12-4-2007

An investigation into the usability of graphical authentication using AuthentiGraph

Paul Minne
Deakin University

Jason Wells
Deakin University

Damien Hutchinson
Deakin University

Justin Pierce
Deakin University

DOI: 10.4225/75/57b54dd9b875f
5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

An investigation into the usability of graphical authentication using AuthentiGraph

Paul Minne[1]
Jason Wells[2]
Damien Hutchinson[3]
Justin Pierce[4]

School of Information Systems[1 4], School of Engineering and Information Technology[2 3]
Deakin University
Victoria, Australia
Email: wells@deakin.edu.au

Abstract

There is increasing coverage in the literature relating to the different facets surrounding the security service of authentication, but there is a need for further research into the usability of graphical authentication. Specifically, the usability and viability of graphical authentication techniques for providing increased security needs to be further explored. There is a significant amount of evidence relating to traditional authentication techniques which highlight the fact that as technological advances grip modern societies, the requirement for more advanced authentication and security approaches increases. The exponential growth in the number of people using the Internet carries with it the high potential for increased security threats, suggesting that there are needs for further techniques to increase security in online environments. This paper presents the findings of how various interface design approaches affect the usability of a previously developed alternative graphical authentication technique called AuthentiGraph. The security design provided by Authentigraph has been established and justified in previous research by the authors. The primary focus of this paper is the usability of this technique. Using an experimental laboratory based approach, combined with an online survey, 20 university students evaluated a combination of five varying graphical interfaces in three different screen sizes. The outcome provides the interface design criteria best suited for the implementation and use of the AuthentiGraph technique.

Keywords

Authentication, Graphical Authentication, IT Security, User Interface Design, Human Computer Interaction

INTRODUCTION

Authentication has been highlighted in the literature to be important to a wide spreading spectrum of industries, with organisations relying heavily on authentication to protect quality of data, business operations and lower the risk of organisational embarrassment, along with reducing the financial burden associated with successful attacks on organisations. Traditional techniques have sufficiently counteracted such attacks, however as Pierce et al. (2004a) state, businesses are more reliant on IT infrastructures resulting in a greater number of highly complex attacks of crippling nature. The growing concern toward authentication is highlighted by Pierce et al. (2004a): security authentication, authorisation and administration is the largest and fastest growing segment of Internet security software ... with revenues expected to increase to a 2000 to 2005 compound annual growth rate (CAGR) of 28 per cent to more than [US] $9.5 billion. Together with the increasing use of the Internet by businesses and consumers for performing online services including monetary transactions, the requirement for more effective authentication techniques to protect customers' credentials remains an issue of paramount importance.

Authentication has been defined in various ways (Sandhu and Samarati 1996, p. 241, Kambil and van Heck 1998, p. 5, Renaud and Smith 2001, Basu and Muylle 2003) converging on a means to verify the identity of a person or a process. This paper defines authentication as the process of determining whether 'someone' i.e. a person or 'something' i.e. an object such as a piece of hardware or software is who they claim to be, and establishing the identity of one party to another. Authentication has traditionally been centred on what you know, a concept typically linked to Personal Identification Numbers (PINs) and passwords. Pierce et al. (2004b) suggest the 'fallibility of passwords and PINs is exemplified in several well-known shortcomings implicit in their use'. Shortcomings which include the difficulty users experience in remembering strong passwords, the susceptibility to a broad range of electronic attacks, combined with the tendency of users to share passwords.

As a consequence of the relative insecurity of passwords and PINs, differing authentication techniques have been used including token based, the notion of what you have, along with biometric authentication, the notion of what you are. Both these approaches suffer from vulnerabilities and shortcomings, including the significant investment in extra hardware required to interface with the users, along with privacy and impersonation issues and the susceptibility to attack (Jain et al. 2000, Pierce et al. 2004a). This exposes individuals and organisations to potential security threats, and does not remedy the main cause of authentication and password insecurity. There is a void left between the traditional authentication information security authors Warren and Hutchinson (2003) suggest needs to be filled.

This paper evaluates the usability of Authentigraph, a low cost graphical authentication application designed to provide improved authentication security. Experiments examine and evaluate various screen design layouts to provide guidelines to improve the techniques usability, acceptance and accuracy.

