Exploring Human Factors Issues & Possible Countermeasures in Password Authentication

A Thesis Submitted to Newcastle University for the Degree of

Doctor of Philosophy

By

Nur Haryani Zakaria

School of Computing Science, Newcastle University

Newcastle Upon Tyne, UK

November 2012

This thesis is dedicated with love and respects to my late parents, my caring husband and not forgetting my two wonderful children.

ACKNOWLEDGEMENTS

I would like to thank few important people for whom without them; this thesis would not have been possible. First and foremost, to my supervisor Professor Peter Wright who has willingly given his support and guidance throughout the research work and construction of this thesis; his continuous support through the good and the bad times has kept me sane throughout professional and personal difficulties which I faced throughout this PhD journey.

Secondly, I would like to thank Professor Michael Harrison as my thesis committee for showing concern not only to my research work but also has been very helpful in helping me cope up while I was stuck in my research work and hence without his support and confidence in me, I would not have progressed to what I am today.

I would also to extend my gratitude to Dr. Peter Andras and Dr. Bryn Jones for helping me to speed up my research work for which if the crucial decision was not made on time, I would have been stuck longer and possibly could not proceed to come up with this thesis. My special thanks goes to Dr Jeff Yan who have worked closely with me in the graphical password experiment without his guidance and assistance, the realisation of this project might not be as it is today. Also my thanks goes to these people individually, who has been involved in my research work both directly and indirectly namely; Dr. Sacha Brostoff, Ms. Catherine McAndrews, Ms. Emma Chaplin, Ms. Sonia Wilson, Paul Dunphy, Suliman Al-Suhibany, Ahmed Al-Saleh, Su Yang, Martin Emms, Ayad Keshlaf and all the rest of the participants that have took part in any of the three experimental works that I have conducted; for which without the full commitment and co-operation from each of you, the research would not have been a success.

Last but not least, I would like to sincerely thank from the bottom of my heart, my beloved husband and children for being patient with me throughout this journey. I would like to apologise for the times when I was not able to play my role as a good wife or good mommy but one thing I know for sure; you guys have been so wonderful to me and that has granted me the opportunity to make this thesis possible at the end.

ABSTRACT

This thesis is concerned with usable security. It describes a series of experiments to understand users' behaviour in the domain of password authentication. The thesis is comprised of two parts. Part 1 reports on experiments into how different persuasion strategies can be used to increase the strength of users' password. Existing research indicates that the lack of persuasive elements in password guidelines may lead to a lack of motivation to produce strong passwords. Thus, an experimental study involving seventy-five participants was conducted to evaluate the effectiveness of a range of persuasion strategies on password strength. In addition this experiment explores how personality variables affect the susceptibility of users to persuasion.

The results showed that passwords created by users who received password guidelines that include a persuasion strategy produce stronger passwords than a control group. In terms of the personality variables, the result shows that there are certain personality types that tend to produce slightly better passwords than others; but it is difficult to draw a firm conclusion about how personality affects susceptibility to persuasion.

The second part of this thesis presents an innovative alternative to text-based passwords, namely, graphical password schemes. Graphical passwords take advantage of the superior ability of humans to remember graphics and pictures over text and numbers. Research shows that graphical password schemes are a promising alternative, but that they are susceptible to shoulder surfing attacks, resulting in scepticism about adoption. Thus in part 2 of the thesis, three innovative shoulder surfing defence techniques are proposed and implemented in a small-scale prototype with a specific focus given to one type of graphical password; The Draw-A-Secret (DAS) scheme. The results of two separate experimental studies involving sixty-five and thirty participants respectively to evaluate the proposed defence techniques from the perspectives of security and usability are presented.

The results show that the technique which, on theoretical grounds, was expected to be quite effective, provides little protection. A second technique which did provide the best overall shoulder surfing defence; created usability problems. But a third technique provided a reasonable shoulder surfing defence and good usability simultaneously; a good balance which

the other two techniques did not achieve. The proposed defence techniques and experimental results are directly relevant to other graphical password schemes of the same category with slight modification to suit the requirements of the scheme intended.

In summary, the thesis contributes to the discussion of some key usability problems which exist around password authentication domains. All the proposed countermeasures are evaluated through a series of experimental studies which present several intriguing discussions and promising findings.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

INTRODUCTION

CHAPTER 1: INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter introduces the idea of the research undertaken; in particular, the background, scope and problems of the research are detailed. It also includes the research aims and objectives with several research questions set out for further investigation.

This chapter also includes the approach to the research, which is empirically based in nature with several experimental works that are carried out to evaluate the proposed idea. Towards the end of this chapter, the organisation of the thesis is detailed.

1.2 Research background & scope

Dependency on information technology (IT) and computer and information security (CIS) has become a critical concern for many organisations. This concern has been mainly about protecting confidentially, integrity and accessibility to information when using computer systems. Hence, much research has been conducted in this area but unfortunately the focus has been primarily on technical problems and solutions [93].

One important aspect of computer security that is often overlooked is the human role in dealing with security systems. Only recently, the security research community has recognised that users' behaviour plays a part in many security failures [48]. Undesirable user behaviour is a significant, perhaps even major cause of many of the security incidents suffered by organizations. There are many reported cases, where user behaviours have been found to enable or facilitate a security breach [157]. Indeed, computer security is often too difficult to be understood by everyone. Terms such as *encryption, public key* versus *private key* or recently sophisticated attacks using *phishing* or *pharming* are too complex for most end users to understand. Not only is this

jargon too complicated, approaches taken to solve the existing problems have changed rapidly, leaving end users unable to cope.

On top of the complexity issues, computer security is often viewed as a *secondary task*. Most often, users find the security mechanism too cumbersome; consequently, they find a way to circumvent security efforts in order to perform their *primary task*. The mismatch between the user's mental model (i.e. the user's idea of how the system works) and how the system actually works also contributes to making inappropriate security-related decisions. There seems to be a lack of motivation on the user's part to care about security because the effects or consequences of not behaving securely do not appear immediately but are often only discovered after they have become problematic for the user.

At present, the problems of users' security behaviours are being studied in two broad domain areas: information security management and usable security. In the first domain area, approaches such as education, training and security awareness programs have been the main focus [195, 90]. Nevertheless, these approaches have not totally solved the problems of encouraging users' motivation in behaving securely. On the other hand, in the area of usable security, researchers have focused their efforts on improving the usability aspects of security mechanisms so that users are more willing to engage in the task [160, 201]. However, there is still a gap in the HCI repertoire in terms of designing usable security pertaining to foster users' motivation towards good security behaviour.

With the background issues presented above, this research intends to fill in the gap by placing its focus on human factor issues. Since computer security is a broad area, this research focuses on the password authentication domain. Given the popular usage of passwords, as well as their vulnerabilities, it is interesting to investigate further the human factor issues pertaining to this domain area. The next section details the problems related to this research.

1.3 Research problems

Password authentication is the most widely used authentication mechanism and will still be with us for many years to come due to the fact that it is effective, simple and

accurate, with no extra cost. Passwords are employed to protect users' online information, including financial information and any personally identifiable information.

Unfortunately, passwords are very vulnerable to hackers' attacks and are regarded as one of the most likely human-error risk factors to impact information systems [35]. The weakness of the password system is not the system itself, but the human behaviours and practices of dealing with the password. Most commonly, the main issue is memorability which leads to several other related issues such as password re-use, password sharing and choosing simple (weak) passwords. These issues are well-known and cited as the human factor problems in the password authentication domain [169, 92].

Most people understand the importance of choosing good or strong[1] passwords. In fact, it is not hard to find guidelines or advice on choosing good passwords. For example, Yan et al. [197] state that a "Password should consist of mixed characters and should not consist of words found in the dictionary".

Similar advice can be found almost everywhere in security operation manuals, policy papers and many websites; nevertheless, after reading these guidelines and advice, users are still found to fail or probably simply refuse to use strong passwords. Although it is acceptable that the importance of the strength of a password may vary, depending on the type of protection required, evidence based on existing research has shown that users commonly underestimate the risks associated with using simple (weak) passwords [66, 199].

Findings from existing research also indicate that users lack the motivation to produce good passwords as they are not convinced of the importance of suggestions given in the guidelines, as revealed by research conducted by research in [162]. It was found that users' awareness of the issues does not deter them from continuing password practice that may put them at risk (e.g.: using dictionary words and names, sharing and re-using passwords).

[1] The usage of the word good or strong passwords versus weak or simple passwords may be used interchangeably throughout this thesis.

1.4 Research questions

Based on the problems discussed above, this research postulates that users not only require support in terms of how they should construct good passwords but, more importantly, that they need to be *persuaded* as to why they should use good passwords and this seems to be lacking in existing guidelines and security advice. Thus, this research aims to explore the feasibility of using the *persuasion* approach in encouraging users to improve their security behaviour.

Furthermore, it is evident that human factor issues are extremely complex as different people may respond and think differently from one another. Based on this point, this research also aims to include an individual personality study, so as to improve understanding of individual characteristics, particularly related to the behaviour of creating passwords.

It is interesting however to note that despite of trying to persuade users to use good passwords, the main problem of password remains – memorability. There have been rigorous efforts from both the academia and industry to propose mechanisms to aid this problem. Among various alternatives being proposed, graphical password is seen to have the closest resemblance to the traditional text-based password in terms of its implementation. The emergence of graphical passwords has been cited to overcome the main weakness of traditional, text-based[2] passwords, namely that of memorability, due to the superiority of graphical images over text and numbers. Hence, this research could not afford to ignore the existence of and the pressure from this alternative approach.

However, since graphical passwords are relatively new, further investigation is required so as to discover whether they can truly replace the traditional, text-based passwords completely, or should be seen as a complementary mechanism to strengthen existing defences. Similar to other alternatives, graphical password scheme are far from being perfect with various challenges particularly with regards to its defence. Thus strengthening its defence is seen as crucial before this scheme becomes more established. This research also aims to investigate the potential of a graphical password

[2] The term text-based password is used interchangeably with alphanumeric passwords throughout this thesis.

scheme in the near future in relation to its role along-side the traditional, text-based passwords as an alternative mechanism.

The following are the research questions that have been set forward to guide the research work as well as the construction of this thesis:

Research question (1):
"To what extent will persuasion approach be able to help in improving users' security behaviour particularly with regards to creating better passwords?"

Research question (2):
"*What can be done to improve the existing solutions to increase the defence mechanism of graphical passwords?"*

Research question (3):
"*How likely is this graphical password scheme to replace the traditional, text-based password scheme"?*

1.5 Research aim and objectives

This research aims to explore human factor issues and to investigate possible countermeasures, particularly pertaining to the password authentication domain. With several research questions to answer as listed above, the research will achieve this aim by meeting four main objectives. The main objectives will then be carried out according to several project activities as listed below:

Objective (1):

- To conduct a review on relevant existing approaches and related theories.
  Project activities:
  1) To review relevant persuasion approaches and related theories of attitude and behaviour change.
  2) To review relevant personality assessment frameworks.
  3) To review existing graphical password schemes and their challenges.

4) To review the existing solutions proposed to overcome this particular challenge for the graphical password schemes.

Objective (2):

- To identify and propose a possible countermeasures of the issues being studied.

  Project activities:

  1) To identify suitable persuasion strategies to be applied in this study.
  2) To identify suitable personality assessment framework to be applied in the study.
  3) To identify one graphical password scheme that can be used for further investigation.
  4) To propose possible defence mechanisms to improve the existing solutions to overcome the challenges of the graphical password scheme.

Objective (3):

- To conduct an evaluation of the proposed countermeasures.

  Project activities:

  1) To conduct an evaluation of the selected persuasion strategies along-side the personality assessment framework in order to discover any significant effect towards the issues being studied.
  2) To evaluate the proposed defence mechanisms for the graphical password and provided further analysis on its implementation.

Objective (4):

- To provide an overall discussion of the findings and lessons learned throughout conducting the research work.

  Project activities:

  1) To provide discussion on how the research has impacted the existing human factors issues pertaining to the password authentication domain.
  2) To provide discussion on possible future work that could be expanded from this research work.

The above objectives have been reached throughout the course of this research, which began in 2009. Many interesting insights and lessons learned throughout conducting this research have been encountered and there are mainly discussed in Chapter 7.

1.6 Research approach

This research is exploratory research which aims to investigate possible countermeasures to the human factor issues related to the password authentication domain. Thus, an empirical-based approach undertaken with three experimental works was set up in order to evaluate the proposed research aim.

The participants involved in all of the experimental works were recruited among the students of this university. The recruitment process was managed through emails and posters distributed among the students on the campus (Appendix A (i), B (i) and C (i)). In order to guarantee that ethical procedures were followed, the methods of recruitment and the process of informed consent (Appendix A (ii), B (ii) and C (ii)) for all the experimental work carried out, was approved by the university's ethical committee (UEC).

The first experimental[3] work that was conducted was the password guideline study which aimed to investigate how to utilise the persuasion approach along-side the personality study. A review on the persuasion approach and relevant theories related to behaviour change, as well as personality assessment framework, was carried out to support this first experiment. This password guideline study involved seventy five participants. Details of the password guideline study, including the results and analysis, will be discussed in Chapter 3.

The second experimental[4] work to be conducted was the security evaluation of the proposed defence mechanisms for the Draw-A-Secret (DAS) scheme. This security evaluation aimed to determine which proposed defence mechanism was strongest in

[3] The first experimental work will also be referred to as the password guideline study.
[4] The second experimental work will also be referred to as the security evaluation study of the Draw-A-Secret scheme.

terms of providing defence to the DAS scheme. Sixty eight participants were recruited for this study.

The third and final experimental work[5] expanded on the second experimental work, where an evaluation of the usability of the proposed defence mechanisms for the Draw-A-Secret (DAS) scheme was conducted. This usability evaluation aimed to determine which proposed defence mechanism provided the best usability, as measured by several factors such as login time, login trials and users' preference. Since both experimental works 2 and 3 are related to the evaluation of the DAS scheme, the details of both studies, including the results and analysis, will be discussed further in Chapter 6 of this thesis.

1.7 Thesis organisation

This thesis is written in a total of seven chapters, mainly reporting and discussing the findings of the research conducted. Figure 1.1 illustrates the overview of this thesis.

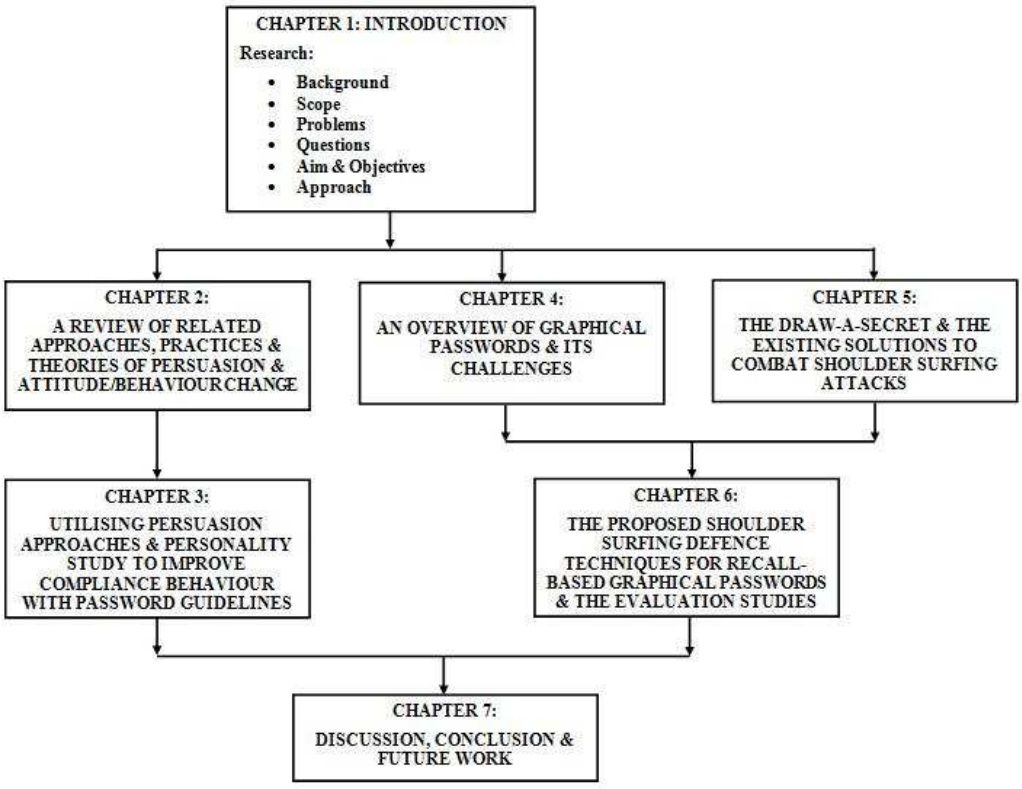


Figure 1.1: Overview of thesis organisation

[5] The third experimental work will also be referred to as the usability evaluation study of the Draw-A-Secret scheme.

In general, all of the research aims and objectives have been successfully achieved. The thesis can be viewed in two main parts. First, this thesis investigates the feasibility of utilising the persuasion approach along-side the personality study to improve compliance behaviour with password guidelines. Thus, following this Introductory Chapter is Chapter 2 which entails a review of work done on the relevant persuasion approaches, as well as some related theories of attitude and behaviour change. This chapter also includes a discussion on the selected individual personality assessment framework. The outcome of Chapters 2 is mainly the suitable persuasion strategies and a personality assessment framework to be applied in the password guideline study to improve users' compliance behaviour issues, which will be discussed thoroughly in Chapter 3.

The second half of the thesis investigates the immediate alternative to traditional text-based passwords – the graphical password. This includes some review work done on the existing graphical password schemes and their challenges, as discussed in Chapter 4. Towards the end of Chapter 4, one graphical password scheme is selected and shoulder surfing attack has been identified as a common challenge facing graphical password adoption.

Chapter 5 narrows the discussion on the selected scheme, known as the Draw-A-Secret (DAS), and presents a rationale for choosing it. This chapter also provides a review of the current solutions to combat shoulder surfing attacks on the DAS scheme.

The next chapter introduces proposed defence mechanisms to combat the shoulder surfing attack problem. In this chapter, two separate evaluation studies are included on the security and usability of the proposed defence mechanism. The findings of both evaluation studies are detailed in the chapter.

Perhaps the most critical chapter is Chapter 7, where all of the research findings are discussed. All research questions are examined thoroughly in parallel with meeting the research aim and objectives set out earlier. Implications of this work and the benefits of the findings will also be discussed. Also included in this final chapter are contributions of the thesis to this field of study towards to the research work followed by several possible future research avenues to be carried out.

1.8 Summary

This chapter begins by introducing the background and the scope of the research and then highlights the problem domain. In order to further investigate the research problems, several research questions have been outlined. The research aim and objectives have also been highlighted. Next, the research approach has been detailed and an overview of the written chapters has been illustrated in a diagram to guide and the reader through this thesis.

CHAPTER 2

A REVIEW OF RELATED APPROACHES, PRACTICES & THEORIES OF PERSUASION AND ATTITUDE/BEHAVIOUR CHANGE

CHAPTER 2: A REVIEW OF RELATED APPROACHES, PRACTICES & THEORIES OF PERSUASION AND ATTITTUDE / BEHAVIOUR CHANGE

CHAPTER 2

A REVIEW OF RELATED APPROACHES, PRACTICES & THEORIES OF PERSUASION AND ATTITUDE / BEHAVIOUR CHANGE

2.1 Introduction

This chapter in general provides a review of related approaches, practices and theories of persuasion and attitude or behaviour change that has been adopted as the focus of this thesis in order to improve users' security behaviour, particularly with regards to password guideline compliance. This chapter will elaborate further the persuasion approach which also includes the discussion of the weapon of influence, introduced by Cialdini [41]. The discussion will then followed by presenting several selected major attitudes and behaviour change theories alongside with comparison on its advantages and disadvantages. A recently introduced persuasion practice popularly known as Persuasive Technology by Fogg [67] will also be discussed thereafter.

In relation to the relevance of this thesis, the review work has led to the discovery that the persuasion domain is very closely related to individual difference factors. Although, there are indeed several other determinant factors of security behaviour such as motivation, habit and prior knowledge, the focus of this thesis has been centred upon individual personality factor. This is simply due to individual's personality might cause an impact on the outcome of the persuasion attempt.

In addition, since the persuasion approach is fairly new to the area of information security, it is interesting to explore this intriguing idea of how an individual's personality characteristics can be used in conjunction with the right persuasion strategy to improve password guideline compliance. Thus, this thesis intends to broaden the persuasion approach by combining it with personality studies.

Therefore, this chapter also includes the discussion of selected personality frameworks known as the Big Five Inventory (abbreviated hereafter as BFI), also known as the Big Five Model. A rationale for choosing the BFI as a framework for measuring personality characteristics will also be discussed.

2.2 An introduction to the persuasion approach

Persuasion as an art has been practised for centuries, evolving into the emerging sciences in the 20th century. As techniques of persuasion continue to evolve from art to science, their effectiveness in controlling behaviour is expected to be enhanced. The question now is whether science can increase the effectiveness of persuasion and if so, in what way. The answer is that it can, by providing researchers with a systematic procedure (i.e.: scientific methodology) with a means of isolating the variables being tested, thereby creating a better chance of identifying factors that are responsible for the outcome of a particular investigation [103]. This creates an interesting avenue to examine persuasion as an approach towards improving users' behaviour in the domain of information security.

Scholars have defined persuasion in many ways. For example Bettinghaus & Cody [14] define persuasion as a "conscious attempt by one individual to change the attitudes, beliefs or behaviour of another individual or group of individuals through the transmission of some message". Another scholar O'Keefe [132] defines persuasion as "a successful intentional effort at influencing another's mental state through communication in a circumstance in which the persuadee has some measure of freedom". It can be seen from these two definitions from renowned persuasion scholars that persuasion refers to the process of charging or reforming attitudes, beliefs, opinions or behaviours toward a predetermined outcome through voluntary compliance.

The word persuasion has been used interchangeably with *influence*. This is not surprising as persuasion can be considered a form of attempted influence [42]. There are also other forms of attempted influence, like material inducements and coercion which differ from persuasion. Material inducements are exchanges of money or other

such things for actions by the person being influenced, whereas coercion implies force such as economic sanctions. Persuasion on the other hand, relies on the power of verbal and non-verbal symbols and allows people to participate voluntarily in the persuasion process [124]. This voluntary nature is what makes persuasion so powerful and long lasting, in contrast to the more short-term effects of coercion. When individuals perceive that they have no choice but to comply, the influence is viewed more as coercive [141].

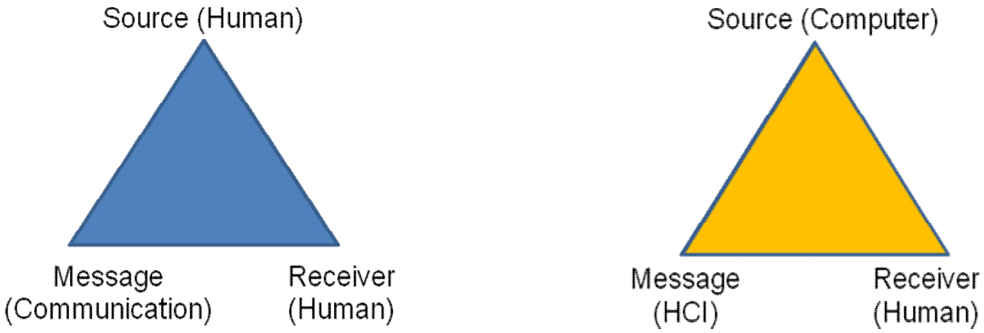
Another important element in understanding the concept of persuasion is that it involves a deliberate attempt to influence another person. The persuader must intend to change another individual's attitude or behaviour and must be aware (at least to a certain extent) that he/she is trying to accomplish this goal. This explains why a baby's cries for milk or toddler's demand for toys do not qualify as persuasion; these youngsters have not reached the point where they are aware that they are trying to change another person's mental state. However, as the children grow, they appreciate these things and eventually develop the ability to persuade others more effectively [105].

Today, numerous companies are in the persuasion business. Persuasion has indeed become institutionalised, from advertising agencies, public relations firms and marketing conglomerates to social activists, speech writers and image consultants, and the list of those involved with various facets of persuasion continues to grow. This explains why persuasion is such a powerful tool and how, when adopted in a positive way, it can lead to a beneficial outcome for both parties – persuader and persuadee.

2.2.1 The elements and effects of persuasion

The discussion thus far has emphasised the definition and concept of persuasion. Persuasion involves three main elements; source (persuader), message, and receiver (persuadee). Figure 2.1 (a) shows a traditional model of persuasion where one human acts as a source communicating a persuasive message to another human (known as the receiver). The communication is basically formed by traditional verbal and non-verbal messages. In contrast, figure 2.1(b) shows another model of persuasion which differs

slightly from the traditional one, where the source is now changed to a computer. This contemporary model is call human-computer-persuasion. The role of the computer in substituting the human as a source (persuader) involves a significant impact on the existing theories of persuasion.



(a) Traditional model of persuasion **(b) Human-computer persuasion model**

Figure 2.1: The model of persuasion

There are indeed different types of persuasive communication, whereby different types may lead to different effects. For example, some messages dramatically influence attitudes, while others may exert a smaller or more subtle impact. Miller [124] has proposed that communication exerts three different persuasive effects that are *shaping*, *reinforcing* and *changing responses*. More recently, Kukkonen & Harjumaa [107] illustrated the potential effects of persuasion, similar to those proposed by Miller [124] as follows (refer to Figure 2.2):

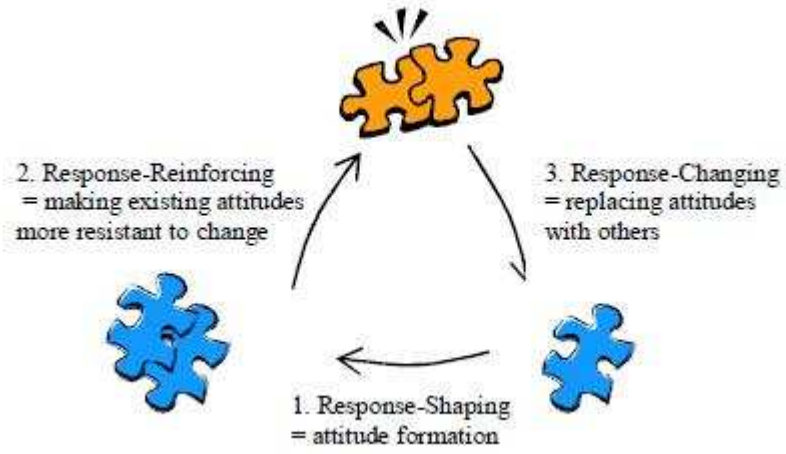


Figure 2.2: The three possible effects of persuasion [107]

- A *shaping* outcome means the formulation of a pattern for a situation which did not exist beforehand. For example, marketers shape attitude by associating cigarettes with beautiful women – hoping they can entice young people into smoking.
- A *reinforcing* outcome means the reinforcement of current attitudes, making them more resistant to change. Contrary to popular opinion, many persuasive communications are not designed to convert people but rather to reinforce a position they already hold. For example, health educators try to reinforce individuals' decisions to quit smoking or to abstain from drinking in excess. Persuaders recognise that people can easily relapse from a commitment to give up unhealthy substances.
- A *changing* outcome means changes in a person's response to an issue (e.g.: social questions). This perhaps is the most important persuasive impact and the one that comes most frequently to mind when persuasion is involved. For example, in the 1950s and 1960s, the issue of race was a sensitive social issue. This has changed dramatically through increased dialogue between races, civil rights campaigns and heart rending media stories which led society to rethink its prejudiced attitudes. This example has shown that persuasive communications have had strong and desirable effects by influencing attitudes and social behaviour.

Persuasion ideally induces an individual to abandon one set of behaviours and to adopt another. However, in many cases a shaping outcome may have a higher likelihood of success than communication that aims to change behaviour. This may happen with people who have limited prior learning histories or in situations where radically new and novel stimuli have been introduced into the environment [107]. In any case, reinforced beliefs and forms of behaviour become the most resistant ones as time goes by. Thus, persuasion will have an effect to some extent on attitude and behaviour change. According to Crano & Prislin [47], a prime factor that must be considered when reflecting on persuasion concerns the fundamental construct of attitude.

The next sub-section will discuss a related example of persuasion approach known as the weapon of influence which was introduced by Cialdini [41]. This approach alongside with real-life examples of how it has been applied in various experimental studies has somehow indicated that persuasion is indeed a powerful tool for attitude or behaviour change.

2.3 An example of persuasion approach - Weapons of influence

Weapons of influence is a set of principles introduced by Cialdini [41] through several studies conducted using compliance professionals such as salesman, fundraisers, restaurant staff and many more. The principles were also derived through a series of controlled laboratory experiments to test hypotheses about compliance. The six principles are *reciprocation*, *commitment and consistency*, *social proof*, *liking*, *authority* and *scarcity*.

The principles of *reciprocation* suggest that people will try to repay (i.e. are obligated to) kindness they receive from others. This principle is universal in the sense that it works simply because it is a natural human tendency to treat people they way they were treated. The sense of future obligation within the rule makes possible the development of various kinds of continuing relationships, transactions and exchanges that are beneficial to society. Consequently, all members of society are trained from childhood to abide by the rule or suffer serious social disapproval [41].

According to Cialdini [42], charities rely on reciprocity to help them raise funds; for example, the American Disabled Veterans organisation started enclosing small gifts in envelopes as to show their appreciation to the donators, the amount of donations nearly double to 35% compared to 18% when the gifts were not included. However, it is not necessary to involve gifts or tokens to make this principle work, as shown in the results of an experiment whereby half of the people attending an art appreciation session were offered a soft drink and afterwards all were asked if they would buy 25 cent raffle tickets; the outcome was that people who had been offered the soft drink purchased twice as many raffle tickets, whether or not they had accepted the drinks [139]. In this

experiment, there was a sense of indebtedness to someone by delivering a number of uninvited first favours over time which was not necessarily tangible gifts.

Cialdini [41] suggests another compliance procedure known as the *rejection-then-retreat* technique (also known as the *door-in-the-face* technique) which relies heavily on the pressure to reciprocate concessions. By starting with an extreme request that is sure to be rejected, a requester can then profitably retreat to a smaller request (i.e. the one that was desired all along) which is likely to be accepted because it appears to be a concession. Research indicates that aside from increasing the likelihood that a person will say yes to a request, the *rejection-then-retreat* technique also increases the likelihood that the person will carry out the request and will agree to such a request in the future [43].

The second principle is known as *commitment and consistency*. According to this principle, once a person makes a choice or takes a stand, the person will encounter personal and interpersonal pressure to behave consistently with that commitment. A simple experiment was conducted to test this principle; an experimenter places a beach mat near selected subjects and asks them to look after his belongings while he is away. Another experimenter, posing as a thief, attempts to snatch some belongings from the beach mat. In the study, 19 out of 20 subjects responded in certain ways to protect the belongings since they had agreed to look after them, while only 4 subjects try to protect the belongings when they do not have any initial commitment to do so [127].

On other occasions, commitment can also be expressed in the form of a written statement, as writing something down is considered an act of commitment. One reason that written testaments are effective in bringing about genuine change is that they can be so easily made public [41]. Two prominent social psychologists, Deutsch & Gerard [54] conducted a famous experiment to illustrate the way public commitments can lead to consistent further action. The basic procedure involved three groups of students who were shown different lines and asked to estimate their lengths. The first group were asked to write down their estimations on paper and show them to the public. The second group were asked to write down the estimations but not to show them in public, and the third group were asked to keep their estimates private. Later, these subjects were given

new evidence that their initial estimates were wrong and then given the chance to change their estimates. The results were obvious: the students who had never written down their estimates were the least loyal to their choices. The third group was highly influenced by the new information that indicated their initial estimates were wrong. The group which wrote down their estimates but did not show them in public were less willing to change their measurements and the group who wrote them down and made them public were the most stubborn. This stubbornness can occur even in situations in which accuracy should be more important than consistency.

This is indeed an interesting principle and might work in situations where commitment is highly desired. For example, in organisations where employees' commitment towards building the information security culture becomes a virtue, this principle might be useful when applied in requesting consistent commitment from everyone. This strategy is therefore relevant to this study as effective password guidelines do require some level of commitment from the users to comply.

The third principle is that of social proof, which states that one important means that people use to decide what to believe or how to act in a situation is to look at what other people believe or do. Powerful imitative effects have been found among both adults and children and in such diverse activities as purchase decision, charity donations and phobia remission [41]. A common example of applying this principle is when advertisers normally make claims like "*fastest selling*" about their product because they do not have to convince the buying public directly that the product is good; they need only say what others think, which seems proof enough.

One experiment uses this principle to eliminate undesirable behaviour among nursery school age children who are terrified of dogs by showing them a little boy playing happily with a dog for 20 minutes a day. After four days, 67% of them were willing to climb into a playpen with a dog and remain confined there patting and scratching the dog while everyone else left the room [9]. Apparently, the principles of social proof work best when the proof is provided by the actions of many others and can also be used as therapy for various other problems.

Cialdini [42] claims that this social proof principle is most influential under two conditions; *uncertainty* and *similarity*. When people are unsure or when the situation is ambiguous they are more likely to be aware of the actions of others and to accept those actions as correct. In addition, people are more inclined to follow the lead of others who are similar to themselves. This is another interesting principle worth further investigation. In many situations, most people tend to follow others in order to maintain their reputation as social proof endorsement is crucial in human society. In relation to this study, this principle can be useful to portray the fact that failure to comply with password guidelines can result in various unwanted incidents that might cause their reputation, as seen by other people, to be tarnished.

The fourth principle is *liking;* people prefer to say yes to individuals they know or like. Recognising this rule, compliance professionals commonly increase their effectiveness by emphasising several factors that increase their overall attractiveness and likeability. One feature of a person that influences overall liking is physical attractiveness, which seems to produce a halo effect that extends to favourable impressions of other traits such as talent, kindness and intelligence [133].

Another factor that influences liking and compliance is similarity, as we like people who are like us and we are more willing to say yes to their requests [31]. Increased familiarity through repeated contact with a person normally facilitates liking. This relationship holds true principally when the contact takes place under positive rather than negative circumstances. One positive circumstance that works especially well is mutual and successful cooperation. A factor that is also linked to liking is association. Most commonly advertisers or politicians frequently seek to share positivity through the process of association. Other individuals (e.g. voters) appear to recognise the effect of simple connections and try to associate themselves with favourable events and distance themselves from unfavourable events in the eye of observers.

The fifth principle, *authority*, states that people are more likely to listen to or follow experts. For example, in studies conducted by Milgram [123], evidence suggests strong pressure in society to comply with the request of a figure of authority. Acting contrary to their own preferences, many normal, psychologically healthy individuals are willing

to deliver dangerous and severe levels of pain to another person when directed to do so by an authoritative figure. The strength of this tendency to obey legitimate authorities comes from systematic socialisation practices designed to instil in members of society the perception that such obedience constitutes correct conduct [41]. When reacting to authority in an automatic fashion, there is a tendency to do so in response to the mere symbols of authority rather than to its substance. Three kinds of symbols that have been shown by research to be effective in this regard are titles, clothing and automobiles [41]. In separate studies investigating the influence of these symbols, individuals possessing one or another of these were accorded more obedience by those they encountered. Moreover, in each instance, individuals who deferred to or obeyed the figures of authority underestimated the effect of authority pressure on their behaviour.

The sixth principle is *scarcity*. According to this principle, people will assign more value to opportunities when they are less available. The use of this principle for profit can be seen in such compliance techniques as the "limited number" and "deadline" tactics, whereby practitioners try to convince us that access to what they are offering is restricted by amount or time. The scarcity principle holds for two reasons: firstly because things that are difficult to attain are typically more valuable, and secondly because, as things become less accessible, we lose freedoms. The scarcity principle is most likely to hold true under two optimising conditions. First, scarce items are heightened in value when they are newly scarce. In other words, people value those things that have become recently restricted more than those that have always been restricted. Second, people are most attracted to scarce resources when there is competition with others for them.

The next sub-section will discuss in more detail the attitudes and behaviour change resulting from successful persuasion. Several important existing theories will also be discussed to accommodate understanding of the underlying issues of persuasion.

2.4 Selected major attitudes and behaviour change theories

An attitude is a *cognition* (i.e. a form of thought) that is formed through experience and which influences one's behaviour. The fact that attitudes are formed through experience

indicates that they can *potentially* be changed. Attitudes have two basic components: beliefs and values [114]. Beliefs are verifiable in the sense that they are assumed to be true or correct when they seem to reflect the world, and false or incorrect when they seem contradict perceptions of the world. On the other hand, values are judgements of worth, such as good or bad, useful or useless, efficient or inefficient. Together, these cognitions (i.e.: thoughts), beliefs and values constitute attitudes.

There are a number of theories developed by scholars (in the psychology domain) in fostering attitude and behaviour change. Some theories try to explain the relationship between attitudes and behaviour, while other theories explain how to utilise the persuasion approach as a means of influencing people. All these theories have their own foci and restrictions.

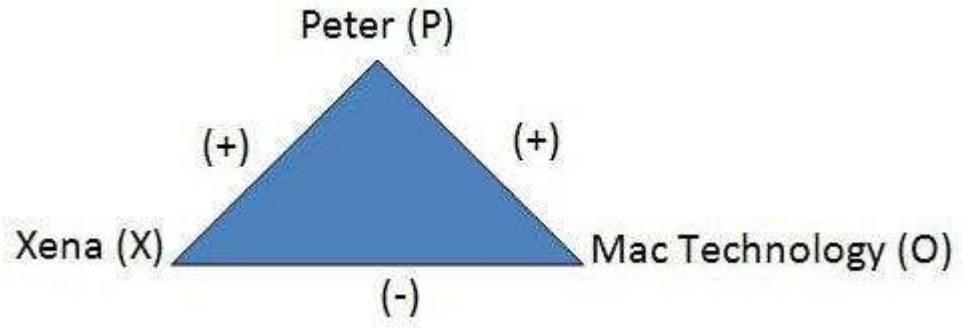
Some of the selected theories of attitudes and behaviour change are the *Social Balance Theory* [89], *Information Processing Theory* [120], *Reasoned Action Theory* [65], *Elaboration Likelihood Model* [144], *Health Believe Model* [151] and *Protection Motivation Theory* [148]. These theories will be briefly discussed in the following sub-section.

2.4.1 Social Balance Theory

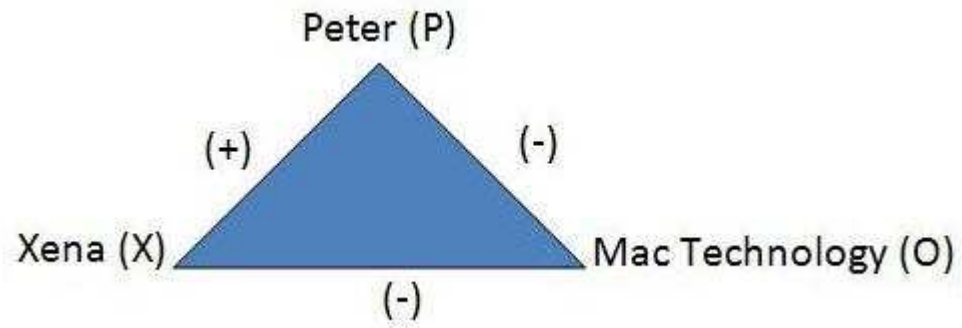
The Social Balance Theory proposed by Heider [88] is one of the most popular cognitive consistency theories and depicts relationships among people's thoughts. It involves a triad of relationships: a person or perceiver (P), another person (O) and an issue or an object (X). The theory seeks to argue that people prefer a balanced relationship among the three elements. Heider [88] also proposes that cognitive elements have a positive or negative relationship. For example, a positive relationship in which P likes O or X is symbolised with a plus (+) sign, whereas a negative relationship, in which P dislikes O or X, is assigned a minus (-) sign.

Figure 2.3 shows the three functional elements (P, O, X), as proposed in Heider's theory. Each of these (i.e.: P-O, P-X and O-X) is assigned with a plus or minus. Attitudes are in harmony when the signs multiplied together yield a plus (i.e. similar to

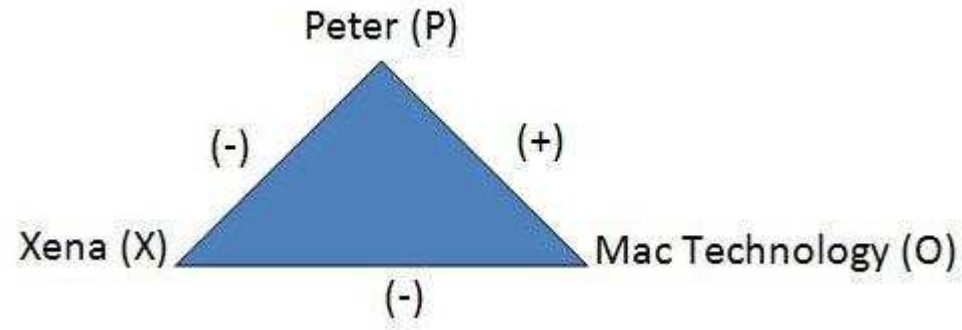
mathematical concept for products of multiplications). This concept is then translated into real life situations to understand how people cope with inconsistencies among attitudinal elements. In order to understand the relationships in the triad better, consider (P) the person as Peter who has a preference for Mac technology (represented as the object O), while his best friend Xena (X) is not so keen on the technology.



