The user is presented with a standard HTML form element to enter username. After entering a username, an option is presented to check if that username exists already in the system. If the username is successful, the user is presented with an image to select a click point from. This image is shaded, with a pseudo-randomly selected rectangular area un-shaded. The user must select his / her password from this un-shaded region. If the user is not happy with the given region, the user can click on a button "Shuffle" to pseudo-randomly select another part of the image. When logging in, the user enters his / her username and selects his / her click points in the same order as entered when creating password. If the user makes a mistake, he / she is shown a different image from the one shown when creating his / her password. This system follows, as closely as possible, the PCCP system introduced by [13].

3.5.1.3 Combination of Graphical and Text Authentication

The text part of the combination is the same as a regular text password. After entering the text password, the user is required to click on a button "Text Login". On clicking this button, the username and password is validated using ajax technology and the user is asked to enter his / her graphical component of the combination. To enter the graphical component, the user clicks a point on a series of 5 images. At login, the user enters his / her password and then selects the

points of the images again. As in the Graphics Only password, a wrong point results in a pseudo-random image being displayed. The graphical part of the combination follows, as closely as possible, CCP system as introduced by Chiasson et al. [12]

3.5.1.3 Data collection module

A special module was built into the application to allow the researcher to collect results. This module records, the time a task was started (creating or login using a password) and the time the task was completed. It also calculated success rates for the various systems.

3.6 Image Choice

The images utilised were initially a collection of wallpapers. However it was then changed to loony toons. This change was a result of the initial evaluation (described below) of the systems. The results of previous studies are conflicting as to if the images affected the usability and security of graphical password systems. [11], [10]. As a result, even though maps and images of constellations were also considered, they were not chosen. They were resized to 640 x 480 resolution.

3.7 Accuracy

Users are not expected to remember the exact pixel they clicked on when entering their graphical password as doing so would make the system almost impossible to use. Previous studies have employed a number of different algorithms for determining the accuracy of the image point; at login; the algorithm that the system uses to determine if an entered point is close enough to the actual point for it to be correct. Chiasson et al did a thorough review of the various methods in her thesis [4].

After reviewing these algorithms, we found that even in the best approach, there is still a chance of a wrong point being accepted by the system or a correct point being rejected by the system. Since we were more interested in testing our concept, we decided to store click points in plain text. At login stage, each point entered by the user would be compared with the corresponding point in the database. The length of the line formed by the two points should not exceed 10 pixels. Thus the users were expected to re-enter their click points within a radius of 20 pixels. This value was chosen after the initial testing, described in section 4.2, was conducted; we found that this value was a good compromise between the system being too secure (smaller radius) and too usable/insecure (larger radius).

3.8 System Features

The main system implementation components are:

- Image loader – Preloads the images for better overall user experience
- Ajax Frontend – Handles all the client side JavaScript for Ajax. This module is also responsible for collection of values for some of the metrics. Like start time, which is used to measure login and password creation time.
- Validation – This module handles the client side validation. This helps to reduce the network load, which would already be high with graphical password and the graphical part of the combination password.

- Statistics Module – This module handles the processing of the raw metrics that are in the database (start and end time) and producing meaning full metric values (time in seconds).
- Feedback Handler – This module processes user feedback.
- Ajax Backend - processes all the service Ajax. This module also updates database with metrics sent by the Ajax frontend.

4: EVALUATIONS

4.1 Focus Group Discussion

As part of our pre-evaluation, we held a focus group discussion on authentication, with emphasis on participants' current behaviour with text passwords and their thoughts on graphical passwords. We believe that this discussion would facilitate a thorough discourse on the issues users currently face with existing authentication systems and to further gauge user's reaction to alternative means of authentication.

Two focus group discussions were conducted with second and third year computer science students from the University of Guyana. Students were invited to participate in the group discussions. A total of six persons participated in the first discussion and 4 participated in the second discussion.

4.1.1 Main Findings

We found that all of the problems discussed with text passwords were evident in the feedback given by participants on their experience with existing authentication systems. Participants expressed some concerns about the concept of graphical passwords. The main concerns include the risk of shoulder surfing, encryption of graphical password and entering passwords would be slow. On the other hand, most of the participants believe that graphical passwords would provide for a more secure user experience.

4.2 Initial testing

An initial testing phase was conducted after implementation was completed and before the actual evaluation. This was to identify implementation issues that may affect the performance (usability and security) of the authentication systems. Initial testing lasted for two weeks and involved reviews done by colleagues. Metrics collected in the initial evaluation were not included in the final results, because this evaluation focused more on testing the software implementation, rather than the concept.