The application area selected is authentication in online environments because of the exponential growth of the internet and the trend towards the adoption of online services such as Internet banking. This growth is highlighted in a media release by the Market Intelligence Strategy Centre (2004) stating that in the last quarter of 2004 a seven per cent increase in transaction activity to 151 million transactions was recorded among Australia's leading internet bankers. It is anticipated that AuthentiGraph may be applicable to other areas such as the usability in ATMs or PDAs.Heading – very minor

TRADITIONAL AUTHENTICATION TECHNIQUES

Renaud and Smith (2001) state that authentication usually happens by a specified user having a user-ID, along with some secret or unique authentication data known or belonging only to the user and the system. This secret authentication is centred primarily on three varying techniques including:

- 'What you know' or knowledge-based systems: a concept which has traditionally been embodied in Personal Identification Numbers (PINs) and passwords.
- 'What you have' or token-based systems: a concept commonly related to smartcards.
- 'What you are' or systems based on biometrics: the notion related to biometric authentication.

These traditional authentication techniques have been used successfully in providing a secure means to keep personal, organisational, national and global information secure. However, as our information rich society becomes heavily reliant on greater measures of security to protect critical information and data, drawbacks of each of the traditional techniques have become clearly evident and have been exposed, placing many individuals and organisations in great fear for the integrity and security of their present and future information systems.

Many authors in the area of authentication, including Pierce et al. (2004a), Furnell et al. (2004), Dhamija (2000), Thorpe and Van Oorschot (2004), Thorpe and Nali (2004), Perrig and Song (1999) and Birget et al. (2003) have suggested that all of the traditional authentication techniques do not remedy the main cause of authentication and password insecurity, which is the human limitation of memory for secure passwords. This leads to considering an alternative method for authentication, graphical authentication.Heading – very minor

GRAPHICAL AUTHENTICATION

Many forms of graphical authentication have been proposed, based on psychological studies showing that humans can remember pictorial representations more readily than textual or verbal representations. These include Déjà vu (Dhamija & Perrig, 2000), PassImages (Furnell and Zekri, 2005), Graphical Passwords (Blonder, 1996), Robust Discretisation (Birget et al., 2003), Draw-A-Secret (DAS) (Jermyn et al., 1999), Passdoodles (Varenhorst, 2004) and Inkblot Authentication (Stubblefield and Simon, 2004). These techniques have the potential to fill the gaps left between traditional authentication techniques, including trade-offs between security levels, expense and error tolerance. The graphical authentication techniques incorporate countermeasures for a large array of attacks including brute force attack, educated guess, and intersection attacks which have been plaguing knowledge-based and token-based authentication.

Graphical authentication authors have also stated that the developed techniques display extremely low authentication failure rates, suggesting that by using the graphical images and pictures to make up passwords, recall is aided compared to remembering strong textual passwords (Dhamija and Perrig 2000). Jermyn et al. (1999) suggest that intrinsically the graphical authentication techniques deal with the heightened vulnerabilities introduced to most systems, resulting directly from bad end user behaviour, where users often write down, or share passwords. The graphical authentication techniques make it exceedingly hard for this end user behaviour to occur.

Although there are many advantages associated with each of the graphical authentication techniques, conversely there are a number of disadvantages. Primarily the developed techniques are not suitable for the visually impaired and are limited in there potential application areas. Graphical input devices are often required during the authentication process essentially limiting the application areas to web authentication, Personal Digital Assistants (PDAs), customer authentication at Automatic Teller Machines (ATMs) or devices which include touch screens. The AuthentiGraph technique has been proposed as one alternative to overcome these limitations.

Overview of AuthentiGraph

Traditional authentication systems require the user to enter a login and password via an interface using keystrokes. The authentication information generally consists of a login and a password that is text based and limited to the keystrokes in the ASCII table. This type of authentication system has a finite number of combinations and is generally constrained by the ability of the user to remember and identify the keystrokes.

The complexity of the information collected using these traditional authentication systems is limited and given the computing power that is currently available, are potentially crackable and therefore insecure. For example "it is desirable to have a larger variety of passwords chosen by users, as the known threat of a dictionary attack is more computationally expensive. A dictionary attack is a brute-force guessing attack where the guesses are drawn from a dictionary composed of "likely" passwords (roughly based on those users easily recall). Such dictionaries are normally ordered from most to least probable. If the probability distribution of the passwords is known to be non-uniform, the entropy of the password scheme is reduced" (Thorpe and Nali 2004).

New and more complex methods of authentication are required but many of the proposed solutions require additional hardware such as biometrics and smart card readers or require complex relationships to be setup with third party institutions to facilitate the authentication process e.g. providers of PKI. Although this technology provides more secure forms of authentication it requires infrastructure adjustments that are both complex and expensive. A simpler solution that improves the authentication security, takes advantage of the visual ability of humans, integrates into existing infrastructure and practices, and is inexpensive would be desirable.