(a) Cognitively imbalanced triad



(b) Cognitively balanced triad



(c) Cognitively balanced triad

Figure 2.3: The model based on Social Balance Theory - Analysis of Peter's attitude towards Mac technology and Xena his best mate who does not so keen in the technology (adopted from [141])

Note: Positive (+) sign indicate favour the object while negative (-) sign is the opposite

Presumably, Peter would find the inconsistencies uncomfortable and would feel compelled to restore mental harmony (as depicted in Figure 2.3(a)). The theory suggests several options: he could either change his attitude towards the object (O) (as depicted

in Figure 2.3(b)), probably trying to find similar advantages that Mac offers on other platform, or alter his attitude towards his friend Xena (X) (as depicted in Figure 2.3(c)), deciding that he cannot be friendly with someone who does not share his preference.

One simple advantage of this balance theory is that it recognises that people will sometimes experience inconsistent cognitions and that this inconsistency can lead to attitude change [89]. However, people do not compare every thought they have to every other thought, so at times people can have inconsistent cognitions without realising it [141]. Unfortunately, this theory does not describe many subtleties in people's judgement. First, it fails to describe those situations in which people manage to like people with whom they disagree; for example, the public was found to continue their support for politicians such as President Clinton even when they opposed his relationship with his liaison, Lewinsky [122].

Another limitation of this theory is that it does not predict the degree of liking towards the object (O). Thus, using positive (+) and negative (-) signs to represent whether a person likes or dislikes an object does not quantify how much the person actually likes the object. This is important as the degree of liking also plays a role in determining the likelihood of attitude change [13]. In addition, people are not equally persuaded by all topics. For example, if a different object or person is replaced in the triad, it might produce a totally different relationship; nonetheless, the balance theory assumes that all people will create the same amount of imbalance.

2.4.2 Information Processing Theory

McGuire [120] proposes the Information Processing Theory which includes six main steps in the process of *persuasion*, from the beginning where an individual is presented with the message until the process of changing attitude or behaviour is finally achieved. The six steps suggested by the theory are depicted in Figure 2.4.

Figure 2.4: The six steps in the process of persuasion – Information Processing Theory [120]

The presentation stage is where the process begins, exposing the intended audience to the persuasive message. It is then followed by the process of "paying attention" as McGuire [120] reasons that people would not be persuaded by a message they ignore. Third, the audience must then understand the message that a persuader is trying to convey, making comprehension the stage after attention. The next phase is the acceptance process of the message that was successfully comprehended; this is termed as "yielding" in the theory. According to McGuire [120], this yielding phase is actually where the formation of attitude changes begins. Once a persuasive message succeeds at changing a person's mind (i.e. attitude), what matters is the following retention phase, which is concerns with how long the attitude change will be retained. Finally, if a person succeeds in the retention phase, the likelihood of the attitude to transform into the desired behaviour is more likely to happen, whereby a change in behaviour has always been the ultimate aim in the process of persuasion. This theory is important in helping towards the understanding of the persuasion process.

In an earlier effort, Hovland et al. [95] worked out a model popularly known as the *Yale Attitude Change Model.* This model focuses on the conditions under which people are most likely to change their attitudes in response to persuasive messages. Figure 2.5 illustrates the idea of the Yale model. The Yale model illustrates an overview of the persuasion framework which consists of several components such as the source factors, message factors and audience factors. These three components will eventually lead to the persuasion process itself, which has the six steps elaborated by McGuire [120] in his theory. Ultimately, the outcome of the persuasion will be subject to either changes of opinion, perception, affection or action.

Based on Figure 2.5 above, the theory proposed by McGuire [120] seems to be an extension of this Yale model, focusing more specifically on the middle part, which illustrates the process of persuasion. Some of the factors studied in the Yale model probably work by influencing different parts of the persuasion process [13]. For example, some factors may work better through comprehension, while others might focus on yielding. The Yale model has drawn interest among other scholars who place their focus more specifically into source factors [193] and message factors [12]. In terms of source factors, attributes such as expertise, trustworthiness and status play a

role in determining the outcome of persuasion. For example, people have a tendency to pay more attention to experts or those whom they trust. Thus, it is important to realise that what matters most in terms of credibility is the audience's perception of the source [193].

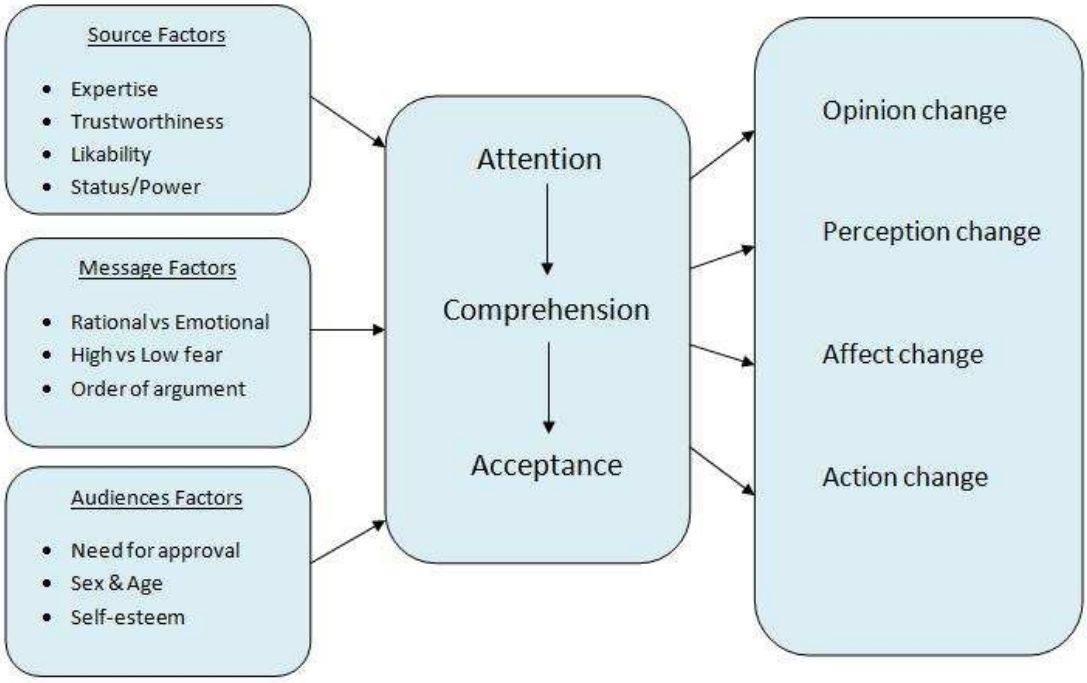


Figure 2.5: The Yale Attitude Change Model [95]

Apart from source factors, message factors also play an important role in determining the success of persuasion. Message factors can be divided simply into message organisation and message content. Message organisation refers to how and when to put forward the message. For instance, the study conducted by Benoit [12] focuses on the effects of *forewarning* of persuasive intent. Benoit [12] claimed that informing the audience of the intention of persuasion at the beginning of the message is more likely to result in reducing the persuasiveness of the message. He adds that people often have a tendency to think that their own beliefs and attitudes are right, so the likelihood of them being more closed-minded is greater especially when they know that someone is trying to change their minds.

On the other hand, message content focuses on what type of argument should be placed in order to provoke the audience. Research demonstrates that argument strength is

directly related to attitude change [5]. This means the stronger the argument; the more an attitude change can be expected. According to Petty & Cacioppo [143], messages with more arguments are more persuasive than those with fewer arguments. These factors probably influence persuasion by aiding the yielding phase because people are more likely to accept arguments that are stronger. Among examples that have been used to strengthen the effects of the arguments are appeal strategies, which involve rational and emotional arguments, providing appropriate evidence as support. Taylor & Thompson [176] suggest that evidence from examples is more persuasive and also creates resistance to counter persuasion. In relation to McGuire's [120] theory, the use of evidence might increase attention and comprehension due to the fact that examples help to increase understanding and allow people to accept the idea more easily. These are highly relevant to this study, as an appeal strategy might be useful in conveying suitable messages or advice to users, for example in password guidelines.

The view of persuasion developed in the years that followed the publication of Hovland et al. [95] and McGuire's [120] theories is known as the cognitive response approach to persuasion, an approach which asserts that people's own mental reactions to a message play a more important role than the message itself.

2.4.3 Reasoned Action Theory

Reasoned Action Theory, by Fishbein & Ajzen [65], assumes that people rationally calculate the costs and benefits of engaging in a particular action and think carefully about how important others will view the behaviour under consideration. The theory comprises four main components (Figure 2.6):

- Attitude towards the behaviour – the person's judgement that performing the behaviour is good or bad
- Subjective norm – the person's perceptions of the social pressures put on him to perform or not to perform the behaviour in question
- Behavioural intention – the intent or plan to perform the behaviour
- Behaviour – the action itself in a particular situation

This theory offers a framework for predicting behaviour from attitudes. Fishbein & Ajzen [65] claim that behaviour can be predicted when both likes and dislikes (i.e. attitudes) and people's natural propensity to want to please others (i.e. norms) is considered. Several studies have tested these proposals. For example, researchers have found that attitudes and subjective norms forecast intentions and therefore help to predict behaviour [172, 83].

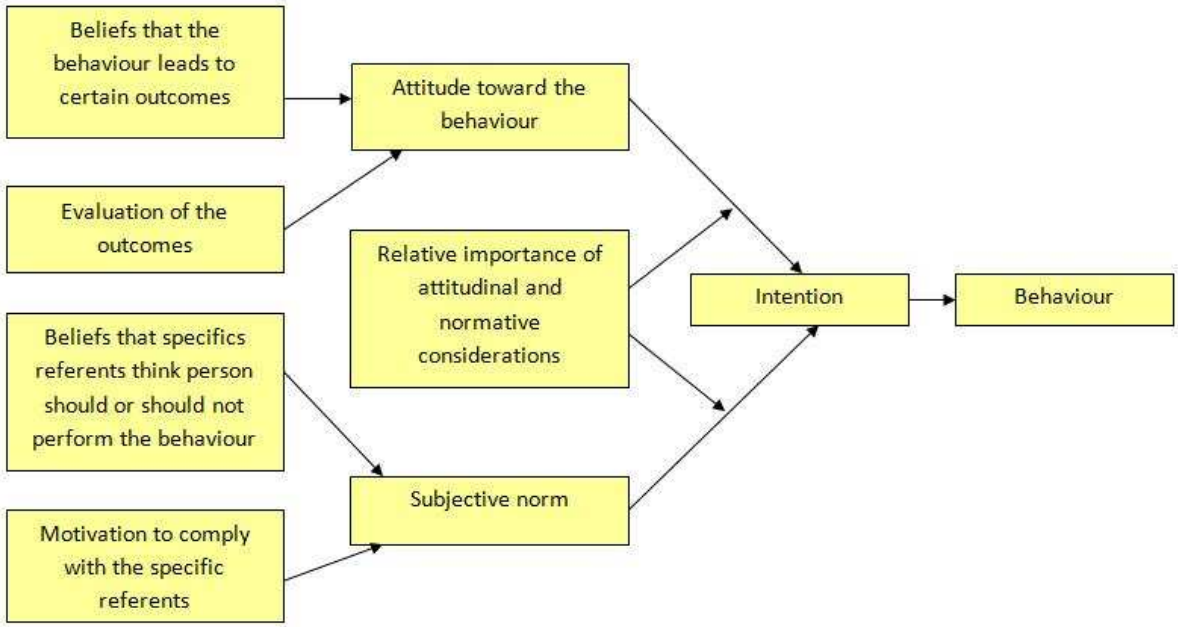


Figure 2.6: The Reasoned Action Theory [65]

Nonetheless, like every other approach, this theory also has its limitations. One of the main critiques is that it assumes that people have control over their behaviour; however, this is not always tenable [63]. Example of this are people who want to lose weight but cannot muster the strength, or those who want to stop smoking but cannot bring themselves to do so. In such cases, the Reasoned Action Theory breaks down because people do not act on attitude or norm if they fail to do that which they intend. Noting the problem, Ajzen who was also involved in the construction of the theory, attempts to rectify this weakness by proposing an alternative approach known as the Theory of Planned Behaviour [2].

2.4.4 Theory of Planned Behaviour

Ajzen [2] developed a theory known as Theory of Planned Behaviour which extends the theory he developed with Fishbein by adding another component,: perceived behaviour control, which is the individual's perception of how much control he or she has over the behaviour [2]. In other words, perceived behaviour control refers to the subjective estimate of how easy or difficult it will be to perform the behaviour. Figure 2.7 below shows the components involved in this theory.

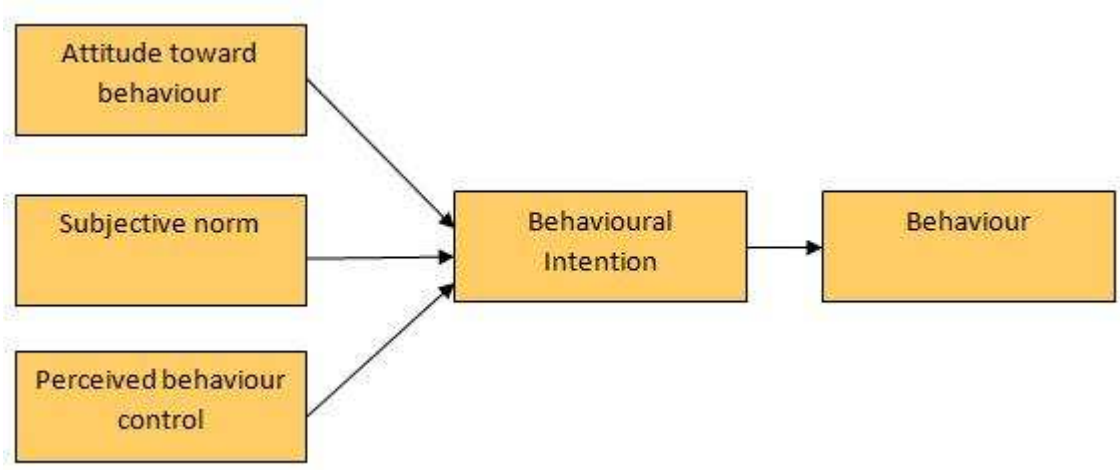


Figure 2.7: The Theory of Planned Behaviour [2]

As illustrated in Figure 2.7 above, the perceived behaviour control means the more an individual perceives that he or she can perform the action, the more successful the individual should be in translating intention into behaviour. Similar to the reasoned action approach, this theory of planned behaviour has an excellent track record in predicting behaviour [172].

However, despite their differences, both theories (i.e. planned behaviour and reasoned action) emphasise that attitudes can predict behaviour under certain circumstances. Both theories also acknowledge that attitudes will not predict behaviour when subjective norms apply, or when people lack the psychological ability to translate attitude into action. Neither reasoned action nor planned behaviour theories claim that attitudes always predict behaviour, only that attitudes are a reasonably accurate indicator of what

people will do, provided certain conditions are met. There will always be circumstances in which people, being complex, will behave on the basis of factors other than attitude.

2.4.5 Elaboration Likelihood Model

The Elaboration Likelihood Model (abbreviated hereafter as ELM) was proposed by Petty & Cacioppo [144] after much debate on the limitations of the cognitive response approach, as discussed in earlier sections. One of the limitations is that it assumes that people think carefully about messages. However, this is not always the case as many people are found to turn their minds off to persuasive communications, making decisions based on mental shortcuts [141]. Another limitation of the cognitive response approach is that it does not explain how to utilise cognitive responses to devise messages to change attitudes or behaviour.

ELM stipulates that there are two distinct ways in which people process communications called *route*[6] suggesting that two different highways crisscross the mind, transporting thoughts and reactions to messages. The ELM refers to the two routes of persuasion as the *central* and *peripheral* routes. According to Petty & Cacioppo [144], the central route of persuasion consists of thoughtful consideration of the arguments, i.e. the content of the message. They add that central processing can only occur when a person has both the motivation and the ability to think about the message and the topic; if the listener does not care about the topic of the persuasive message, he or she will almost certainly lack the motivation to centrally process it. On the other hand, if the listener is distracted or has trouble understanding the message, he or she will lack the ability for central processing.

[6] The term route is a metaphor – it is not known for sure that these routes exist (anymore than it is known with absolute certainty that any mental construct exists in precisely the way theorists use it).

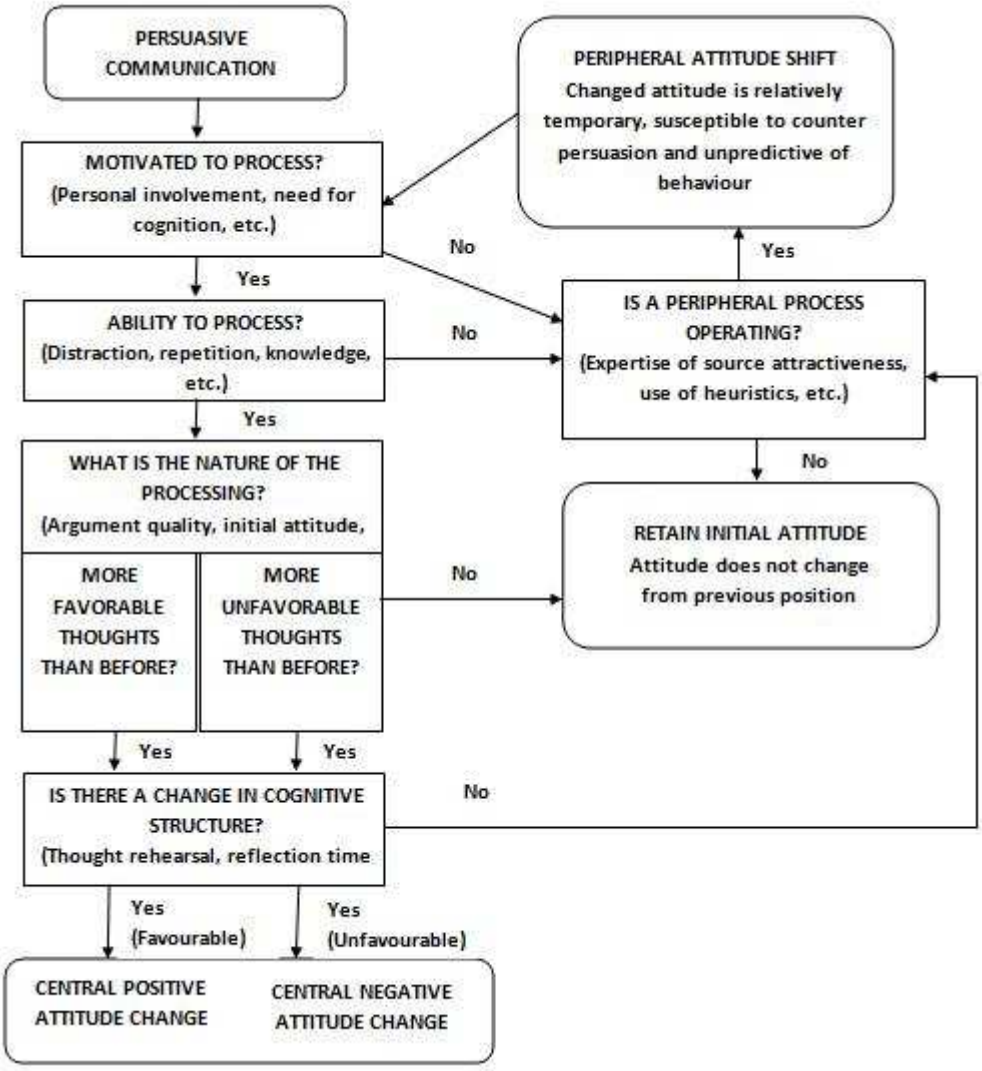


Figure 2.8: The Elaboration Likelihood Model of persuasion [144]

Unlike the central route, the peripheral route occurs when the listener chooses to agree with the message, based on other cues besides the strength of the arguments or ideas in the message [144]. For example, a person might choose to agree with the message because the source appears to be an expert, or looks very attractive. Sometimes, it could also be due to that fact that the person notices that a message has many arguments but he or she lacks the motivation or ability to consider each one individually. In other words, peripheral routes rely on cues, such as the credibility of the source or the number of arguments in the message. This route occurs when the person is unable or unwilling to engage in much thought about the message [11]. Receivers engaged in peripheral routes are more passive than those in the central routes.

The main assumption of the model is that the effects of attitude change in these two routes are different; those attitudes that are changed through the central route will show greater temporal persistence, greater prediction of behaviour and greater resistance to counter persuasion than attitude changes that result from peripheral routes [144]. Although ideally persuaders would want their audiences to use the central route so that greater temporal persistence towards attitude changes can be obtained, unfortunately in reality, the audiences do not always have the same motivation and ability to process the message. Understanding the process of how a person would most likely process a persuasive message as proposed by the ELM (refer to Figure 2.8) would therefore certainly help persuaders to increase their ability to persuade.

2.4.6 Health Belief Model

The Health Belief Model (HBM) is one of the oldest theories developed by Rosenstock and colleagues working in the US Public Health. The theory was developed in response to the failure of a free tuberculosis (TB) health-screening program and since then the HBM has been adapted to explore a variety long and short term health behaviours which focus on the attitudes and beliefs of individuals.

According to Rosenstock [150], this theory is based on the understanding that a person will take a health-related action if that person feels that a negative health condition can be avoided, has a positive expectation that by taking a recommended action, they will avoid a negative health condition, and believes that they can successfully take a recommended health action.

Figure 2.9 shows the major elements of the HBM adapted from Nutbeam & Harris [131]. The major elements are comprised of the following elements:

- **Perceived susceptibility:** The subjective perception of the risk the individual is facing from a state or condition.
- **Perceived seriousness:** Subjective evaluation of the seriousness of the consequences associated with the state or condition.

- **Perceived benefits.** The subjectively understood positive benefits of taking a health action to offset a perceived threat. This perception will be influenced not only by specific proximal factors, but an individual's overall 'health motivation'.
- **Perceived barriers.** The perceived negatively valued aspects of taking the action, or overcoming anticipated barriers to taking it.
- **Perceived threat:** This combined quantum might be seen as indicative of the level of motivation an individual has to act to avoid a particular outcome.
- **Outcome/Expectations:** This may be seen as indicative of the extent to which the individual will try to take a given action.
- **Self-efficacy:** This refers to the belief in one's ability to execute a given behaviour

With regards to the context of the discussion of this thesis, similarities can be drawn between preventive healthcare behaviour and protective security behaviour. This can be further interpreted by looking at each domain where preventive healthcare refers to behaviours that will prolong an individual's healthy life or practices that otherwise lessen the effects of diseases [97] whereas protective security behaviour refers to behaviour that will reduce the risk and or impact of security incidents [130].

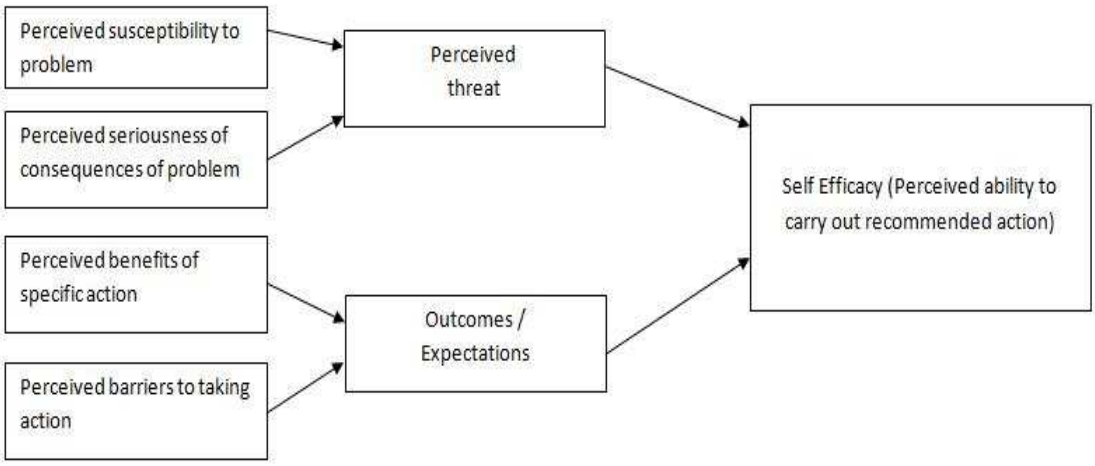


Figure 2.9: The Health Belief Model [131]

Both domains involved practicing preventive and protective behaviour to avert an unwanted situation. The success of preventive healthcare and security practices is seen in the non-occurrence of diseases (for preventive healthcare) and security incidents (for

security practices) respectively. The occurrence of diseases disrupts the normal functioning of one's body whereas the occurrence of security incidents disrupts the functioning of one's computer system and possibly affects the organisation. Practising preventive healthcare and security countermeasures both create inconvenience for the individuals in terms of extra effort.

The HBM has been applied in other diverse areas such as preventive behaviours against piracy threat [87] and emigration intention [80] which appears to have implications for work motivations as well as a broad range of human behaviours [186].

2.4.7 Protection Motivation Theory

The Protection Motivation Theory (PMT) was developed as a framework for understanding the impact of fear appeal [148]. The theory was based on the fear-drive model which proposed that fear acts as a driving force that motivates trial and error behaviour. In other words, if a communication evokes fear, then the recipient will be motivated to reduce this unpleasant emotional state.

The theory has been extended by Rogers [149] to provide a more general account of the impact of persuasive communications with an emphasis on the cognitive processes that mediate behaviour change. Figure 2.10 shows PMT framework and its major components. PMT includes three factors that explain how threats are perceived which is termed as threat appraisal factors. These threat appraisal factors are comprises of the following:

- **Vulnerability**: the extent to which the individual is perceived to be susceptible to threats.
- **Perceived severity**: the magnitude of threat
- **Rewards/benefits**: any intrinsic or extrinsic motivation for increasing or keeping the unwanted behaviour.

In addition, PMT also includes three factors that explain an individual's ability to cope with the threat which is termed as coping appraisal factors. These coping appraisal factors are comprises of the following:

- **Response efficacy**: the belief in the perceived benefits of the coping action by removing the threat.
- **Self-efficacy**: the degree that he or she believes it is possible to implement the protective behaviour.
- **Response cost**: to the individual in implementing the protective behaviour.

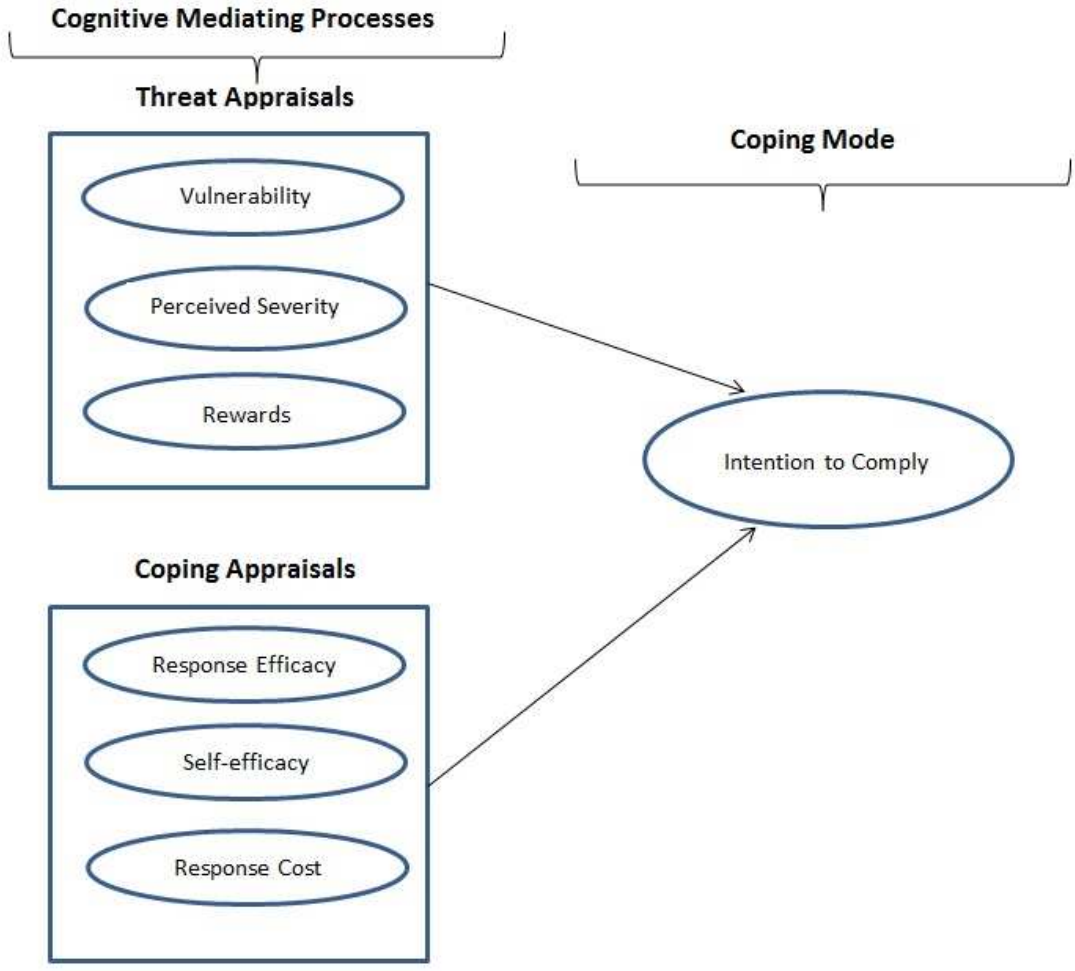


Figure 2.10: The Protection Motivation Theory [149]

Due to the general nature of this PMT, it has been applied across many domains particularly in health-related issues and recently information security as such in study by these following scholars [136, 90, 101]. Nevertheless, those studies did not focus on

all the components of the PMT but mainly on vulnerability and severity. This is probably due to this two components are more directly relevant to the outcome of compliance. However, recently Vance et al. [183] have extended the full PMT model to include habit (i.e.: measurement of past behaviour or behavioural frequency) as an antecedent effect. Their findings have indicated that habit is an important role in the context of employees' compliance with information security policies. As these studies provide some insight to the context of this thesis, there are however, some limitations to these studies in which particularly they have relied on the use of intention as dependent variable. Although measures of intention are widely accepted, it would be more realistic if the exact level of compliance is measured.

The following section continues the discussion looking into an example of persuasion practiced - known as Persuasive Technology.

2.5 An example of persuasion practice - Persuasive Technology (PT)

Persuasive technology (abbreviated hereafter as PT) has been introduced by Fogg [67] based on a set of practices which involved persuasion. PT suggested how computers[7] can motivate and influence users to behave in a desired way. Fogg [67] provides a framework which views the computer from three different perspectives of functionality: as a *tool*, *medium* and *social actor*.

A computer functions as a *tool*, giving humans the capability to do things they could not do before or make things easier for them. From another perspective, the computer is also viewed to function as a *medium*, conveying content in forms that can be easily interpreted by users, for example using symbols (i.e. text, graphs, icons) or sensory stimuli (i.e. real time video, simulations, virtual worlds). In many situations, computers are also regarded as *social actors*. This is especially true when computers are able to animate characteristics such as emotions and use voice communication, able to animate roles (i.e. assistant, opponent etc.) or follow certain social and dynamic rules such as greetings or apologies.

[7] The term computers here also refers to computer applications or computer systems and the like.

Figure 2.11 shows the overview of PT framework focusing on the three functionality elements, each with its own principles and attributes.

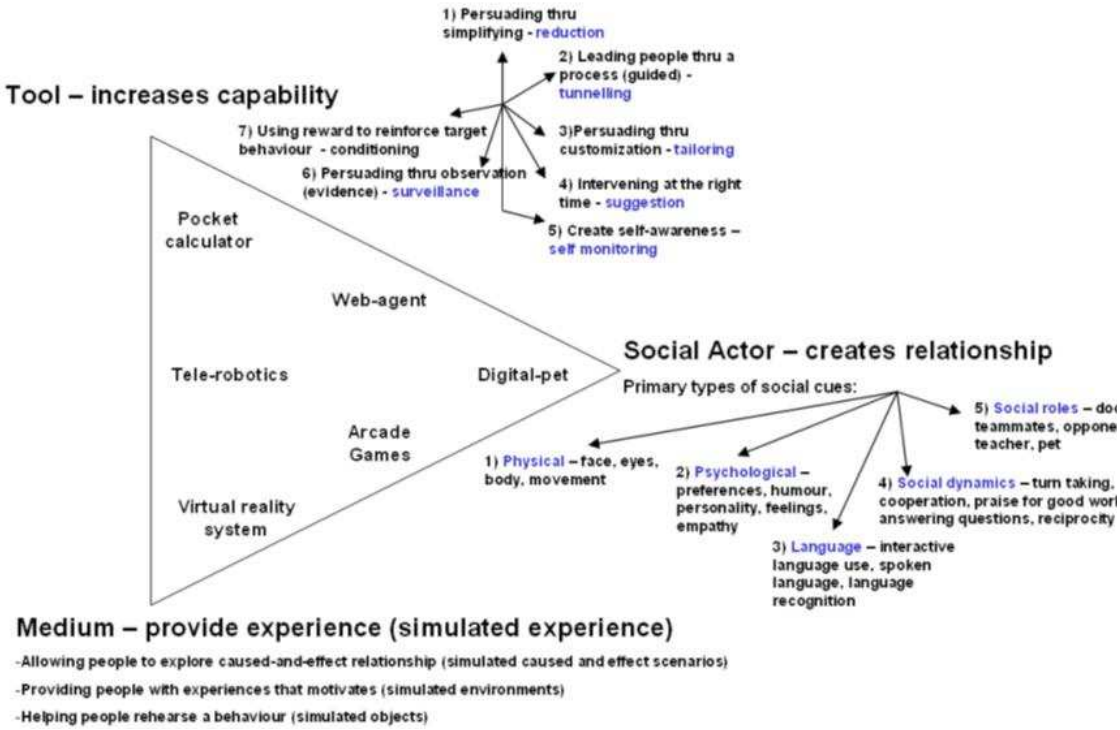


Figure 2.11: The Persuasive Technology framework [67]

However, the framework above does have its limitations. First, it does not provide an explanation of how the suggested principles should be applied for further implementation as actual system features, as this is crucial as a basis for developing computer applications or a system based on PT. It also seems challenging to view the three functions (tool, medium, social actor) separately as they tend to overlap one another.

At present, most researchers in the area of human-computer-persuasion have placed their focus on PT. Most arguments are thus based on the PT framework and its principles. While this area of knowledge is relatively new, it appears that researchers are adopting the suggested principles of PT without further argument; however, it is interesting to see further studies and experimental work being carried out to strengthen the existing theories.

2.6 Rationale/motivation for the selected persuasion strategies

In the previous sections, a review on related approaches, practices and theories of persuasion and attitude/behaviour change has been discussed including some comparisons made on their strengths and limitations. Based on the review, several persuasion strategies have been selected to be applied in the password guideline experiment.

The aim of the study is to investigate whether persuasion strategies can be applied to promote compliance behaviour among users towards password guidelines; thus, only appropriate strategies will be selected in order to suit the aim of the study.

There will be two main persuasion strategies involved in this study: appeal strategy and two of Cialdini's weapons of influence. Within the appeal strategy, we have chosen to adopt rational and emotional appeal. One of the rationales for choosing an appeal strategy is that the advertising literature has shown that this strategy is well known for its success in promoting goods and services to consumers [125]. The rational appeal focuses on providing logical and practical examples in order to persuade, while the emotional appeal focuses on involving audiences in real situations so as to trigger their feelings. Statistical evidence or published reports are usually used to support rational appeal presentations, while true stories or real cases are normally employed to support emotional appeals [152].

The second persuasion strategy is adopted from Cialdini's six weapons of influence, namely *reciprocation*, *commitment and consistency*, *social proof*, *liking*, *authority* and *scarcity*. Out of Cialdini's six weapons, only two will be used in this study, those of social proof and commitment & consistency. The principle of social proof states that humans determine what is correct by finding out what other people think is correct. This principle works best in two situations: uncertainty and similarity. If people are in an uncertain situation, they will find somebody to copy or have a tendency to follow what others have decided [42]. This principle postulates that the idea of being similar to others is also appealing, since deviation might indicate weirdness and this is obviously not favourable to most people [42]. On the other hand, the principle of commitment &

consistency states that once people make a decision or take a stand, they encounter personal or interpersonal pressures to behave consistently with that commitment, and that the best way to enforce this principle is by getting people to write down their commitment or make it known publicly.

As mentioned previously, the persuasion strategies act as a mechanism to maximise the effectiveness of the password guideline content. For that purpose, this study will utilise the rational appeal, emotional appeal and social proof principles to frame the rationale presented to users explaining to them why a good password is important. On the other hand, the commitment & consistency principle will be used in a slightly different way, whereby instead of providing rational argument, users are requested to formalise their commitment to comply to the password guidelines. This is aligned with the principle that humans will be more obligated to comply when they have stated their agreement and would therefore adhere to this commitment.

2.7 Individual differences in susceptibility to persuasion

It is interesting to learn from the attitude and behavioural theories discussed above that there will always be circumstances in which people will have a tendency to behave on the basis of factors other than attitude. According to Karlins & Abelson [103], there is ample evidence to indicate that the same appeal is received and acted upon differently by different listeners due to variations in their personality characteristics. Langer et al. [108] demonstrate individual differences in susceptibility to persuasion in a well-known "*copy-machine*" study. In these studies, the participants were tested with any of three appeals when a colleague attempted to approach a participant preparing to use a photocopier machine. The first appeal comes with no reason as such "*May I use the Xerox machine?*", the second appeal comes with a substantive reason "*May I use the Xerox machine because I'm in a rush*?", while the third appeal comes with a placebic reason such as "*May I use the Xerox machine because I have to make copies*?".

The results showed that the placebic reason was effective due to mindless conformity whereby the word "because" has made the participants assume that a good reason will follow. However, the study also revealed that not everyone complied with the placebic

reason and they suggested that individual differences are the factor that caused these differences. Furthermore, Perloff [141] also supports this claim by suggesting that certain people are more susceptible to persuasion strategies than others. In another study, Halko & Kientz [84] investigated the relationship between personality and persuasive technology principles with regards to health-promotion on mobile application domains. The results of their study are very promising and show that personality traits can be used as a method for adapting persuasive strategies to better fit the needs of users.

Although there are other determinants of security behaviour (i.e.: motivation, habit and prior knowledge), there are quite a number of studies that supports the idea of exploring personality as a determinant factor especially when its related to persuasion. There are few examples of studies that have shown some good reason to explore individual differences in relation to persuasion [84, 7, 164, 183]. However, a few questions need to be asked: are certain people more gullible than others? Should communicators take personality into account when devising messages? These questions are the ones typically asked when considering the role personality plays in persuasion. The next sub-section will discuss in general the review of individual personality studies focusing on the selected assessment framework known as the Big Five Inventory.

2.8 Individual personality study

All theories of personality assume that individual differences exist and that these differences can be measured. It is this assumption that is critical to the area of personality assessment. A personality assessment procedure is a way of gaining information about a person. More specifically, as Weiner & Greene [188] explain, personality assessment consists of procedures for identifying similarities and differences among people in their personal characteristics and capacities.

Personality assessment derives its purpose from the relevance of personality characteristics to making decisions in clinical, health-care, forensic, educational and organisational settings. It also contributes to treatment planning and outcome evaluation by identifying individuals' personality strengths and weaknesses, their adaptive

capacities and limitations, their preferred coping style, their underlying needs and concerns and their attitude toward themselves and other people. This information is commonly used to help clinicians formulate treatment goals in psychotherapy and implement strategies for achieving these goals [15].

Moreover, when psychologists began to conduct consultations, personality assessment started to emerge in other non-traditional clinical settings. Table 2.1 shows some examples of how personality assessment plays its role in other non-traditional clinical settings.

Table 2.1: Examples of personality assessment findings & their role in other non-traditional clinical settings

	Settings	Examples of use	Reference
(1)	Forensic	can be used as indications of mental impairment; can contribute to criminal cases into determinations of competence and sanity	Archer [6]
(2)	Civil cases	related to psychological dysfunction or incapacity; often relevant in adjudicating injury and disability claims.	Weiner [187]
(3)	Family Law	can be used to obtain information about personal qualities and psychological adjustment of children and their parents to decide the child's custody and visitation rights.	Budd [28]
(4)	Organisational	can prove useful in evaluating candidates for employment or promotion and test findings can help determine the fitness-for-duty of persons who have become psychologically impaired or who have behaved in ways that raise concern about their potential for being violent	Hough & Furnham [94]
(5)	Educational	can identify the need to provide counselling or special educational services for students with behavioural or learning problems.	Braden [21]

Looking deeper into personality studies, Burger [30] has classified personality theories into six major types, namely *psychoanalytic*, *traits*, *biological*, *humanistic*, *behavioural/social learning* and *cognitive*. The *psychoanalytic* theory was proposed by Sigmund Freud in the late 1800s and is based on behavioural observations. This theory

emphasises the concept of the conscious-unconscious mind in understanding human personality. Other theorists associated with these concepts were Carl Jung, who later invented the theory of psychological types, and Alfred Adler, who considered individual personality as hereditary behaviour [104].