The initial testing asked participants to create a login using each of the three implemented authentication schemes. Participants were then asked to login using each of the created logins. After attempting these two steps, participants were asked to give their feedback, as to how they felt while using the systems and what issues they may have had while using the website.

This initial evaluation revealed some performance issues relating to dialup network performance. It was found that users had to wait long periods for images to load while creating or entering their graphical passwords. We fixed this by preloading the images. This helped to significantly reduce the time needed to create a password using slower internet connections.

One of the most important finding from the initial evaluation is that images have a significant impact on how memorable graphical and combination passwords are. We found that landscapes and very graphical wallpaper type images may not be very suitable for this purpose. Participants complained of having too many objects on screen to select a password from. To fix this issue we looked at several alternatives; maps, constellations and loony toons. We consulted with existing work and found mixed results (some research say that images have a significant impact while others say that it may not have a big impact on usability and security performance of the graphical passwords). [11], [10].Thus we decided to go with, what we believe, would be the simplest type of images, loony toons. After making this change, it was found that participants were more likely to remember their passwords.

The initial testing also helped in setting the tolerance region. This region is the distance from the original point where the system would accept as being that point. Initially it was set at 5 pixels from the original point as suggested by Chiasson et al [4]. However many of the participants were unable to successfully login using this tolerance and they complained of clicking as close as possible to the original point and not having their click accepted as legitimate. In light of this, we decided to experiment with other tolerance lengths and found that the best results were gathered from a length of 10 pixels from the original point.

4.3 Design of Final Evaluation

Several methods of evaluation were considered, including lab and field evaluation, as suggested by van Oorschot [14]. We considered the option of a remote evaluation. Remote evaluation involves an online implementation and the use of the system.

The main reason for this is because of the unavailability of participants to conduct a laboratory study.

Each of the participants was requested to create a login using one of the three systems. They would then login using the created login. Whether or not the participant was successful in logging in, he / she was requested to fill a feedback form.

We choose computer science students for this evaluation because participants from the focus group discussions were faced with the same issues with current authentication schemes. Emails were sent to the generated list of second and third year computer science students requesting participation in the evaluation.

5: RESULTS

5.1 Participants

A total of 102 unique students responded to the request for participation and were placed in 3 groups. The table lists how many tried each individual system.

Table 5

Authentication System	**Number**
Graphical Only Authentication	35
Text Only Authentication	58
Combination Authentication	35

5.2 Results

The following graph shows the percentage of users who successfully created a password using each system. The table below graph presents information this numerically.

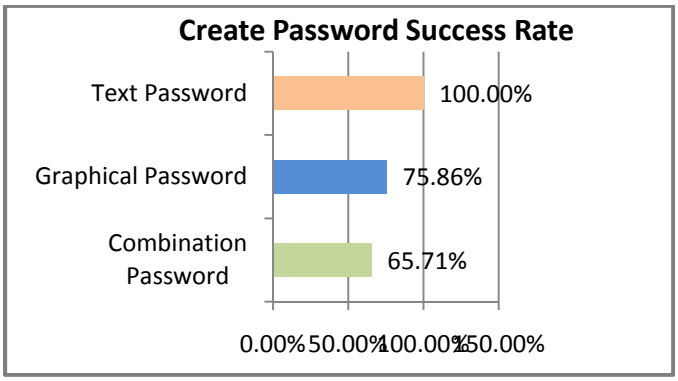

Figure 5.1 – Create Graphical Password Success Rate

System	Total	Successful
Graphical Password	58	44
Text Password	36	36
Combination Password	36	24

The following graph shows the average time participants took to create a password for each system.

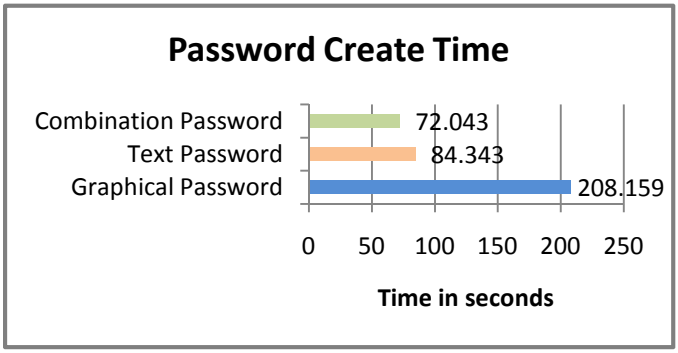

Figure 5.1 – Password Create Time

The graph below shows the percentage of users who successfully logged in using each system. The table below shows this information numerically.