AuthentiGraph is a middle-ground solution between text-based or knowledge-based (Dhamija and Perrig, 2000) and biometric authentication. AuthentiGraph was developed to provide a more secure authentication system that utilises existing authentication infrastructure and methods thereby ensuring it could be implemented without high costs and the need for additional infrastructure and expertise (Pierce et al. 2004b). AuthentiGraph uses a combination of bitmapped data, mouse points and keystrokes to display and collect the authentication information. It maintains the use of character strings as the basis for the authentication information but adjusts the way the user is presented with the authentication information and identifies it.

As shown in figure 1 users are presented with a dialog where all characters are randomly displayed based on a seed received from the server (Pierce et al. 2003). For the purpose of ensuring an increased level of security this seed is always different. This means the position of the characters displayed on the interface as presented to the user will be unique for each iteration of authentication. Each character is selected using the mouse. The co-ordinates of each character selected are recorded and subsequently returned to the server. The server maps the co-ordinates of each item selected, forms a password string and authenticates the information. Where a mouse cannot be used to select the characters, users can use the keyboard to type in their password. Each character is converted to a set of co-ordinates and authenticated on the server.

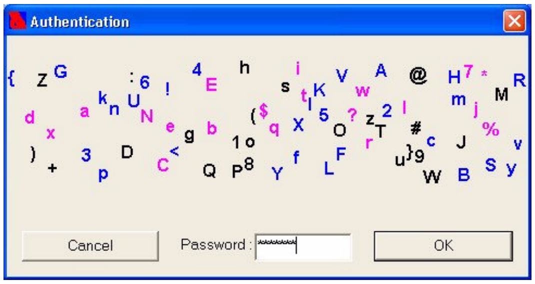


Figure 1. Character Bitmap Authentication Interface

The following highlights the advantages and disadvantages associated with the AuthentiGraph technique (Pierce et al. 2003).

- Advantages:
  - Decreased chance of hackers intercepting information;
  - Maintains look and feel currently used;
  - Validation by server is similar to formats currently used;
  - Reduced need for users to change passwords regularly, because authentication screen is randomly generated by a unique seed sent from the server;
  - Computers are not good at identifying characters within a bitmap.
- Disadvantages:
  - Identification of characters within a bitmap is more difficult than keyboard characters;
  - System not suitable for visually impaired users;
  - Susceptible to shoulder surfing and observation attacks.

According to Pierce et al. (2004b) graphical authentication has the potential to address the gap in traditional authentication approaches, by providing an alternative which takes advantage of the innate ability in humans to recognise visual information, integrates into existing infrastructure and practices eliminating the need to invest in expensive hardware and software to interface with the approach. This approach to authentication has the potential to eliminate the possibility of spyware and Trojans relaying password strings to remote servers, by removing the need for keyboards. ASCII codes are not used during the authentication process and therefore not transferred between client and server (Pierce et al., 2004b).

Initial experiments using the system identified several usability issues that resulted in a negative perception of the method. Users found it difficult to identify the characters. Some characters were difficult to distinguish (e.g. : i, l, 1). Despite the user understanding that the system would provide more security of their information, this resulted in errors, frustration and a perception the system was unusable. To overcome the usability issues, additional experiments were conducted to identify the best method to present and collect the character information. The outcome of these experiments is the focus of this paper.

RESEARCH METHODOLOGY

The laboratory based experiment approach was selected because of the requirement of determining the usability of the AuthentiGraph application.

The approach incorporated an experimental component, online survey component, and post task questionnaire component, which were completed by participants in three phases. The first phase involved setting up the application. The second phase involved the completion of the three experiments, along with the survey questions. The third phase involved the completion of the post task questionnaire.

Experiment Design

The intention of this experiment was to determine how various interface designs affect the usability of AuthentiGraph. A broader range of usability issues including memorability of passwords over time, time required to create and confirm passwords and other issues such as users requiring two or more Authentigraph passwords would form the scope for further inquiry.

Three experiments were developed which incorporated five varying graphical interfaces. Each of the three experiments consisted of five methods of displaying and identifying characters within an interface. For the purpose of measuring the usability of the various interface designs, the participants were required to select the characters which made up the search string, displayed in the header bar of each of the interfaces. For the experiment this string which represents the password to be entered is displayed on the actual interface, whereas in practice the string would be in the user's memory.

For each of the three experiments, a different search string is required to be selected. The difference between the three experiments is the size of the screen, where experiment one uses a quarter size screen, experiment two uses a half size screen, and experiment three uses a full size screen. The experiment screen sizes are depicted in figure 2.