The *trait* theory has been recognised as the most widely accepted approach in describing and predicting behaviour [29]. Factor analytic studies of human characteristics or traits produce a set of personality dimensions known as the "*Big Five*" or Five Factor where each personality trait is associated to human behaviour, represented by human responses to a specific situation [57]. For example, the Agreeableness trait represents a personality dimension that involves the more humane aspects of humanity. Characteristics such as compliance, altruism, nurturance and tender-mindedness describe one end of the dimension, whereas hostility, distrust, self-centredness and suspicion describe the other [59, 57].

The *biological* approach involves genetic influence and physiological processes in describing personality, whereas the *humanistic* approach identifies differences in behaviour based on personal responsibility and individual perception towards the environment [30]. On the other hand, the *behavioural/social learning* approach takes into account personality characteristics which are composed of individual learning experiences, gathered through observations of other people's behaviour [30]. Finally the *cognitive* theory focuses on cognitive structures or the way people process information and explains individual differences in personality.

In the study of personality, there are two main general approaches which are based either on "*trait*" or "*type*". Personality tests based on the trait approach tend to place individuals at various points on a number of scales, while type theory methods of assessing personality generally return a certain type which includes a spectrum of characteristics belonging to that individual. In simpler words, the "type" approach aims to classify individuals into distinct categories (i.e. this type or another), while the trait approach takes a continuous approach, where individuals can be anywhere within a continuum range (e.g. extraversion to introversion), with most people clustered in the

middle and fewer people towards the extremes. Nevertheless, according to Richard [147], there is not always a clear distinction between trait and type.

Furthermore, an important factor when considering the trait versus type discussion concerns how trait and type relate to personality theories. While personality types are usually derived from existing theories, traits are often identified using certain statistical processes and then the theories are developed around the observations in an attempt to explain the patterns of personality traits identified [26].

Several examples of personality frameworks which are most often used in research into computing and personality psychology domains are the *Cattell's Sixteen Personality Factor, the Eysenck Personality, the Myers Briggs Type Indicator (MBTI), the Keirsey Temperament Sorter (KTS)* and *the Big Five Model* [64, 142, 85].

2.8.1 The role of personality in CS/IT research

The inclusion of personality study as part of CS/IT research is not new. Most commonly, the personality study intends to provide more information on the human/user perspective in order to increase the effectiveness and efficiencies of the CS/IT related domain and applications. For example, work by Arteaga et al. [7] has focused on using the personality study to guide design in developing fitness programs on mobile applications to encourage obesity patients to adopt the technology. Another similar study has also been carried out by Halko & Kientz [84], which aimed to explore the relationship between personality and technology on health promoting mobile applications. Both studies have utilised the Big Five model as their personality framework and concluded that designers of technologies may achieve more success if applications consider an individual's personality type.

Personality study has also been involved quite frequently in computing-education research. According to Ahmed et al. [1], the learning pattern of students is influenced by personality types; individuals with different personality types have varying learning patterns. As a result, researchers have adopted various personality frameworks, mainly to examine the effect of students' personality traits to improve the effectiveness of their

learning styles. For example these studies [49, 161, 156] have utilised personality studies to help students to improve their learning ability of programming skills.

On a professional level, personality study helps to determine career preference and satisfaction. As Couger et al. [46] point out, computing professionals today are expected to have a broader range of skills compared to the past because they not only deal with technical issues, but also provide services to end users. Thus, personality study is commonly utilised to explore the personality attributes of computing professionals that are best suited to major computing subtasks, such as system analysis, system design and programming [177]. This will in turn result in a more positive and productive environment, both for the individual professionals and the organisations.

Quite recently, personality study has also received attention from information security scholars. Shropshire et al. [164] and Vance et al. [183] have considered the use of personality study in relation to information security. Shropshire et al. [164] attempts to investigate the differences between individuals who are most likely to pose security risks, and those who will likely follow most organisational policies and procedures. Meanwhile, Vance et al. [183] have focused on how differences between individuals will affect their habitual information security compliance. Both studies have utilised the Big Five model as their personality framework. Unfortunately, both studies seem to be at an early stage as no further results have been revealed. As personality study has shown encouraging results in exploring better understanding of human characteristics, this has led to the necessity for extensive research to be conducted in order to improve end users' information security compliance.

As mentioned previously, this thesis intends to explore further the differences in individuals' characteristics and their relationship with persuasion strategies to improve password guideline compliance. Thus the following sub-section will provide a general discussion on the selected individual personality assessment frameworks - the Big Five Inventory (abbreviated hereafter as BFI), also known as the Big Five Model. The BFI will be used as a framework for measuring personality characteristics in the study.

2.8.2 The Big Five Model

The Big Five is a taxonomy of personality comprising five broad personality traits; *Openness to experience*, *Conscientiousness*, *Extraversion*, *Agreeableness* and *Neuroticism*, and which is commonly known as "*OCEAN*". Some researchers use the label the *Five Factor Model* (FFM) instead of the Big Five. This is due to the fact that the term "Big Five", which was coined by Goldberg [74], was originally associated with studies of personality traits used in natural language while the term the "Five Factor Model" has been more commonly associated with studies of traits using personality questionnaires. In current practice, the two research terms are often used interchangeably.

According to McCrae & John [119], the taxonomy provides a structure that categorises dimensions of differences in human personality and was derived using factor analytic research based on *trait* theory. Factor analytic research refers to multiple studies that analyse the comprehensive set of natural-language terms used to describe an individual's personality, where replication of the studies identifies the five clusters of traits [100]. However, it is important to note that the big five are an empirically based phenomenon, not a theory of personality [166]. The following briefly describes the five personality traits:

1) ***Openness to experience*** – This trait features characteristics such as imagination and insight. Those high in this trait also tend to have a broad range of interests, whereas those at the opposite end of this spectrum usually show a lack of aesthetic sensibilities, preference for routine and favour conservative values [10].

2) ***Conscientiousness*** – Common features included in this dimension are high levels of thoughtfulness with good impulse control and goal-directed behaviours. Those high in conscientiousness tend to be organised and mindful of details, whereas low conscientiousness relates to negative traits such as being irresponsible, impulsive and disordered [59].

3) ***Extraversion*** – This trait considers characteristics such as excitability, sociability, talkativeness, assertiveness and high levels of emotional expressiveness. A person is considered an extravert if he/she feels comfortable in a social relationship, is friendly, assertive, active and outgoing.

4) ***Agreeableness*** – This personality dimension includes attributes such as trust, altruism, kindness, affection and other pro-social behaviours. People high on agreeableness tend to have positive traits such as cooperativeness, kindness, trust and warmth, whereas people low on agreeableness tend to be sceptical, selfish and hostile.

5) ***Neuroticism*** – This personality dimension considers traits related to experience of emotional instability, anxiety, moodiness, irritability and sadness. Someone low in neuroticism tends to appear calm, confident and secure, whereas a high level of neuroticism tends to be manifested as moody, anxious, nervous and insecure [59].

It is important however to take note that each of the five personality traits represents a range between two extremes. For example, extraversion represents a continuum between extreme extraversion and extreme introversion. Nevertheless, in the real world, most people lie somewhere in between the two polar ends of each dimension [188]. Table 2.2 briefly summarises each of the five traits along the continuum of the facets, i.e. more specific personality characteristic dimensions and includes possible interpretations of the facet scores.

Table 2.2: The Big Five personality traits, facets and possible interpretation along the dimensions of the facet scale (adapted from NEO-PI-R & NEO-FFI [188])

Domain	Facets	Facets Scale	Possible Interpretation
Openness	• Fantasy • Aesthetics • Feelings • Actions • Ideas • Values	High (T > 55)	Individuals have an active imagination and fantasy life. They are intrigued by the patterns they find in art and nature. They feel a wide range of emotions or feelings. They think that it is interesting to learn and develop new hobbies. They enjoy playing with theories or abstract ideas and solving problems or puzzles. They consider themselves to be broad-minded and tolerant of others' lifestyles.

		Low (T < 45)	Individuals try to keep all their thoughts directed along realistic lines and avoid flights of fancy. They are bored watching ballet or modern dance, and poetry has little effect on them. They rarely experience strong emotions and seldom pay attention to their feelings of the moment. They find philosophical arguments boring and sometimes lose interest when people talk about abstract, theoretical matters. They believe that letting students hear controversial speakers only confuses and misleads them.
Conscientiousness	• Competence • Order • Dutifulness • Achievement striving • Self-discipline • Deliberation	High (T > 55)	Individuals are competent and known for their prudence and common sense. They like to keep everything in its place so they know just where it is. They try to perform all the tasks assigned to them conscientiously. They have a clear set of goals and work hard to accomplish them in an orderly fashion. They think things through and always consider the consequences before making a decision or taking action.
		Low (T < 45)	Individuals often come into situations without being fully prepared and do not seem to be completely successful at anything. They are not very methodical and never seem to get organised. They are not as dependable or reliable as they should be. They are easy-going, lackadaisical and do not feel driven to get ahead. They have trouble making themselves do what they should do and waste a lot of time before settling down to work. They often do things on the spur of the moment and do not think things through before coming to a decision or taking action.
Extraversion	• Warmth • Gregariousness • Assertiveness • Activity • Excitement-seeking • Positive emotions	High (T > 55)	Individuals are known as warm, friendly people who enjoy talking to others. They like to have a lot of people around them and enjoy parties with lots of people. They are dominant, forceful and assertive and are often leaders of groups to which they belong. They often crave excitement and like to be where the action is. They are cheerful, high-spirited persons who laugh easily.
		Low (T < 45)	Individuals do not get much pressure from chatting with people and they do not take a personal interest in the people with whom they work. They shy away from crowds of people and

			usually prefer to do things alone. They sometimes fail to assert themselves as much as they should and usually let others do the talking. They are not as quick and lively as other people and their work is likely to be slow and steady. They seldom crave excitement and they do not like to be where the action is. They are not cheerful optimists and do not consider themselves especially light-hearted.
Agreeableness	• Trust • Straightforwardness • Altruism • Compliance • Modesty • Tender-mindedness	High (T > 55)	Individuals believe that most people are basically well-intentioned, honest and trustworthy. They are not crafty or sly and could not deceive anyone even if they wanted to. They try to be courteous, thoughtful and considerate. Most people they know like them. They would rather cooperate with others than compete with them. They try to be humble and would rather not talk about themselves and their achievements. They believe that all human beings are worthy of respect and can never do too much for the poor and elderly.
		Low (T < 45)	Individuals tend to be cynical and sceptical of other's intentions and believe that most people will take advantage of them if they let them. They are willing to manipulate people to get what they need and sometimes trick people into doing what they want. They are thought to be selfish, egotistical, cold and stubborn and can be sarcastic and cutting when they need to be. They do not mind bragging about their talents and accomplishments.
Neuroticism	• Anxiety • Angry hostility • Depression • Self-consciousness • Impulsiveness • Vulnerability	High (T > 55)	Individuals often feel tense, jittery, anxious and easily frightened. They are easily embarrassed, self-conscious and feel inferior around other people. They feel sad, blue and depressed and sometimes experience a deep sense of guilt and sinfulness. Individuals often get angry and mad and they are known as being hot blooded and quick tempered. They sometimes do things on impulse that they later regret and often give in to their impulses. They feel helpless, unstable emotionally, and sometimes feel like they are going to pieces.
		Low (T < 45)	Individuals do not worry and rarely feel fearful or anxious. They are even tempered and it takes a lot to get

			them mad. They rarely feel lonely, sad or depressed. They are comfortable around other people. They rarely overindulge and seldom give in to impulses, craving or temptation. They can handle themselves pretty well in a crisis or emergency.

There are various instruments which have been developed to measure personality using the big-five traits. One of the most commonly used in research is the Big Five Inventory (BFI), introduced by Oliver P. John [99]. The BFI is a self-report inventory designed to measure the Big Five dimensions. It contains 44 items (in total) which consist of short phrases with relatively accessible vocabulary (Appendix A (iii)). A shorter version of the BFI construct, consisting of only ten items, was developed by Gosling et al. [76]; however, there is substantial measurement tradeoffs associated with using such a short instrument [146]. A major advantage of the BFI over other personality frameworks is that no permission is required to use it for non-commercial research [166] and this has contributed to its popularity in many studies across several domain areas.

In addition to the BFI, there are several other options for measuring the Big Five. For example, the NEO Personality Inventory (NEO-PI) is one of the instruments that is well accepted, widely assessed and extensively used to measure the big five personality dimensions [27]. The word NEO originates from the three domain scales measuring Neuroticism (N), Extraversion (E) and Openness (O), to which, several years later, two more scales, Agreeableness (A) and Conscientiousness (C), were added in a revised model known as NEO-PI-R [45]. The NEO-PI-R contains a 240 item inventory measuring not only the Big Five but also six facets, i.e. more specific personality characteristics of each of the Big Five. However, unlike the BFI, NEO-PI-R is a commercial product, controlled by a for-profit corporation that expects people to get permission and in many cases pay to use it. Costa & McCrae [45] have also developed a shorter version of NEO-PI-R containing 60 items, known as NEO-FFI, which only measures the five factors [3].

Another alternative for measuring the Big Five, which uses single adjectives rather than full sentences (like the NEO's versions) or short phrases (like the BFI), is Goldberg's set of 100 trait-descriptive adjectives [74]. Two years later, Saucier [158] reduced the

100 sets to 40 items known as the 40 Big Five Mini Markers. More recently, Saucier [158] developed new trait marker sets which maximise the orthogonality of the factors, and which are available in the public domain.

2.8.3 The rationale for the Big Five Model

In general, the MBTI and the Big Five model were found to be the most commonly used in many studies, especially those involving the health, business and educational domains [128, 142, 84]. Although MBTI has been reported as one of the most popular instruments to measure individual personality for non-psychiatric populations, there has been some criticism of the reliability and the validity of this instrument for not having a bimodal distribution in terms of its statistical structure, which in turn may result in any data distortion causing serious psychometric shortcomings [118]. The use of MBTI as an instrument not only requires someone who has strong a foundation or relevant background in psychology, such as licensed counsellors, psychologists, college instructors or personnel, but also involves additional cost as the instrument is a licensed product which incurs charges for any type of use.

On the other hand, the Big Five model has been regarded by personality psychologists as the predominant taxonomy of personality [45, 29]. Moreover, there seems to be raising consensus among personality researchers that this Big Five model is generally accepted as an adequate representative of broad trait dimensions of human personality attributes [10]. Furthermore, there are various instruments which have been developed to measure personality using the big five traits, and the most commonly used in many research studies is the *Big Five Inventory* (BFI). In contrast to the MBTI and other personality frameworks, no permission is required to use it for non-commercial research and this has contributed to its popularity in many studies across several domain areas [166].

Therefore, in this research, the Big Five Inventory (BFI) will be utilised as the framework to measure the individual's personality due to its comprehensive nature and its ability to capture basic temperament and dispositional factors relevant to our study.

Its advantages over other personality frameworks were also considered in making the decision.

2.9 Summary

This chapter mainly provides the literature review work to support the password guidelines experiment which will be presented and discussed thoroughly in the following chapter. This chapter has started with presenting the persuasion approaches from the literature of social psychology which will be utilised in improving password guideline compliance. The discussion has included the fundamental idea of persuasion, its elements and the expected effects. It is then followed by more discussion on several relevant theories related to changing attitudes and behaviour which lead to persuasion. The discussion included relevant existing work that has been carried out by other researchers.

This chapter has also identified several persuasion strategies that will be applied in this password guidelines study and a rationale for these choices was included. The outcome of this chapter has also led to the discovery that the persuasion domain is very closely related to individual difference factors. In other words, an individual's personality might cause an impact on the outcome of the persuasion attempt. Thus, this thesis intends to broaden the persuasion approach by combining it with personality studies. In addition, since the persuasion approach is fairly new to the area of information security, it is interesting to explore this intriguing idea of how an individual's personality characteristics can be used in conjunction with the right persuasion strategy to improve password guideline compliance.

The discussion in this chapter also proceeds to elaborate on the literature of personality studies; specifically, the focus will be directed towards the study of personality assessment, which is used to evaluate an individual's personality characteristics. The *Big Five Inventory* (BFI) has been selected as an instrument to measure the personalities of the participants in our study. The rationale for this choice is also included in this chapter as being due to its comprehensive nature and its ability to capture basic temperament and dispositional factors relevant to our study.

With the review work on both persuasion and personality study elaborated and discussed in detailed, the next chapter will elaborate on the password guideline study, whereby a control-laboratory experiment was conducted. The experiment was meant to evaluate several persuasion strategies applied in presenting the content information of the password guidelines. Personality assessment will also be employed during the experiment to investigate its relationship with the persuasion strategy. Ultimately, the experiment intends to evaluate how to utilise persuasion strategies and personality study to improve compliance behaviour with password guidelines.

CHAPTER 3

UTILISING PERSUASION APPROACHES & PERSONALITY STUDY TO IMPROVE COMPLIANCE BEHAVIOUR WITH PASSWORD GUIDELINES

CHAPTER 3: UTILISING PERSUASION APPROACHES & PERSONALITY STUDY TO IMPROVE COMPLIANCE BEHAVIOUR WITH PASSWORD GUIDELINES

CHAPTER 3

UTILISING PERSUASION APPROACHES & PERSONALITY STUDY TO IMPROVE COMPLIANCE BEHAVIOUR WITH PASSWORD GUIDELINES

3.1 Introduction

This chapter brings together the two main ideas of utilising persuasion approaches and personality study to improve compliance behaviour with password guidelines. As described in Chapter 1, the human factor problem, particularly in the information security domain, has not been fully understood as it is complex and complicated. Thus, this study aims to explore two main avenues – persuasion approaches in combination with personality study - in order to broaden understanding of complex human behaviours, particularly focusing on password guidelines.

Initially, this chapter introduces the motivation of focusing the study on password guideline domains. A controlled-laboratory experiment has been carried out as a mechanism to evaluate the proposed idea. In the experiment, two persuasion approaches - the appeal strategy and Cialdini's weapons of influence [41] - were chosen for further evaluation. In addition, the Big Five Inventory (BFI) [100] was chosen as the personality framework. Rationales for these choices have been discussed in previous chapters.

The experimental design, procedures and measurements involved will be detailed. Then the findings will be discussed, focusing on the impact of the adopted approaches on improving users' compliance behavioural issues.

3.2 Password guidelines compliance study - Motivation of the focus

Password based authentication remains the most commonly used authentication mechanism, in spite of the rapid introduction of several other authentication mechanisms such as smart cards, graphical passwords, USB tokens and biometrics [34]. Unfortunately, the weakness of the password system is not in the system itself but the human behaviours and practices of dealing with the password.

Typically, end users rely on a set of rules known as password guidelines, to which users must adhere when choosing a password. A password guideline mainly contains specific requirements on how a password should be composed. For example, the password must contain a minimum number of characters that must include uppercase letters or numbers and should not include words from the dictionary. There exist various types of password guidelines; however, there is consensus in the literature that well written password guidelines can provide increased security to the organisations [34, 169].

Unfortunately, few studies have focused on the construction of password guidelines. As pointed out by Komanduri et al. [106], there is lack of empirical data on passwords and the guidelines under which they were created. For instance, the NIST guidelines [32] which are used to design password composition policies are based on theoretical estimates, while several other guidelines, such as in Proctor et al. [145] and Vu et al. [185] are based on a very small-scale laboratory studies.

Nevertheless, the content of password guidelines is important in providing suggestions to users on how to carry out security tasks such as creating good passwords. A recent study by Grawmeyer & Johnson [78] investigated users' password generation behaviour and revealed that users tried to match the perceived security level of the service to the estimated security level of the password. Surprisingly, all the passwords estimated as highly secure (i.e. uncrackable), and most passwords regarded as secure (i.e. hard to crack) were in fact insecure passwords that contained a single word. Additionally, most of the passwords which were estimated as fairly secure (i.e. hard to crack) were passwords that included common words or names. This finding has drawn the authors to

suggest that password guidelines contained in security policies should be devised in order to avoid misconception among users.

Herley [91] investigated the reason behind the rejection by users of security advice. By making comparisons between potential and actual benefits of security messages, it is concluded that most security advice is rejected by users due to the fact that it offers a poor cost-benefit trade-off. This is due to user's perception of security advice as a burden; while the benefits of compliance with the advice are not necessarily evident (i.e. users do not appreciate their act of compliance unless they eventually become victims themselves).

Findings from existing studies seem to indicate that users are not convinced that such suggestions given in the guidelines are extremely important. This was indirectly pointed out in recent studies by Shay et al. [162], where, in spite of users' awareness, they were not deterred from continuing password practice that might put them at risk such as using dictionary words and names and sharing and reusing passwords. This study also confirms findings from previous studies [25, 191] where users were also found to practise poor password habits, such as using names and birth dates to construct their passwords and using the same password across multiple accounts.

Forget et al. [68] introduced the "persuasive text password" which integrates five of Fogg's seven persuasive technology principles [67]. In the persuasive text password system, the users are allowed to choose their preferred password which is generated by the system by clicking the *shuffle* button. The researchers claimed that their proposed system was able to improve security while maintaining usability and at the same time persuading users to generate better passwords [68]. However, sufficient empirical evidence through user studies has yet to be obtained to support the researchers' opinion that the shuffle option in the system is indeed a persuasive rather than a coercive tool.

Protection Motivation Theory (PMT) has predominantly been applied to motivate secure compliance behaviour, as reported by these studies [199, 90]. Among the five elements in the PMT constructs, the fear element has been studied quite frequently. For example, Weirich & Sasse [190] proposed the use of fear appeal in order to motivate

password behaviour compliance. They highlighted that, in order for fear appeal to work, changes to existing password guidelines are necessary to include the idea that punishment is being enforced by organisations and no misbehaviour will go unnoticed. Xu et al. [196] proposed threats (e.g. spyware attacks) as the fear elements to arouse users' attention to motivate compliance behaviour. Although fear elements may result in changes in attitudes or behaviour, their effectiveness is still questionable over longer periods of time, especially when punishment is associated. A punishment regime is seen as a coercive mechanism which may result in rebellion once the end-users realise that surveillance is no longer being enforced.

Therefore, this study aims to investigate ways to improve the content of password guidelines. It is posited here that password guidelines should include rationales as to why creating good (strong) passwords is important for users. Providing a rationale will increase the likelihood of compliance to a certain request [42]. This is especially lacking with the existing password guidelines, which focus more on providing information on how to compose a good password. In conjunction with the inclusion of a rationale in the password guidelines, this study attempts to utilise two persuasion approaches: appeal strategy and two of the Cialdini's weapon's of influence, to increase the likelihood of compliance.

Furthermore, the literature also suggests that, in an attempt to persuade, the persuader is more likely to succeed if more information about the audience is known [20, 141]. This has brought this study to consider including an individual's personality construct (i.e. the Big Five Inventory) as a mechanism to categorise the users into several personality traits. Generally, in order to guide this study, several research questions were formulated. This study seeks to discover the following:

1) Will users create better passwords when a rationale (i.e. an explanation of why creating good passwords is important) is included in the password guidelines?
2) Which persuasion strategies are more likely to result in influencing users to create better passwords?
3) Are there any personality trait(s) that are more likely to produce better passwords than others?

4) Is there any significant relationship between the personality traits and the persuasion strategies applied?

The next section describes the controlled experimental study which was conducted to evaluate the chosen approaches.

3.3 The experimental study – password guidelines

A controlled laboratory experiment was carried out to investigate the research questions of this study. The first part of the study focuses on the users' behaviour in creating good passwords when password guidelines include a rationale. Therefore, the first hypothesis is as follows:

$H_{1:}$ *Users will create better passwords when they are exposed to password guidelines which include a rationale, compared to password guidelines without.*

Secondly, whilst the rationale included in the password guidelines was framed using selected persuasion approaches, it is interesting to see whether there is any significant difference between the approaches applied. Although persuasion approaches are quite commonly used in other fields, such as education and health, there are limited examples of such applications to information security, particularly to the passwords domain. We intend to measure the difference in terms of the mean password strength created in each persuasion group in comparison with the control group. Hence, an assumption is that:

$H_{2:}$ *Users will create better passwords when they are exposed to password guidelines which are framed using persuasion approaches compared to the standard password guidelines.*

This study also includes the personality framework (i.e. the Big Five Inventory); therefore, it is interesting to explore whether there exists any relationship between the individual personality attributes and the effectiveness of persuasion approaches. The effectiveness of the persuasion approaches is measured directly by the passwords the

users produced during the experiment. Therefore, the assumption made in relation to this is that:

$H_{3:}$ *There exists a relationship between personality attributes and the password strength produced by the persuasion approaches groups.*

Furthermore, this study attempts to explore whether personality has any effect on the effectiveness of persuasion approaches. As discussed in the review in Chapter 2, much research has been done in the psychological sciences on personality, and there is much debate within psychology as to the appropriate theories and models. In addition, the science of personality assessment has not been applied to this area of persuasion and security before. Consequently, it is difficult to make strong predictions as to the effects of personality variables on password strength; however, it is possible to imagine certain relationships. For example, one of the five traits from the BFI is the agreeableness trait. People with the agreeableness trait tend to cooperate with others in most situations. In this example then, it might be the case that there will be some effect with the persuasion approaches applied.

However, it is difficult to make specific assumptions at this stage as there could be many possible outcomes upon which personality traits would be more impactful. A more exploratory stance is therefore adopted in this study, looking after the fact for significant effects. The following sub-sections describe the experimental design, procedures and measurements that have been carried out to investigate the above hypotheses.

3.3.1 The experimental design

The experiment used the between-subject design, where each participant is exposed to only one of the experimental conditions. The independent variable of this experiment is the persuasive approaches, while the dependent variable is the strength of the password created by the participants. There will be one control group (no inducement) and four experimental groups as follows:

1) Rational appeal group
2) Emotional appeal group
3) Social proof group
4) Commitment & consistencies group (C&C)

3.3.2 The experimental apparatus

The apparatus used in this experiment are as follows; the BFI – 44 questions of personality test [99], the instructions set, the five password guidelines for the experimental groups (including the control group), a password login prototype, and a set of questionnaires. All the experimental apparatus are included in the section Appendix A.

The BFI personality test questions were administered manually where participants were given the 44 listed questions on a sheet of paper. The answer options were in the form of a 5 point likert-scale which is from (1) *strongly disagree* up to (5) *strongly agree*. The participants were given sufficient time to complete the questions by marking of the appropriate choice of options in the allocated boxes. The average time taken by the participants to complete the personality test was approximately 15 minutes.

The instructions sets were uniform across all participants; everyone received the same instructions and was informed that the Information System & Services Department of the university wanted all the students to create a new login account to replace the existing one. The instructions were typed on a piece of paper with a slightly larger font (i.e. 16 font *Times New Roman*) to make it clear and readable to participants.

The password guideline sets which were distributed to the participants vary according to the group to which they were assigned. The participants in the rational, emotional and social proof groups received a short paragraph of persuasive arguments informing them of why creating good passwords is important, in addition to the standard NIST password guidelines. The persuasive argument for the rational group was framed using logical reasoning by providing relevant examples such as the fact that the variety of usable characters in the passwords will significantly increase the difficulty in hacking

the passwords. The persuasive argument for the emotional group was framed by attempting to invoke the participants' emotions; this was achieved by giving examples of real hacking incidents which resulted in the passwords being compromised due to weakness. The persuasive argument for the social proof group was framed by attempting to associate the participants with the current scenario of popular social networking sites (e.g. Facebook) where passwords being compromised could not only jeopardise important personal accounts but also reputation among friends as the hackers are able to take charge of their profile in the social networking sites.

Slightly different from the first three experimental groups, the participants in the commitment and consistency group did not receive a persuasive argument informing them why creating a good password is important; instead, they received a recommendation statement to request them to create a strong password as it is very important to ensure compliance behaviour is met. The participants in this group were then requested to formalise their agreement (i.e. to create strong password) by signing in the commitment page. Furthermore, the participants were told that the commitment page would be handed to and reviewed by the ISS departmental staff. Finally, the participants in the control group only received the standard NIST password guidelines similar to those received by the participants from other groups and nothing else. The standard NIST password guidelines are as follows:

The way to set a password:

- Password does not contain all or part of the user's account name
- Password is at least 8 characters long
- Password is not "password" or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$"*etc.)

Figure 3.1: The standard NIST password guidelines

The participants were shown a simple prototype of a login page for them to enter their username and password. At the beginning of the experiment, the participants were given

an ID number and were told to use it as their username. The interfaces of the login prototype are as illustrated in Appendix A.

The last apparatus involved in the experiment is the set of questionnaires containing several questions on demographic details of the participants and also some questions related to password constructions and usage. The questionnaires can be referred to in Appendix A.

3.3.3 The experimental measurements

There are several measurements involved in the experiment: password strength, password compliance and the BFI test personality scores. The password strength was measured using a combination of several important attributes that constitute a particular password, such as length (i.e. characters), the frequency of uppercase, lowercase, alphabetic characters, numerical characters and alphanumeric characters (e.g.: @, #, !, etc.). A tool known as the "*Password Meter*" is adopted in this study to measure password strength [178].

The password strength is calculated by adding points (+) if the password exhibits certain required attributes and deducting (-) points if the password fails to exhibit certain attributes. The score given is in the form of percentages, where the maximum will be 100%. The passwords will be categorised as weak, acceptable and strong according to the following scores; ($\leq$ 30%), (30% $\leq$ x $\leq$ 60%) and ($\geq$ 60%) respectively [178]. The formula used to measure the score of the passwords can be referred to in Appendix A.

The next element that was also measured in this experiment is the password compliance. It is basically refers to how close each participant follows the requirements given in the password guidelines. Therefore, each requirement was allocated some points accordingly to indicate the total score of compliance for each of the password created by participants. The schematic calculations for the points can be referred to in Appendix A. In general, the required score to indicate the compliance level is 30 points, which means any point below 30 (i.e.: <30) will indicate non-compliance condition.

Another item that is also measured in the study is the personality traits of the participants. As mentioned previously, the personality framework chosen for this experiment is the BFI (refer to rationale of choice in section 2.8.3 in Chapter 2). The BFI personality test contains forty-four statement items where participants respond to each of the statements using a 5-point likert scale, (1) being *Strongly Disagree* and (5) being *Strongly Agree*. The participants' aggregated responses are used to determine a participant's overall weighting on each of the five BFI personality traits. The scores are then converted into percentages and categorised according to low and high category [117]. The scores used to form the categories can be referred to as depicted in Table 2.2 in Chapter 2.

3.3.4 The experimental procedures

At the beginning of the experiment, all participants were given a unique id number. This id number automatically placed them randomly into one of the five experimental groups. They were given a brief introductory session to sign the consent form and supply demographic details. Then, each participant was administered the BFI personality test. Once they had completed this, they were requested to submit the completed questionnaire to the experimenter. For those participants who were interested in knowing their personality test results, an email address was requested. Next, each participant was given the following experimental scenario. Participants were told that the ISS (Information System & Services) Department of the university wanted all students to create a new login account to replace the existing one. This new login account would provide access to important online services including university email, course registration, access to their personal data storage and many others.

Following the experimental scenario, all participants were given a standard NIST password guideline. The first three experimental groups were exposed to the rationale (i.e. why a good password is important) which was framed based on different persuasion approaches, according to the experimental group to which they had been assigned earlier (i.e. rational appeal group, emotional appeal group or social proof group). The fourth experimental group was exposed to a slightly different persuasion approach; instead of exposing the participants in this group to the rationale, they were

requested to sign a commitment as a way of formalising their dedication once they had agreed to use a good password for their account. They were also told that the commitment they had signed would be kept by ISS staff for records. In the control group, participants were only given the standard NIST password guidelines and nothing else. All the materials given to the participants in this experiment are in Appendix A.

Participants were then asked to create a password for their university login account. Information on the frequency of character types that constitute each participant's invented password was collected. For example, if the password was p@ssword123, the data collected would have been: 7 lower case letters, 3 numbers, 1 special character and 11 as the length. The participants were requested to log in immediately after the account had been created. Next, each participant was given a mini-jigsaw puzzle to complete. This puzzle took about 13 – 15 minutes to complete. Once they had completed the puzzle, they were requested to log in once again using the password they had just created to ensure that they do not simply type-in any random characters for their password and do not have any intention to memorise them after the initial login. Finally, the participants were asked to fill in short questionnaires on some related to password usage and creation including tendency to memorise their password within short-term (in one week time) and longer term (in one month time). Participants signed the remuneration form before leaving the experimental room where each participant was rewarded £5 for their time and effort in participating.

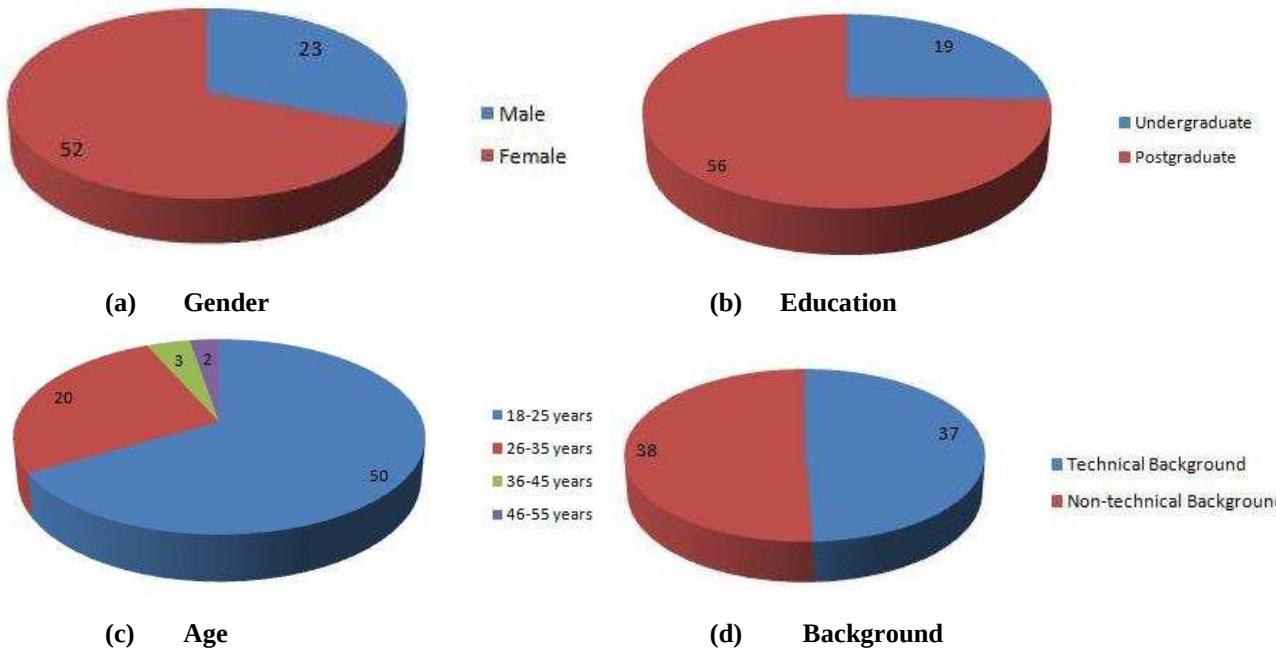
3.4 The results & analysis

The following sub-sections will continue with presenting the results and the analysis of the experiment.

3.4.1 The demographic details

Seventy five participants took part in the experiment in total, of which 31% were male. More than half of the participants (67%) who took part were aged between 18 – 25 years old, of whom about 75% were post-graduate students. The participants were almost equally divided in terms of technical and non technical background; 49% and

51% respectively. Participants in the technical category included university students from science and engineering, while the non-technical category came from business and social sciences. In terms of the number of years using the computers (Internet), more than half of them (67%) have more than 10 years of experience. Figure 3.2 illustrates the demographic details of the participants involved in the experiment.



(a) Gender **(b) Education**

(c) Age **(d) Background**

Figure 3.2: Participants demographic details

3.4.2 The password analysis

The password created by all the participants from the five experimental groups will be examined according to several factors (i.e.: compliance, strength, length, unique characters used and number of different character sets) as summarised in Table 3.1 below.

Table 3.1: Mean and (standard deviation) of several password elements analysed according to the five experimental groups

Groups/ Passwords Factors	Password Strength	Password Compliance	Length	Unique Characters Used	Number of Different Character Sets
Rational	79.93 (18.39)	32.87 (4.03)	9.80 (1.52)	8.40 (1.29)	3.40 (0.63)
Emotional	85.67 (17.01)	35.0 (4.80)	10.33 (1.99)	8.33 (1.68)	3.53 (0.63)
Social proof	85.80 (19.80)	33.93 (3.73)	11.27 (2.63)	8.87 (2.03)	3.13 (0.52)

Commitment & Consistencies	74.33 (20.94)	31.73 (4.50)	10.40 (2.27)	8.40 (1.68)	2.87 (0.74)
Control	63.27 (27.85)	30.87 (5.96)	9.87 (1.92)	8.00 (1.85)	2.80 (1.01)

**In each cell – The mean of password factors scores followed by the standard deviation in brackets.*

Meanwhile, Table 3.2 reports on the One-way ANOVA test on all the password elements analysed.

Table 3.2: The results for One-way ANOVA of all the password elements analysed

Groups/ Passwords Factors	Password Score	Password Compliance	Length	Unique Characters Used	Number of Different Character Sets
One-way ANOVA	F=2.97, **p-value=0.025**	F=1.89, p-value=0.12	F=1.24 p-value=0.30	F=0.48 p-value=0.749	F=2.91 **p-value=0.027**

**The items in bold shows the p-value for statistically significant difference detected*

The results of password compliance have shown that all the experimental groups including the control group have reached the mean compliance score above 30 points which indicates that in general majority of the participants in this experiment have complied with the requirements given in the password guidelines. This can be seen from Table 3.1 whereby the highest compliance mean score was seen to be coming from the emotional group (35.0) followed by the social proof group (33.93) while the lowest mean score comes from the control group (30.87). However, there was no significance difference detected with One-way ANOVA test (F=1.89, p-value=0.12) which seems to indicate that the persuasion strategies applied did not have much of an effect on compliance level among participants in this study.

Looking further into the passwords created by the participants, the results of their password strength have shown that the social proof group has the highest mean (85.80) followed by the emotional group (85.67), with the lowest being the control group (63.27). The results were further analysed using One-way ANOVA and the results reveal a significant difference across the five conditions (F=2.97, p-value=0.025). This indicates that participants create stronger passwords when they receive guidelines with persuasive rationales, compared to passwords without persuasive rationales included in the guidelines. However, further tests are required to identify which of the various

approaches applied is the most effective. A Tukey post hoc test was conducted to examine this question. The Tukey test revealed with 95% confidence intervals, that the social proof and emotional groups are significantly different from the rest of the groups, indicating that more participants are persuaded with these two approaches compared to the others.

Moreover, the passwords constructed by the participants from the social proof and emotional groups, 67% of both groups had passwords that were categorised as very strong passwords (password score ≥ 80%). However, participants in the social proof group constructed much better passwords than the emotional group when comparing each element that contributed to the password score (i.e. length, unique characters used, number of different character sets). As can be seen from Table 3.1 above, the mean for all the elements mentioned above was higher for the social proof group compared to the emotional group. Moreover, approximately 40% of passwords constructed in the social proof group had a perfect score (i.e. 100%) compared to only 27% in the emotional group.

The One-Way ANOVA test was also conducted towards other password elements as well as reported in Table 3.2 above. Based on the results displayed on that table, two elements of the passwords that are length and unique characters used indicated no significant difference – however, there was a statistically significant difference detected for the number of different characters sets used by the participants to construct their password which indicates a supporting factors for the significant effect detected in the password strength.

This password guidelines experiment was also interested in looking into the memorability aspects. Participants were asked on the tendency for them to remember their password based on short-term and long-term period. The tendency was measured according to the likelihood scale as follows: (1 – very likely, 2 – likely, 3 - neither likely nor unlikely, 4 – unlikely and 5 – very unlikely). The results are as shown in the following Table 3.3.

Table 3.3 Mean and (standard deviation) for memorability aspects of the passwords constructed

Groups/ Passwords Factors	Short-term (1 week)	Long-term (1 month)
Rational	1.67 (0.62)	2.20 (1.01)
Emotional	1.33 (0.49)	2.07 (0.88)
Social proof	1.60 (0.73)	2.60 (0.91)
Commitment & Consistencies	1.2 (0.41)	1.93 (0.79)
Control	1.60 (0.91)	2.53 (1.25)

**In each cell – The mean of likelihood to memorise the password followed by the standard deviation in brackets.*

Based on Table 3.3 above, the results seems to indicate that majority of the participants have a very high tendency to remember their password over one week period of time. However, as time goes by, the memorability seems to reduce slightly as can be seen from the overall mean scores for the long term memorability of the passwords have shown an increased in value comparatively. A One-Way ANOVA test has also been conducted towards this memorability aspects for both short and long term period of time and the results however have detected no significant difference for both as follows ($F = 1.42$, p-value = 0.24) and ($F = 1.31$, p-value = 0.27) respectively. Nevertheless, these results were only based on likelihood to remember their constructed passwords and further experimental procedure will have to be conducted to confirm whether participants can actually succeed in login to their accounts within certain lapse period of time.

3.4.3 The combination of passwords & personality analysis

In this sub-section, the analysis is extended towards examining passwords constructed by the participants from all experimental groups in relation to their personality test scores. Thus, Table 3.4 displays the percentages of participants, arranged according to two categories of scores for each of the BFI traits (i.e. low and high).