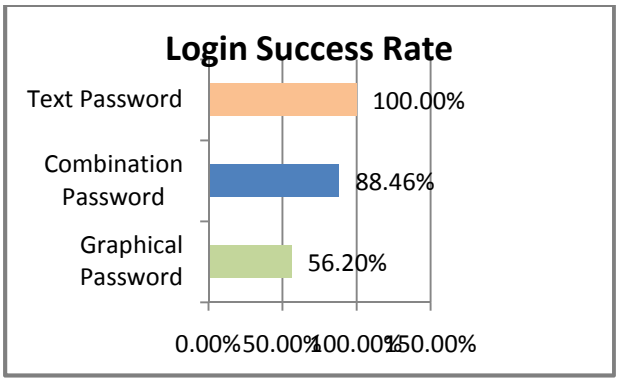

Figure 5.2 – Login Success Rate

System	Total	Successful
Graphical Password	122	69
Text Password	36	36
Combination Password	27	23

The graph below shows the relative complexity between text passwords and the text component of the combination password. It is a measure of how complex the passwords are. Higher score means that the password contains more different types of characters (letters, numbers, symbols, etc) and combination of these characters.

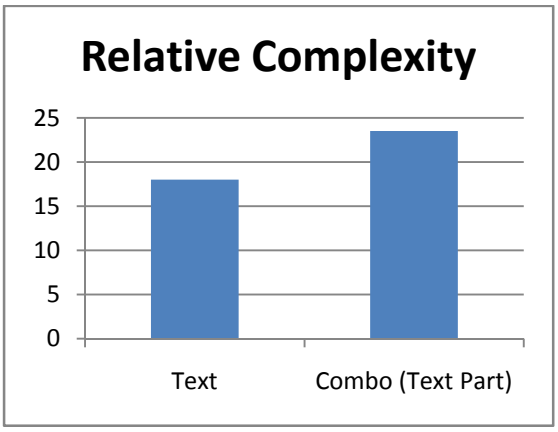

Figure 5.2 – Relative Complexity (Text vs. Combination Password (Text Component))

The following scatter plots shows on the horizontal axis, a scale of 640, representing the width of the images used in the graphical passwords. The vertical axis has a scale of 480 and represents the height of the images used in pixels. The dots on the graph are actual points which users selected as part of their passwords. Note that this is for all images and all users.

Scatter Plot

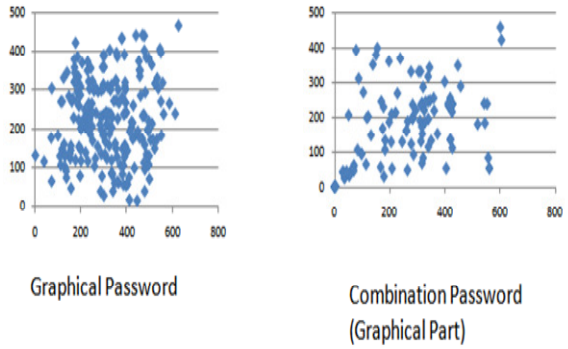

Figure 5.3 – (Graphical Password and Combination Password (Graphical Part))

6: ANALYSIS AND DISCUSSION

Password creation success rate measures the percentage of users that are able to successfully create a login. Our evaluation found that all users were able to create a text password while only 23 out of 35 managed to create a combination password (65.71%). Graphical password was second with 43 participants out of 58 creating a password. We assume that the 100% success in text passwords can be attributed to the fact that all of our participants had email addresses and as a result would have been exposed to text passwords before. We also believe that it maybe be possible that the additional steps involved may have contributed to the combination having less users being able to create a password. Our evaluation did not cover an extended period and this corroborates with earlier findings, [10] [4], that users make more mistakes in the earlier sessions, when using graphical passwords.

Password create time measures the time taken to create a password using an authentication system. We found that the combination and text passwords had much shorter create time than graphical password. We believe that this may be because of the shuffling that maybe involved with creating a password using PCCP. In comparison, Wiedenbeck et al, [10] found that users took longer to create and enter graphical passwords compared to text passwords. It is possible that the combination password had more advanced users. The fact that the users who tried the combination took the least time to create a login further emphasises this possibility.

Login success rate is a percentage of the number of successful login attempts. It is not clear why graphical passwords performed so poorly compared to the other systems in this test. One thought is that PCCP, when creating password, has the image shaded, with the user selecting their click point from the un-shaded region. Our theory is that some users might have used that box as a guide to select his / her click point. On the other hand the difference between combination password and text password appears significant.

The password complexity shows that the average combination password had a more complex text component, compared to text passwords. As mentioned before, it is possible that more advanced users may have attempted the combination password and thus the higher score. The above results show that, although there might some promise in the graphical and combination password, text passwords might just be the best authentication scheme. This is because it performs well in the usability tests conducted and its security appears promising.