The following sections present each of the five interface designs used within the AuthentiGraph application for this experiment. Each interface was designed to evaluate if any method would improve the users ability to identify and select the desired characters from within the interface and to reduce the potential for errors where characters are difficult to distinguish.

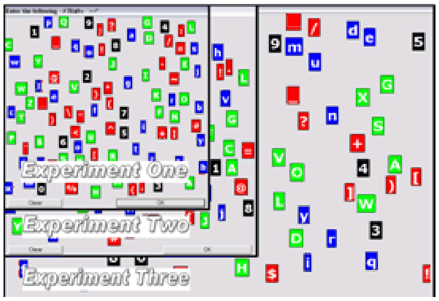


Figure 2 Experiment Screen Sizes

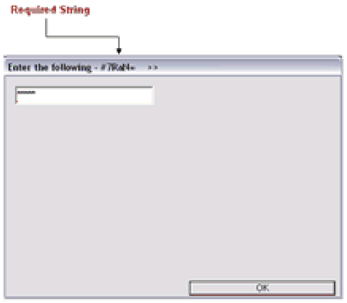


Figure 3 Interface One Design

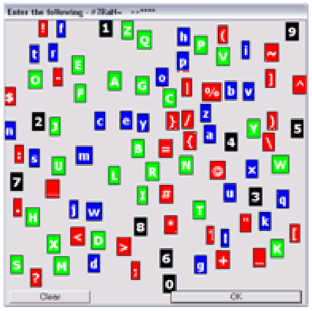


Figure 4 Interface Two Design

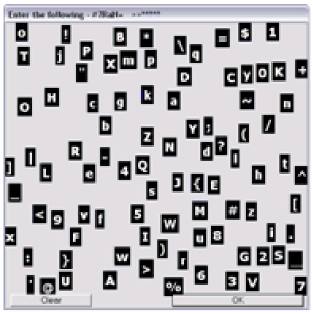


Figure 5 Interface Three Design

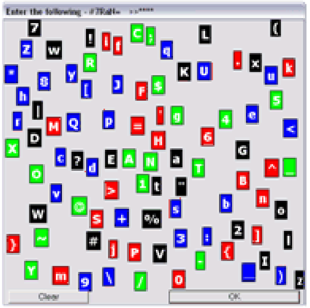


Figure 6 Interface Four Design

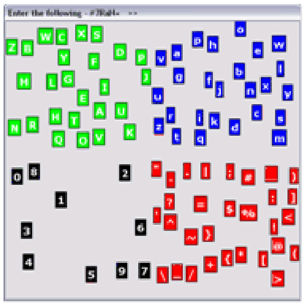


Figure 7 Interface Five Design

Interface One

The design of interface one as shown in figure 3 incorporates the use of a standard Microsoft Windows text box, which allows the participant to enter the required string using the keyboard. The required search string is presented in the header bar of the interface. This interface was selected primarily to compare task time latencies and task accuracy purposes between the keyboard and mouse method of entering data.

Interface Two

The design of interface two as shown in figure 4 incorporates the use of all uppercase, lowercase, numeric, and non alphanumeric characters displayed throughout the screen. Each character set is displayed in specific coloured square box allocated randomly when the interface is displayed. Each individual character is randomly positioned throughout the interface each time the application is run.

Interface Three

The design of interface three as shown in figure 5 displays each character in a black square box as opposed to a coloured square box as in interface 2. Each individual character is randomly positioned throughout the interface each time the application is run.

Interface Four

The design of interface four as shown in figure 6 displays each character within a randomly selected coloured box. Each individual character is randomly positioned throughout the interface each time the application is run.

Interface Five

The design of interface five as shown in figure 7 displays each character set within a specific region of the screen. Each of the character set is displayed within a coloured square box. Each time the application is run, each of the character types is assigned one of the four coloured boxes at random, along with each of the different character types being displayed entirely in one of the four regions of the screen. This layout is referred to as a grid display.

Performing the Experiment

All participants were required to select the characters with the mouse in the sequence indicated on the interface header bar. When the participant selects one of the required characters, an asterisk will appear in the header bar to confirm how many characters have been selected. Once the participant is satisfied all required characters have been selected, the ‘OK’ button can be selected to move to the next interface. During the character selection process the time taken to enter the required character string is recorded, along with the characters the participant has selected.

However if the participant believes an incorrect character is selected, or chooses to re-enter all the required characters, the 'clear' button can be selected. In the event of the 'clear' button being pressed, all the selected characters will be removed, and the timer will continue to count until the 'OK' button is pressed, indicating the required string has been selected.