Since the personality construct (i.e. the BFI) used in the study comes from the trait approach, individuals fall in between the continuum range, from one extreme point to another opposite point. The above results can be interpreted as such that the participants in this study fall in between a continuum range that is for example in between extraversion to introversion. Although in principle majority of participants clustering in

the medium category with fewer people towards the extremes, but in this analysis we are focusing more towards the extreme lows and highs.

Table 3.4: Percentages of participants, mean of password scores and mean of compliance scores for two categories of personality test scores

BFI Traits / Groups	Openness (O)					
	Low			High		
	(%) participants	Mean passwords strength	Mean compliance	(%) participants	Mean passwords strength	Mean Compliance
Rational	40	87.83	34.0	60	74.67	32.11
Emotional	60	87.2	35.44	40	83.33	34.33
Social proof	80	92.83	34.5	20	57.67	31.67
C & C	73.3	75.82	31.82	26.67	70.25	31.5
Control	46.67	63.71	31.43	53.33	62.88	30.38
(N = 75)	**60**	**81.48**	**33.44**	**40**	**69.76**	**32.0**
BFI Traits / Groups	**Conscientiousness (C)**					
	Low			**High**		
	(%) participants	**Mean passwords strength**	**Mean compliance**	**(%) participants**	**Mean passwords strength**	**Mean compliance**
Rational	33.33	87.21	33.6	66.67	76.3	32.5
Emotional	40	82	32.0	60	87.5	36.5
Social proof	46.67	88.43	35.86	53.33	83.5	32.25
C & C	66.67	72.9	32.4	33.33	77.2	30.4
Control	60	61.44	31.43	40	66.0	30.38
∑ (N = 75)	**49.33**	**78.40**	**33.01**	**50.67**	**78.1**	**32.41**
BFI Traits / Groups	**Extraversion (E)**					
	Low			**High**		
	(%) participants	**Mean passwords strength**	**Mean compliance**	**(%) participants**	**Mean passwords strength**	**Mean compliance**
Rational	40	77.33	32.67	60	81.67	33.0
Emotional	26.67	76.75	31.0	73.33	88.91	36.45
Social proof	6.67	93.0	35.0	93.33	82.29	33.86
C & C	40	91.67	33.17	60	62.78	30.78
Control	26.67	76.25	33.25	73.33	58.55	30.0
∑ (N = 75)	**28**	**83.0**	**33.02**	**72**	**74.84**	**32.82**
BFI Traits / Groups	**Agreeableness (A)**					
	Low			**High**		
	(%) participants	**Mean passwords strength**	**Mean compliance**	**(%) participants**	**Mean passwords strength**	**Mean compliance**
Rational	40	84.5	33.0	60	76.89	32.78

Emotional	20	80.0	33.67	80	87.08	35.33
Social proof	33.33	82.2	34.8	66.67	87.60	33.5
C & C	20	86.33	32.0	80	71.33	31.67
Control	33.33	81.0	33.2	66.67	54.4	29.7
$\sum$ (N = 75)	**29.33**	**82.81**	**33.33**	**70.67**	**75.46**	**32.60**
BFI Traits / Groups	**Neuroticism (N)**					
	Low			**High**		
	(%) participants	**Mean passwords strength**	**Mean compliance**	**(%) participants**	**Mean passwords strength**	**Mean compliance**
Rational	66.67	77.7	31.3	33.33	84.4	36.0
Emotional	86.67	90.0	36.15	13.33	57.5	27.5
Social proof	66.67	92.7	35.1	33.33	72.0	31.6
C & C	80.0	76.25	31.83	20.0	50.0	31.33
Control	80.0	59.67	30.75	20.0	77.67	31.33
$\sum$ (N = 75)	**76.0**	**79.26**	**33.03**	**24.0**	**68.31**	**31.55**

Based on Table 3.4 above, the first and the fourth column showed the percentages of participants in each category of the personality traits. More participants were detected to be in the low category of two personality traits; openness (60%) and neuroticism (76%). Meanwhile, for these following personality traits; extraversion (72%) and agreeableness (70.67%), participants were seen more towards the high category. The only personality traits that has more a less the same number of participants from the low and high category was the conscientiousness with (49.33%) and (50.67%) respectively.

Hence, what is probably interesting to extract from the table above is how the participants from the lower and the higher category of scores from each trait performed with their password construction task. For the openness trait, the results have shown that the strength of passwords constructed from the low category is much better compared to the high category with (81.48) and (69.76) respectively. This scenario goes the same to the extraversion traits (83.0) and (74.84) respectively, agreeableness traits (82.81) and (75.46) respectively, and neuroticism traits (79.26) and (68.31) whereby the strength of passwords constructed from the low category is much better compared to the high category. Meanwhile, the conscientiousness traits have appeared to be more a less the same for the low (78.40) and high (78.10) category probably due to the tabulation of the number of participants are similar in both category. Looking at the mean of compliance

for the passwords guidelines, the results seem to be consistent with the passwords strength above.

In order to confirm further whether there are any differences or interaction between the personality traits and the persuasion strategy applied, two-way ANOVA test has been conducted and the result is summarised in Table 3.5 below.

Table 3.5: The results of Two-Way ANOVA test

BFI traits / Traits level	**Openness Level (Low / High)**		**Groups (Different Persuasion Strategies)**		**Interactions (Openness Level versus Groups)**	
	F	**p-value**	**F**	**p-value**	**F**	**p-value**
Openness	5.13	**0.02**	2.45	**0.05**	1.22	0.31
Conscientiousness	0.01	0.95	2.55	**0.04**	0.38	0.81
Extraversion	1.50	0.22	1.27	0.29	2.18	0.08
Agreeableness	1.83	0.18	1.40	0.24	1.40	0.24
Neuroticism	1.75	0.19	0.98	0.42	2.35	0.06

**The items in bold shows the p-value for statistically significant difference detected*

Based on Table 3.5 above, openness traits have shown that there is a significant difference for the level of traits given that we have accounted for the persuasion strategies applied with (F = 5.13, p-value = 0.02). There was also a statistically significant difference for the persuasion strategies applied with regards that we accounted the level of traits with (F = 2.45, p-value = 0.05). It is interesting therefore to look whether there is any interaction effect (refer to Figure 3.3 below) going on between the levels of traits and the persuasion strategies applied, but however the results have indicated that there was no statistically significant difference detected (F = 1.22, p-value = 0.31) which can be interpreted as due to the random variation of the data and further analysis would probably needed to confirm this with bigger data sets.

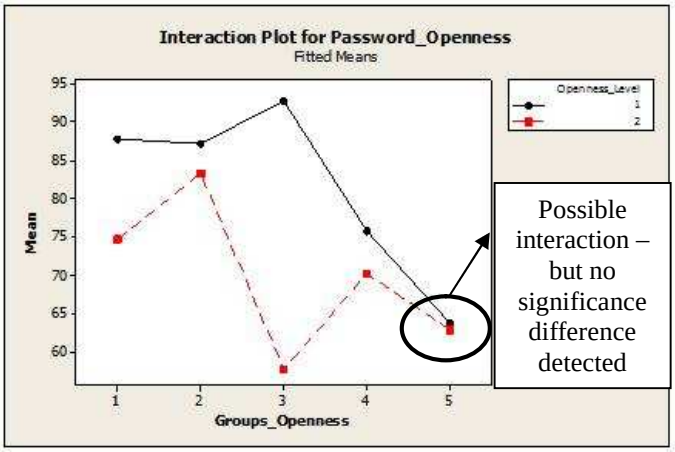


Figure 3.3: The interaction plot of password strength for the openness traits

As for the conscientiousness traits, there was statistically significant difference detected for the persuasion strategies applied (F = 2.55, p-value = 0.04). However, there was no significant difference detected for the level of conscientiousness as well as for the interactions (refer to the interaction plot in Figure 3.4 below) between the levels and the persuasion strategies applied. This result can be interpreted as although there might be some evidence showing that persuasion strategies applied towards the participants with conscientiousness traits might have some effects, however since the effects are not significant, it is assumed to be due to just random variation in the data.

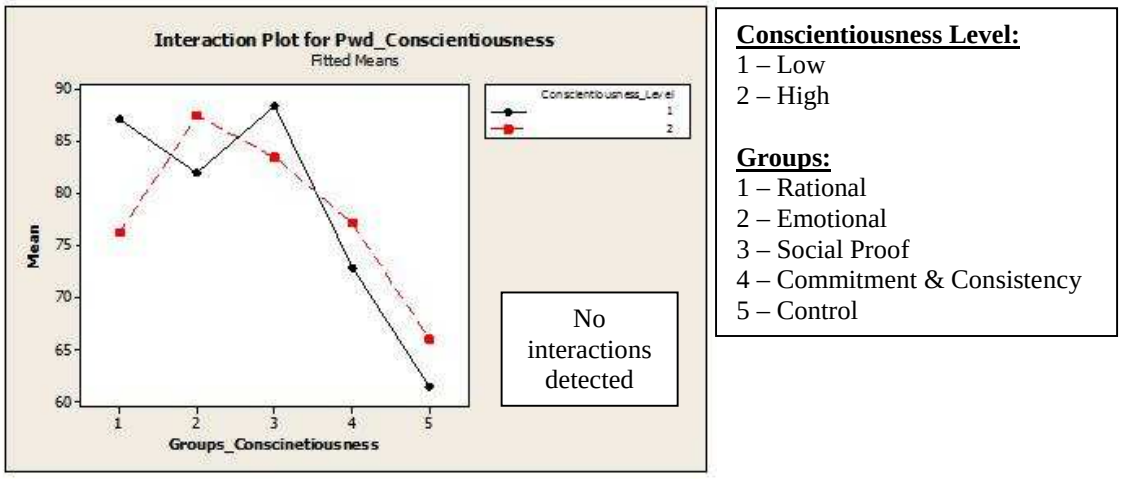


Figure 3.4: The interaction plot of password strength for the conscientiousness traits

Looking further down of Table 3.5, there were no significant difference detected for the other three personality traits that are extraversion, agreeableness and neuroticism. This can be interpreted as there is not enough evidence to say that neither the traits level nor

the persuasion strategies applied have any significant effects or interactions that can be accounted for with regards to the data set analysed. It would be interesting to expand the data sets by involving more participants in the future work.

Next, the analysis proceeds to investigate further whether there are any relationships between password strength and the BFI personality scores. In order to report this result; a Pearson correlation test was conducted as depicted in Table 3.6 below. In general, the results in Table 3.6 show that relationships do exist between personality attributes and persuasion approaches, as depicted by some of the Pearson correlation values.

On one hand, the majority of these positive correlations were found to fall between medium to weak relationships. There were also strong positive correlations detected between password strength of the rational group and the neuroticism trait (r = 0.496, p-value =0.085). Moreover, there were two significant, positive correlations detected between password strength of the rational group and extraversion (r = 0.639, p-value = 0.019), and password strength of the emotional group and the openness trait (r = 0.523, p-value = 0.05).

Table 3.6: The Pearson correlation test between password strength & the BFI test scores

Groups / **BFI traits**		**Pearson correlation**				
		Openness (O)	**Conscientiousness (C)**	**Extraversion (E)**	**Agreeableness (A)**	**Neuroticism (N)**
Rational	(r)	0.002	-0.21	**0.639**	-0.046	0.496
	p-values	0.994	0.492	**0.019**	0.882	0.085
Emotional	(r)	**0.523**	0.324	-0.384	0.269	0.317
	p-values	**0.05**	0.259	0.18	0.35	0.27
Social proof	(r)	-0.489	-0.017	0.234	-0.362	0.174
	p-values	0.076	0.95	0.42	0.20	0.55
Commitment & Consistency	(r)	0.011	-0.057	-0.545	-0.168	-0.26
	p-values	0.97	0.86	0.07	0.603	0.414
Control	(r)	0.467	-0.256	-0.334	**-0.754**	0.041
	p-values	0.21	0.51	0.38	**0.019**	0.916

**The items in bold indicate significant correlations detected*

On the other hand, the majority of these negative correlations were also found to fall between medium to weak relationships. There were two strong negative correlations detected between password strength in the social proof group and the openness trait (r = -0.489, p-value =0.076), and password strength of the commitment & consistency group

and extraversion trait (r = 0.545, p-value = 0.07). Moreover, there were also significant negative correlations detected between password strength of the control group and the agreeableness trait (r = -0.754, p-value = 0.019). Several positive and negative correlations have been detected, as summarised in Table 3.7 below.

Table 3.7: Summary of the positive and negative correlations detected between password strength and the BFI personality test scores

Groups	Pearson Correlations	BFI Traits
Rational	(+)	Openness
	(+)	**Extraversion**
	(+)	**Neuroticism**
	(-)	Conscientiousness
	(-)	Agreeableness
Emotional	**(+)**	**Openness**
	(+)	Conscientiousness
	(+)	Agreeableness
	(+)	Neuroticism
	(-)	Extraversion
Social proof	(+)	Extraversion
	(+)	Neuroticism
	(-)	**Openness**
	(-)	Conscientiousness
	(-)	Agreeableness
Commitment & Consistency	(+)	Openness
	(-)	Conscientiousness
	(-)	**Extraversion**
	(-)	Agreeableness
	(-)	Neuroticism
Control	(+)	Openness
	(+)	Neuroticism
	(-)	Conscientiousness
	(-)	Extraversion
	(-)	**Agreeableness**

**Note that the bold items indicate strong positive/negative correlations.*

The analysis also extends further looking into regression analysis between passwords strength and the level of the personality traits as displayed in Table 3.8 below.

Table 3.8: The regression analysis between password strength & the level of personality traits

Passwords strength / BFI traits	**Regression Analysis**				
	Openness (O)	**Conscientiousness (C)**	**Extraversion (E)**	**Agreeableness (A)**	**Neuroticism (N)**
b	-11.389	2.874	-5.635	-7.101	-5.146
t	-2.23	0.56	-0.99	-1.26	-0.85
p-value	**0.029**	0.579	0.328	0.210	0.396

**The item in bold shows the p-value for statistically significant difference detected*

Based on Table 3.8 above, the results of the regression analysis has shown that the openness level supports significantly predicted the password strength (b = -11.389, t = -2.23, p-value = 0.029). This indicates that both the level of the personality traits and passwords strength play a significant role in the regression model. However, there was no statistically significant difference appeared for the rest of other personality traits level as shown by the high p-value (>0.005) depicted from the Table 3.8 above. This indicates that the level of personality traits for the conscientiousness, extraversion, agreeableness and neuroticism and its corresponding passwords constructed do not play any significant role in each of its regression model.

3.4.4 Revisiting hypotheses

This sub-section is intended to revisit all the three hypotheses written earlier in relation to participants' password construction behaviour. The first and second hypotheses are as follows:

$H_{1:}$ *Users will create better passwords when they are exposed to password guidelines which include a rationale, compared to password guidelines without.*

$H_{2:}$ *Users will create better passwords when they are exposed to password guidelines which are framed using persuasion approaches compared to the standard password guidelines.*

The findings indicate that both H_1 and H_2 are supported. The means of both passwords compliance and strength from the groups that were given the rationales (i.e. the rational, emotional and social proof group) are higher compared to the group for whom the password guidelines did not include a rationale (refer to Table 3.1). Moreover, the results from the one-way ANOVA test, followed by the Tukey test, also strengthen support for both hypotheses. These findings suggest that participants are more likely to comply with the assigned task (i.e. creating better passwords) when they receive appropriate explanations as to why such a task is important.

A hypothesis was also formulated to investigate the relationship between the persuasion approaches applied (as measured by the password strength) and personality attributes (as measured by the BFI test scores) which is as follows:

$H_{3:}$ *There exists a relationship between personality attributes and the password strength produced by the persuasion approach groups.*

In general, the results displayed in Table 3.6 - 3.8 show support for this third hypothesis. There were several positive and negative correlations detected and among them several correlations were found to be significant as discussed and elaborated in section 3.4.3 above. The following section will discuss further the overall analysis of this password guidelines experiment.

3.5 Discussion

The control-laboratory experiment conducted has yielded results as presented in previous sections. At the beginning of the experiment, several research questions were formulated. In this section, those research questions will be revisited and discussed.

The first question asked whether users would create better passwords when a rationale explaining why creating a good password is important is included in the password guidelines. The results indicate that passwords created by users who receive password guidelines including a rationale are stronger compared to passwords created by those

who did not. The results of password compliance seem to be consistent with the passwords strength constructed.

Thus, these findings suggest that it is worth providing extra information to users on why such task as creating a good password is important. However, the challenge is to ensure that users will make an effort to read this information, as that which is depicted in the control-laboratory experiment might not happen in the real world. However, one possible way to overcome this is to include reading and understanding the password guidelines as a compulsory phase before someone could actually construct a password. This is especially worth considering if the systems or applications require a high level of password security.

The second question focused on which persuasion strategies are more likely to result in influencing users to create better passwords. The results show that participants who are exposed to the emotional appeal and social proof strategies produce stronger passwords than the others. These two strategies are probably more effective than the others as the explanations provided in the strategy easily relate to the participants (i.e. the emotional appeal uses a real life scenario) and social proof endorsement is probably very important to them.

On the other hand, participants in the commitment & consistency group were found not to produce passwords as strong as the other experimental group, probably due to the fact that this strategy might not work so well in the experimental setting but might yield better performance in a real world scenario. This is because the impact portrayed by the surveillance factor is important to ensure this strategy works; otherwise, the audience might not be immersed in the effect of noncompliance.

The third question was whether there were any personality trait(s) would be more likely to produce better passwords than others. As displayed in Table 3.4, the results of the openness trait have shown that the strength of passwords constructed from the low category is much better compared to the high category with (81.48) and (69.76) respectively. This scenario goes the same to the extraversion traits (83.0) and (74.84) respectively, agreeableness traits (82.81) and (75.46) respectively, and neuroticism traits

(79.26) and (68.31) whereby the strength of passwords constructed from the low category is much better compared to the high category. Meanwhile, the conscientiousness traits have appeared to be more a less the same for the low (78.40) and high (78.10) category probably due to the tabulation of the number of participants are similar in both category. Moreover, the two-way ANOVA test conducted (as displayed in Table 3.5) have shown that there are potential significant interactions between the passwords constructed and the level of personality traits.

Based on previous work in [164], the researchers seem to have suggested in their research model that there is high tendency for two of the personality traits; conscientiousness and agreeableness would show higher compliance which hence constructed better passwords, but nonetheless the results of this experiment has only show partial support for this. This is due to as mentioned previously that the personality assessment construct was administered in parallel with the persuasion strategy; hence by doing this, spontaneous results were yielded, rather than something that was planned. Therefore, in order to make concrete conclusion upon this, a new setting of experimental-work needs to be planned involving a different experimental design with larger sets of participants.

The final research question is about whether there are any significant relationships between the personality traits and the persuasion strategies applied. In general, the results indicate that relationships do exist between personality attributes and the password strength produced by the persuasion strategies groups. Several positive and negative relationships have been detected, as summarised in Table 3.7. Among these relationships, a few strong positive relationships have been detected. For example, extraversion and neuroticism traits were found to have a strong positive relationship with the passwords constructed by the participants from the rational group, while the openness trait was found to have a strong positive relationship with the passwords constructed by the participants from the emotional group.

On the other hand, several negative relationships have also been detected. For example, the openness trait was found to have a strong negative relationship with the passwords constructed by participants from the social proof group, while the extraversion trait was

found to have a strong negative relationship with the passwords constructed by the participants from the commitment & consistency group.

Thus far, the results generally have shown some interesting findings; however, what is more important is the implication for the study. First, there has been some evidence in support of considering persuasion strategies to present information about the contents of password guidelines. As persuasion strategies might increase compliance behaviour among users, personality attributes will certainly help to heighten the effect of the strategies applied. This is especially applicable for organisations which commonly include personality assessments for their employees, as better compliance rates can be obtained if appropriate persuasion strategies are channelled accordingly. Moreover, this study has initiated a foundation platform for other researchers to explore further the use of persuasion in conjunction with personality study to improve compliance behaviour with password guidelines. More interesting discussion and critical comment, as well as suggestions, can be found in Chapter 7.

3.6 Summary

This chapter has presented the control-laboratory experiment conducted to evaluate the combined study of persuasion and individual personality assessment. This chapter has included the experimental design, apparatus, measurements and procedures involved. The results and findings have been discussed, focusing on the impact and implications of the adopted approaches on improving users' compliance behavioural issues.

While motivating users' security compliance through persuasion is practical for the password authentication domain, there is a more fundamental problem in this domain that needs addressing – namely the problem of memorability. Most people are found to cope with memory overload by relying on one or two obvious passwords (e.g.: birth dates or combination of partner's name) but unfortunately although these weak passwords tend to ease the overload problem but they fail to offer adequate levels of protection [22]. Even a highly motivated user with a compliant personality who has been persuaded to produce a strong (and therefore possibly more unfamiliar) password may still simply forget it, or in anticipation of forgetting it, write it down.

Therefore, in the next part of the thesis the research focus turns towards looking into alternative countermeasures which may help solve the memorability problem. Several alternative mechanisms exist (e.g.: biometrics and smart cards), however graphical passwords have been identified as a promising and simple alternative to text-based passwords because the interaction remains more a less the same; the only difference lies in the nature of the password itself which instead of using text, numbers or special characters, uses graphic images such as icons, pictures and even lines as a password.

Although the use of traditional text passwords is still popular and still commonly used by many, graphical passwords are becoming a very promising alternative and much research shows support for their use. The following chapters will entail discussion upon the issues of graphical password use and challenges.

CHAPTER 4

AN OVERVIEW OF GRAPHICAL PASSWORDS & ATTACKS CHALLENGES

CHAPTER 4: AN OVERVIEW OF GRAPHICAL PASSWORDS & ATTACKS CHALLENGES

CHAPTER 4

AN OVERVIEW OF GRAPHICAL PASSWORDS & ATTACKS CHALLENGES

4.1 Introduction

What has been presented and discussed thus far has indicated that the human factor issue in the password authentication domain is something quite complex but is a very interesting domain of study that is worth exploring. This is in order to enhance our understanding and knowledge of "non-technical" issues which have commonly been overlooked or overshadowed by other technical and mechanical solutions.

Despite many criticisms about the weaknesses of traditional passwords, it is predicted that they will remain in common usage for quite some time to come [91]. Meanwhile, numerous authentication alternatives and enhancements to traditional passwords have been proposed. Some of these alternatives will be discussed at the beginning of this chapter in order to provide a general overview of their advantages and disadvantages.

Among these proposed alternatives, the graphical password is claimed to preserve the usability and convenience of passwords while overcoming their most serious shortcomings. Hence, this thesis will now place its focus onto the most promising alternative solutions to traditional passwords.

In general, this chapter reviews the literature on graphical passwords, describing several types, as well as their design and implementation. It also evaluates the advantages and disadvantages of each scheme. Relevant studies that have been conducted by other researchers on each scheme will also be included to support the fundamental work of exploring graphical passwords in depth. This chapter also includes a discussion on the issues of adopting graphical passwords, particularly pertaining to the attack challenges facing them.

4.2 An overview of alternatives in authentication systems

Authentication systems can involve variety of methods, but none are currently perfect or problem free. This section focuses on the discussion of available alternatives in authentication systems. Among the alternatives are such as memory cards, smart cards, token devices, digital signature, biometrics and graphical passwords. Each of these alternatives will be discussed in turn looking into its implementation as well as their advantages and disadvantages. The overview presented here will provide a general idea of the available alternatives which leads to the thesis to focus on one particular alternative to elaborate the research further.

First is the memory card which holds user information within a magnetic strip and relies on a reader in order to process the information. The authentication works when the user inserts the card into the reader and then enters a set of credentials. A popular example of a memory card is an automated teller machine (ATM) card. The user inserts the ATM card into the ATM machine and then enters his or her PIN number. The card supplies the account number (user information) and then the user provides the secret code (PIN), together providing a credential set. Within companies, employees will often carry ID badges with magnetic strips. In many of these implementations, a PIN is hashed and stored on the magnetic strip. In order to enter a building, the employee must enter a PIN number and swipe the badge through a reader. The reader hashes the inputted PIN number and compares it to the value on the card itself. If they match, access is granted.

The advantages of using memory cards is that the size is small that makes it easy to carry everywhere as it can fit into most wallets. Although the size is small, it has large data storage capacity which works really easy and fast. The cost of these memory cards is also cheap comparatively to other similar alternatives. However, the main drawbacks of it, is that it can easily get corrupted if not handled carefully which commonly leads to the loss of data.

Another quite similar alternative is the smart card which is a step above the memory card in the sense that it can process information because it has a microprocessor and integrated circuits. The way it works is when the user inserts the smart card into a reader which has electrical contacts that interface and power the smart card processor. The user

will then enter a PIN value which unlocks (i.e.: giving access to) the information contained on the smart cards. A smart card can hold a user's private key, generate a one-time password or respond to a challenge-response request.

The advantages of smart cards are much more temper proof when compared to memory cards and usually after a certain number of incorrect PIN values have been inputted the card can lock itself which would require the user to contact the vendor to receive an overriding PIN value to unlock the card again. In contrast, the downside of it which is similarity between both smart cards and memory cards have the extra expenses of creating new cards and purchasing the required readers which must be included in their implementation and lifetime costs [36].

A token device is usually associated with one-time passwords which is generated and supplied to a user that can be used to prove a subject's identity at one time and one time only. This means that after the password is used, it is destroyed and no longer acceptable for authentication. In any case, if the attacker manages to obtain the password during transmission, the attacker would have a limited time to try and use it which most likely it was already used once thus render useless to the attacker. This is among the advantages of one time password used in token devices which greatly reduces the vulnerability of someone sniffing network traffic to obtain password and being able to successfully authenticate as an actual legitimate user. Token devices also protects against password guessing, replay attacks and electronic eavesdropping. Nevertheless the drawback is that it can be exposed to masquerading attacks where an attacker gains control of the token device and uses it to impersonate the valid user. This is why many token devices require the user to enter a proper PIN value before it can be used.

A digital signature is also commonly used as a method of authentication. It relies on cryptographic means through which many of these may be verified. The digital signature of a document is a piece of information based on both the document and the signer's private key. In daily life, people sign their names to letters, credit card receipts and other documents which demonstrating they are in agreement with the contents – that is they authenticate that they are in fact the sender or origin of the item which allows others to verify that a particular message indeed originate from the signer. The

similarity between digital signatures and hand-written signatures is that both rely on the fact that it is very hard to find two people with the same signature [200].

The advantage of digital signature is that people use public-key cryptography to compute digital signatures by associating something unique with each person. When public key cryptography is used to encrypt a message, the sender encrypts the message with the public key of the intended recipient. When public-key cryptography is used to calculate a digital signature, the sender encrypts the digital fingerprint of the document with his or her own private key. Anyone with access to the public key of the signer may verify the signature. However, there is a possibility that people can lift signature off one document and place them on another which then creates fraudulent documents. Written signatures are also vulnerable to forgery because it is possible to reproduce a signature on other documents as well as to alter documents even after they have been signed.

Another promising alternative is the biometrics which is a type of access control mechanism that can be used to verify an individual's identity with a unique personal attributes such as fingerprints, palm scans, retina scans, iris scans and many others. In order for biometric systems to work, the user has to go through an enrolment period where personal attributes are captured and stored in a reference file. The reference file can be held in a local or remote database or even within a biometric template of a smart card. This is to enable a user to input his or her identification (e.g.: finger print) onto the reader in order to enter the secured system. The user will be successfully authenticated and allowed to have an access if the image matched to the one in the reference database.

The uniqueness of this type of authentication systems is that it gathers a lot of information that can be hard to imitate, thus they provide a higher level of protection compared to other authentication technologies. However, biometric systems are usually relatively more expensive and do not usually have a high acceptance rate by society because they are perceived to be intrusive of one's personal information. Furthermore, biometrics are sometimes associated with usability problems – enrolment phase can require a sensitive and time consuming process due to the necessity of requiring users to stay calm in controlled environment [22].

This thesis has opted to draw its focus on one particular alternative that is graphical passwords. Therefore the next section will focus entirely elaborating further in detail of concepts and implementation of graphical password system.

4.3 Graphical passwords - what & why?

A graphical password is an immediate alternative to traditional text-based passwords, whereby instead of typing alphanumeric characters, users are allowed to choose selected images or draw their secret (password) to be authenticated. The idea of graphical password was first introduced by Blonder [19] in a click-based scheme in which the user was required to choose a sequence of pre-defined click regions in a particular image. The era of pervasive computing has vigorously promoted the use of other input devices than the normal keyboard, such as mouse, stylus and touch screen. In a way, this has also boosted the usage of mobile devices, enabling more useful applications to be used.

This increasing interest in graphical authentication is driven by the assumption that pictures are easier to remember and more secure than words. The increase in security is associated with the difficulty in communicating or recording pictures, which should inhibit insecure practices [189]. The increase in memorability is predicted by the picture superiority effect demonstrated in several cognitive psychology studies [163, 167, 168]. According to this effect, humans have a vast, almost limitless, visual memory and pictures tend to be remembered far better and for longer than words [137].

There are several interesting theories that have been proposed to explain these experimental results, such as *common-code theory, dual code theory and abstract-propositional theory*. A framework to explain the effect is the dual-code theory, which attributes the superior retention of pictures to their greater likelihood of inducing both an imaginable and a verbal code [138]. An alternative is the suggestion that pictures induce a richer, more detailed representation in memory than words, and this makes them more distinctive at the time of retrieval [129].

According to Dewhurst & Conway [55], pictures are represented in a rich sensory-perceptual code and have direct access to semantic knowledge, while words are

mediated by lexical access and lead to semantic processes only if required by the encoding or retrieval task. The most compelling reason for exploring the use of a picture-based password scheme is that humans seem to possess a remarkable ability for recalling pictures, e.g. line drawings and objects.

While the strongest evidence thus far for the picture effect can be best explained by dual code theory, an understanding of picture memory and the means by which we acquire and maintain information about the visual environment is still an ongoing challenge. Nonetheless, the research to date provides strong arguments in terms of the memorability of drawings over words in recognition tasks, hence its applicability to computer security.

4.4 Categories of graphical passwords

Graphical passwords have gained much attention as potential alternatives to text-based passwords. Several researchers have conducted surveys on or reviews of graphical passwords schemes [170, 82, 17]. There are several types of graphical passwords and most commonly they are classified according to categories. For example, De Angeli et al. [52] have proposed to classify the graphical password scheme into three categories; *Cognometric*s, *Locimetrics* and *Drawmetrics*. The term *cognometrics* was used by the founder of the *Passfaces* scheme [140] which designs authentication systems based on the cognitive abilities of the human brain in recognising images, e.g. in the case of Passfaces recognising human faces. On the other hand, *Locimetric* systems refer to mechanisms that require identification of a particular target point(s) within an individual image, while *drawmetric* systems require the user to reproduce a pre-drawn outline drawing.

However, the more common terms used to classify the graphical password schemes are as follows; *Recognition-based system*, *Cued-recall based system* and *Recall-based system.* Based on the three categories above, it is evident that these terms represent the same meanings as those given by De Angeli et al. [52]. In other words, the *recognition-based* equates to the term *cognometrics* system; *cued-recall* based system is similar to *locimetrics* system; and *recall-based* system is similar to *drawmetric* system. Therefore,

throughout this chapter, the graphical password schemes will be classified using the more common terms used.

The following sub-sections will continue by discussing each of the graphical password schemes according to the three major categories. For each scheme, its design implementation, advantages and disadvantages will be discussed. Where appropriate, relevant studies conducted pertaining to the schemes will also be discussed as a foundation to understand the bigger picture of graphical passwords as the nearest alternative to traditional alphanumeric passwords.

4.4.1 Recognition-based system

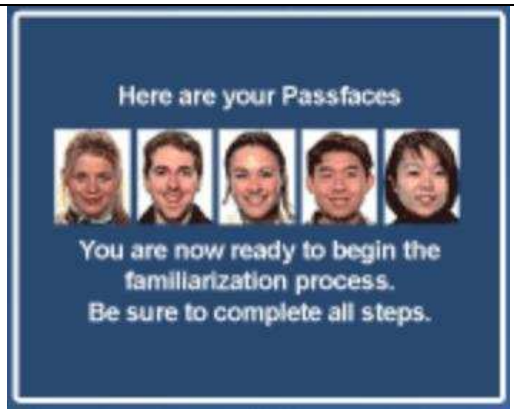
In recognition-based systems, users are required to memorise a set of selected images during password creation and then to recognise their pre-selected images from among decoys in order to log in. This type of scheme relies on exceptional human ability to recognise previously seen images, even those viewed very briefly [168]. Currently, proposed recognition-based systems use images such as faces, random art, daily objects and icons. Among the most extensively studied graphical passwords that fall into this category are Passfaces [140], Story [51] and Déjà Vu [56]. The following sub-sections will elaborate on each scheme in detail.

4.4.1.1 Passfaces

Passfaces is the canonical example of a recognition-based scheme which uses human faces as a unique verification technology for authentication procedures. It offers two-factor authentication to provide a high level of authentication assurance which can be easily integrated with existing security systems in financial, government, healthcare and corporate networks [140]. Passfaces was based on research and experimental studies which indicate that viewing and recognising faces leaves an impact on one's memory recognition. This can be specially illustrated when infants are born with a capacity to recognise faces and show a preference for looking at faces well within the first hour of birth. Infants are also found to recognise their mother after only two days [33]. Hadyn et al. [81] further explain that face recognition is a dedicated process that is different from general object recognition; both inference and direct neurological measurement indicate

that our brains have a special component, the sole function of which is to recognise faces. In addition, the human brain commits faces to memory without any conscious effort and familiar faces are recognised rather than recalled.

In order to enrol in Passfaces, users are first presented with a set of three to five faces. They are required to familiarise themselves with the faces presented; this is known as the familiarisation process. The process begins with studying each face and looking for similarities between the face and people they may know. Then they are taken through a face recognition exercise which requires them to pick one of the assigned faces from a grid of nine faces; this is done for each face. Once the user has demonstrated the ability to recognise the faces, they are considered ready to log in. The Passfaces are presented in five grids, which each containing one Passface and eight decoys. The following Figure 4.1 (a) – (d) shows the interfaces of the procedures involved in Passfaces enrolment.



a) Set of five faces to memorise

b) Familiarisation process – the five faces shown earlier will be shown one after another

c) Face recognition exercise

d) Main login interface – choose one Passface among eight decoys

Figure 4.1: Interfaces of the procedures involved in Passfaces scheme [140]

The set of images in a panel remains constant between logins, but images are permuted within a panel, incurring some usability cost. The original prototype systems had $n = 4$ rounds of $M = 9$ images per panel, with one image per panel from the user portfolio. The user portfolio contains exactly 4 faces, so all portfolio images are used during each login.

Brostoff & Sasse [24] conducted a field trial investigation comparing the Passfaces scheme with passwords. The result found that fewer login errors were made with Passfaces, even when periods between logins were long. This supports Valentine's [182] study that shows people are good at recognising faces and can remember the faces from a single password for months after the initial training. However, in terms of login time, Passfaces took more time compared to traditional passwords, probably due to several rounds of challenges to identify the portfolio images from among the decoys.

Davis et al. [51] reveal that allowing people to select the faces that make up their password can lead to bias in terms of personal preferences; for example, more attractive faces are possibly chosen frequently, thus significantly reducing security. Dunphy et al. [60] look into the issue of social engineering attacks, whereby attackers convince users to describe the images in their portfolio. The results reveal that 8% (of 158) participants could log in based on verbal descriptions of the portfolio images. The results further show that one way to reduce social engineering attacks is by using decoy images more or less similar to the portfolio images, though this led to increased difficulties in recognising the correct portfolio images.

In a more recent study, Everitt et al. [62] chose the Passfaces scheme to examine the effect of frequency access on a graphical password and the interference effect resulting from interleaving access to multiple graphical passwords and patterns of access while training. The study was conducted in five weeks and users were prompted by email to log on to four different (fictitious) accounts according to different schedules. The results revealed that those who logged in more frequently were more successful at remembering their passwords. This study is the first of its kind in graphical password domains looking into the issues and effect of having multiple graphical passwords, as people typically have a need for more than four passwords. Thus, the effects of interference are even more crucial in a widespread deployment of graphical passwords.

Unlike typical studies that examine only single graphical passwords, these findings call for more realistic evaluation of multiple graphical passwords usage.

4.4.1.2 Story

Story is a graphical password scheme which was closely modelled on the Passfaces scheme. In the Story scheme, a password is a sequence of *k* images selected by the user to make a "*story*" from a single set of $n>k$ images, each drawn from a distinct category of image types which are capable of producing $n!/(n-k)!$ choices [51]. The image category of the Story scheme is based on nine categories; animals, cars, women, food, children, men, objects, nature and sports (Figure 4.2).

In order to log in to this scheme, users are presented with one panel of images and they must identify their portfolio of images from among the decoys. In the prototype system, the password was set to be a selection of four images from a panel of nine. This produces a full password space of (9x8x7x6) = $3024 \approx 2^{12}$ passwords. Unlike in Passfaces scheme, this scheme adds a new element – a sequential component where users must select images in the correct order. Users were instructed to mentally construct a story to connect the images in their set. This was done in order to aid memorability as the pre-selected images must be in the correct order to be authenticated by the system.

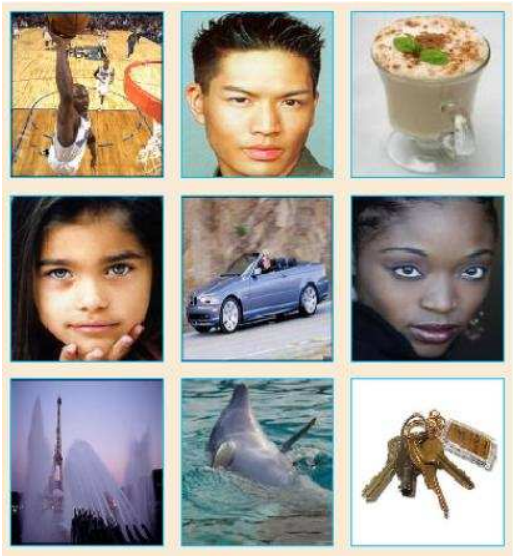


Figure 4.2: Example of images in a 3x3 panel set [51]

Story and Passfaces have a lot in common besides the images used, and an experimental study was conducted involving both schemes to find out the effect on users' image choice. The results have shown that the Story scheme encouraged users to choose more varied images; however, some exploitable patterns (such as between male and female choices) can be detected [51]. Users were also found to have difficulties in memorising the Story password (success rate $\approx$ 85%) due to errors in the image sequence. Users who participated in the experiment revealed that they rarely used the "story" method to aid memorability (despite the designers' intentions) which may explain such results. An improvised version of the instructions on using a story to link the images (as to aid memorability) might therefore yield different results.

In another project based on the idea of storytelling, Maetz et al. [113] invented a scheme called Recall-A-Story. This mechanism is based on the user setting a framework for the story by selecting a background picture, before selecting several images and placing them on the background picture to populate the framework. This eventually creates a storytelling scenario given by the sequence and position of the images. The authors of this scheme have probably thought of a better way to include the *storytelling* scenario as part of the mechanism. A possible use for this scheme is unlocking a touch screen device (e.g. mobile phones, portable media players, web tablets etc.), authenticating online services, and accessing encrypted data storage. The Recall-A-Story password space is computed for a password of length exactly l ordered images among i, over p places and b backgrounds, formulated as follows:

$$\textit{Recall-A-Story password space} = b \,.\, (i \,.\, p)\, l$$

Figure 4.3: Implementation of Recall-A-Story scheme for a tactile mobile phone [113]

Although, theoretically, this scheme proposes a more feasible way of including storytelling as part of the password mechanism, unfortunately no empirical evidence has been presented to support the claim that this scheme is better than the previous story scheme.

4.4.1.3 Déjà Vu

This scheme was proposed by Dhamija & Perrig [56] to address the short-comings of traditional alphanumeric passwords and PINs. In general, Déjà Vu consists of three major phases; portfolio creation, training and authentication. During the portfolio creation phase, users select a specific number of images from a larger set presented by the server. Figure 4.4 shows the image selection phase in the proposed prototype system. The authors of this scheme argue that the strategy of choosing images from random art instead of photographs reduces the predictability of the portfolio, hence increasing the security of the system. They believe that the images of *Random Art* are more difficult for users to write down as their password or to share with others by describing the images from the portfolio.

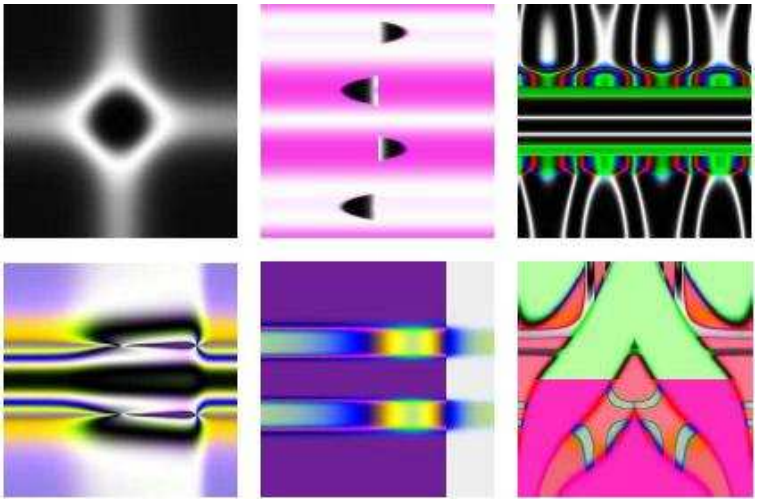


Figure 4.4: Example – selection of random art images in Déjà Vu scheme [56]

Following the portfolio selection phase is a training phase, where users choose the images in the portfolio from a challenge set which contains decoy images. The selection and training phase must be done in a secure environment, where no other person can see the image portfolio. During the authentication phase, a user will be validated if he or she manages to identify all portfolio images correctly among the decoys contained in the challenge set. In the prototype system, a panel of 25 images is displayed, five of which belong to the user's portfolio. The authors of this scheme propose that a fixed set of 10,000 images is adequate, but the "attractive" images should be hand-selected to increase the likelihood that images have similar probabilities of being selected by users.