The scatter plots show the distribution of click points. If points are more scattered and less grouped, it is a reasonable indicator that this system generated more random click points and is thus perhaps more secure. As is shown, the graphical password plot appears to have more grouped and less scattered click points as compared with the graphical part of the combination password. This seems contrary to what was found in previous studies comparing CCP and PCCP, where PCCP was shown to generate more random click points. [4] It should, however, be noted that the graphical password had 58 users compared to 36 for the combination password and this may have skewed the results.

Comparison between the combination and the other two password systems seems to suggest that except for create success rate, the combination does not appear to hinder usability. With regards to security, it seems likely that the combination may have improved security to some extent. This comparison is encouraging for our proposed system.

9: CONCLUSION

In this paper we present a comparison of text and graphical passwords, with their strengths and weaknesses as it relates to security and usability. We investigated the link between usability and security. We proposed a combination of text and graphical passwords as a possible solution to the password problem. This system maintains some aspects of existing authentications systems and should improve on security and usability. Finally we implemented and evaluated three types of authentication systems; Text, Graphical and A Combination of Text and Graphical Password. We found that text performed best authentication systems. It had the highest success rates, and good password entry times. The graphical password system, overall, had average results in all of the tests except login success rate. The combination password showed promise in most tests but had poor create success rate. However, our findings are preliminary and inconclusive. More user evaluations need to be conducted.

REFERENCES

Bibliography

1. *Computer Science: Curriculum 2008.* **Taskforce, CS2008 Review.** 2008.

2. *The Protection of Information in Computer Systems.* **Saltzer, Jerome H. and Schroeder, Michael D.** 1975.

3. **Zurko, Mary Ellen.** *User-Centered Security: Stepping Up to the Grand Challenge.* 1999.

4. *Usable Authentication and Click Based Graphical Passwords.* **Chiasson, Sonia, Biddle, Robert and van Oorschot, Paul.** 2008.

5. *Human Selection of Mnemonic Phrase-based Passwords.* **Kuo, Cynthia, Romanosky, Sasha and Cranor, Lorrie F.** 2006.

6. **Blonder, G.** *Graphical Passwords. United States Patent 5559961* 1996.

7. *A Comprehensive study of Frequency, Interference and training of multiple graphical passwords.* **Everitt, katerine M., et al.** 2009.

8. **Hinds, Chery and Ekwueme, Chinedu.** *Increasing Security and Usability of Computer Systems with graphical Passwords.* 2007.

9. *Securing Passfaces for Description.* **Dunphy, Paul, Nicholson and Olivier.** 2008.

10. *PassPoints: Design and longitudinal evaluation of a Graphical Password System.* **Wiedenbeck, Jean-Camille Birget, Alex Brodskiy.** 2005, Symposium On Usable Privacy and Security.

11. **Chiasson, Sonia, Biddle, Robert and van Oorschot, P. C.** *A Second Look at the Usability of Click Based Graphical Passwords.* PittsBurgh : s.n., 2007.

12. *Graphical Password Authentication Using Cued Click Points.* **Chiasson, Sonia, Oorschot and Biddle.** 2007.

13. *Influencing Users Towards Better Passwords: Persuasive Cued Click-Points.* **Chiasson, Sonia, et al.** 2008.

14. *TwoStep: An Authentication Method Combining Text and Graphical Passwords.* **van Oorschot, P. C. and Wan, Tao.** 2009.

15. **Cynthia Kuo, Sasha Romanosky, Lorrie Faith Cranor.** *Human Selection of Mnemonic Phrase-based Passwords .*

16. *Securing Passfaces for Description.* **Dunphy, James Nicholson, Patrick Olivier.** 2008, Symposium on Usable Privacy and Security.

17. *Armchair Authentication.* **Renaud, Karen and Maguire, Joseph.** s.l. : HCI 2009, 2009.

18. *Use Your Illusion: Secure Authentication Usable Anywhere.* **Hayashi, Eiji, et al.** 2008.

19. *A Privacy-Respectful Input Method for Public Terminals.* **De Luca, Alexander and Frauendienst, Bernhard.** Lund, Sweden : s.n., 2008. NordiCHI.

20. *Modeling user choice in the Passpoints graphical password scheme.* **Emir A, Dirik, Nasir Memon, Jean-Camille Birget.** 2007.

21. *Oxford.* [Online] [Cited: 28 February 2010.] http://www.askoxford.com/oec/mainpage/oec02/?view=uk.

22. **Persaud, Amarnauth and Singh, Lenandlar.** *Multimedia Focus Groups.*