The required character string is displayed in the header bar of the interface, and each time a character is selected an asterisk will appear. The completion time and characters selected are recorded whilst the participant is completing the task.

DATA CAPTURE, ANALYSIS AND DISCUSSION

Quantitative analysis was performed on all the data collected during this experiment involving the AuthentiGraph tasks, the survey and post task questionnaire. Statistical techniques were used to present the time latency and accuracy of data collected from the experiment and represented on a series of charts. These techniques included measuring the arithmetic mean, spread and shape of the data, the percentage pass rates for each of the experimental tasks, along with establishing the presence of any outliers. Frequency analysis was used to present the survey data, with response percentages displayed for each of the questions. In addition individual responses made by each participant, were included allowing any trends to be extracted and presented. Based on the sample size for the experiment being less than 30 participants, the statistical significance of the results cannot be proven.

This section reports the standard summary measures relating to the various data sets collected from participants involved in this experiment. Throughout this section, when referring to experiment one, it is referring the quarter screen size experiment; experiment two is referring to the half screen size experiment; and experiment three is referring to the full screen size experiment. In addition, task 1 through to task 5 represents interface 1 through to interface 5 respectively.

Participant Sample

Participant recruitment was achieved by utilising the students of an undergraduate Information Technology course unit called World Wide Web and Internet. The experiment was conducted during a scheduled tutorial in accordance with the guidelines of the Deakin University ethics committee. A summary of the participant sample follows:

- Total of 20 participants comprised of 4 females (20%) and 16 males (80%); 55% within the age group of 20 to 25 years with remaining 45% being less than 20 years of age;
- All 20 participants had previous experience using computers with 45 per cent of participants having between five and seven years experience;
- 25% were wearing glasses or contact lenses to complete the experiments;
- 5% of the sample population completed the experiment with some form of colour blindness;
- The first spoken language of all participants was English.

Experiment Tasks

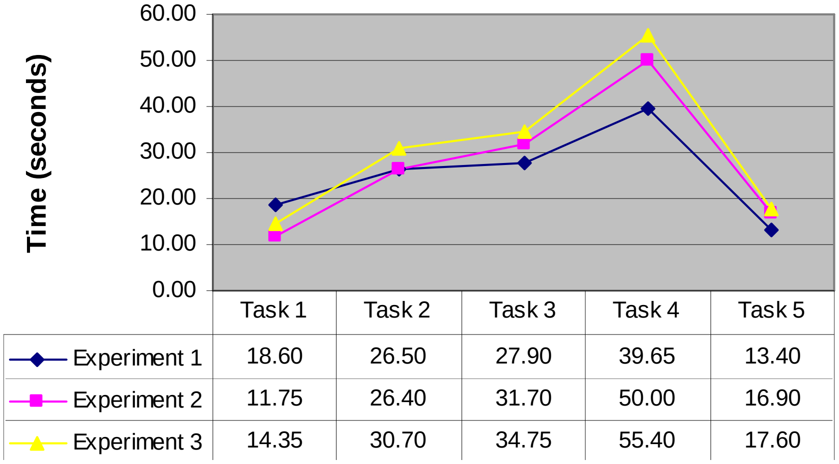
To measure the usability of the graphical authentication application, both time latencies and accuracy measurements were recorded for each of the participants whilst completing each of the experimental tasks. The accuracy, which compares the required search string for each of the experimental tasks to each of the participants input search strings were recorded as either pass or fail, along with determining the number of incorrect characters entered.

Time Latencies

Figure 8 displays a summary of task completion times together with combined experiment mean task completion times. Overall, when combining experiment one, experiment two, and experiment three mean completion times for each of the experimental tasks, it can be seen that task one was the fastest taking on average 14.90 seconds to complete. Task five was marginally slower with a mean task completion time of 15.97 seconds, followed by task two with a mean completion time of 27.87 seconds, then task three with mean completion time of 31.45 seconds. The slowest task completed by the participants was task four with a mean completion time of 48.35 seconds, which was 69 per cent slower than task one.

Experiment three produced the slowest mean completion times for each of the experimental tasks, apart from task one in experiment one which displayed a marginally slower completion time. This suggests that participants found it harder to locate the required characters when using a full size screen, compared to using a quarter size screen, and a half size screen.

Task four displayed higher mean task completion times than any other of the experimental tasks, which suggests that participants found it more difficult to locate characters when each character was randomly assigned a colour, along with being randomly positioned throughout the screen.