The Déjà Vu scheme was user-tested alongside standard web-authentication using traditional alphanumeric passwords and PINs. Two types of image portfolios were used in the study: *Random Art* and photographic images. The result shows that a user requires more time to create image portfolios than to create passwords and PINs. Moreover, photograph portfolios took longer to create than *Random Art* because people spent more time browsing and looking at each image. From a login time perspective, users took longer to login with *Random Art* compared to photographs, which suggests that people can recognise photographic images more quickly than abstract images. In terms of memorability, the results found that performance for PINs and passwords were more degraded compared to the images. Looking at the performance of password memorability, the authors suspected that performance could be worse if more restrictions were placed on the password (no restrictions other than length were placed on password choice during the study). Users in the study were also asked to describe

their chosen images and the outcome supported the assumption that using abstract images is more difficult to describe compared to photographs.

The Déjà Vu scheme is advantageous because it uses abstract images which help to reduce social engineering attacks, trying to gather enough information to log in by tricking the user into verbalising their password. Similarly, it would seem difficult to identify images belonging to a particular user based on knowing other information about the user; however, problems resulting from predictable user choice remain possible, whereby users might make their choices based on favourite colours or shapes. Moreover, the usability issue was raised due to the fact that no feedback was given when users click on particular images, making it difficult for a user to be certain whether an image has been selected, which is obviously for security since providing too much feedback might lead to security being compromised.

4.4.2 Cued-recall based system

In cued-recall based systems, the user is required to remember and target specific locations within an image. The cue was intended to reduce the memory load on users and has been found to be a much easier memory task than pure recall. However, it is important that an ideal design of such a scheme ensures that the cue in an authentication system is only helpful to legitimate users, not to attackers trying to guess a particular password.

The first graphical password scheme introduced by founder Blonder [19] uses this cued-recall mechanism. Many researchers have since extended Blonde's idea, which has recently produced subclass research in the cued-recall domain area known as *click-based graphical password* schemes [17]. Among the most extensively studied graphical passwords that fall into this category are PassPoints [192] and Cued Click Points [40]. The following sub-sections will elaborate each scheme in detail.

4.4.2.1 PassPoints

The PassPoints scheme was developed based on Blonder's [19] original idea that overcomes its limitations of needing simple, artificial images, predefined regions and

consequently many clicks in a password. Developed by Wiedenbeck et al. [192], PassPoints allows any image to be used and, as a result, a user can click on an image (as opposed to some pre-defined areas) to create a password. The image obviously acts as a cue to help the user remember their click-points (password).

There is a tolerance area around each chosen pixel. In order to be authenticated, the user must click within the tolerance (i.e. within 0.25 to 0.50cm) of their chosen pixels, and also in the correct sequence (as shown in Figure 4.5 below). The tolerance is needed because the user's click point is literally a single pixel, which is too precise for a user to click on successfully. The system allows the tolerance to be adjustable, which gives a certain margin of error around the click point, in which the user's click is recognised as correct. This feature is enabled by a technique called *"robust discretization"* and proposed by Birget et al. [18]. Later, two other discretization methods were eventually introduced as alternatives: the *centred discretization* proposed by Chiasson et al. [38] and the *optimal discretization* proposed by Bicakci [16].

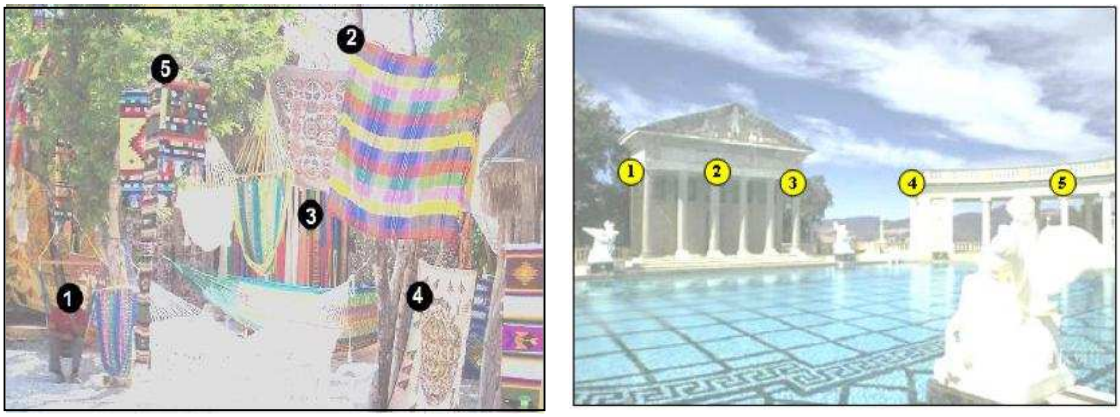


Figure 4.5: Example of two different possible images for PassPoints [192, 39]
(Note: *The numbered labels do not appear in practice*)

Since any picture can be used, and a picture may contain hundreds to thousands of possible memorable points, the possible password space is quite large. For example, with five or six click points, one can make more passwords than eight character Unix-style passwords. Figure 4.5 above shows two examples of possible images for PassPoints, where the numbers indicate the sequence of click-points (i.e. the password).

The authors of the scheme conducted an empirical study comparing PassPoints with alphanumeric passwords, from both usability and security perspectives. The results showed that memory retention over a period of five weeks for PassPoints was similar to alphanumeric passwords. This result is very encouraging, considering it was achieved with very intermittent use, since most users had very little experience using graphical passwords. It was expected that users requires more time to login with PassPoints compared to alphanumeric passwords; nonetheless, the results indicated that, with more practice and continuous use of the graphical password, login time can be improved [192]. On the other hand, from a security perspective, it is easy to obtain large password spaces with PassPoints due to various possible click points in a variety of images. Moreover, in the same user study, the results revealed that users rarely chose points that were within the tolerance around the click points of other participants. This indicates that users were unlikely to choose the same salient areas for their click points.

In a separate user study, Wiedenbeck et al. [192] evaluated the effect of tolerance clicking during the authentication stage and the image choice in the system. The results revealed that memory accuracy for the graphical password was significantly reduced by using a smaller tolerance for the user click points, but the choices of images did not show any significant difference. This indicates that the system is indeed suitable for a large variety of images. A revisited usability evaluation was conducted by Chiasson et al. [39] on the PassPoints scheme, involving both lab and field study. In general, the results supported the previous findings; however, this study revealed that participants were more accurate in targeting their click-points than previously suggested, indicating that a smaller tolerance area may be acceptable. However, it was also found, contrary to previous work, that the choice of image does significantly influence success rates.

Security analysis on PassPoints revealed that the scheme is vulnerable to *hotspots* and simple geometric patterns with images [75, 58, 180, 155, 39, 135]. *Hotspots* are specific areas in a particular image that have a higher probability than others of being selected by users as part of their passwords [39]. Hotspots have proved to be problematic if attackers can accurately predict the hotspots in an image and then build a dictionary of passwords containing combinations of these hotspots. This is the major drawback of PassPoints, resulting in an amended version called *Cued Click Point* scheme - intended to overcome the *hotspots* problem.

4.4.2.2 Cued Click Points (CCP)

This scheme, called Cued Click Points (abbreviated as CCP hereafter), was proposed by Chiasson et al. [40] as a modification of the original PassPoints cued-recall scheme. In this scheme, users have to select one click point on each of five images presented in sequence, one at a time, providing one-to-one cueing. Each image after the first is a deterministic function of the current image, the coordinates of the user-centred click-point and a user identifier [40].

Figure 4.6 shows the implementation of the CCP scheme with five challenge rounds of clicking the correct point on each image. Unlike the PassPoints scheme, users receive immediate feedback if they enter an incorrect click-point during login, being presented with an image that they do not recognise.

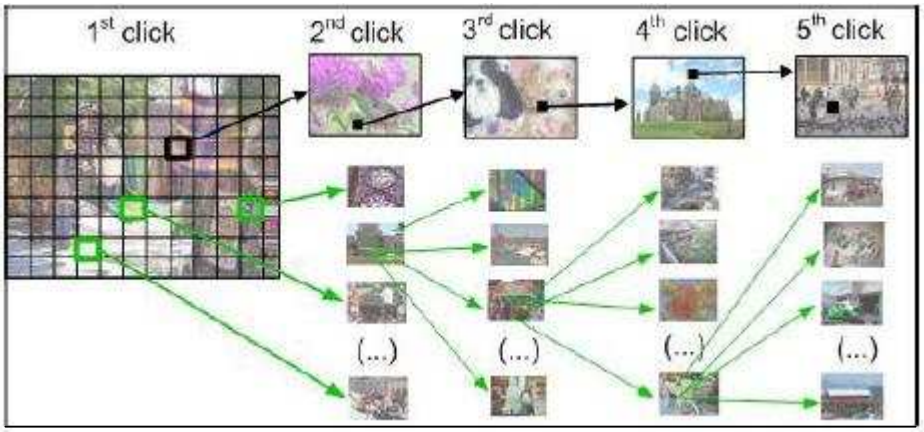


Figure 4.6: The implementation of CCP [40]

Based on Figure 4.6 above, each click will result in being shown the next, eventually leading users along a "path" as they click on their sequence of points. A wrong click leads to an incorrect path; however, authentication failure will only be revealed after the final click. This feature improves the usability aspect as users will be able to rectify this issue even before completing the login trial (i.e. as at this point, they can re-enter their password). At the same time, in spite of the implicit feedback being more user-friendly, it does not become useful information for potential attackers as they would not be able to recognise the subsequent images that will appear after each click points. Users are given the flexibility to choose their images to the extent that their click-point dictates

the next images; if they dislike the resulting images of a particular click point, they could create a new password involving a different click point to a different image.

The CCP scheme also uses the *discretization* method to determine a click point's tolerance area and the corresponding grid, whereby for each click point in a subsequent login attempt, the grid is retrieved and used to determine whether the click point falls within tolerance of the original point [40]. Similar to the PassPoints scheme, the CCP prototype system uses images of size 451x331 pixels and tolerance area of 19x19 pixels.

The authors of CCP conducted a lab-based user study, involving 24 participants, to evaluate the scheme. The results showed that participants performed similarly well for both schemes in terms of login accuracy and success rates. As expected, users took the longest time to compose the password (25 seconds), but progressively quicker during the confirmation and login stage. The study also included some qualitative findings looking into users' preferences between CCP and its predecessor scheme; nine out of twelve people strongly preferred CCP and three remaining people preferred PassPoints, although two of them stated that CCP was more secure.

Although the proposed CCP scheme has good potential as a graphical authentication system and has improved usability and security aspects from the original PassPoints scheme, *hotspots* are still the main concern. Recently, work by Salehi-Abari et al. [155] have proven that it is possible to launch a dictionary of passwords based solely on patterns, even without knowing or having knowledge of the particular image. Based on visual attention research by Wolfe [194], different people are attracted to the same predictable areas while looking at a particular image. This suggests that, without proper guidance, users will select their own click points and *hotspots* will remain as a major concern. The next variation scheme of CCP, which is called *Persuasive Cued Click Points*, was proposed to overcome the *hotspots* problem in both PassPoints and CCP, and is elaborated in the next sub-section.

4.4.2.3 Persuasive Cued Click Points (PCCP)

This scheme, known as Persuasive Cued Click Points (abbreviated as PCCP hereafter), is an extended version of the CCP scheme and is based on the *Persuasive Technology* (henceforth abbreviated as PT) concept. PT was first introduced by Fogg [67] as a technology that can motivate and influence people to behave in a desired manner. The PT concept has been applied in many areas, mostly in health and education.

In the computer security domain, the PT concept has been applied to authentication systems to improve text password security. For example, an authentication system should guide and encourage users to select stronger passwords instead of imposing system generated passwords that will result in more usability problems. Forget et al. [68] have applied the PT concept into a password authentication system known as the *Persuasive Text Password* scheme which motivates users to create stronger text passwords. The shuffle button on the interface, which helps users to scramble their original password, is considered as a persuasive tool that allows users to choose a strong password while being memorable.

Using a similar concept, the PCCP scheme intends to persuade its users to avoid hotspots during password creation, which is still a concern for both CCP and PassPoints schemes. With CCP as a base system, persuasive features were added with the aim of encouraging users to select more secure passwords and to make it more difficult to select passwords where all five click-points are *hotspots* [38]. This was implemented during the password creation stage, where the images were slightly shaded except for a randomly positioned *viewport* (Figure 4.7 below). The viewport was purposely positioned at random, as this was done with the intention of avoiding known hotspots since such information could be used by attackers to improve guesses and could lead to the formation of new hotspots. The viewport's size was intended to offer a variety of distinct points while covering only an acceptably small fraction of all possible points.

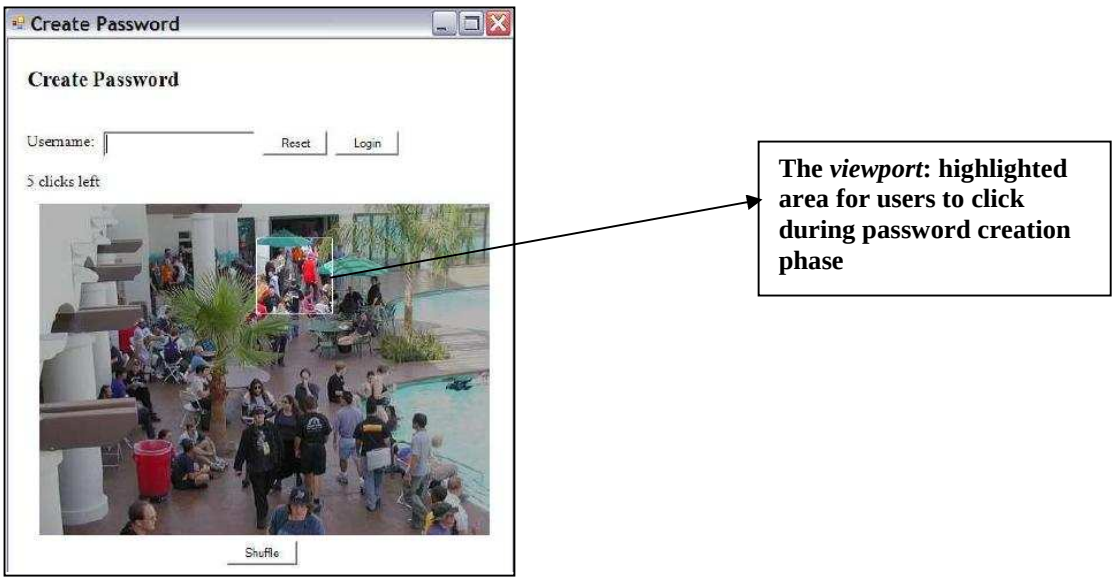


Figure 4.7: The interface of PCCP – showing viewport [38]

During password creation, users were required to select a click-point within the viewport area (which is highlighted among the other shaded areas in the image) and not permitted to click outside of the viewport. Users, however, are given choice if they are unwilling or refuse to select in the "suggested" *viewport;* by pressing a shuffle button, a different viewport area will be produced in another random position of the same image. The shuffle button only appears as an option during the password creation stage, while in the confirmation and login stages the images are displayed normally, without shading or highlighting the viewport area, and users are allowed to click anywhere around the image presented. Figure 4.7 shows an example of the PCCP interface where the small highlighted box is the *viewport* area.

The PCCP scheme was evaluated in a user study involving 39 participants who completed an hour-long session. The user study found that the use of the viewport reduces the users' tendency to select click-points that fall into known hotspots. Based on the data they collected, the distribution of the click-points was more randomly dispersed and thus unlikely to form new hotspots. However, in terms of login success rate, the PCCP scheme was found to be slightly lower than the CCP scheme.

The authors of the scheme reason that PCCP click-points may require slightly more practice before being successfully memorised; due to the fact that the viewport has actually encouraged users to avoid hotspots, it seems intuitive that the less preferred areas of an image will require more practice before being successfully memorised.

Another possible reason is due to the possibility of the image being initially dimmed during password creation, which may have caused users to have less chance of memorising the location of their point in reference to the rest of the image.

Although these initial results show promising findings, further work is needed to test the long-term memorability of PCCP passwords, including the effect of interference when users must remember multiple passwords, similar to the real world setting. The option given to users to shuffle the viewport (i.e. until they find a suitable or preferred one) will definitely result in a longer time needed for password creation. This might not become an issue in a lab-based study but will have an effect in real world implementation.

4.4.3 Recall-based system

The Recall-based system is another category of graphical password. As the name implies, users need to recall and reproduce a secret drawing (i.e.: password) on a blank canvas or grid. Compared to the other two systems, this is the closest to the traditional text-based password, except for the fact that the password used is a drawn image (i.e. involves geometrical shapes and lines) instead of alphanumeric characters.

Unlike the cued-recall system, users of this scheme are not given any reference but rely solely on their memory of their password. However, users sometimes devise ways of using the interface as a cue, even though it is not intended as such, eventually transforming task into one of cued-recall [17]. Although this may be unintentional, it might cause some challenges to the scheme as attackers might take advantage of this vulnerability. Examples of popular schemes that fall in this category are Draw-A-Secret (DAS) [98], Passdoodle [72], Pass-Go [174] and GrIDsure [79]. Draw-A-Secret (DAS) is the canonical example from this category of such a scheme, for that it has been chosen as a case study in this thesis and will be presented separately in the next chapter. The next sub-section will elaborate on the remaining schemes.

4.4.3.1 Passdoodle

The idea of this scheme was first proposed by Goldberg et al. [72], who conducted a user study exploring the feasibility of the hand-drawn doodle as a password (Figure 4.8). The scheme is quite similar to that of Draw-A-Secret (DAS), introduced by Jermyn et al. [98], except that users are free to doodle their secret (i.e. password) without the limitations of the grid lines in the DAS scheme.

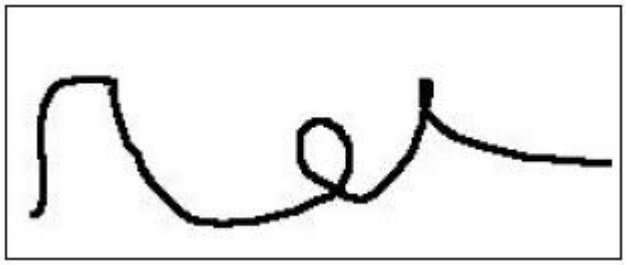


Figure 4.8: Example of Passdoodle [184]

A "paper-based prototype" was used in the user study that evaluates the usability aspects of the scheme. The findings revealed that participants could recall all visual elements of the doodle as well as they could recall alphanumeric passwords; however, most of them could not perfectly redraw their selected doodles.

This finding was generated after the authors considered *visual match*[8] as a measurement to accept the correct doodles rather than using the *exact match*[9] as participants were found unable to reproduce the shape exactly following stroke by stroke orders [72]. This has lead the authors to conclude that, in order to remember a doddle, participants generally depend on the mental picture of the entire image of their doodle or a vague concept of the semantic qualities of their doodle, as opposed to a specific stroke-by-stroke memory.

Using the same scheme, Varenhorst [184] investigated the use of Passdoodle as an authentication mechanism in a pervasive environment. He improved the method of evaluation by using three features to identify the Passdoodle during the authentication

[8] Visual match refers to the description of the Passdoodle that they have produced.
[9] Exact match refers to the actual Passdoodle and to produce this they need to redraw it exactly as it was produced.

process; any two of the three must show a high degree of similarity to confirm the identity of the doodle. The three features involved were distribution grid, instantaneous speed and point variance across the distribution grid.

The results of his study found that two of the features - distribution grid and point variance across the distribution grid - have the highest success rates with 97 and 95 percent respectively. The speed feature does not perform as well as the other two, with only a 57 percent success rate. This may be attributed to speed changes actually involved in drawing a large doodle versus the same doodle scaled down. The users who had a low variance (i.e. in the time it took to trace the doodle) were more likely to receive a match on the speed comparison; if users had been instructed to replicate their speed during the training, the system may have been more accurate [184].

Later, Govindarajulu and Madhvanath [77] proposed a web-based manager using a master doodle instead of a master password. The system requires one sample of the master doodle to be collected during enrolment. In order to evaluate the doodle recognition accuracy, the false reject and false accept rate was measured. This was done by comparing doodle samples from a user and random other doodles respectively before matching them against one or more samples of the user's master doodle.

The authors report an overall accuracy of approximately 91% (using their dataset consisting of Tamil's symbols) which was encouraging, considering that a single training sample of each doodle was used, whereby accuracy is expected to improve significantly as more samples of the user's doddle become available as a by-product of usage.

Passdoodle is an interesting scheme with some further improvements needed before it can be deployed in a real authentication system. The recognition techniques used to identify the doodle (secret) must ensure that legitimate users are granted access to the systems whenever necessary, while obviously denying access to attackers. There seems to be a lack of user studies reporting on login time and login success rate of the Passdoodle. Moreover, comparative studies of the Passdoodle scheme and text-based password will provide a better insight into the worthiness of adopting such a scheme.

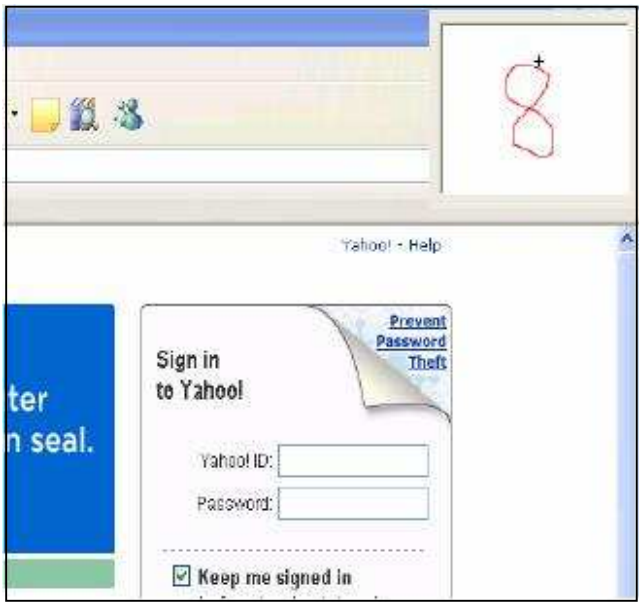


Figure 4.9: Master doodle interface [77]

4.4.3.2 Pass-Go

The Pass-Go scheme was introduced by Tao & Adams [174] who were inspired by an ancient Chinese game known as "Go". This scheme was considered an improvement to the implementation of the Draw-A-Secret (DAS) scheme as it improves the usability issue, the difficulty of accurately duplicating sketches whose lines cross near grid lines or grid line intersections.

Unlike the DAS scheme, Pass-Go requires a user to select intersections, instead of cells, as a way to input a password and, consequently, the coordinate system refers to a matrix of intersections rather than cells, as in the DAS scheme [174]. The main advantage of changing from cell to intersection is that drawing diagonal lines becomes feasible; Pass-Go users can now draw a shape more freely compared to the DAS scheme. In Pass-Go, dot and line indicators are displayed to show the intersections and grid lines that correspond most closely with the input trace (Figure 4.10). For example, a dot indicator appears when one intersection is selected while a line indicator appears when two or more intersections are touched continuously (i.e. using the stylus or any input devices).

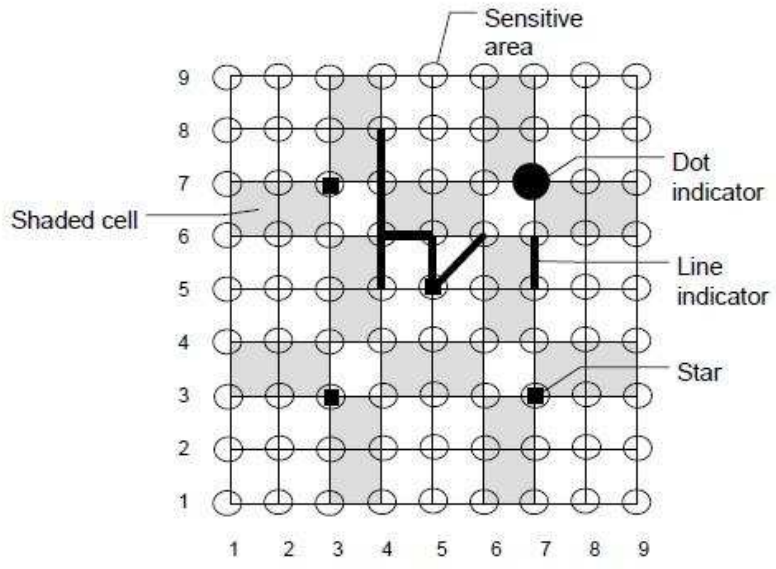


Figure 4.10: The design of Pass-Go scheme [173]

Based on Figure 4.10, the sensitive area is an area surrounding each intersection which was introduced as an error tolerant mechanism. This is due to the fact that, theoretically, it would be impossible for a user to touch an intersection point (which is actually just a point). The sensitive area (which is invisible to users) can use any shape and size, depending on a pre-defined setting which in the implementation was set to round circles with a radial size of 0.4 x *d* (where *d* is the side length of a grid cell) [173].

The Pass-Go scheme borrowed the idea of the reference aid from the "Go" game, where small dots (known as stars) are evenly distributed on a 19x19 "Go" board. Pass-go introduced shaded cells and uses 9x9 grid cells (as shown in Figure 4.10) to enhance usability, especially the memorability aspect. In addition, a colour scheme is included to strengthen security.

A large user study, involving 167 participants, was conducted to evaluate the Pass-Go scheme. During the three month period of the study, the results revealed an overall login success rate of 78%. This was claimed to be acceptable by the authors as the trend showed login success rate was low in the first three weeks but continued to rise until it became stable at 90% on the seventh week [174].

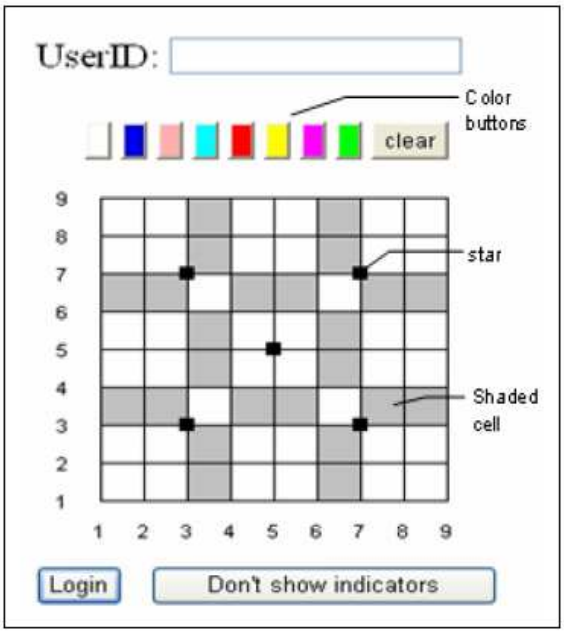


Figure 4.11: The main interface of Pass-Go scheme [173]

In contrast, the opposite trend was found for the forgotten password report rate; out of 21 forgotten passwords, 95% were reported to be during the first five weeks with only one report in the subsequent two months [174]. Despite the findings of the login success rate, no login time data was reported in the study. Other elements of Pass-Go, such as length, stroke-count, dot and colour, were also evaluated in the user study. Users were found to select longer passwords, and the use of colours resulted in increasing the complexity of the password beyond that of the DAS scheme.

The authors of Pass-Go also proposed some variations on the scheme, known as PassCells, which explore the space resource on the grid with the aim of improving usability and security. In PassCells, a matrix of cells substitutes the grid display (as shown in Figure 4.12). The matrix of cells functions in a similar way to the sensitive areas in Pass-Go. This change was introduced to overcome the usability weakness in the previous scheme so that the sensitive areas are now visible to users.

Unfortunately, PassCells has a major drawback in that it is not scalable because reference aids are difficult to deploy. For this, the authors suggested it be used for small matrix size 5 x 5 or 7 x 7 [174]. However, no user study was conducted to test the scheme. Furthermore, some of the variations are more complicated than the basic scheme, which might lead to increased user training and support costs.

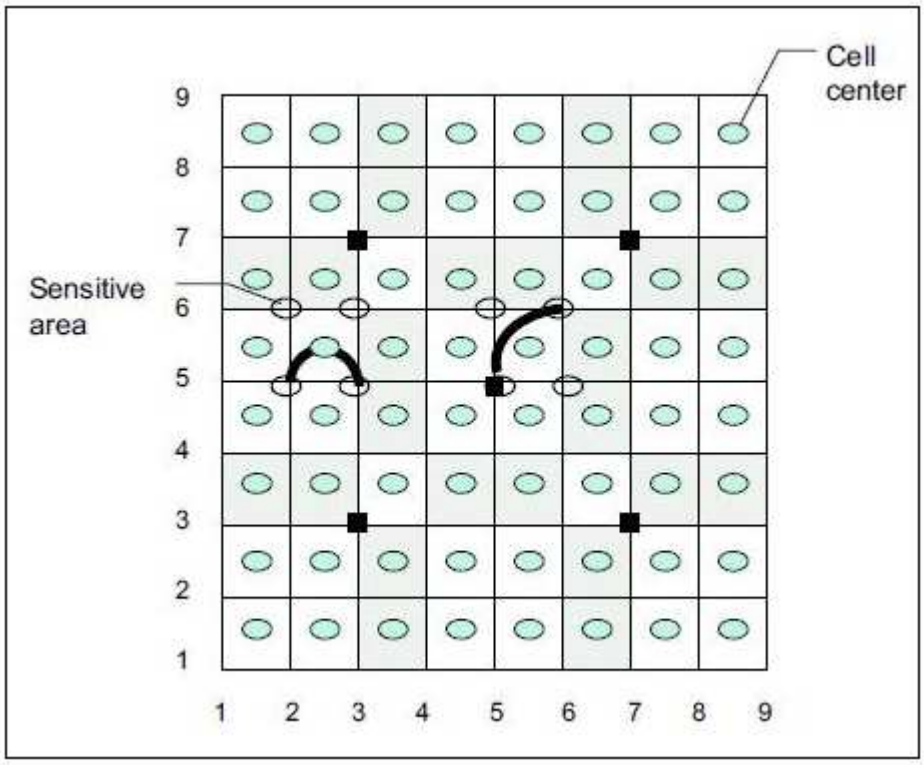
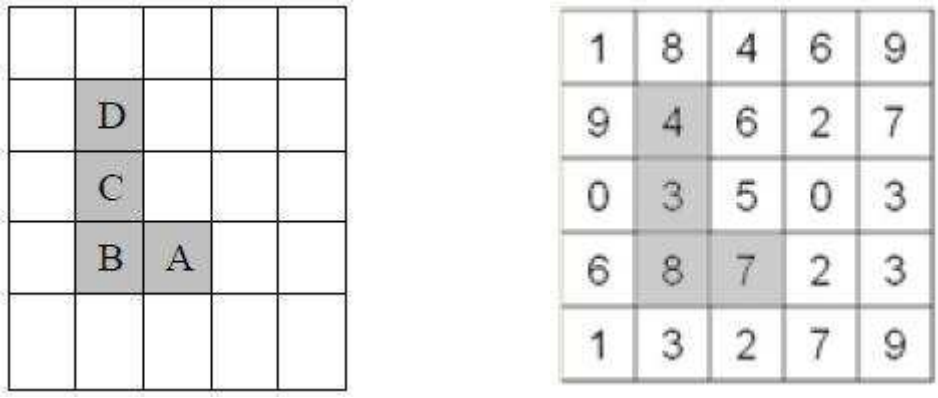


Figure 4.12: The design of PassCells scheme [174]

4.4.3.3 GrIDsure

GrIDsure [79] was introduced as a commercial product and extends the standard 'shared-secret' authentication model to create a secure methodology. Although it is used to generate a one-time PIN, it is considered a graphical password as it involves a graphical scheme. To create a password, users select four cells from an ordered subset of the 25 grid squares (i.e. in a 5 x 5 grid display) and enter the corresponding input by using a keyboard. For example, users choose cells A, B, C and D, which form the "L" shape pattern (Figure 4.13 (a)). Upon subsequent logins, digits are randomly displayed within the grid cells and users enter the new sequence of digits found within the cells of their memorised pattern (Figure 4.13 (b)). The size of the grid and the number of cells chosen to make up the one time PIN may vary in the GrIDsure scheme.



(a) (b)

Figure 4.13: (a) During enrolment: User selects cells A, B, C, D. (b) During authentication: User reads off random numbers chosen cells [23]

Brostoff et al. [23] conducted two separate user studies, with a gap of two years between each study, to evaluate the scheme on PDAs used at home or in the workplace. The first study revealed that there was a tendency among the participants to select certain patterns. For example, out of the total passwords collected, 32 percent formed a line, while another 32 percent formed basic shapes such as diamonds, squares and corners. The authors argued that this was due to the fact that the instructions given to users were not specific; indeed, no guidance was included on how to choose the passwords. Therefore, during evaluation of the second study, the instructions given were carefully re-worded to encourage greater diversity in the patterns chosen.

This improvement has shown to be effective because the second evaluation revealed that 32 percent of the total passwords collected had uncategorisable shapes. Both studies showed that 87 percent of login attempts were successful first time. Although greater diversity in the patterns produced by the improvements in the instructions might reduce the memorability of the patterns, this was not the case, as shown by the results, which illustrate that the recall of patterns and ease of use is at least as good in both evaluations. In terms of security of the scheme, GrIDsure reduces the technical risk of interception, whether by shoulder surfing, phishing or compromised equipment. Moreover, the risk of brute-force or guessing attacks by providing a larger pattern space than the number of possible 4-digit PINs is reduced [23]. The GrIDsure mechanism provides a very interesting graphical scheme, although it is used to produce a one-time

PIN. This is a good example of collaboration between both schemes, resulting in a system that is more secure and yet more usable.

4.5 Attacks challenges in graphical passwords adoption

In common with traditional text-based passwords, graphical passwords also face some challenges. These challenges refer to the various types of possible attacks such as *brute force attack, dictionary-based password attack, phishing attack, social engineering, smudge attack* and *shoulder surfing attack.* According to Biddle et al. [17], most standard attacks on the traditional text-based passwords convert directly to attacks on some graphical passwords schemes.

The following sub-sections will discuss these attacks briefly in order to provide an overview of how these challenges might have an effect on graphical password adoption as an alternative authentication mechanism to the traditional method. The knowledge on these attacks is also important for developers of new schemes to be aware of in order to design against them.

4.5.1 Brute-force attack

Brute-force attack is commonly used by attackers who use a trial and error method to exhaustively explore all possible passwords of users. It is based on "probabilistic techniques" whereby, when one object is selected randomly from a class of objects, the probability that the result would be the same as the desired result is more than zero. This attack can be done both online and offline, the latter of which does not require interaction with a live system to verify guesses.

In the traditional text-based password, attackers try to brute force attacking by testing millions of passwords for every possible combination of letters, digits and special characters until a desired password is found; this obviously requires time to reveal a password, depending on the capabilities of the machine used.

With graphical passwords, for example those from the recognition category, this attack are possible once the attackers have access to the database which keeps all of the

images. In the recall-based category, an attack can be launched using smart programs to automatically generate accurate mouse motions to imitate the human [17].

In addition, this attack will be more successful if conducted offline as, with sufficient time and computing power, all passwords can be found. Nevertheless, a full search of large password spaces is limited in practice by time or processing power available; using subsets might be faster but does not guarantee success. Thus, *theoretical password space*[10] should be large enough to minimise this exhaustive search attack. Unfortunately, this is not the case for many existing recognition-based systems; for example, Passfaces has only 9-image panels with 4 rounds, which results in only 9^4 = 6561 passwords.

In order to prevent this attack, a complementary mechanism (e.g. multifactor authentication) might be required. Password management policies can also force users to change passwords from time to time before the attackers manage to check all possible combinations.

4.5.2 Dictionary-based password attack

This attack is slightly more sophisticated than pure "trial and error" methods such as that implemented in the brute force attack. An attacker constructs a dictionary of either textual of graphical possible passwords which is used later to comprise an account with a username and the passwords in the created dictionary. For example, in text-based passwords, a dictionary could be constructed based on common memorable words and phrases, like date of birth or a combination of family names as passwords. This is one of the most common and successful attacks for text-based passwords as humans are prone to choose passwords which come from their personal lives because they are easily remembered [111].

On the other hand, with graphical passwords, this type of attack is popular, especially for the cued-recall type, as dictionaries can be built based on popular spots of an image. These popular spots are known as hotspots, where users have higher tendencies to click-

[10] Theoretical password space refers to the number of possible passwords that a scheme allows or in others words refers to the number of passwords an attacker must guess to ensure success.

on (i.e. select) their passwords [75]. This attack is more successful in capturing user's visual attention with the help of sophisticated algorithms. For example the algorithms might be able to capture the person's *bottom-up*[11] and *top-down*[12] visual and later use this information to build a dictionary that will be used to launch the attacks. However, from another point of view, dictionary attacks against graphical passwords may require more effort than against text-based passwords, as attackers need to collect one or more set of images. Furthermore, images gathered for one system will not help attacks on another, assuming each system uses different sets of images.

4.5.3 Phishing attack

Phishing attack is simple and yet very effective as it tricks users into entering their credentials (i.e. passwords) at fraudulent websites. This is done simply by directing users to follow a fake link that seems "believable" enough and which is commonly found in an email or specially engineered to return as search engine results [96]. Although the process of setting up a fake website might sound complicated, reports show that it is much easier these days with supportive tools, better known as "phishing kits", that can help create a phishing site within a short time [121, 50].

Phishing attacks on recall-based graphical passwords are very similar to those for text-based passwords. This is possible by creating a fake login page and simulating the area for drawing passwords; once the user draws his or her password, the sketch can be used for a legitimate website [181]. However, phishing attacks on recognition-based or cued-recall based systems require additional steps of presenting specific images to the users. In order to do so, a phishing site may have to conduct probes on the server to collect the images or conduct *man-in-the-middle* (MITM) attacks by retrieving and relaying information from the legitimate site [17]. Furthermore, using the MITM attack, attackers may also exploit the legitimate site by logging in at least once, hijacking a single correct authentication response during the attack.

[11] *Bottom-up* visual refers to human attention being drawn towards hot spots, for example recognisable shapes, bright colours or objects that are more likely to be selected [134].
[12] *Top-down* visual refers to the visual search where a user controls his/her attention by searching for a specific item in a picture [109].

There are several anti-phishing techniques developed to overcome this problem which generally can be classified as either the list-based technique or the heuristic-based technologies. List-based techniques maintain a black list or a white list (or both). However, what is more important is to maintain the black/white lists to prevent users from accessing fraudulent phishing sites. On the other hand, heuristic-based mechanisms employ several criteria to determine whether a website is a phishing site. Among the criteria used for identification are domain name, URL, image similarities, keywords and specific input fields.

4.5.4 Social engineering

Social engineering is one of the oldest attacks and has proven to be successful without incurring much cost. This type of attack does not involve any bugs or weakness of the system but instead manipulates users into believing that they need to provide the attacker with their personal information, thus, the aforementioned phishing attack is one example of this.

For text-based passwords, the attacks are much simpler; victims can easily describe their private information verbally or, even more straight forwardly, write it down. For graphical passwords, the success of this attack depends on how easy (or difficult) it is for the victim(s) to reveal their passwords. Research on the Passface scheme revealed that, although the scheme is vulnerable to description attack, a wise choice of decoy pictures can decrease its vulnerabilities [60].

On the other hand, the social engineering attack is a little bit more challenging for graphical passwords of the cued-recall based and recall-based systems, as the victims have to describe the chosen images, click point or pictures drawn. For example, in the PassPoint scheme, providing information on each click point on an image background can be quite challenging as there are too many possible spots that can be chosen from the background image. In the Passdoodle scheme, it is more challenging as it will not be easy for victims to describe the strokes drawn for their passwords.

Social engineering attack cannot be defeated easily as it requires only strong motivation of the attackers' part, while the weakness lies in the users, who are well known as the

weakest link in the whole system. Therefore, countermeasures depend on increasing awareness training and security policies. A good means of strengthening the defence from this attack was proposed by the developer of the Déjà Vu scheme who introduced abstract images which will be tougher to describe than images used as daily life objects [56].

4.5.5 Smudge attack

The smudge attack is relatively new as personal computing devices now commonly use touch screen inputs such as found in smart phones and personal digital assistants (PDAs). Touch screen basically involves interactions by touch which leaves oily residues or *smudges* on the screen as a side effect. These smudges not only become usable to infer recently or frequently touched areas of the screen but also dangerously becomes a form of information leak.

The Android password pattern is considered a type of graphical passwords where a user traverses an onscreen 3x3 grid of contact points [8]. A pattern can be formed of shapes which can be defined as an ordered list of contacts points. Figure 4.14 shows an example of "L" shaped password which can be represented as an ordered list of {1, 4, 7, 8, 9} where users begin by touching contact point 1, drawing downward towards point 7, and finally across to point 9.

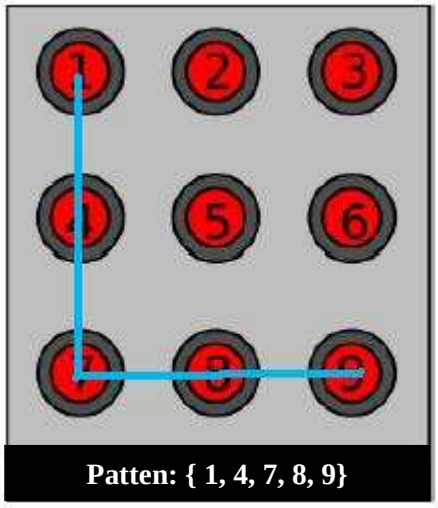


Figure 4.14: An example of "L" shaped Android password [8]

Aviv et al. [8] conducted a study to explore the feasibility of smudge attacks against android password patterns using photographs taken with a variety of lighting and camera positions. Their results have shown that, in many situations, complete or partial pattern recovery is possible even with smudge "noise" from simulated application usage or distortion caused by incidental clothing contact. Smudge data can be combined with statistical data on human behaviour (i.e. pattern usage distributions) for large sets of users to produce likely sets of patterns for a particular smudged phone. Another graphical password which might also be prone to this type of attack is Passdoodle and its type, especially if performed on a touch screen.

4.5.6 Shoulder surfing attack

Shoulder surfing attack is a type of attack that uses direct observation techniques such as looking over someone's shoulder to get information. This attack is relatively easy and yet effective, especially in crowded places where attackers can pretend to stand next to someone and watch as they fill out a form or enter a PIN number at an ATM machine. With advances in technological equipment, shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. For traditional text-based passwords, one way to prevent this attack is by concealing the output on the screen. However, this cannot be done in graphical passwords as it will suffer from usability problems. Thus, shoulder surfing attacks have been identified as one of the main concerns against adopting graphical authentication among users [174].

Aligned with this concern, much research has focused on improving protection against this problem, using various techniques. For example, Sobrado & Birget [165] developed the Convex Hull Click (CHC) scheme, using a huge number of pass-icons to confuse shoulder surfers trying to determine the correct pass-icon. However Man et al. [116] proved CHC to be unusable as so many objects had to be fitted on-screen at once that they were all too small, making it difficult for users to distinguish between pass-objects and non-pass-objects.

Besides creating confusion to distract attackers' attention, some studies have attempted to conceal users' input from the attackers. Using eye–tracking technology, DeLuca et al. [53] attempted to increase shoulder surfing resistance by using gaze to enter sensitive

input from an on-screen keyboard. Although promising, the approach requires expensive eye tracking equipment. The finger pressure technique introduced by Malek et al. [115] is another possible way to enter sensitive input while being resilient against shoulder surfing attack; however, their user study revealed some usability challenges.

Human cognitive ability has also been used as an approach to increase resistance against shoulder surfing. For example, Roth et al.'s [153] scheme requires users to answer a sequence of challenges posed by the system. Although this approach is claimed to provide better resistance to shoulder surfing attacks, it requires users to perform mentally demanding computation to pass the sequence of challenges and thus reduces usability.

Another approach that has been taken is to minimise the visibility of users' input. Gao et al's [71] scheme requires users to draw a curve across their password images in the correct order rather than click directly on them. In addition, they also displayed degraded or distorted images, as also used in UYI (UseYourIllusion) [86] with the intention of reducing the visibility of users' input in the hope of increasing protection.

Apart from software-based approaches toward providing shoulder surfing defence, there is also at least one hardware-based approach. A type of screen filter specially made for mobile devices known as privacy screen protector, using a polarization technique, is claimed to be able to enhance the privacy of its users [4]. The screen filter enables users to see from the front but is dark when viewed from the side by an angle of more than 30 degrees. However, this device burdens user with an additional cost of approximately £15 to purchase the device compared to our proposed approach using software-only, a far cheaper solution which does not limit the ability of device owners to share content by physically holding up the device for others to see.

4.6 Summary

This chapter provides an overall discussion on three different categories of graphical passwords. For each category, several examples were elaborated and discussed further focusing on design implementation and also the advantages and disadvantages of those

schemes. This chapter excludes discussion of the Draw-A-Secret (DAS) scheme as this was chosen as a focus study for further analysis.

This chapter also includes discussion on the possible attacks challenges for graphical passwords as most attacks on the traditional passwords are directly relevant to graphical passwords. It is interesting to note that graphical passwords are highly vulnerable to shoulder surfing attacks. This is due to the fact that concealing the input (i.e. as a mechanism of defence) is not possible for graphical passwords as it could result in usability problems.

Thus, the following chapter will continue the discussion on the selected scheme – the Draw-A-Secret (DAS) with a focus on shoulder surfing attack challenges. Several existing solutions to combat shoulder surfing attacks to the DAS scheme will be discussed in the next chapter so as to broaden our understanding of what could possibly be done to overcome this issue.

CHAPTER 5

THE DRAW-A-SECRET & EXISTING SOLUTIONS TO COMBAT SHOULDER SURFING ATTACKS

CHAPTER 5: THE DRAW-A-SECRET & EXISTING SOLUTIONS TO COMBAT SHOULDER SURFING ATTACKS

CHAPTER 5

THE DRAW-A-SECRET SCHEME & EXISTING SOLUTIONS TO COMBAT SHOULDER SURFING ATTACKS

5.1 Introduction

The previous chapter presented the literature on graphical password schemes. Among various types of graphical password schemes, Draw-A-Secret (DAS) has been chosen as a study focus to be discussed in this chapter. This is due to the fact that the DAS scheme is a good example of the recall-based category. The scheme is worth discussion as it has been shown to be promising, both from security and usability perspectives.

In addition, as previously mentioned, shoulder surfing attacks are highly problematic, especially for graphical passwords. Thus, this chapter will place its focus on the existing solutions to combat shoulder surfing attacks for the DAS scheme. This will provide a better understanding and support for possible solutions to overcome this issue.

5.2 The Draw-A-Secret (DAS) Scheme

5.2.1 Overview

Draw-A-Secret (DAS) was the first recall-based graphical password system proposed by Jermyn et al. [98]. As the name implies, it involves a password which is drawn as a free-form picture on an N x N grid. Unlike traditional text-based passwords, the graphical password approach is free from having to remember any type of alphanumeric string; instead, users can use hand-written designs (drawings) to represent their secret (password). This graphical password scheme works best on mobile devices, especially on “personal digital assistants” (PDAs), which allow users to provide graphical input to the device via a stylus.

The developers of this scheme proposed the idea of a graphical interface for providing input to enable users to decouple the position of the input from its temporal order [98].

In comparison to textual password input via a keyboard, the temporal order in which the user types characters uniquely determines their position in the password. In contrast, for this graphical password scheme, which consists of several drawn lines, the final position of each line can be determined independently of the temporal order in which the lines are drawn. This independence property not only produces an interesting scheme uniquely for this DAS graphical password scheme, but also significantly enhances its password strength compared with textual passwords, without increasing the memory demands on users.

The DAS scheme works differently from the recognition-based type of graphical passwords as it allows the device to recognise an input as being sufficiently similar to but not necessarily the same as the previously stored input. However, one major disadvantage of the recognition-based scheme is that it requires the password to be stored on the device; hence, the password is vulnerable to an attacker who acquires or tampers with the device.

In the DAS scheme, the passwords are repeatable in nature allows it to derive a secret key (e.g. to be used to encrypt and decrypt files) without the need to store the password itself on the device. This property protects both the password and the encrypted content from the attacker if the device is stolen or falls into the attacker's hands. The next section elaborates in detail how the DAS scheme works.

5.2.2 How the scheme works?

The DAS scheme allows users to draw their secret (password) on a plain grid canvas for any size of N x N. The grid is denoted by discrete rectangular coordinates (x, y) which are used to indicate the cells that are crossed by the user's drawn password. Figure 5.1 illustrates an example of a DAS password which is recorded by the system as a sequence of coordinate pairs: (2, 2); (3, 2); (3, 3); (2, 3); (2, 2); (2, 1); (5, 5), where (5, 5) is distinguished as a "pen-up" indicator. If, for example, there were a second stroke (or possibly more) then its sequences would be appended to the end of the sequence above. In order for a drawn secret to be accepted in authentication, it needs to cross the same grid of cells while ensuring the breaks between the strokes occur in the same place.

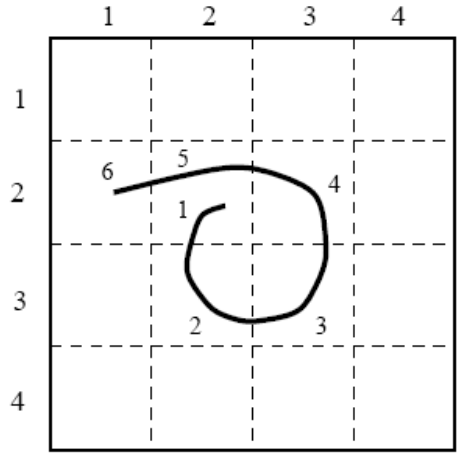


Figure 5.1: Example of DAS password [98]

The DAS password scheme, however, gives the user sufficient tolerance, provided that the cell sequence follows the same encoding, even though the drawing produced is not exactly the same. A drawing-secret will be disallowed if it crosses through a cell corner or traces the grid lines. These are known as illegal crossings due to fuzzy boundaries as it is difficult to ascertain which destination cell had been intended [98]. Figures 5.2 (a) and (b) show an example of fuzzy boundaries caused by tracing the grid lines and crossing through a cell corner respectively.

(a) Tracing grid lines **(b) Crossing through a cell corner**

Figure 5.2: Example of fuzzy boundaries [61]

There are several important factors that have been indentified to understand how the scheme works [98]. The terminology and definitions for each factor are as follows:

- The ***neighbours*** $N(x, y)$ of cell (x, y) are $(x – 1, y)$, $(x + 1, y)$, $(x, y - 1)$ and $(x, y + 1)$.

- ***Stroke***: a stroke is made up of a sequence of cells $\{c_i\}$ in which $c_i \in N_{ci\text{-}1}$ crossings are bound at both ends by pen-up events (exclusive of the pen-ups themselves). For example, the sequence pen-up (1,2) (1,3) (1,4) will define a stroke of (1,2) (1,3) (1,4).
- ***Length of a stroke***: is the number of coordinate pairs it contains. Therefore, if a stroke is made up of (1,2) (1,3) (1,4), then the length of stroke is equal to three.
- ***Stroke count:*** also known as the number of strokes which determine the length of password.
- ***Length of password*****:** is the sum of the lengths of its component strokes (exclusive of pen-ups). For example, if the password is made up of 3 strokes where each stroke has length of three, then the length of the password is equal to nine. This length of password is an important security metric to measure the strength of the DAS password.

The following section provides more discussion on the security of the scheme relating to the significance of each of the factors defined above in determining the strength of a DAS password.

5.2.3 The security of the scheme

In order to discuss the security of a particular password scheme, it is important to highlight the definition of "*information content*". The information content of a password space is defined as the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose. From another point of view, information content is the correct measure for describing difficulty of attack, since it determines the optimal choices to be made when trying different possibilities for a password. The level of information content (i.e. high or low) determines a password scheme more or less invulnerable.

The developers of the DAS scheme computed the size of the information content (i.e. the raw size of the password space) and assumed that all passwords of total length greater than a fixed value (L_{max}) have a probability of zero. They recursively computed the size of the full password space for passwords of total length $\leq L_{max}$ on a grid of size

of G x G. Table 6.1 shows the results for the number of passwords of total length ≤ L_{max} on a 5 x 5 grid [126]:

Table 5.1: Number of passwords where total length ≤ L_{max} on a 5 x 5 grid

L_{max}	1	2	3	4	5	6	7	8	9	10
$\log_2$ (# passwords)	5	10	14	19	24	29	33	38	43	48
L_{max}	11	12	13	14	15	16	17	18	19	20
$\log_2$ (# passwords)	53	58	63	67	72	77	82	87	91	96

In comparison to the traditional text-based password scheme for a 5 x 5 grid and L_{max} = 12, it is 2^{58} which surpasses the number of textual passwords of 8 characters or less constructed from the printable ASCII code ($95^8 \approx 2^{53}$). The results in the above table also indicate that, as the amount of total length increases, so does the strength of the DAS password.

This factor has been further investigated by Thorpe & Oorschot [179] who attempted to quantify the relationship between DAS password space and the length of passwords and their composites strokes. Their work was motivated by an observation that all permutations of dots are counted in the DAS password space (as shown in Figure 5.3):

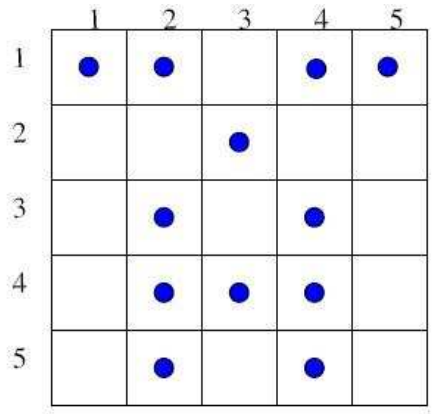


Figure 5.3: Example of DAS password consisting entirely of dots (single-celled strokes) [179]

This produced a large number of passwords, as the number of dot permutations for a given L_{max} on a W x H grid is $\sum_{i=1}^{L\max} (WxH)^i$. Therefore, for example, when L_{max} = 12, H = 5 and W = 5, the number of dot permutations is approximately 2^{56} (compared to a full password space of $2^{57.7}$). This result is reasonable since, if a password of fixed

length has longer composite strokes, it must have a smaller stroke-count and thus fewer permutations of its composite strokes. Figure 5.4 below explains further Thrope & Oorschot's [179] interesting findings.

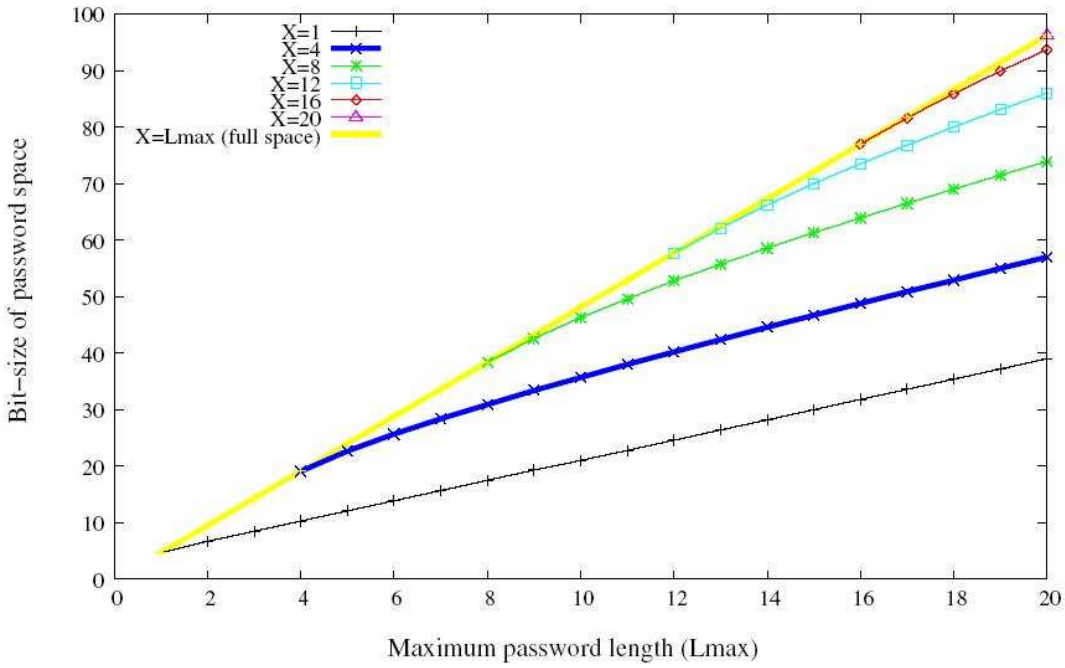


Figure 5.4: Size of graphical password space for passwords of at most *X* strokes (for 5x5 grid and a fixed maximum password length L_{max}) [179]

Figure 5.4 illustrates the role of strokes in the DAS password space; the size of the password space is significantly smaller (40 bits as opposed to 58 bits for the full space), provided that users choose a password of length at most 12, composed of 4 strokes or fewer. The password space size still increases with longer password lengths (refer to the rise in each curve), but the amount of increase is less for smaller stroke-counts (refer to the gradual slopes for lines with smaller values of *X*).

In addition, for a fixed L_{max}, a smaller maximum stroke-count X (refer to lower lines) implies a longer average stroke length. These findings suggest that the strength of DAS is determined by taking into account the temporal order in terms of the direction of the strokes and also the order in which these strokes are drawn. This justifies why increasing the stroke count achieves such gains in the size of the password space, which are due to the fact that there are many more permutations of these strokes.

The results shown in Figure 5.4 above can also be viewed from a practical point of view, for example, the time taken to exhaust a DAS password dictionary consisting of all passwords of length less than 12, on a 5 x 5 grid, for each maximum stroke-count *X*. Thrope & Oorschot [179] further calculate two sets of time estimation: one is by assuming that one attacker has a *Pentium 4*, 3.2 GHz machine and another has 1000 such machines (in which linear speed-up is achieved). Table 5.2 below displays the output of their estimation.

Table 5.2: Estimated time taken to exhaust various dictionaries using 3.2GHz machines (for 5x5 grid and a fixed maximum password length of 12) [179]

Maximum number of strokes (*X*)	Time to exhaust (1 machine)	Time to exhaust (1000 machine)
12	541.8 years	197.8 days
11	409.7 years	149.5 days
10	205.3 years	74.9 days
9	72.6 years	26.5 days
8	18.1 years	6.6 days
7	3.2 years	1.2 days
6	157.1 days	3.8 hours
5	14.9 days	21.4 minutes
4	1.1 days	1.5 minutes
3	1.2 hours	4.4 seconds
2	2.3 minutes	0.1 seconds
1	1.9 seconds	0.002 seconds

The above table suggests the importance of stroke-count. For example, if users choose passwords of length at most 12, with a stroke count of at most 4, an attacker could guess their password using one machine in only 1.1 days. Hence, the greater the number of stroke-counts, the better the password will be.

5.3 Existing solutions to combat shoulder surfing attacks for the DAS scheme

The issue of shoulder surfing attacks has been discussed in previous chapters, within the discussion of attack challenges for graphical passwords. As the DAS scheme is also a type of graphical password (from the recall-based category), it is also vulnerable to similar types of attack, particularly shoulder surfing. This is due to the fact that DAS

users typically draw their passwords on a white canvas consisting of NxN gridlines which make it visible to attackers (shoulder surfers), especially when these users are commonly found handling authentication procedures in public places such as at the airport while waiting for their flights, on train journeys or even in the clinic while waiting for an appointment.

Several efforts to overcome the shoulder surfing attack problem, particularly from the other two categories - recognition-based and cued-recall based - have been discussed in the previous chapter. As this chapter focuses mainly on the DAS scheme, this section will focus on the existing solutions to overcome the problem of shoulder surfing attack pertaining to the DAS scheme.

Although Dunphy & Yan [61] proposed Background Draw-A-Secret (BDAS) , which introduces a background scheme to the original white canvas in the DAS scheme, this solution is not intended to overcome shoulder surfing attacks, but to increase the memorability of the DAS password. Currently, there are several researchers working to reduce shoulder surfing attacks in recall-based graphical passwords. The next sub-section elaborates those interesting attempts to overcome the problem.

5.3.1 Passgraph: Haptic-based input mechanism

One particularly interesting effort is based on the finger pressure technique (also known as *haptic-based input* mechanism) introduced by Malek et al. [115]. Their argument is straightforward in that the only way to thwart shoulder surfing attacks is by using finger pressure (caused by the stylus while entering the input) to reduce the ability of attackers to clearly watch all the sensitive information being entered into the login terminal. The *haptic-based input* mechanism is not visually observable but allows users to deliberately enter the password and achieve a repeatable and solid password scheme. Their proposed scheme is known as Passgraph and is based on a type of recall-based graphical password scheme: Pass-Go, introduced by Tao & Adams [174].

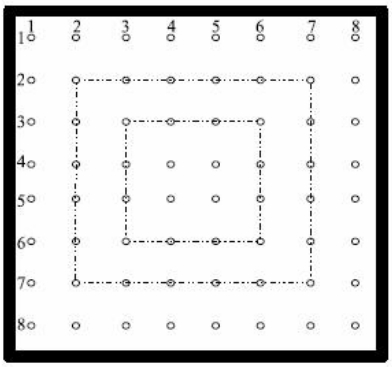
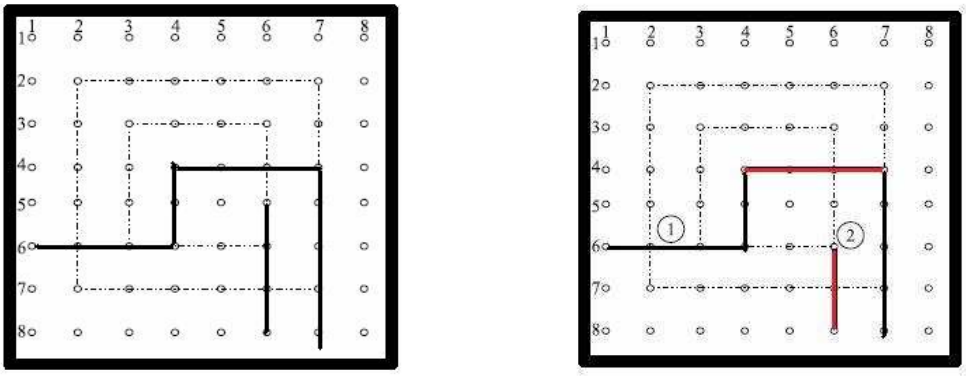


Figure 5.5: Visual interface of Passgraph scheme [115]

Figure 5.5 shows a visual interface for the Passgraph scheme where users can connect any two points on the grid selectively. By allowing users to connect the two points on the grid, the size of possible password space is increased more than for Pass-Go [115]. Passgraph includes a pressure element as an additional component for choosing a password; therefore, the user's password will be a combination of coordinates and the pressure of the input device, which is recorded as binary input.



(a) Example of Passgraph drawn by user **(b) The red lines indicate the high pressure applied by user**

Figure 5.6: Example of Passgraph [115]

Figure 5.6 provides an example of Passgraph. The information captured from the Passgraph drawn in Figure 5.6 is a tuple (*x*; *y*; *p*) where *x* and *y* represent the position of the selected points on the horizontal and vertical axes respectively, and *p* is a binary input indicating if high (more than the user's average) pressure is exerted when two points on the grid are connected. For example, the Passgraph drawn in Figure 5.6 above is recorded as the following (where (¡1;¡1;¡1) indicates a pen-up event :

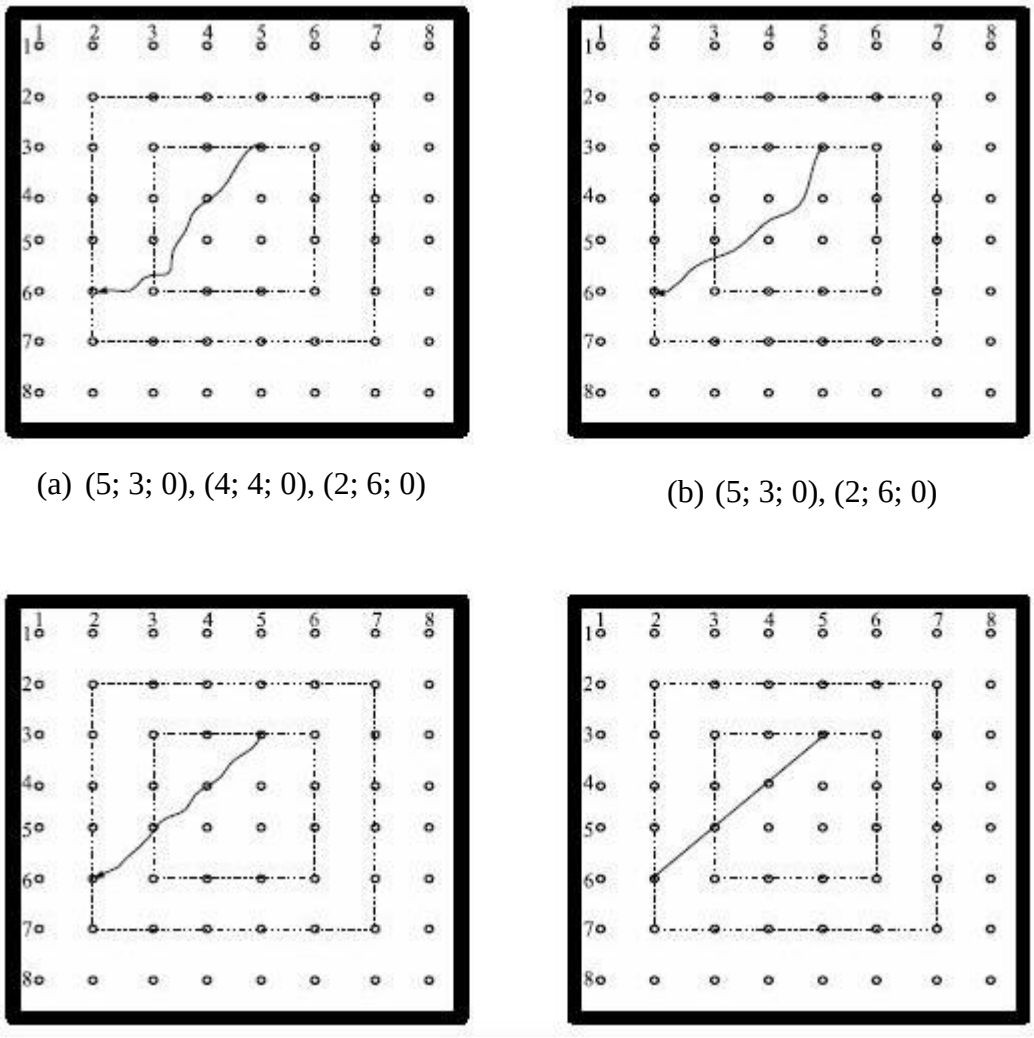
(1;6;0); (2;6;0); (3;6;0); (4;6;0); (4;5;0); (4;4;0); (5;4;1);
(6;4;1); (7;4;1); (7;5;0); (7;6;0); (7;7;0); (7;8;0); (¡1;¡1;¡1);
(6;6;0); (6;7;1); (6;8;1); (¡1;¡1;¡1):

The length of the Passgraph above is 17, consisting of the tuples and a number of pen-up events (the last pen-up event is not counted as it contains no information). The pressure exerted by the user while drawing a Passgraph is recorded as binary input and given the value of 0 when it is equal to or less than the user's average pressure which is otherwise given a value of 1.

According to Malek et al. [115], the input pressure is estimated at 20% above the user's average pressure (when the user is instructed to apply high pressure as part of their password). In other words, if the input pressure is less than 120%, it is assumed high pressure is not applied by the user, and hence the third component (p) in the tuple ($x; y; p$) is recorded as 0. The Passgraph scheme differs from DAS in that user can connect any two points on the grid without having to cross other points; that is, in the Passgraph scheme, the sequence of every tuple can be put together irrespective of where on the grid the users draw the password. Figure 5.7 shows several possibilities of drawings that users may use to connect two pints on the grid.

A user study on Passgraph was conducted involving 18 volunteers and the results have shown that, although more than half of the participants applied pressure at some point while drawing their password, they admitted to not feeling comfortable doing so [115]. Usability issues have commonly become a drawback of adopting a particular technique, especially when security becomes the main target to achieve. Nevertheless, the authors of the Passgraph scheme are optimistic that the hesitation to apply pressure was due to lack of familiarity with the new technique rather than a usability issue per se. It is interesting to discover that more than half of the volunteers involved in the study actually recorded their Passgraph which indicates that users actually do write down their passwords, even when using graphical authentication. In view of this issue, the pressure, as an additional component to the password, increased the memorability burden and this probably explains why users noted down their Passgraph (although it is supposedly simpler than the DAS scheme). Although the haptic based mechanism is indeed

showing promising results in overcoming shoulder surfing problems, the issue of usability is a highly important consideration, especially for such a new scheme.



(a) (5; 3; 0), (4; 4; 0), (2; 6; 0)

(b) (5; 3; 0), (2; 6; 0)

(c) (5; 3; 0), (4; 4; 0), (3; 5; 0), (2; 6; 0)

(d) Actual Passgraph

Figure 5.7(a) – (d): Different possibilities that users may use to connect two points on the grid [115]

5.3.2 Qualitative Draw-A-Secret (QDAS)

Inspired by the DAS scheme as an example of recall-based graphical passwords, Lin et al. [112] extended the original scheme into something called Qualitative Draw-A-Secret (QDAS). In this new scheme, not only did they try to improve the flexibility aspects, but also to increase shoulder surfing protection of the original scheme. As mentioned previously, the main drawback of the DAS scheme is the restriction on free-form

images on the drawing grid, whereby users are not permitted to trace or cross the gridlines because this will result in error (known as fuzzy boundaries).

QDAS employs a new way of encoding each stroke, consisting of its starting cell and the sequence of qualitative direction changes in the stroke relative to the grid. Figure 5.8 illustrates a simple stroke being drawn with the new encoding scheme, starting at cell 6 and followed by “down”, “right” and “up”. The difference in QDAS is that it enables users to deviate from the literal spatial definition of their secret. Figure 5.8 shows that both long and short strokes share the same encoding thus increase the flexibility of not having to memorise all the cells that cross to produce the password, as in the original DAS scheme.

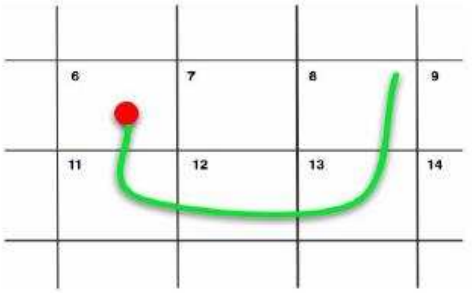
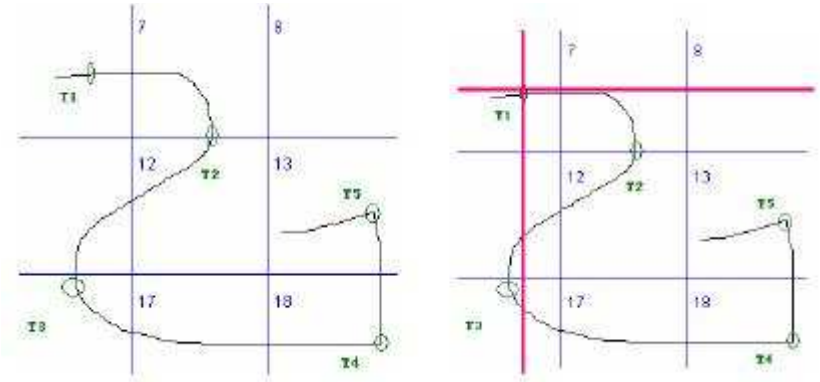


Figure 5.8: An example of stroke drawn in QDAS scheme – employing new encoding scheme using direction rather than the cells it crosses [112]

QDAS employs a technique called dynamic grid transformation to mask the ongoing process of creating the secret (password), thus providing a level of protection against shoulder surfing [112]. Figure 5.9 below shows an example of grid transformation:



(a) (b)

Figure 5.9: (a) Culculating turning points of the stroke (b) An example of dynamic grid transformation [112]

In order to transform the grids, turning points in the stroke are calculated and for the first four of these turning points a vertical line, where x is equal to the x value of the turn, followed by a horizontal line, is drawn, where y is equal to the corresponding y value of the turning point. This result in two perpendicular lines (red colour lines as shown in Figure 5.9 (b)) that intersects at the current turning point.

A preliminary study was conducted involving 20 students and aimed to compare both schemes (QDAS versus DAS) according to three aspects: usability, ease of shoulder surfing and memorability. There was no significant difference found between both schemes in terms of usability and memorability. In order to test shoulder surfing resistance, participants in the study were shown a video recording of moderators drawing QDAS and DAS; versions of the same secret were shown to the subjects (who were advised that they should act as a shoulder surfer, trying to capture enough information). The result shows that none of the participants in the QDAS group managed to successfully recreate a *stolen* password, while in the DAS group, 70% were able to successfully recreate the password. The results of the preliminary study seem promising and feasible; nevertheless, further analysis is required to improve the ecological validity of the experimental findings.

5.3.3 YAGP: Yet another Graphical Password

The YAGP scheme extends the original DAS scheme by trying to improve several of its restrictions. Unlike the original DAS, YAGP is a position-free scheme, in which a user can draw the graphical password anywhere on the canvas. For example, the user can make a drawing in a small corner where it is harder to been seen by shoulder surfers. Another unique characteristic of this scheme is that the stroke sequence cannot be reflected by the graph and the authentication process sees it as a critical checking factor [70]. This property ensures that shoulder surfers still cannot sign in, even upon successfully glimpsing the drawings (of the password), because they cannot recall the correct stroke sequence set by the legal user. Figure 5.10 below shows the prototype interface of the YAGP scheme.

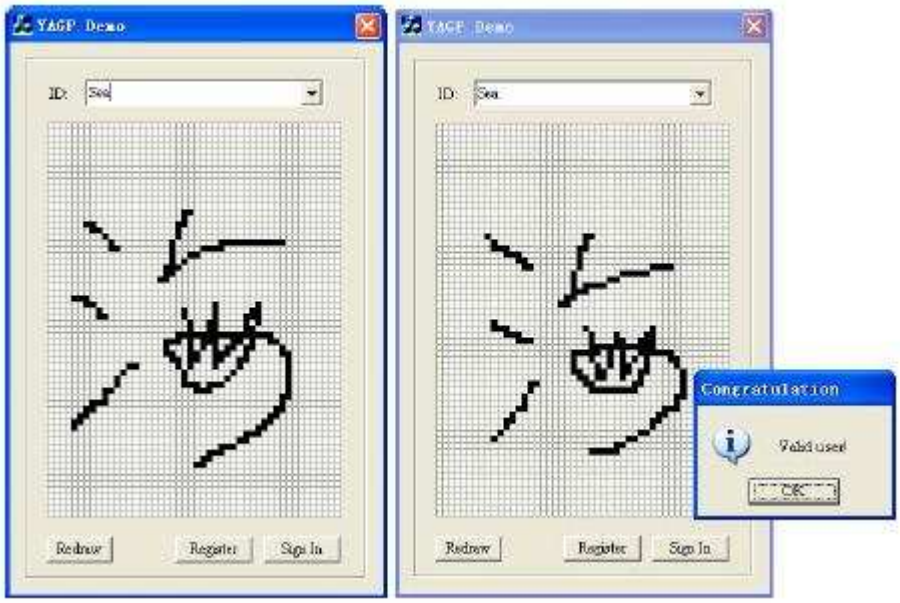


Figure 5.10: Prototype interface of YAGP scheme [70]

The authors of the scheme claim that YAGP takes into account drawing trends, whereby a user's drawing style is recorded to a certain extent. This is possible by using a method called *trend quadrant* in order to compare the stroke trends between two drawings. Figure 5.11 illustrates the concept of the *trend quadrant* proposed.

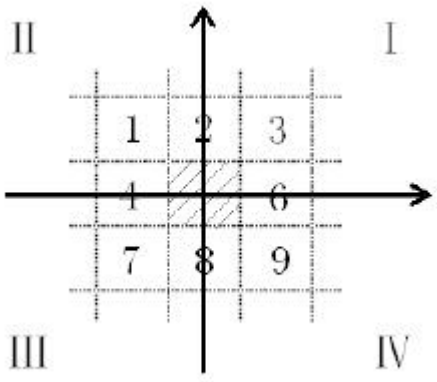


Figure 5.11: Trend quadrant concept [70]

Based on Figure 5.11 above, there are four trend quadrants denoted by I, II, III and IV. Each represents an up-right, up-left, down-left and down-right trend respectively. Each stroke drawn is divided into several segments in order to compare number of trends and to evaluate the similarity of the corresponding segments of the original and re-entered passwords. The authentication is considered successful when the two counts (number of trends) are equal and the similarity is higher than a predefined threshold value. For

instance, as illustrated in Figure 5.12 below, different people may produce different styles when drawing the same letter “Q” on the grid canvas.

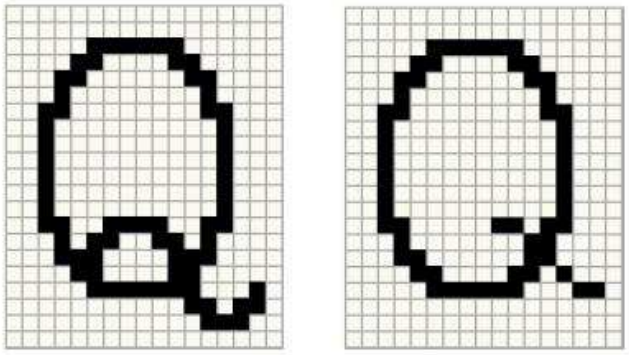


Figure 5.12: Trend quadrant trends of different styles of drawing letter “Q” [70]

A preliminary experiment was conducted to test the YAGP scheme involving 30 university members. The participants were asked to draw their password and then re-draw it for authentication purposes. At the same time, every participant was asked to peek at their neighbours’ password and attempt to attack. The experiment tested several density grids, as well as several threshold values of similarity to determine the most appropriate use for the scheme. The results have shown that the best density grid used was 48x64 as this allowed all of the participants to be authenticated successfully. However, the results did not indicate whether the successful login attempt was done instantaneously or that several attempts were required. Based on the results of the appropriate density grid to be used, the experiment recruited another 18 new participants to determine the threshold value of similarity. A similar procedure was carried out, varying the level of threshold between 55% - 80%. The results showed that 60% of the threshold value was found to be the most appropriate for usage.

The two properties above (density grid versus threshold value) are crucial in determining the balance between security and usability. This can be clearly seen from the results, whereby successful shoulder surfing attacks occurred most often with the 48x64 density grid and 55% threshold value. It is predicted that in order to accommodate usability, security becomes the trade-off. Nevertheless, this scheme introduces the novel idea of incorporating a user’s personal style of drawing, which is difficult to imitate, and the concept seems promising in increasing shoulder surfing protection.

5.3.4 Rotation Draw-A-Secret (R-DAS)

Rotation Draw-A-Secret (R-DAS) is a scheme that enhances the original DAS scheme by adding rotation as part of the password component. Chakrabarti et al. [37] proposed the idea of rotating the canvas of a drawn password on the z-axis, either in a clock-wise or anti-clock-wise direction. Unlike DAS, the R-DAS user is allowed to rotate the drawing grid not only in between strokes, but also after completing the drawing the entire password. Thus, the event of rotation occurs after a pen-up event. Consecutive rotations in the same direction share the same encoding unless the direction is changed, in which case the encoding is modelled as two separate events. Figure 5.13 below shows an example of an R-DAS password being drawn, beginning with empty canvas followed by several strokes and rotations involved.

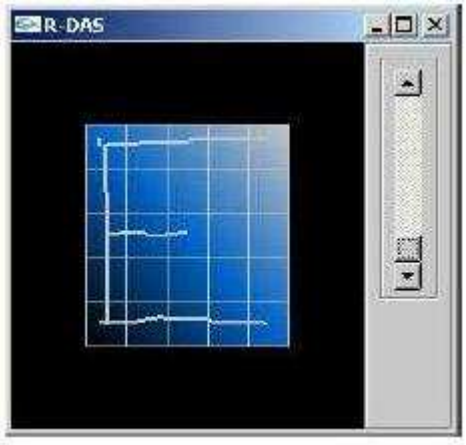
(a) The blank drawing canvas

(b) First stroke drawn: (1,1)(2,1)(3,1)(4,1)(5,1)(6)

(c) Rotation of 90^{o}and another stroke drawn: (-90)(5,1)(5,2)(5,3)(5,4)(5,5)(6)

(d) Rotation of +90^{o}, rotation of -45^{o}, then another stroke drawn: (+90)(-45)(1,1)(1,2)(1,3)(1,4)(1,5)(6)

(e) Rotation of +225^{o} and the final stroke drawn: (+225)(3,1)(3,2)(3,3)(6)



(f) Final rotation of +180^{o}

Figure 5.13: Example of R-DAS password being drawn involving several rotations [37]

The developers of the scheme claimed that introducing rotation to the original scheme increases resistance to shoulder surfing attacks to certain extent. This is by considering the scenario in which an attacker manages to get a glimpse of the final drawing on the canvas while the user is making an attempt to log in; in this case, the attacker would have to guess the sequence in which the strokes were made (including the direction of the strokes and the rotations).

The developers of the scheme admitted however that, by knowing whether the user is right or left-handed, the attacker can guess the direction of the strokes and possibly the rotation too. Although this might be true to some degree, no user study or preliminary evidence has been reported by the authors of the scheme to support the above claims. Nevertheless, it is quite obvious that the scheme can easily be penetrated by shoulder surfers who equip themselves with sophisticated camera or recording devices which enable the entire login procedure to be recorded.