	Task 1	Task 2	Task 3	Task 4	Task 5
◆ Experiment 1	18.60	26.50	27.90	39.65	13.40
■ Experiment 2	11.75	26.40	31.70	50.00	16.90
▲ Experiment 3	14.35	30.70	34.75	55.40	17.60

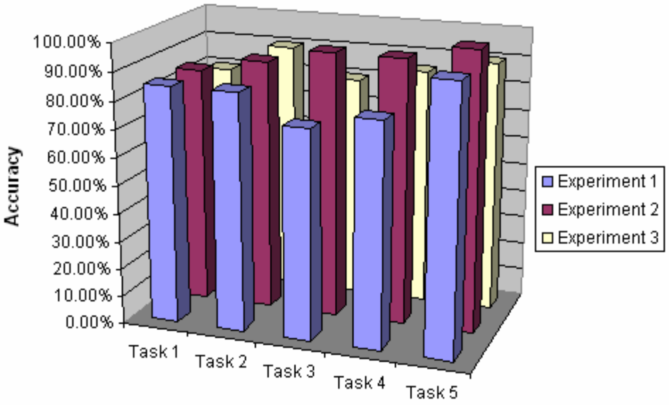
Combined Mean	14.90	27.87	31.45	48.35	15.97

Figure 8. Task completion time summary

Further, it can be seen that for task one, task two, task three, and task four where selecting characters from the screen was required, the mean task completion times increased for each experiment. This suggests the larger the screen size, the longer the participants took to find characters.

Task Interface Accuracy

Figure 9 shows that overall, when combining the task accuracies for experiment one, experiment two, and experiment three, task five had the highest pass rate with 95 percent, suggesting that the participants found it easier to accurately locate the required characters when colour coordinated in the grid arrangement.



Combined % Pass Rates	83	88	83	87	95

Figure 9: Relative frequency of task accuracy

Experiment Survey Response Analysis

Prior to and at the completion of the three experiments, 23 survey questions were asked relating to each of the interface designs. Table 1 provides a summary representing opinions relating to the usability of AuthentiGraph as experienced by the participants. The numbers in parenthesis represent the frequency of responses for that item.

Response	Question: How did you rate the ease of…	Easy	Difficult	Mean time (seconds)	Accuracy
Mouse Usage	*using the mouse to select characters?*	60% (12)		N/A	89% (easy)
			10% (2)		92% (difficult)
Character Locating	*locating characters on the screen?*	0	55% (11)	31.32	N/A
Colour Coordinated	*locating the characters when colour coordinated?*	75% (15)		29.42	87%
Non Colour Coordinated	*locating the characters when NOT colour coordinated?*	0	60% (12)	43.22	86%
Grid Arrangement	*locating the characters when colour coordinated in the grid arrangement?*	100% (20)		15.95	97%
Colour Differentiation	*Were the colours used in the experiment easy to differentiate?*	95% (19)	5% (1)	N/A	N/A
Experiment Usage	*Did you find it easier to locate the characters as you used the system more?*	75% (15) did find it easier to locate the characters as they used the system more, with the remaining 25% (5) participants stating that they did not.			
Security	*Would you use this graphical authentication technique if it proved to be secure?*	85% (17) stated they would use this graphical authentication application if it proved secure, with the remaining 15% (3) participants stating they would not.			
Character Differentiation	*Did you find any of the characters difficult to differentiate from other characters?*	80% (16) stated that they had no difficulty. Remaining participants had difficulty with uppercase or lowercase or alphanumeric or numeric characters.			
Interface 5 – Grid Layout					
Preferred Screen Layout	*Which of the screen layouts did you prefer?*	85% (17)	N/A	15.97	95%
Perceived Task Time	*Which of the screen layouts did you feel you entered the required string in the fastest time?*	90% (18)	N/A	N/A	100% in naming correct interface
Screen Size		Quarter	Half	Full	Errors
Preferred Screen Size	*Which of the screen sizes did you find easier to use?*	20% (4)			16%
			50% (10)		7%
				30% (6)	15%

Table 1. Summary of survey responses

The major trends and themes that have appeared from the responses made by participants to the survey questions include:

- The screen layout which the majority of participants preferred was interface 5 where the characters were colour coordinated and displayed in a grid layout according to their character type.
- The least preferred screen layouts were interface 4 where the characters were randomly displayed throughout the screen and randomly assigned a colour, along with being assigned black and white in interface 3.

- Most of the participants found it easier to locate the characters when they were displayed in the grid layout and colour coordinated as in interface 5, along with finding it easier to locate the characters on screen when they used the system more.
- Most of the participants named the screen layout they perceived was their fastest, as the screen layout that was measured as their fastest.
- The majority of participants who stated they found some of the characters hard to differentiate from other characters, actually listed different character types to the ones they produced the most errors.
- Half of all sample participants named the half screen size as the one they felt was the easiest to use.