5.4 Summary

This chapter has placed its focus of discussion on one selected graphical password from the recall-based category that is the Draw-A-Secret (DAS) scheme. The discussion provides an overview and analyses design implementation and security of the scheme.

Due to the fact that shoulder surfing attacks are cited as among the main concerns for adopting most graphical password schemes, this chapter has included in the discussion several existing solutions to combat shoulder surfing attacks for the DAS scheme. The existing solutions were found to suffer from either an imbalance of security and usability or a lack of extensive study conducted to evaluate the proposed approach. Hence, this study proposes three general defence techniques for recall-based graphical passwords to help minimise shoulder surfing attacks.

The next chapter will introduce and elaborate on these three proposed defence techniques. A prototype of the three defence techniques has been implemented on the DAS scheme as it represents a basic example of the recall-based category. An evaluation study has also been conducted to test the scheme from both security and usability perspectives. The details of the evaluation study will be discussed in the next chapter.

CHAPTER 6

THE PROPOSED SHOULDER SURFING DEFENCE TECHNIQUES FOR RECALL-BASED GRAPHICAL PASSWORDS & THE EVALUATION STUDIES

CHAPTER 6: THE PROPOSED SHOULDER SURFING DEFENCE TECHNIQUES FOR RECALL-BASED GRAPHICAL PASSWORDS & THE EVALUATION STUDIES

CHAPTER 6

THE PROPOSED SHOULDER SURFING DEFENCE TECHNIQUES FOR RECALL-BASED GRAPHICAL PASSWORDS & THE EVALUATION STUDIES

6.1 Introduction

In chapter four, the discussion indicated that many of the existing studies on resistance to shoulder surfing attacks on graphical passwords have mainly focused on recognition based authentication techniques. Motivated by the lack of attention given to recall based techniques this study explores the possibility of providing an effective defence. Thus, this chapter introduces three proposed defence techniques to minimise shoulder surfing attacks for recall-based graphical passwords. It is important to note that, in order to evaluate the proposed techniques, a prototype has been implemented of the DAS recall-based graphical password scheme. Therefore, although the proposed defence techniques were designed as a generic model for recall-based graphical passwords, the discussion will relate to the DAS scheme.

This chapter will also discuss the evaluation studies that have been conducted with the aim of determining the most effective shoulder surfing defence techniques among the three that have been proposed. The evaluation has been conducted in two separate experiments; the first experiment examines the security perspective, followed by a second experiment which focuses on usability of the proposed schemes.

Details for each experiment, such as the hypotheses, design, apparatus and procedures, will be included in the discussion. Each experiment will also have its own analysis, followed by a discussion to reflect upon its objectives.

The outcomes from both experiments will validate the strengths and weaknesses of the proposed defence techniques and thus suggest the most effective defence technique for recall-based graphical password.

6.2 The three proposed defence techniques

Inspired by some of the previously discussed, existing solutions to enhance the protection of graphical passwords from shoulder surfing attacks, this study proposes three defence techniques which have been designed to protect recall-based graphical passwords. The three proposed defence techniques are named as follows: the decoy stroke, the disappearing stroke and the line snaking. Each of these techniques will be detailed in the following sub-sections.

6.2.1 Decoy strokes

The first defence technique is called decoy stroke, as the idea of using decoy strokes as a defence involves creating real time strokes along-side a user's password. The decoy strokes appear to be "believable" enough as they resemble strokes that could have been drawn by a user.

The aim of this technique is to distract an onlooker's (i.e. attacker's) attention away from the actual password drawn by the user. As the aim of introducing the defence technique is mainly about enhancing security, it is important that the existence of decoy strokes does not affect usability. Therefore, the decoy strokes must appear without confusing the user so as not to prevent correct entry of the password, which would drastically reduce the usability of the system. This defence is also expected to give the appearance of added complexity to a password by adding extra strokes, without actually modifying the user's password. This technique is expected to add security in particular to simple passwords that could easily be memorised and replicated by an attacker. Figure 6.1 shows the pseudo code which was outlined as a basis for developing the decoy strokes method.

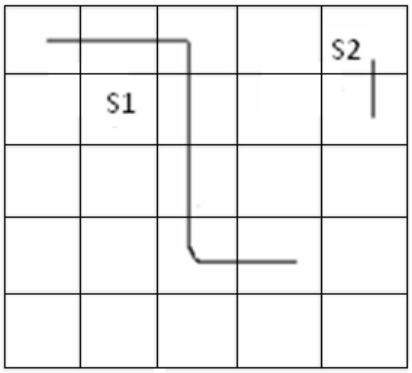
It was decided that the strokes had to be generated randomly and displayed as the user was drawing; otherwise, strokes that were from a library could become repetitive and would therefore be spotted by an attacker as a decoy (thereby introducing weakness to the system).

```
Location[] decoy;
while(int i = 0; i <4; i++)do
X = generate random number < grid boundries
Y = X = generate random number < grid boundries
Location l = (X, Y);
Add to decoy(l)
od
drawCurve (decoy);
```

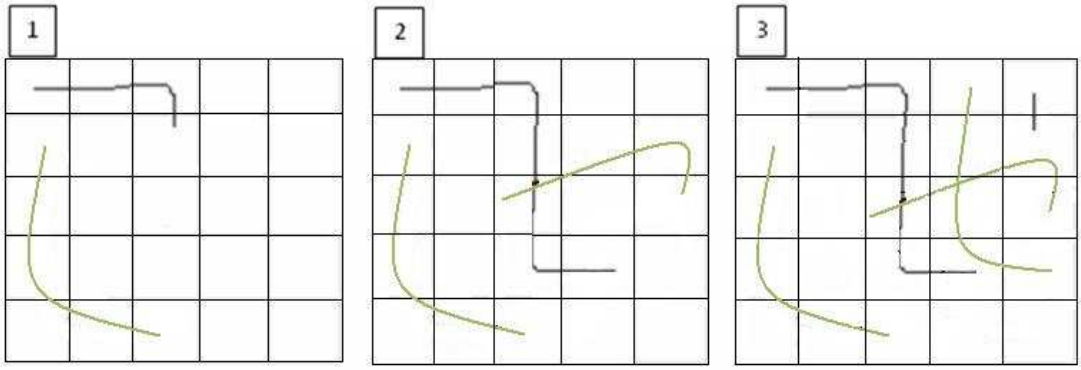
Figure 6.1: Simple random point generation pseudo code

Moreover, if the decoy strokes appeared randomly when a user had not yet started drawing, an attacker would be given further information which would help him/her to distinguish between the user and the decoy strokes. Again, this would result in making the solution less effective at resisting shoulder surfing.

In order to retain the usability of DAS, two variables (the colour and thickness of decoy strokes) have been added as user controlled features in the prototype system. This controlled feature enables users to clearly distinguish between the two strokes, with the intention of keeping the attacker bemused by all the information on the screen. Figures 6.2(a) and (b) were created as a story board to show how the output of the defence should appear.



(a) When the defence is not activated



(b) When the defence is activated

Figure 6.2: Decoy stroke defence technique

(*Note: Left to right proceeds with time, S1 – Stroke 1, S2 – Stroke 2 and decoy strokes are in green*)

Figure 6.2(a) shows a user password (in black) and Figure 6.2(b) shows a decoy stroke (in green) being drawn. The choice of colour for the decoy is crucial. In this study, it was decided to use dark brown in order to ensure that it is not too similar to the user's password strokes. This is because maintaining the same colour (i.e. black) as the user's password strokes might lead the user to confuse the actual password with the decoy strokes and thus affect usability.

However, as the aim of having a defence technique is for security purposes, the strokes must not be too different; for example, using red as the colour for the decoy strokes might be too obvious in contrast to the black of the original colour of the password strokes and this might render the defence useless. As the user draws the password, the decoy stroke is drawn at a similar rate. In the interests of not confusing the user during the login phase, a relatively small number of decoy strokes were used. In this study, the limit was four decoy strokes, but this could be easily changed or added as a user controlled feature.

In terms of implementation details, a decoy stroke begins at a randomly selected point within the DAS drawing grid that the user is allowed to draw on with the stylus, and is limited to being of a "believable" length. The algorithm then randomly generates new co-ordinate points which are to form part of the decoy stroke. However, in order to make the stroke realistic, the distance away from the previous stroke and the direction

change had to be limited; although still random, the distance away from the previous stroke has a maximum value and a random direction change is only allowed every four points.

A typical decoy stroke could entail the following steps (where point refers to a co-ordinate):

1) Generate four random points that lie within grid confinements.
2) Add the points to the stroke data structure.
3) Display part of the stroke, slowly revealing more of the stroke.
4) Repeat while the user is still drawing until the maximum number of decoys has been created.

The decoy strokes are only generated whilst the user is still drawing. This is because, if they continue to appear for too long after the user has finished drawing a stroke (i.e. when the user has lifted the stylus away from the PDA) then it would be easier for an attacker to distinguish between the user's stroke and the decoy stroke. In order to make decoy strokes display as realistic, smooth curves rather than straight interconnected (jagged) lines, the cubic Bezier curve fitting algorithm was implemented as follows:

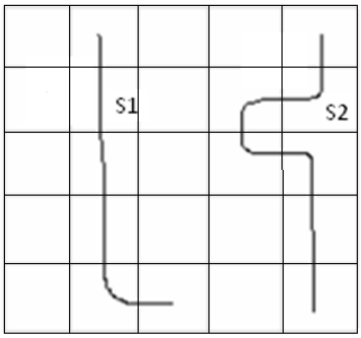
$$B(t) = (1-t)^3 P_0 + 3t(1-t)^2 P_1 + 3t^2(1-t)P_2 + t^3 P_3 \; ; \; t \in [0,1]$$

This algorithm enables four points to be fitted to a curve, making the stroke look more realistic and "*human-like*" and hence more likely to improve shoulder surfing resistance.

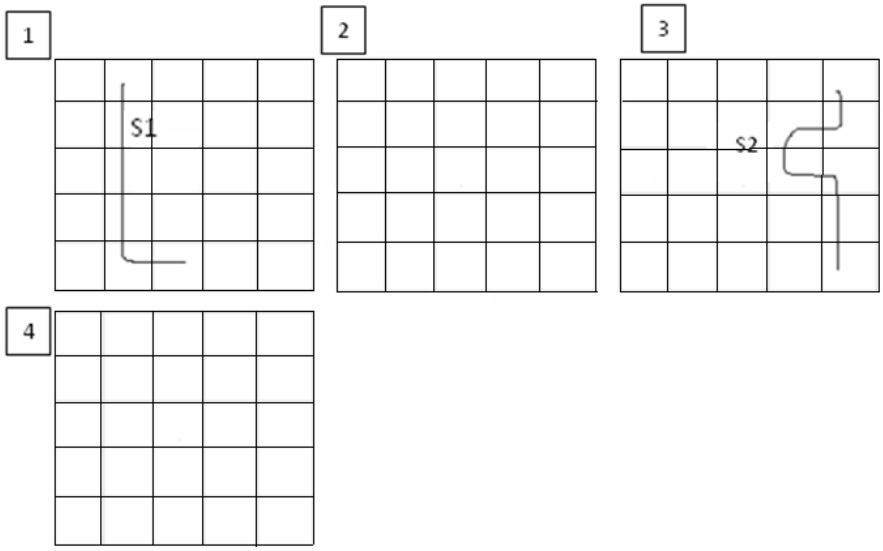
6.2.2 Disappearing Strokes

The disappearing stroke solution entails the user stroke being removed from the screen after it has been drawn. The idea behind this is that the password information of an individual stroke is removed, which gives the attacker less time to store the image to memory. This solution is designed for both passwords that have multiple strokes, and passwords of one long stroke, although it might work better for the former type of password.

The stroke was designed to be wiped from the screen only after the user has finished drawing that particular stroke (i.e. when the stylus is removed from the screen). This was designed using a timer, of which the purpose was to remove the stroke after a certain period of time (after the pen up event). Figure 6.3(a) shows an example of a DAS password without any defence, while 6.3(b) shows how the output of the defence technique should function as time proceeds.



(a) When the defence is not activated



(b) When the defence is activated

Figure 6.3: Disappearing stroke defence technique

(*Note: Left to right proceeds with time, S1 – Stroke 1, S2 – Stroke 2*)

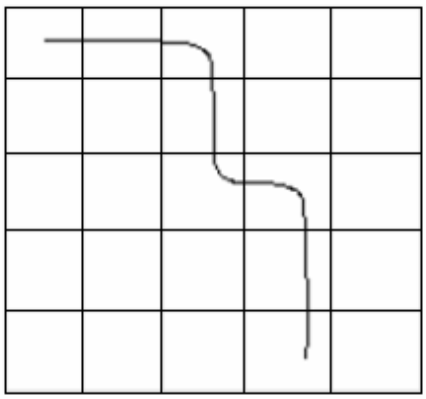
The variable factor in this defence technique is that the amount of time that has to elapse before the stroke disappears from the screen should be kept within a restricted range. This is to ensure that the shortest time does not affect usability and the longest time does not have an adverse outcome on the effectiveness of the defence. A possible

implementation for this defence could be starting a timer after a user pen up event, which would clear the stroke from the screen after a certain time period.

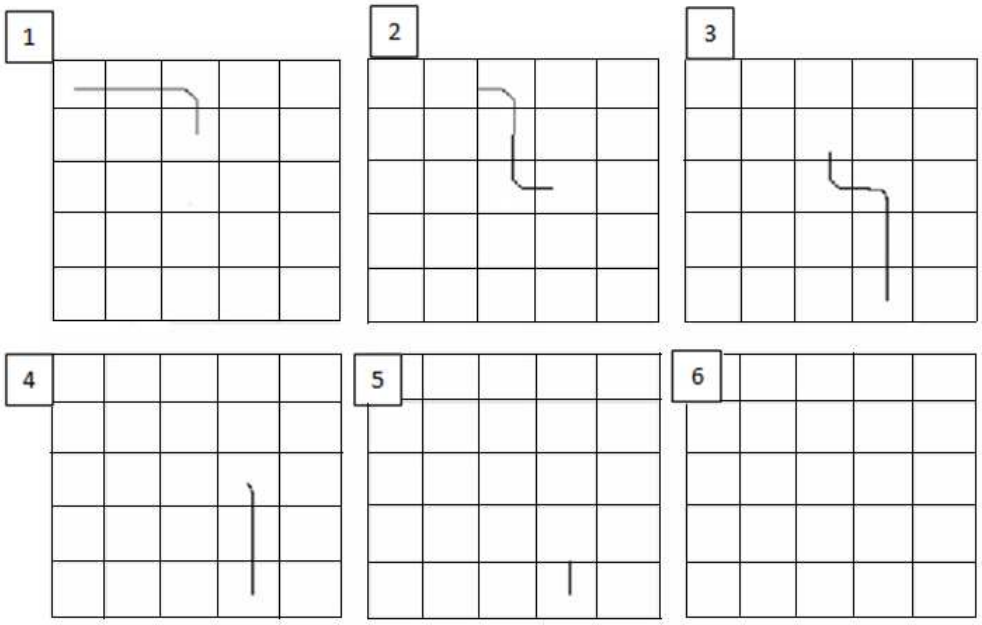
6.2.3 Line Snaking

This defence is based on the disappearing stroke solution but was intended to leave the vital password information onscreen for an even shorter period. An attacker is therefore not given a chance to see a complete user stroke onscreen. It would involve the start of the user stroke being removed from the screen as the user is still drawing, giving the appearance of the line snaking towards the user's stylus.

The line snake defence was designed to combat shoulder surfing for passwords containing long singular strokes. Hence, allowing stroke information to be removed from a long singular stroke, whilst the stroke is still being drawn. The variable factor for this solution was decided upon as being the speed at which the user stroke disappears (or snakes away) from the screen. This again was thought to be limited to within a sensible range so as to maintain the usability and effectiveness of the solution; otherwise, the stroke may be removed too quickly or too slowly. Figure 6.4(a) shows an example of a DAS password without any defence, while 6.4(b) shows how the output of the defence technique should function as time proceeds.



(a) When the defence is not activated



(b) When the defence is activated

Figure 6.4: Line snaking defence technique

(*Note: Left to right proceeds with time*)

The way how this defence was implemented is based on the starting of a timer from when the user begins drawing the stroke which eventually controls the line snake. A simple procedure removes points from the beginning of the stroke. This procedure is followed every time the timer ticks which resulted in giving the appearance of the line snaking towards the stylus's current position. It is however, independent of the speed of the strokes drawn (e.g.: if a user tries to speed up drawing a particular stroke) as the timer will control the speed and thus the appearance of the line snaking effect on the screen. The following sections will discuss two separate studies conducted to evaluate the proposed defence techniques.

6.3 Security evaluation - Experiment 1

The aim of this first experimental study is to determine the strongest defence technique among the three being proposed, by conducting a controlled laboratory experiment. Before this experiment was conducted, approval was obtained from the University Ethics Committee (UEC).

6.3.1 The experimental design

This experiment was based on between-subjects design. Although this type of design requires more participants, it ensures that the exact same passwords were used in each experiment condition so that they would not be a compounding factor, biasing the results. The main independent variable for this experiment is the defence technique. In addition, this experiment also explores password strength as a secondary independent variable. The dependent variable is the participant's response.

In order to guide our analysis, the following hypotheses were set out:

H_1 – Disappearing Strokes will not work as well as Line Snaking, as, for the latter, the strokes are snaking away while being drawn, leaving a very short time for the strokes to stay visible on the screen and be observed.

H_2 – Decoy Strokes are the weakest defence as all the strokes of the password remain visible on the screen.

6.3.2 The experimental procedures

At the beginning of the experimental session, informed consent and demographic information was obtained from each participant. They were asked to provide their age, gender, educational background, and experiences using PDAs. The participants were randomly assigned to one of the following four experimental groups:

1) Decoy Stroke
2) Disappearing Stroke
3) Line Snaking
4) Control Group (The undefended DAS scheme)

Each group had equal numbers (17) of participants who each spent approximately 15 minutes completing the experiment. Reviewing the issues which arose in previous work [112] regarding ecological validity, this experiment attempted to simulate a shoulder

surfing scenario. The participants were asked to play the role of shoulder surfers, trying to steal 3 passwords by observing them during individual login attempts. To ensure they acted as shoulder surfers (i.e. a true shoulder surfer would have the intention of stealing the passwords), an additional incentive to increase their motivation was offered. The participants were told that there would be a competition between them and that there would be only one prize given to the participant who performed the best from the best defence technique group.

During the experiment, each participant was given a brief introduction to the DAS graphical password scheme. For participants who were assigned to the treatment groups, extra information about the assigned defence technique was also provided. This was done under the assumption that shoulder surfers are aware of the defence technique being employed and are equipped with similar knowledge. Printed information was also supplied to support the briefings.

Participants were highly encouraged to ask the experimenter any questions, especially on how to construct the passwords, as they needed to reproduce them later in the experiment. Then, a quick demonstration on how the prototype system works was shown to the participants. The participants were then allowed quick, hands-on experience of using the prototype system. A short training session on shoulder surfing was then conducted. The aim of this was to ensure that participants understood their task. In order to conduct this training, the participants were instructed to act as a shoulder surfer and make an attempt to steal the password drawn by the experimenter while logging in. The password used in this training was similar to the example provided in the printed information given to them earlier.

It was decided that the experimenter would act as “the victim” to the shoulder surfing attack throughout this experiment. The reason for having just one person (the experimenter) being the victim was to reduce the effects on the results of inconsistency or bias produced by two different people’s login skills. The experimenter also underwent sufficient training to ensure consistent speed in drawing the passwords.

The training proved sufficient as the experimenter managed to conduct the login procedure without any failure in all sessions undertaken during the experiment. The experimenter remained seated throughout. Also important to note is that the experimenter was not trying to cover up the PDA screen or apply any defence technique other than the one being tested. The purpose of having this scenario was to have tight control so that the victim had no other protection mechanism than the one being tested, although in a real life situation, PDA users might tilt the screen to avoid it being seen.

Each participant played the role of a shoulder surfer. They had free roam of the laboratory room and were asked to choose an optimal viewing position (on the left of "the victim" as the experimenter is a right-handed person). The participants were given only a single chance to observe each login session. The rationale behind this design is to emulate a casual shoulder surfer. The participants were allowed to take notes on their observations. The details of the experimental task that the participants carried out are as follows:

- The experimenter attempted to login by drawing the passwords (one password at a time) on the PDA screen and then clicking the login button.
- After a password was drawn, the participant was asked to reproduce on a piece of paper containing (5x5) grid lines (similar to the interface of the DAS prototype) the password that he/she had captured by observation.
- Then, the participant was asked to play a mini jigsaw puzzle game for about one minute. This was to help clear their recent memory of the password that they had attempted to shoulder surf to avoid potential interference with the next password.
- The same procedure was repeated for the second and third passwords.

At the end of the experiment, each participant returned the papers (containing the three passwords as they had captured them) to the experimenter before being permitted to leave the room. Each participant was offered a printing credit of 50 A4 pages, which can be used on campus as a reward for completing the experiment.

6.3.3 The experimental apparatus

A prototype of the DAS graphical password system was implemented together with all three shoulder-surfing resistance techniques, on a major-brand PDA. A 5x5 grid for the DAS scheme was chosen, as a previous study [178] had shown that this size would provide a good balance between usability and security. The PDA has a 3.5 inch TFT active matrix display with dimensions of 2.9in x 0.7in x 4.7in (W x D x H) and a 240 x 320 display resolution.

The proposed techniques were specifically tested on the DAS instead of the BDAS[13] scheme for the following reasons:

1) To make sure that the results produced reflect the effectiveness of the proposed techniques and are not due to other factors such as the background in the BDAS scheme.

2) To ensure the instructions given to the participants are as simple as possible so that the experiment is less burdensome and more fun for participants, avoiding bias in the results caused by participants who would be otherwise bored by the experiment and thus act less naturally; the DAS is less complicated to explain than the BDAS scheme.

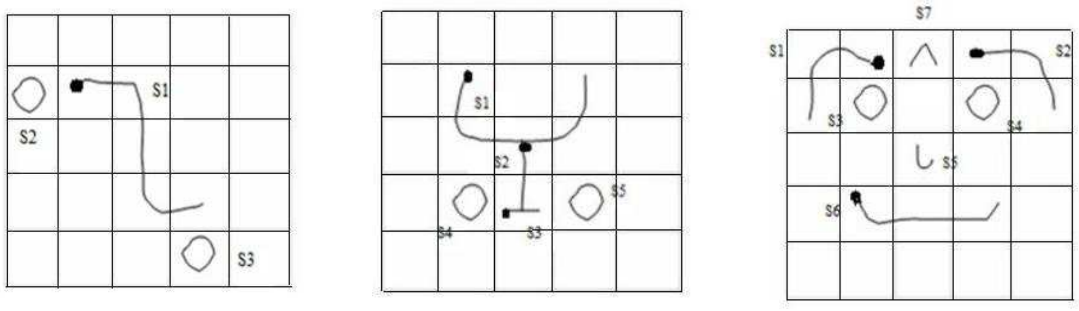
It is interesting to see the effects each defence technique will have on passwords of different strength. In contrast to work done by Tari et al. [175], our experiment did consider more than one password and the proposed defence techniques were tested across three levels of password difficulty (weak, medium and strong). Hence, three passwords of different security levels (weak, medium and strong) were tested for each experiment condition. The strength of a DAS password can be determined by its length and stroke count when the drawing grid size is fixed. The configuration of the password length and stroke count for each security level, together with the bit-size strength of each level, is chosen as in Table 6.1 below:

[13] BDAS is an abbreviation for Background Draw-A-Secret which is an improved version of the DAS scheme and uses a background added to the original white canvas with the aim of improving the memorability of the scheme.

Table 6.1: Password choices and configurations [179]

Password category	Password length	Stroke count	Bit-size strength
Weak	7	3	≈25.1
Medium	10	5	≈39.1
Strong	13	7	≈53

Based on Table 6.1 above, the weak password has a search space of about 25 bits; the medium password is around 39 bits. The strong password level is approximately 53 bits, equivalent to strong, 8-character text passwords. Figure 6.5 shows the three passwords chosen for the experiment.



Weak password **Medium password** **Strong password**

Figure 6.5: Three passwords of different strength used in the experiment
(Note: S_i indicates the order of the strokes and the black dots indicate the starting point of a stroke)

In order to maintain the ecological validity of this experiment, the passwords tested must be memorable; otherwise, they would be less likely to be chosen in the real world. As suggested by previous studies [98, 179], DAS users tended to employ centring and symmetry in their drawing as typical ways to help remember their secrets.

However, global symmetry and centring would lead to weaker DAS passwords. These are more likely to be vulnerable to dictionary attacks. In the case of BDAS, such weaknesses can be compensated for by the relatively larger bit size of BDAS passwords. Hence, it was speculated that in real life scenarios, people will still prefer passwords that exhibit symmetry and centring (at least to some extent).

Thus, in this experiment these characteristics were therefore emulated in our chosen passwords. For example, the medium and the strong passwords (as shown in Figure 6.5

above) are symmetrical in nature and have some recognisable features (i.e.: a shape of a glass wine for the medium password while a shape of a face for the strong password). From one perspective, as the strength of the password increases (i.e.: medium to strong password) the common method used by users to cope with memorability issues is to use something that can be easily remembered and this unfortunately also the case for graphical passwords [179]. From another point of view, these choices also arguably serve one of the experiment rationales: to empower the shoulder surfer with an optimal attack setting.

6.3.4 The experimental measurements

In this experiment, all the participants successfully completed their given tasks. A password that is captured by a shoulder surfer is considered correct only if it contains all of the following elements (an example is given in Figure 6.6):

- Strokes are in the correct order (2 strokes)
- Strokes are in the correct direction (as shown by the arrows)
- Strokes are the correct length (that is, the number of cells the stroke cuts through)

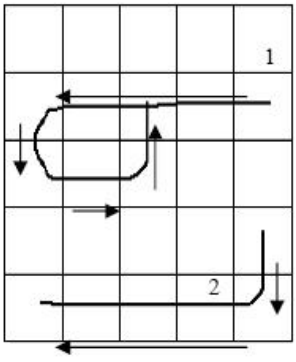


Figure 6.6: An example of how a DAS password is correctly reproduced (hand-drawn)

A stroke by stroke analysis using the three elements stated above was performed on each password captured for each participant. For example, the weak password tested has a stroke count of 3. Therefore, the possible outcome for a shoulder surfing attack on this password can be 0 (a complete failure), 1/3, 2/3 or 3/3 (a complete success). This stroke

by stroke analysis seems feasible with regards to this experiment due to the shoulder surfers relied on human eyes alone and were only allowed to capture the first look of the password they shoulder surfed. This however would not account for repeated observation attack using more sophisticated techniques or devices to aid the shoulder surfing attacks.

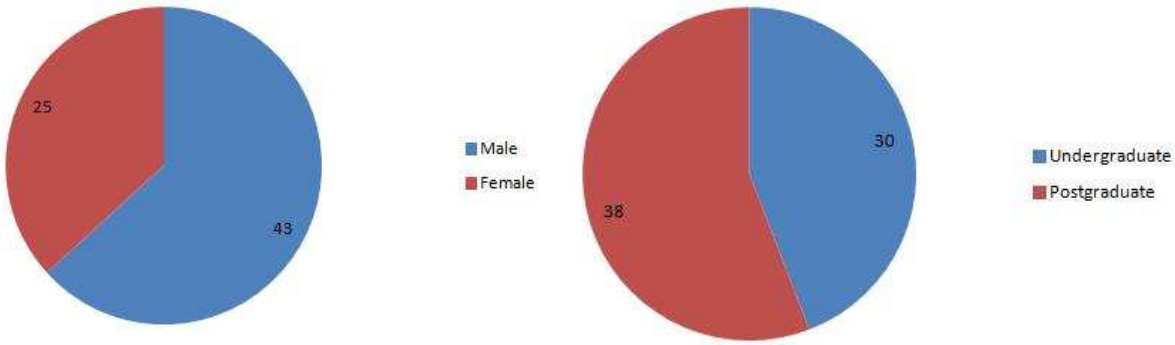
6.3.5 The result & analysis

The following sub-sections will present the results and the analysis of experiment 1.

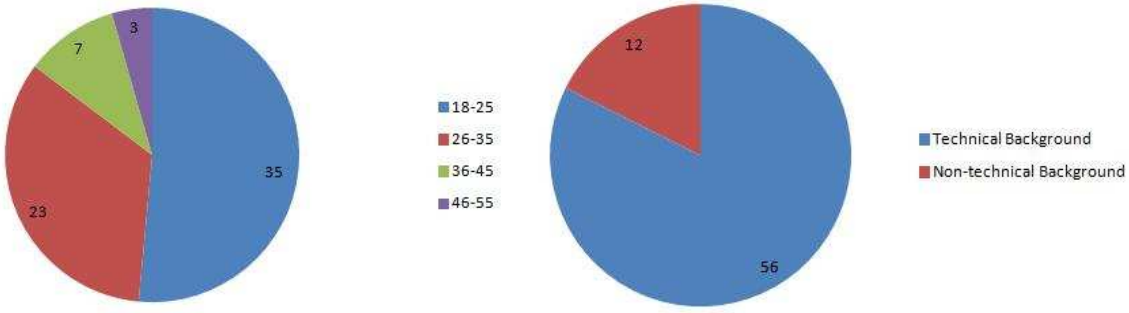
6.3.5.1 The demographic details

The experiment was conducted in a controlled laboratory environment to avoid any distractions. The total participants recruited for this experiment was sixty-eight, of whom 63% were male. The mean age for the participants was approximately 28 years with a standard deviation of 7.9 years.

The majority of the participants (82%) came from a technical background, while the remainder came from a non-technical background. Participants from the technical category included university students from the science and engineering faculties, while the non-technical category came from business and social science disciplines. Less than half (40%) of the participants had used a PDA frequently. Figure 6.7 illustrates the demographic details of the participants involved in the experiment.



(a) Gender **(b) Education**



(c) Age **(d) Background**

Figure 6.7: Participants' demographic details

6.3.5.2 The analysis on the defence strength performance

The defence strength will be analysed from two perspectives. First, the overall strength of the defences is examined by looking at the proportion of strokes that were captured by shoulder surfing. Secondly, the immediate threat of successfully collecting complete DAS passwords by shoulder surfing is explored, with and without the protective techniques. This refers to cases where shoulder surfing could not capture complete DAS passwords. Furthermore, the analysis probes how much information in the password was still possible to recover by shoulder surfing.

Table 6.2 shows the total proportion of strokes that were stolen for each defence type. The results appear to fall into two groups at each end of the spectrum: DAS only (the control group that had no defences) and Decoy Stroke, with approximately 77% of strokes captured. The remaining defences - Disappearing Stroke and Line Snaking - had between 40% and 50% of strokes stolen.

Table 6.2: Proportion of DAS password strokes stolen, reported according to defence used

Password strength	Proportion of strokes successfully stolen Mean (SD)			
	DAS only (control)	Decoy stroke	Disappearing stroke	Line snaking
Weak	1.00 (0)	0.86 (0.29)	0.69 (0.28)	0.59 (0.42)
Medium	0.8 (0.3)	0.79 (0.33)	0.45 (0.36)	0.41 (0.37)
Strong	0.52 (0.35)	0.7 (0.3)	0.33 (0.29)	0.20 (0.29)
Overall (n=51)	0.77 (0.33)	0.78 (0.31)	0.49 (0.34)	0.40 (0.39)

**In each cell – The mean of passwords scores followed by the standard deviation in the brackets.*

This characterisation was confirmed by testing for differences between the defences using non-parametric Mann-Whitney U tests. The U test was chosen because the distribution of proportions was highly skewed and so not suitable for parametric tests. In accordance with Lewis & Sauro's [110] guidance, when reporting task completion (e.g. successfully stealing DAS passwords) we show 95% confidence intervals using the Adjusted Wald method. Moreover, adjustment was made for multiple comparisons using the Bonferroni method, by setting the criterion value for significance to 0.0042 for the 12 inferential statistics reported in this section, to achieve an overall alpha of 0.05.

In order to be efficient with the total number of comparisons in this study, only three comparisons were made to test for differences within each of the two groups (e.g. Control vs. Decoy Stroke, and Disappearing Stroke vs. Line Snaking), then between a member of each group (Decoy Stroke vs. Disappearing Stroke). No significant difference in proportions was detected between DAS only and Decoy stroke (U=1285, z=-0.11, p=0.91, r=-0.01), showing that Decoy Stroke did not offer any protection.

A statistically significant difference was found between Decoy Stroke and Disappearing Stroke (U= 699.5, z= -4.1, p<0.0005, r=-0.41), showing that Disappearing Stroke offered improved strength compared to an undefended DAS. No statistically significant difference was found between Disappearing Stroke and Line Snaking (U=1087.5, z= -1.4, p=0.149, r=-0.14), showing that Line Snaking offered equivalently good strength.

The effect of password strength on the proportions of strokes stolen was examined using Wilcoxon tests. These are non-parametric tests used for related data when there are only two groups and are used in preference to an ANOVA because the data is highly skewed and would contradict ANOVA's assumptions. Weak passwords were found to have a statistically significantly higher average proportion of strokes stolen (0.78 strokes, SD=0.33) than did Medium strength passwords (0.61 strokes, SD=0.38) (z=-4.1, p<0.0005, r=-0.35). Medium passwords had a statistically significantly higher proportion of password fragments stolen than Strong passwords (0.44 strokes, SD=0.36) (z=-4.8, p<0.0005, r=-0.41).

Next, the analysis examines the immediate threat of successfully collecting complete DAS passwords by shoulder surfing. Table 6.3 shows the numbers of passwords that were successfully stolen (i.e. correctly shoulder surfed) for each of the three password strengths. Based on results shown in Table 6.3, the pattern of proportions of strokes stolen is repeated here. Overall, 63% of the passwords were stolen in the undefended control group (which correlates with a true rate in the population of between 25 and 38 passwords stolen). Decoy Stroke offered equivalent performance to the control group, with 57% of the passwords stolen (correlating with a true rate in the population of between 22 and 35 passwords out of 51).

Table 6.3: Number of DAS passwords successfully stolen despite each defence technique

Password strength	**Complete DAS passwords successfully stolen (out of total 17 for each group)**			
	DAS only (control)	**Decoy stroke**	**Disappearing stroke**	**Line snaking**
Weak	17 (14 -17)	13 (9 – 15)	6 (3 – 10)	7 (4 – 11)
Medium	11 (7 – 14)	11 (7 – 14)	4 (2 – 8)	3 (1 – 7)
Strong	4 (2 – 8)	5 (2 – 9)	0 (0 – 3)	0 (0 – 3)
Overall (n=51)	32 (25 – 38)	29 (22 – 35)	10 (6 – 17)	10 (6 – 17)

**In each cell – The number of passwords successfully stolen, followed by the confidence interval in the brackets.*

We now examine our two hypotheses about the numbers of passwords that would be stolen with each defence technique.

H_1 was that the Disappearing Stroke defence would not work as well as Line Snaking defence. H_1 was not supported by the data; these defences had identical overall performance, allowing only approximately 20% of the passwords to be stolen each.

H_2 was that the Decoy Strokes defence would be the weakest of all defences, as it allowed strokes to remain on screen. This was tested using two Mann-Whitney U tests, which are appropriate tests where two unrelated groups of non-normally distributed data are being compared, such as the password stolen/not stolen outcomes under examination here. The hypothesis was supported; a statistically significant difference was found between Decoy Stroke (with ≈ 57% of passwords stolen) and Disappearing Stroke (with ≈ 20% of passwords stolen) ($U=699.5$, $z=-4.15$, $p<0.0005$, $r=-0.41$).

Disappearing Stroke has identical performance to Line Snaking, so Decoy Stroke is the weakest of all defences.

The analysis attempts to identify whether the Decoy Stroke (with ≈ 57% of passwords stolen) performed better than having no defence at all (the control group, with 63% of passwords stolen). Using a Mann-Whitney U test again, it was found that there was no statistically significant difference ($U=1285.5$, $z=-0.11$, $p=0.91$, $r=-0.01$). The effect of password strength was also examined. Stronger passwords should be stolen less frequently than weaker passwords. This hypothesis was tested using a Friedman test to check for the main effect of password strength. Friedman tests are appropriate for non-parametric data such as the password stolen/not stolen binary outcomes in this experiment, and are used when there are more than two groups and the data in each group are related. This is the case here, where each participant attempts to steal all three password types. A statistically significant effect of password strength was detected ($Chi\text{-}square=51.5$, $N=68$, $df=2$, $p<0.0005$).

Wilcoxon tests were used as post-hoc test to determine the differences in password strengths in terms of the number of passwords stolen. Wilcoxon tests are used for related non-parametric data when there are only two groups. Weak passwords were found to be stolen in statistically significantly larger numbers than medium strength passwords ($z=-3.7$, $p<0.0005$, $r=-0.32$). Moreover, medium strength passwords were found to be stolen in statistically significantly larger numbers than strong passwords ($z=-4.5$, $p<0.0005$, $r=-0.39$).

Next, differences between the defence techniques were examined in relation to their ability to prevent partial theft of DAS passwords. Table 6.4 illustrates the numbers of passwords that were partially stolen (i.e. shoulder surfed). It was noted previously that DAS only and Decoy strokes had equivalent numbers of passwords completely stolen, but far more than both Disappearing Stroke and Line Snaking defences, which had approximately equal numbers of password completely stolen. Comparisons are restricted only to those within two groups of defences to avoid confusion. Mann-Whitney U tests were used, as they are suitable for comparing non-parametric data in two unrelated groups.

Table 6.4: Number of DAS passwords that were partially stolen through each defence technique

Password strength	DAS passwords partially stolen (shoulder surfed)			
	DAS only (control)	Decoy stroke	Disappearing stroke	Line snaking
Weak	0 (0 – 4)	3 (1 – 7)	11 (7 – 14)	6 (3 – 10)
Medium	6 (3 – 10)	5 (2 – 9)	11 (7 – 14)	9 (5 – 13)
Strong	11 (7 – 14)	11 (7 – 14)	12 (8 – 15)	8 (4 – 12)
Overall (n=51)	17 (11 – 24)	19 (13 – 26)	34 (27 – 40)	23 (16 – 30)

**In each cell – The number of passwords partially stolen followed by the confidence interval in brackets.*

There was no statistically significant difference between the number of passwords partially stolen through the Decoy Strokes defence (≈ 57% of passwords) than from the undefended control group (≈ 33% of passwords) (U=1249.5, z=-0.41, p=0.68, r=-0.04). No statistically significant difference was found between the numbers of passwords partially stolen through Disappearing Stroke (≈ 67% of passwords) and through Line Snaking (≈ 45% of passwords) (U=1020, z=-2.2, p=0.029, r=-0.22) (although the difference had been statistically significant before a Bonferroni adjustment to the criterion value for significance).

Due to the concept of partially stolen introduced to measure the strength of the defence techniques in this experiment, the results seem to indicate that strong password was more likely to have more number of passwords to be stolen across all the techniques. This is due to strong password is more complex and contain more lines and strokes which therefore intuitively has a higher probability of intersection between the random strokes (compared to a simpler password which have less strokes).

Previously, it was found that Line Snaking and Disappearing Stroke allowed equal numbers of passwords to be fully stolen. This was further investigated by comparing the defences against the numbers of passwords that could not be stolen through them, focussing inferential tests only on Line Snaking and Disappearing Stroke. Table 6.5 shows a number of DAS passwords that were completely resistant to shoulder surfing.

Table 6.5: Number of DAS passwords that were completely resistant to shoulder surfing

Password strength	DAS passwords completely resistant to shoulder surfing			
	DAS only (control)	Decoy stroke	Disappearing stroke	Line snaking
Weak	0 (0 – 4)	1 (0 – 5)	0 (0 – 4)	4 (2 – 8)
Medium	0 (0 – 4)	1 (0 – 5)	2 (0 – 6)	5 (2 – 9)
Strong	2 (0 – 6)	1 (0 – 5)	5 (2 – 9)	9 (5 – 13)
Overall (n=51)	2 (0 – 7)	3 (1 – 8)	7 (3 – 13)	18 (12 – 25)

**In each cell – The number of passwords completely resistant to shoulder surfing followed by the confidence interval in brackets.*

Based on Table 6.5, the results show that when partial thefts are taken into account, it appears that both defences are still equal. A Mann-Whitney U test was used again, and for the same reasons. Although the Line Snaking defence appeared to defend more passwords completely ($\approx$ 35% of passwords) than the Disappearing Stroke (with $\approx$14% of passwords fully defended) again, after the Bonferroni adjustment, no statistically significant difference was found – (U=1020, z=-2.5, p=0.012, r=-0.25). However, the effect of this size (r = -0.25) is substantial, approaching Cohen's criterion value of 0.3 for a "medium" sized effect [44]. Line Snaking and Disappearing Stroke should be subject to more focused study, in order to achieve greater statistical power.

6.3.6 The focused study

The analysis thus far has shown that both Line Snaking and Disappearing Stroke are equal in terms of defence strength. Hence, it was decided that a focused study be conducted in order to achieve greater statistical power. For this purpose, in a separate experiment, a more focused study involving only the Line Snaking and Disappearing Stroke group was conducted. The focused study involved 34 participants with each group containing 17 participants in additional to the previous experiment conducted. It is important to note that all the procedures and apparatus used in experiment 1 (i.e. the previous experiment) were maintained exactly. However, none of the participants of this focused study participated in the previous experiment.