Post Task Questionnaire

The Post Task Questionnaire partially based on the NASA Task Load Index (US Department of Defence, 2003) was used to provide subjective workload assessments based on a weighted average of ratings on six subscales for each of the five experimental tasks. Participants rated themselves on a scale from 1 to 10, for each of the six subscales, following the completion of all experimental tasks.

The six subscales included Mental Demand, how much mental perceptual activity was required; Physical Demand, how much physical activity was required; Temporal Demand, how much time pressure did the participant feel due to the rate of pace at which the task occurred; Effort, how hard did the participant feel they had to work to accomplish their level of performance; Performance, how successful does the participant think they were in accomplishing the goals of the tasks; and Frustration, how insecure, discouraged, irritated, stressed and annoyed, versus secure, gratified, content, relaxed and complacent did the participant feel during the task?

Summary of Post Task Questionnaire Results

Based on the responses made by participants when completing the Post Task Questionnaire, figure 10 indicates that task one produced the lowest mean for all subclasses except for physical demand in task five. Task three was perceived to have the highest mental demand along with having equally the highest frustration levels shared with task four.

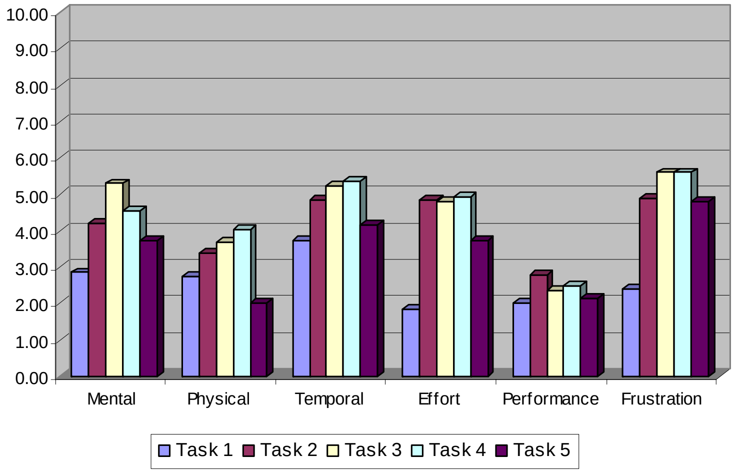


Figure 10: Mean values for all tasks

A clear trend highlighted by the data is that the level of frustration experienced by the participants for each of task one, task two, task three, and task four was relatively high and produced on average the highest mean values. Further, it can be seen that all of the performance mean values were relatively low suggesting that the participants felt they achieved good results over all the tasks, with task one producing marginally the lowest value followed by task five, with task two producing the highest performance values. Temporal demand and effort both produced relatively high results for all tasks, in each of the subclasses except task one for effort, where a significant increase in the mean values is displayed.

KEY FINDINGS OF EXPERIMENT

Combining the experiment tasks, survey response and post task questionnaire, the main findings for the usability of AuthentiGraph according to this experiment indicate that:

- Participants preferred the interface design in task five, where the individual characters were colour coordinated according to their character type and displayed in a grid arrangement. This preference was reinforced by the results obtained from the experimental tasks.
- The least preferred interface designs were task three, where the characters are randomly positioned throughout the screen in black and white, and task four where the characters are randomly positioned throughout the screen and randomly assigned a colour.
- The preferred screen size was a half screen, followed by the full screen and quarter size screen.
- Participant learning was an issue, where it was established that task completion times did not get faster as the system was used more, which allowed the conclusion to be made that screen size has a significant impact of task completion times.

FUTURE RESEARCH

As a result of this study, a number of opportunities for future research into the area of graphical authentication have become apparent, which may include:

- Testing the usability of AuthentiGraph in an actual environment for an application such as Internet banking.
- Using a larger participant sample to allow the analysis of data to be more conclusive opposed to being only indicative.
- Investigating a number of different interface designs. This study has displayed that participants preferred the interface design with more structure, in terms of a grid arrangement opposed to random displays. Therefore more structured interface designs could be developed and investigated.
- Focusing primarily on only one of the specific interface designs used in this experiment. The results have highlighted that the preferred interface design was the grid layout with colour coordinated characters; therefore further investigation into an application using interface 5 could be conducted.
- Developing this application and implementing it into an organisation to determine users views when it is an imperative part of there business security. Through implementing the application into an organisation, users would provide genuine feedback on perceived security levels, time latency issues, accuracy issues, usability in terms of locating characters and using the mouse, and so forth, because it is relevant to them in there business environments.

CONCLUSION

This paper has presented the results from participants evaluating the usability of AuthentiGraph using five varying graphical interfaces with three different screen sizes. It was established that four separate measures comprising survey responses, task time latencies, task accuracy, and post task questionnaire responses all supported task five (interface 5) as being the preferred interface design for AuthentiGraph. The half screen size was preferred by the majority of participants and confirmed by the task interface completion times and accuracy measures. The work completed has provided a proof of concept relating to the usability of AuthentiGraph and an infrastructure to support future work in relation to authentication using graphical interfaces.

REFERENCES

Basu, A., & Muylle, S. (2003). Authentication in E-Commerce, *Communications of the ACM*, 46(1), 159 – 166.

Blonder, G. (1996). Graphical Passwords, United States Patent 5559961.

Birget, J. C., Hong, D., & Memon, N. (2003). Robust Discretisation: with an Application to Graphical Passwords, Cryptology ePrint Archive.

Dhamija, R. (2000). Hash Visualisation in User Authentication, Proceedings of the Computer Human Interaction 2000 Conference, The Hague, Netherlands.

Dhamija, R. and Perrig, A., (2000), Déjà Vu: A User Study Using Images for Authentication, Proceedings of the 9th USENX Security Symposium, Denver, Colorado, USA.

Furnell, S.M., Papadopoulos, I., and Dowland, P., (2004), A Long-Term Trial of Alternative User

Authentication Technologies, *Information Management and Computer Security*, 12(2), 178-90.

Furnell, S. M., and Zekri, L. (2005). Replacing passwords: in search of the secret remedy, Network Security, 2006(1), 4-8.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric Identification, Communications of the ACM, 43(2), 90-98.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The Design and Analysis of Graphical Passwords, Proceedings of the 8th USENX Security Symposium, Washington, D.C., USA.

Kambil, A., & van Heck, E. (1998). Reengineering the Dutch Flower Auctions: A Framework for Analyzing Exchange Organizations, *Information Systems Research* 9(1), 1-19.

Market Intelligence Strategy Centre (2004). Internet Banking, Media Release, May 5th, URL www.marketintelligence.com.au, Accessed 16 June 2005.

Perrig, A., & Song, D. (1999). Hash Visualisation: A New Technique to Improve Real World Security, Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce, City University of Hong Kong.

Pierce, J.D., Wells, J.G., Warren, M.J., and Mackay, D.R. (2003). A Conceptual Model for Graphical Authentication, Proceedings of the 1st Australian Information Security Management Conference, Perth, Australia.

Pierce, J.D., Warren, M.J., Mackay, D.R., and Wells, J.G., (2004a). Graphical Authentication: Justifications and Objectives, Proceedings of the 2nd Information Security Management Conference, Fremantle, Australia.

Pierce, J.D., Warren, M.J., Mackay, D.R., and Wells, J.G., (2004b). Graphical Authentication: an Architectural Design Specification, Proceedings of the 2nd Australian Computer Network and Information Forensics Conference, Fremantle, Australia.

Renaud. K, and Smith, E.J. (2001). Helping Users to Remember Their Passwords. Annual Conference of the South African Institute of Computer Scientists and Information Technologists, SAICSIT'2001, Pretoria, South Africa, pp. 25-28.

Sandhu, R., & Samarati, P. (1996). Authentication, Access Control, and Audit, *ACM Computing Surveys*, 28(1), 241-243.

Stubblefield, A. and Simon, D. (2004). Inkblot Authentication, Microsoft Research Technical Report MSR-TR-2004-85, URL http://research.microsoft.com/research/pubs/view.aspx?id=790&type=Technical+Report, Accessed 18 September 2005.

Thorpe, J., & Van Oorschot, P. C. (2004). Towards Secure Design Choices for Implementing Graphical Passwords, 20th Annual Computer Security Applications Conference, pp. 50-60.

Thorpe, J., & Nali, D. (2004). Analysing User Choice in Graphical Passwords, URL www.scs.carleton.ca/research/tech_reports/2004/TR-04-01.pdf, Accessed 18 September 2005.

United States Department of Defence (2003). NASA Task Load Index (TLX) V1.0 Users Manual.

Varenhorst, C. (2004). Passdoodles: A Lightweight Authentication Method, Research Science Institute.

Warren, M.J., & Hutchinson, W. (2003). A Security Risk Management Approach for E-Commerce, *Information Management & Computer Security*, 11(5), 238-242, Emerald Group Publishing Ltd., United Kingdom.

COPYRIGHT