In general, slightly more than half (58%) of the participants in this focussed study came from the technical background and were female. The average age of the participants was

approximately 29 years old, less than half of whom having had had some experience of using PDAs previously. The distribution was found to be highly skewed; hence, the Mann Whitney U test was used to compare the two groups. A statistically significant difference was detected (U= 72.5, z=-3.57, p=0.001, r=-0.31) which indicates that differences exist between the Disappearing Stroke and Line Snaking technique.

Next, the number of passwords that were successfully shoulder surfed was examined. The Disappearing Stroke group managed to successfully shoulder surf (14%) of the passwords, whereas the Line Snaking group managed none. This was found to be statistically significant (U= 102, z=-2.38, p=0.017, r=-.41). In terms of the number of passwords that were completely resistant to shoulder surfing, Line Snaking managed to protect around 12% of the total passwords from being completely stolen, compared to the Disappearing Stroke with just 4%. However, this difference was not found to be statistically significant (U= 102, z=-1.71, p=0.087, r=-.29). As such, it was found that Line Snaking outperformed Disappearing Stroke, and hence provided better protection.

6.3.7 Discussion

The Decoy Stroke defence technique performed the worst in experiment 1, as presented above. This is due to the fact that it allows all the strokes to remain on screen visibly during the whole login process. It was expected that this defence technique would work to some extent. However, it transpires that this technique provided little protection, as shown in Tables 6.2 – 6.5, which indicate similar performance in the Decoy Stroke group and the undefended DAS group, and applicable statistical tests did not yield any significant difference between these two groups.

In some circumstances, the Decoy Stroke group performed worse than the undefended DAS group. This discrepancy can be likely explained as follows. The decoy strokes helped the attackers to locate and remember the legitimate strokes that were intended to be obfuscated by the decoys. This is due to the fact that the relative positions of decoy and legitimate strokes can be exploited by attackers to aid their location, such as the starting and ending cells of legitimate strokes in the drawing grid.

On the other hand, the focused study has confirmed that the Line Snaking has indeed shown better performance than the Disappearing Stroke. This can be explained when the stroke appears to be snaking away while users still drawing which gives a little less time for the shoulder surfers to capture the strokes, compared to disappearing stroke technique where the stroke only disappear once the stylus was put away on each stroke.

It is also important to take note that this analysis was based on the pre-selected passwords used in this experiment. Therefore, it would be interesting to investigate further the performance of those proposed techniques with more sets of passwords. It would also probably be worthwhile in the future research to reconstruct the design experiment which considers the participants to choose their own passwords (rather than something that has been pre-selected by the experimenter).

Although, the existing experimental design that has been conducted which involved pre-selecting the three passwords for the participants would render to be one of the weakness of this experiment, the main purpose of doing so is to allow greater control in the experiment and makes the experiment much more reproducible. This would also allow comparisons to be made across studies much more easily than if an unknown mixture of passwords were used.

With this, the evaluation now shifts its focus from security to usability perspectives. The following sections will detail the second evaluation study which emphasises usability of the defence techniques.

6.4 Usability evaluation – Experiment 2

It is important now to recapitulate the research aim, that is, to find a technique that is good in terms of both security and usability. As mentioned earlier, a separate experiment was conducted to evaluate the usability of the defence techniques across three levels of password difficulty (weak, medium and strong). It was decided that the Decoy Stroke defence technique should be excluded from this study as the results obtained from experiment 1 indicated that this technique provided little protection. In

common with experiment 1, this experiment was approved, before being carried out, by the University Ethics Committee (UEC) as a study with minimal risk.

6.4.1 The experimental design

Unlike the previous experiment, experiment 2 was based on a *within subject* design, whereby all participants are exposed to all of the following experimental conditions:

- Disappearing Stroke
- Line Snaking
- Undefended DAS scheme (control group)

The hypotheses were as follows:

H_1 – *It takes more time for users to login when Line Snaking is enabled, than when Disappearing Stroke is enabled.*

H_2 – *The Line Snaking technique will cause a higher login error rate than Disappearing Stroke.*

H_3 – *The Disappearing Stroke technique is preferred by the users compared to the Line Snaking technique (as in the latter, the line starts snaking away while users are still drawing).*

6.4.2 The experimental procedures

The experiment was conducted in a controlled-laboratory environment to avoid any distractions. The same apparatus used in experiment 1 were retained (refer to Apparatus in section 6.2.2). Informed consent and demographic information were obtained from each participant. The participants were asked to provide their age, gender, educational background, and details of their experiences of using a PDA.

The experiment began with an introductory session, in which participants were given a brief explanation of the DAS system and all the defence techniques. Printed information was also supplied to support the briefings. This was followed by a short demonstration to show how the system works and a quick hands-on session was allowed to ensure the participants had some experience of using the system prototype.

As mentioned previously, this experiment aimed to evaluate the two defence techniques across three levels of password difficulty (weak, medium and strong). Therefore, throughout this experiment, the same three passwords were used. The three passwords used in experiment 1 were retained in this study (refer to the password choices and configuration in Table 6.1 & Figure 6.5). The reason for controlling the password choice rather than allowing the participants to create their own was to avoid bias caused by different password choices. All three passwords were drawn on a separate piece of paper within (5x5) gridlines similar to the prototype system.

Participants were shown one password at a time, beginning with the weak, followed by medium and then the strong password. With each password, the participants were instructed to perform the following tasks:

- Treat the shown password as theirs.
- Become familiar with the password by using it to log in to the system several times. In order to ensure a consistent amount of training, each participant was allowed approximately 10 minutes (this amount of time was found to be adequate during a pilot study).
- Once the training period was over, the participants returned the paper containing the password to the experimenter.
- Participants were then instructed to log in using the passwords they had used in the training session, for each of the experimental conditions. To minimise the training effect caused by the same password being used, the experimental conditions were arranged in a random order. Time taken to login and login error rate were recorded.

- Then, the participants were asked to play a mini jigsaw puzzle game for about one minute. This was to help clear their recent memory of the password they used, before moving on to the next password.
- The above procedure was repeated for the second and third passwords.

After participants had completed all tasks with all three passwords, they were asked about which defence technique they preferred and why. All answers and comments given were noted. Each participant was offered £10 for their effort in participating in the experiment.

6.4.3 The measurements

The outcome metrics that were measured in this experiment were as follows:

- *Login time*: time taken to complete a successful login. If a participant had to make several attempts, his/her login time was measured as the sum of the time taken by each attempt.

- *Login error rate*: measured by the number of attempts taken to complete a successful login.

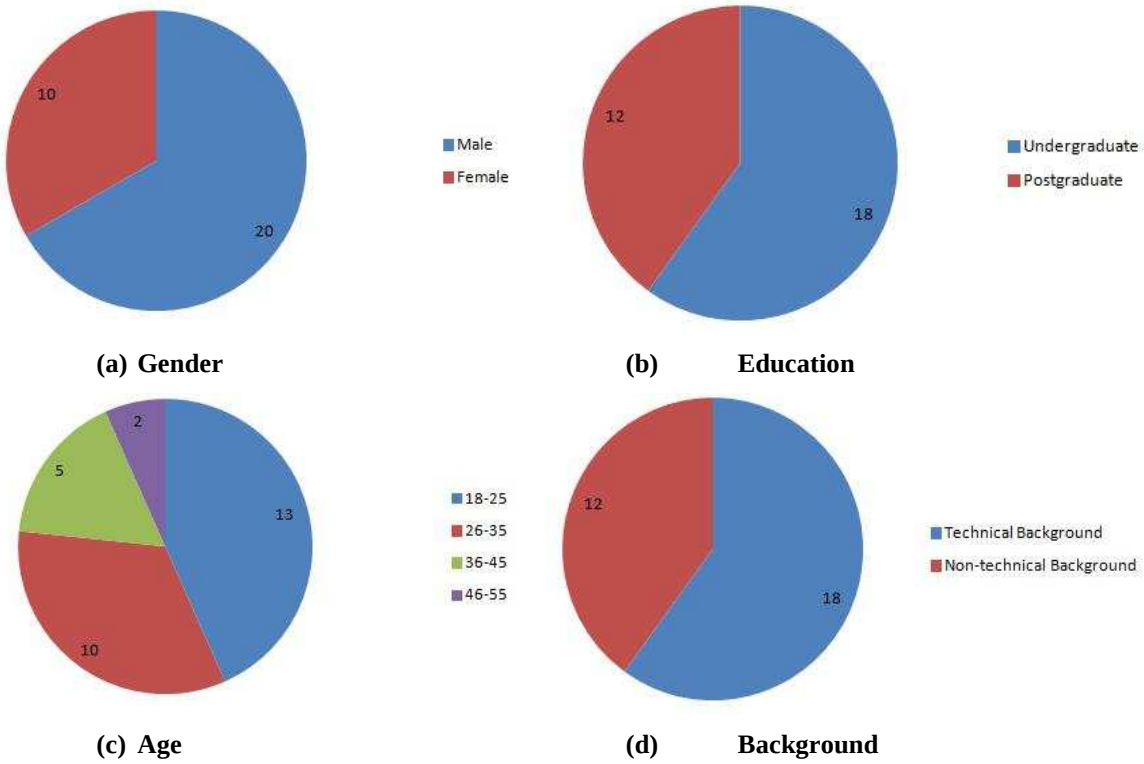
6.4.4 The results & analysis

The following sub-sections will present the results and analysis of experiment 1.

6.4.4.1 The demographic details

The overall number of people participating in this experiment was thirty, of whom 67% were male. The mean age for the participants was 31.1 years, with a standard deviation of 9.1 years. More than half of participants (60%) came from technical backgrounds, and the remainder came from non-technical backgrounds. Participants from the technical category included university students from science and engineering while the non-technical category came from business and social science disciplines. More than

half (63%) of the participants reported having used PDAs frequently. Figure 6.8 illustrates the demographic details of the participants involved in this experiment.



(a) Gender **(b) Education**

(c) Age **(d) Background**

Figure 6.8: Participants' demographic details

6.4.4.2 The analysis on usability performance

In this experiment, all the participants successfully completed their given tasks. Table 6.6 shows the mean and standard deviation of login time (in seconds) for all techniques across three levels of password strength. From a defence techniques perspective, Line Snaking has the highest mean login time, followed by Disappearing Stroke and DAS only (undefended group). This suggests that the Line Snaking technique poses some challenges for participants in completing the login task. On the other hand, from a password level perspective, a strong password requires more time to log in compared to medium and weak passwords.

Table 6.6: Mean and standard deviation for login time (in seconds) for all techniques across three levels of password difficulty (N = 30)

Pwd. strength / Techniques	Weak	Medium	Strong
	Mean (SD)	**Mean (SD)**	**Mean (SD)**
DAS only	4.5 (0.52)	5.4 (0.73)	7.5 (0.54)
Disappearing stroke	5.3 (1.06)	6.5 (1.15)	9.6 (2.38)
Line snaking	5.9 (1.35)	7.9 (2.62)	12.4 (4.42)

**In each cell – The mean for login time followed by the standard deviation in brackets.*

A two-way within-subjects (repeated measures) ANOVA test was performed to compare the interaction effect of password levels on the defence techniques applied. This test was chosen since the same participant was exposed to all conditions, and the data are ratio data, approximately normally distributed, while the test is robust against violations of homogeneity when the sample sizes are equal. Figure 6.9 shows the main effects plot for all the time taken to login using the three techniques applied across three different levels of password.

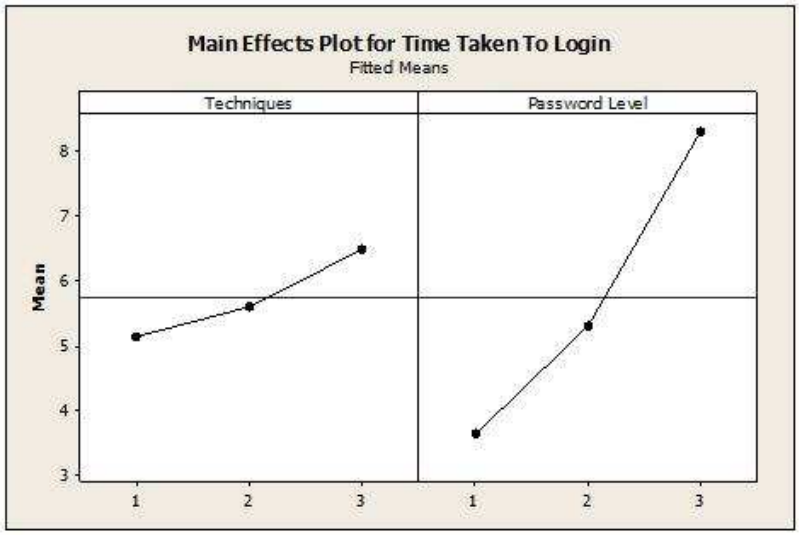


Figure 6.9: The main effects plot for time taken to login

Based on Figure 6.9, time taken to login for both techniques DAS only and Disappearing stroke for both password levels weak and medium seems to be below the mean level (mean = 5.74, standard deviation = 2.19). However, the mean plot seems to have a dramatic increased in value comparatively with the overall mean for the Line Snaking techniques particularly for strong passwords. The result (with a Greenhouse-

Geisser correction) shows a statistically significant interaction effect ($F(2.03, 58.75) = 12.84$, $p=0.001$). This effect demonstrates that the time taken to log in using the techniques applied is different across the three levels of password.

Paired sample t-tests were then used to make post hoc comparisons between conditions. All the nine t-tests show significant differences with ($p \leq 0.005$) indicating that password levels have a significant effect on the techniques used, where increasing password strength produces a larger increase in login time for Disappearing Stroke than for unprotected DAS, and a larger increase still for Line Snaking than for Disappearing Stroke. The results above show that Hypothesis 1 is supported.

Table 6.7 summarises the number of attempts taken to complete a successful login for all techniques across the three levels of password difficulty. A Friedman test was used to assess the numbers of login attempts required across techniques, because the distributions of number of login attempts were not normal, and the observations were related.

The analysis shows a statistically significant overall difference between the different techniques (Chi square=32.2, df=2, $p<0.0001$). Wilcoxon signed-rank tests were used to test for difference in the numbers of login attempts required between each pair of techniques, because the data were not normal, though were related. The Line Snaking technique required statistically significantly more attempts to login than both undefended DAS ($z=4.7$, $p<0.0001$) and Disappearing Stroke ($z=3.4$, $p=0.001$). Disappearing Stroke also required more login attempts than the undefended DAS ($z=2.8$, $p=0.005$). These results support Hypothesis 2.

Table 6.7: Mean number of attempts taken to complete a successful login for all techniques across three levels of password difficulty (N = 30)

Pwd. strength / Techniques	Weak	Medium	Strong
DAS only	1.0	1.0	1.0
Disappearing stroke	1.1	1.1	1.1
Line snaking	1.1	1.3	1.4

Qualitative data collected, such as participants' preferences and additional comments on the techniques used also yielded interesting results. Most of the participants (77%) (i.e. 23 out of 33) preferred the Disappearing Stroke technique; 10% (i.e. 3 out of 30) of the participants preferred the Line Snaking technique, and the remaining 13% (i.e. 4 out of 30) did not have any preference. These results indicate that Hypothesis 3 is supported.

6.4.4.3 Discussion

Experiment 2 has shown that the Disappearing Stroke defence is generally more usable compared to the Line Snaking defence. As shown in Table 6.6, participants require more time (8.7 secs) on average to log in and also use more attempts to log in (1.3 secs) on average using Line Snaking compared to the other techniques. These create some usability challenges for the Line Snaking technique.

The challenge is more obvious with strong passwords compared to medium and weak passwords. A possible explanation for this is that the participants were not given the freedom to choose their own passwords. Should they have had this flexibility, different results might have been yielded. However, such a hypothesis requires a different experimental design, and is a next step in the investigation of these defence techniques, building upon the first proof of their effectiveness as reported here.

The results have also shown that an interaction effect on time taken to log in was detected between password levels and defence techniques, such that a combination of password and technique choice might determine login time. An implication of this is the possibility that users might be discouraged from using stronger passwords, especially when using the Line Snaking technique. The participants who preferred Disappearing Stroke did so for different reasons:

- More than 65% (15 out of 23 participants) stated that they preferred this technique because they felt more comfortable and confident while drawing the passwords, as the stroke only starts to disappear the moment the stylus is pulled up. This aspect is important as the previous stroke will become a vital reference point for drawing the adjacent strokes.

- 10 out of these 15 participants (67%) instantaneously spotted the security advantage of the Line Snaking technique. They all mentioned that the snaking effect quickly removed the strokes from the screen, which was obviously good for security defence. They realised the security advantage of Line Snaking technique, but because feeling more comfortable with the DS was more important to them, they chose DS as their favourite.
- The remaining 8 participants (35%) pointed out that the "snaking stroke" (as an effect of the Line Snaking technique) was actually annoying and distracting, making them like the technique less.

The participants who did not have a preference between the techniques commented that, as long as they knew their password, the techniques applied did not affect them. To confirm this, their performance on each technique was cross-checked and it was found that the average difference in performance between the techniques was indeed small for these participants. This result possibly supports the earlier assumption that, if users are highly familiar with their passwords, the defence techniques might not affect their performance significantly.

6.5 Summary

This chapter has detailed the design implementation of the three proposed defence techniques. The defence techniques were proposed with the aim of reducing shoulder surfing attacks for recall-based graphical passwords.

It is important to note that the proposed techniques were not supposed to be used during password enrolment (i.e. where users create their new passwords). Instead they are enabled only during a login procedure. The rationale for doing this minimise distraction when creating new passwords.

In order to evaluate the proposed defence techniques, a prototype version has been developed on the DAS scheme. A series of evaluation studies have been conducted with the aim of determining the most effective shoulder surfing defence techniques among

the three that have been proposed. The most effective technique is that which achieves a good balance between security and usability.

This chapter has presented two separate evaluation studies that were conducted with the aim of determining the most effective proposed defence technique. Experiment 1 placed its focus on security, while experiment 2 was mainly to examine the usability of the proposed techniques.

The findings in experiment 1 indicate that the Line Snaking technique provides the best defence compared to Disappearing Stroke, while Decoy Stroke appeared to provide the least defence. In terms of usability, results from experiment 2 have shown that Disappearing Stroke provides good usability and is preferred by most users. The results have also shown that Line Snaking does incur some usability challenge to participants as the strokes start to disappear (i.e. snake away) while they are being drawn. Nevertheless, what seems interesting is that some participants were cited to realise that the security potential (i.e. defence ability) of the Line Snaking technique is better than Disappearing Stroke.

In general, both experiments have produced interesting findings which suggest that the proposed techniques, particularly Line Snaking and Disappearing Stroke, can be applied to other recall-based type graphical passwords (i.e. similar to the DAS scheme category). However, slight modification will be needed to suit the requirements of the scheme intended.

The next chapter intends to provide a discussion upon the issues that have been presented thus far. The discussion chapter aims to reflect on the lessons learned throughout all the experimental work that has been conducted and how the findings support the aim and objectives of this research project.

CHAPTER 7

DISCUSSION, CONCLUSION & FUTURE WORK

CHAPTER 7: DISCUSSION, CONCLUSION & FUTURE WORK

CHAPTER 7

DISCUSSION, CONCLUSION & FUTURE WORK

7.1 Introduction

This chapter provides an overall discussion of the research work that has been undertaken. This is done by revisiting all of the research questions that were set forth in Chapter 1. The research questions have been divided into three parts: the first part focus on the issue of improving compliance behaviour with password guidelines by utilising persuasion techniques. The second part discusses the investigation of the emerging alternative to traditional text-based passwords – graphical passwords. The third part answers the final research question and provides the conclusion and a summary of the whole research project.

Furthermore, this chapter also relates those main research questions to several specific research questions that have been drawn from each experimental study, so as to support the goal and objectives of this research. As mentioned previously, this research is exploratory in nature; thus, the findings reported and discussed here do not attempt to support or refute any existing theories. Rather, it is suggested that the findings can be used to initiate an open platform for further investigations.

This chapter also discusses the contributions of this research as well as possible future work that can be carried out as an extension to these research findings. The ultimate aim of this chapter is to provide critical comment and suggestions about the findings of the research that has been conducted.

7.2 Discussion

This section provides the discussion of this thesis in directly provides the overall conclusion of the research work undertaken. In order to facilitate the discussion, this section will be divided into three different parts discussion on each of the research question that was set fourth at the beginning of the thesis. Those research questions will

be revisited and elaborated further as to provide critical analysis particularly with regards to the experimental work conducted.

7.2.1 Research question (1)

"To what extent will persuasion approach be able to help in improving users' security behaviour particularly with regards to creating better passwords?"

Research question (1) poses a challenge question about how a persuasion approach can be utilised to enable an improvement in users' security behaviour, particularly with regard to creating stronger passwords. Based on the review work of persuasion approaches and related theories of attitude and behaviour change, it seems that in order to convince users to create better passwords, a rationale (i.e. reasons as to why creating good passwords is important) should be included in the password guidelines; thus, several persuasion strategies have been selected to frame this rationale. In addition to providing this rationale to users, the study also investigated the effectiveness of commitment & consistency strategies in ensuring better compliance rates for creating good passwords among users.

An experiment on password guideline compliance has been conducted to investigate this issue further. Specifically, the experimental work seeks to investigate further whether by including rationale in the password guideline; the users will be able to create better passwords. In relation to that, the experiment would also hope to determine which persuasion strategies are more likely to result in influencing users to create better passwords.

The results indicate that passwords created by users who receive password guidelines including a rationale are stronger compared to those of users who did not. This finding suggests that it is worth informing users that there are actually valid reasons as to why creating and using good passwords is important for them. The rationale included in the password guidelines is viewed as "on-site" support, which is not only meant to provide a constant reminder for users, but also to educate them in the long run. This is indeed the ultimate goal of persuasion, which attempts to tackle the retention phase in order to maintain compliance behaviour.

In making comparisons between the persuasion strategies applied, participants in the social proof and emotional groups were found to construct passwords of significantly higher mean scores than the rest of the groups. This was probably due to the fact that the rationale highlighted that using these two strategies was more likely to affect them personally if they failed to comply. The effect, as portrayed by the rationale in the social proof group, was on an individual's reputation among the social circle, while becoming a real hacker's victim was used as a scenario to outline the personal effect on users in the emotional appeal group. With regards to the password guidelines, it seems that a rationale which affects individuals directly or indirectly helps to increase the likelihood of compliance.

On the other hand, the result of the experimental study was that participants of the study from the commitment & consistency group only performed slightly better (i.e. 11% higher in terms of password scores) than the control group. The participants in this group were told to formalise their commitment to create and use strong passwords by signing a special form produced by the Information System Department (ISD) of the university. The participants were also told that the forms would later be handed to the ISD staff for record purposes. Although the literature [127, 41] has shown that commitment & consistency is a strong factor in gaining compliance, it was predicted that the nature of the controlled laboratory work conducted in this study may have affected the results. The study might yield different results if it is conducted in the context of "real-world" experiments or a case study, as there will be other contributing factors to consider, such as an element of fear due to surveillance from the top management for incompliant behaviour.

The experimental work on password guideline compliance does not only consider persuasion strategies but also an individual personality assessment framework known as the Big Five Inventory (BFI). This BFI has been used as a construct to measure the participant's personality characteristics according to five different traits: openness, conscientiousness, extraversion, agreeableness and neuroticism. The experimental work conducted was interested in looking into whether there are any particular personality traits that is more likely to produce better passwords than others.

It is however difficult to obtain an immediate answer to this question as it is important to note that the personality assessment construct was administered in parallel with the persuasion strategy. This was purposely done in such a way as to yield a spontaneous rather than planned result. It is interesting to note from the results that there seem to be several personality traits which produce slightly better passwords than others. For example, those participants who were found to be low in openness tend to construct better password strength than those in the high category. This seems to be consistent with the extraversion trait, agreeableness trait and neuroticism trait whereby those from the lower category produced better password strength than those in the high category. The only trait that seems to be showing a level-up in the password strength is the conscientiousness traits. This probably due to the distribution of numbers of participants is quite similar in both categories (low and high respectively).

However, since the study was more interested in extracting spontaneous results, unfortunately there were not many instances that could be extracted. Although the initial findings of this study might suggest that certain personality traits are more likely to produce better passwords than others as suggested by researchers in [164], further studies involving more participants are required before further result can be established.

Nevertheless, what seems more important to discuss here, is the implications for information security management generally. As discussed in Chapter 2, individual personality assessment is a common practice in many organisations as a mechanism for evaluating candidates for employment or promotion [94]. The findings on individual personality assessment can be extended to predict how likely a person is to comply with rules regarding the creation and use of good passwords so that management can take preventive countermeasures (e.g. proper education and training can be arranged), or provide more support for those who exhibit tendencies of incompliant behaviour.

The password guidelines experiment has also extended its perspective looking into whether any relationship exists between password strength and the persuasion strategies applied. In general, the results show that relationships do exist between personality attributes and the persuasion strategies applied, as measured by password strength. For example, extraversion and neuroticism traits were found to have a strong positive relationship with the passwords constructed by the participants from the rational group,

while openness was found to have a strong positive relationship with the passwords constructed by the participants from the emotional group. In the context of this study, these findings seems to suggest that the rational appeal strategy might be more effective for those participants who appeared to have high levels of extraversion and neuroticism, while the emotional appeal strategy might be more effective for participants with a high degree of openness.

On the other hand, several negative relationships were detected. For example, the openness trait was found to have a strong negative relationship with passwords constructed by the participants from the social proof group, while extraversion was found to have a strong negative relationship with passwords constructed by the participants from the commitment & consistency group. In the context of this study, these findings suggest that the social proof principle might be more effective for those participants who appear to be low in openness, while the commitment & consistency principle might be more effective for participants with low extraversion.

Again, the interest of this discussion is the implications of these findings in terms of how to leverage this information. The literature on persuasion suggests that persuasion attempts are more likely to succeed if the audiences are aware. Thus, the findings can be utilised to match appropriate persuasion strategies to certain intended individuals based on their personality characteristics. This can also be used in conjunction with the previous findings of this research that, if certain individuals are less likely to exhibit compliance behaviour, management can apply an appropriate persuasion strategy to boost the likelihood of compliance.

The password guideline study provides interesting insights into possible measures to improve users' security compliance behaviour through the persuasion approach. The suggested measure is simple yet, when applied appropriately, can result in positive results as demonstrated in the experimental study. Although motivating users' security compliance behaviour through the persuasion approach may seem practical, the vulnerability of password authentication remains an issue. Thus, this research redirects its focus onto other measures. The emergence of an alternative mechanism to the traditional text-based passwords is something this research could not ignore. Graphical passwords have been identified as an immediate alternative to text-based passwords as

the concept remains more a less the same because the only difference lies in the nature of the password itself; instead of using text, numbers or special characters, graphical passwords use graphic images such as icons, pictures and even drawing lines as a password.

However as similar to other alternative schemes, graphical passwords are far from being the silver bullet solutions. There are various challenges that the scheme faces particularly with regards to its defence strength. Thus the next research question will explore this issue further.

7.2.2 Research question (2)

"*What can be done to improve the existing solutions to increase the defence mechanism of graphical passwords?"*

This is indeed a practical question to investigate, particularly when the graphical password scheme proposed is new to the password authentication realm. The majority of people regard alphanumeric passwords as synonymous with authentication procedures. However, this simple and ubiquitous technology has some well-known usability problems, especially in terms of memorability. The human ability to remember pictures more easily than text has been well documented in numerous cognitive and psychological studies, as reviewed in [98, 174, 17]. As a result, much research has been inspired in both the security and HCI communities in recent years to explore graphical authentication systems as an alternative, or an enhancement, to text-based passwords. As the name implies, graphical authentication uses graphics (pictures, icons, faces etc.) instead of the commonly used text strings.

As been discussed in Chapter 4, there are various types of graphical password which can be categorised as *recognition-based*, *cued-recall based* and *recall-based.* Then from each category, several schemes were discussed further in terms of design implementation, advantages and disadvantages. The discussion also included several attack challenges for graphical passwords, such as brute-force, dictionary-based password, phishing, social engineering, smudge and shoulder surfing attacks. Hence, graphical passwords are still far from perfect. Among various attacks challenges that

have been discussed, shoulder surfing attacks have been identified as one of the main concerns against adopting graphical authentication in real use [170]. This is due to the nature of graphical passwords because a password supplied for authentication by a user in a public place, if not properly protected, can be stolen by a bystander who observes over the user's shoulder. The traditional text-based passwords are defended against this by substituting asterisks for the password characters in the display as the user logs in. To make graphical passwords reliable in the real world, it is essential to arm them with good shoulder surfing defence mechanisms.

The issue of shoulder surfing attack has therefore been a major focus of security researchers and practitioners to find solutions to minimise, if not eliminate, the risk. However, the effort is ongoing as the problem remains, due to the fact that balancing security and usability has indeed become the real challenge. This research then focused on the issue of shoulder surfing attack on graphical passwords to investigate possible countermeasures to minimise the risk.

The research has focused on shoulder surfing defences for recall-based graphical password systems such as Draw-A-Secret (DAS) and Background Draw-A-Secret (BDAS). DAS is a representative graphical password scheme and worthy of extensive study for many reasons. First, its theoretical password space can be larger than that of text passwords. Second, unlike many other graphical password systems, DAS can be used for not only user authentication, but also for key generation. Although some research has revealed that the user choices of DAS passwords could render this theoretically sound scheme less secure in practice [179], it appears that many of the weaknesses could be improved by introducing a background image into the drawing grid [60], together with other countermeasures.

DAS and BDAS authenticate people through stylus input, providing an easy alternative to text-based passwords. They are particularly suitable for PDAs and mobile phones with a touch screen. As such mobile devices are highly portable, it can be assumed that users venture into public places, and as a result will authenticate in areas where they may be left open to shoulder surfing attacks. Hence, a shoulder surfing defence is necessary to increase the security of the DAS/BDAS scheme, which in turn could make the scheme a more appealing alternative to text passwords for mobile device users. To

the best of our knowledge, currently there is little study of shoulder surfing defences for such graphical password systems, except for work in the following [115, 112, 37, 70]. The existing solution to shoulder surfing attack for the DAS scheme has been discussed in Chapter 5.

Defences against shoulder surfing include the finger pressure technique, as introduced by Malek et al. [115], as another possible way to enter sensitive input. By using a haptic input device, which measures pen pressure while users draw their passwords, an adversary would find it difficult to distinguish variances in pen pressure. However, their user study revealed some usability challenges when users are found to apply very little pen pressure and hardly lifted the pen while drawing. There has also been an effort to revise the original DAS scheme by introducing qualitative spatial relations and dynamic grid transformation to enhance shoulder surfing resistance [112]. Although this revised scheme provided good shoulder surfing defence, it has some usability issues.

The YAGP scheme attempts to improve the original DAS by allowing a position-free scheme where users can draw the passwords anywhere on the canvas [70]. The main factor that determines the success of this scheme is the balance between the density grid and the threshold value set as this is crucial in determining the balance between security and usability. It is predicted that, in order to accommodate usability, security becomes the tradeoff. Another scheme, known as Rotation-DAS (R-DAS) enhances the DAS scheme by adding rotation aspects as part of the password component [37]. Unfortunately, this scheme was not further tested as there was no user study reported to support the developers' claims about their proposed scheme.

There are also several other defence mechanisms which were not discussed in Chapter 5 due to the fact that these solutions were not directly relevant to the DAS scheme. However, it is worth including these proposed approaches here since they are relevant to shoulder surfing attack issues on graphical passwords in general. For example, in recognition-based systems, Sobrado & Birget [165] developed the Convex Hull Click (CHC) scheme, using a huge number of pass-icons to confuse shoulder surfers trying to determine the correct one. However, Man et al. [116] proved CHC to be unusable as so many objects had to be fitted on-screen at once that they were all too small, making it difficult for users to distinguish between pass-objects and non-pass-objects. Another

possible technique to provide shoulder surfing resistance is to display degraded or distorted images, as used in the Use Your Illusion (UYI) scheme [86]. This is done with the intention of reducing the visibility of users' input in the hope of increasing protection.

In cued-recall based systems, Suo [171] creates a variation of PassPoints to protect the scheme by using a blurring technique. The image is obscured, except for a small focus area where the authentication is achieved after ten rounds of click-on inputs on different focus areas. Although the scheme looks promising, an adversary can successfully recover the secret password by observing a few rounds of login [17]. Another scheme, known as Cued Gaze-Points (CGP), introduced by Forget et al. [69] uses an eye-gazing technique instead of a mouse click to input points and this has been claimed to increase shoulder surfing resistance. However, the initial study showed a clear trade-off between usability and security; obviously, the larger tolerance size proved considerably more usable but would not enhance security.

The discussion presented thus far has revealed that the existing solutions for strengthening defence against shoulder surfing attacks on graphical passwords generally, and specifically on the DAS scheme, were found to be promising yet still either suffered from imbalance of security and usability or lack of extensive study conducted to evaluate the proposed solutions. Hence, this has led our research to progress to the next research question, looking into possible suggestions for improving the existing solutions for strengthening defence mechanism against shoulder surfing attacks, particularly for the DAS scheme.

Thus, this has led the research to propose three innovative shoulder surfing defence techniques and conduct two separate, controlled laboratory experimental studies to evaluate both the security and usability perspectives of the proposed techniques. The three defence techniques proposed were: *Decoy Strokes*, *Disappearing Strokes* and *Line Snaking*.

The results of the first experimental study showed that the Line Snaking defence technique had the best overall performance in terms of defence, while the Disappearing Stroke technique is the second best defence. However, in many circumstances, both

techniques worked equally well (Tables 6.2 – 6.5). At the beginning of the experimental study, it was expected that the Decoy Stroke technique would provide some defence against shoulder-surfing; however, it achieved little protection. The likely reason is that all the password strokes remain visible on screen, and the decoys do not work well to distract attackers. It is possible in the future to consider an enhancement or modification to the proposed techniques. For example, the Decoy Stroke defence technique could be improved by introducing extra decoys, or the way the decoys are introduced, but this should be done with careful consideration and evaluation as it is important not to confuse the user; otherwise, usability problems might ensue instead. The line snaking algorithm can also be considered to be independent of timing so that the effect of the length stroke drawn using this technique can be observed. However, further work is required to establish this.

It is also important to take note that this analysis was based on the pre-selected passwords used in this experiment. Therefore, it would be interesting to investigate further the performance of those proposed techniques with more sets of passwords. It would also probably be worthwhile in the future research to reconstruct the design experiment which considers the participants to choose their own passwords (rather than something that has been pre-selected by the experimenter). Although, the existing experimental design that has been conducted which involved pre-selecting the three passwords for the participants would render to be one of the weakness of this experiment, the main purpose of doing so is to allow greater control in the experiment and makes the experiment much more reproducible. This would also allow comparisons to be made across studies much more easily than if an unknown mixture of passwords were used.

In terms of the experimental design perspective, we faced the dilemma of choosing a design which has a balance between well controlled and repeatable study versus far less controlled and less repeatable but more ecologically valid study – thus we decided to choose the former. The strength of our study is that it provides a ceiling of attack performance from relatively unskilled opportunist attackers. In the complex social dance of the real world, attackers would have lower quality opportunities for shoulder surfing – and thus would be expected to perform less well. This experiment therefore

provides a more difficult challenge for the security techniques being tested than it would do if the experiment built in the social dance of real world.

The second user study was conducted to compare the usability of Line Snaking and Disappearing Stroke techniques. In general, the results suggest that Disappearing Stroke is preferred by users, compared to the Line Snaking technique. Both the average login time and the login error rate for Line Snaking were higher than for Disappearing Stroke, indicating that the former imposes greater usability challenges for users. However, our results also reveal that, for some users, there is a possibility that usability will not be affected by the defence techniques applied, especially when users are highly familiar with their passwords. Further research should be conducted to investigate this issue.

Reviewing the results from both user studies, it can be concluded that, although line snaking has better defence performance, the Disappearing Stroke technique is more appropriate for general deployment, since it offers reasonable protection and good usability, as well as being preferred by users. However, with regards to technique choice, it is possible that users themselves be able to decide which defence technique to apply, depending on their situation, as our results indirectly show that, although users reported Disappearing Stroke as more comfortable to use, they immediately spotted the security advantage of Line Snaking.

Our techniques and experimental results are directly relevant to other graphical password schemes such as Background Draw a Secret (BDAS) [61] and Pass-Go [174]. However, it is useful future work to empirically evaluate the effectiveness of these defence techniques on each of the schemes. Finally, it is interesting to see how the defence techniques can be combined to provide better defence and, at the same time, maintain good usability.

Although this work provides a practical, low-cost and deployable shoulder surfing defence for recall-based graphical password systems, it is vulnerable to shoulder-surfing attacks by those equipped with a video camera. It is import future work to investigate other shoulder-surfing defence mechanisms that are invulnerable to camera attacks. An apparent direction is to combine our approaches with haptic input devices. Another

worthwhile direction is to further investigate truly usable zero-knowledge interaction based techniques.

7.2.3 Research question (3)

"*How likely is this graphical password scheme to replace the traditional, text-based password scheme"?*

The final research question opens an interesting discussion on the future of graphical passwords as an alternative mechanism. However, before answering the question literally, it is worth reviewing the journey of text-based passwords, also known as alphanumeric passwords, as the most well-known and ubiquitous authentication mechanism. This is important because alternative mechanisms such as graphical passwords would not exist if there were no necessity; indeed, the alternatives exist due to the weakness of traditional mechanisms.

Users have been comfortable using text-based passwords for many years now, in spite of the fact that the mechanism suffers from a number of problems that suggest its demise. The most commonly cited problems of text-based password mechanisms are that users often choose weak passwords, re-use the same passwords across several accounts, share their own passwords with other people or write down passwords on post-it-on notes, among many other unwise activities. The root of these problems indeed lies with the fact that passwords need to be secure and for that they need not only ideally to be unique, but also to meet the requirement of having a mixture of alphanumeric characters and a certain length. This has caused a tremendous cognitive challenge on the users' part and, in response; the aforementioned problems can occur as coping mechanisms.

Those problems are not the only issues; the password mechanism also faces other challenges such as theft of passwords by attackers through various techniques, phishing, social engineering, man-in-the-middle attack, key-logging attacks and many others. Nevertheless, with all of these problems, the alphanumeric password remains the dominant method for access control. The introduction of alternative mechanisms, such as graphical passwords, has shed some light on the possibility of minimising, if not

solving, the existing problems of alphanumeric passwords. It was introduced due to the superiority of picture or graphic memories over alphanumeric characters in the hope that they can reduce the users' cognitive challenge. However, as with other proposed mechanisms, graphical passwords also face challenges. Ironically, it seems that most of the challenges facing alphanumeric passwords are somehow directly transferred to graphical passwords, probably due to the nature of their use and practice being similar to one another.

Nevertheless, it is worth being optimistic about the future of graphical passwords as an alternative mechanism. There are indeed several reasons to be optimistic; for example, many banks have employed the graphical password as a two-factor authentication method, in combination with another mechanism to strengthen the security of customers' bank accounts. There has also been a tremendous surge of activity in academic research, in close collaboration with practitioners from industry, to improve the existing graphical password mechanism. However, the likelihood of this graphical password mechanism replacing the more well-known and ubiquitous text-based authentication mechanism remains a question to be answered.

There are several issues to ponder in relation to moving beyond traditional alphanumeric passwords. First, users are the priority in any consideration to move from one piece of technology to another. As mentioned earlier, the traditional alphanumeric passwords are synonymous with authentication procedures and thus can be considered the most common security measures that front-end users employ when confronted with any systems that require a form of access-control permission. Thus, it is rather difficult to change the users' routine to something completely new and this is yet more challenging if this new mechanism is totally different from the one to which they are more accustomed. Users are sometimes reluctant to adopt any new mechanism when they already feel comfortable with the existing mechanism.

Although graphical passwords do retain most of the procedures of the traditional text-based passwords, in many instances, due to the graphical nature, the input mechanism requires users to input their password by drawing, touching a screen or clicking icons. The involvement of a colouring element as part of the authentication factor may induce discrimination to users who are colour blind. To the best of our knowledge, to date there

have been no studies to investigate users' opinions of adopting any particular graphical password scheme on a larger scale. Thus, without proper investigation into users' willingness to adopt this new mechanism, it is difficult to predict the likelihood of it replacing the existing password mechanism.

Secondly, the existing alphanumeric passwords are used to protect a wide-range of services, ranging from financial transactions to free webmail and social networking sites. One of the important factors to consider if there were any new mechanisms to replace the existing one is compatibility and adaptability. This diverse and wide ranging services involved in the existing alphanumeric password have resulted in no single proposed authentication mechanism to date being suitable for all services, this weakens the chances of any alternative mechanism, such as the graphical password, replacing the existing password mechanism. The common practice often depends heavily on users' choices in specific use cases.

To elaborate on the point of diversity, there are also various stakeholders who promote the adoption of a particular mechanism, which is also a factor to consider. For example, security technologists, browser manufacturers, anti-virus software vendors, industry standard bodies, governments as well as end-users are entitled to different views on the costs and benefits of the proposed mechanism. Thus, there is the possibility of a scenario in which an organisation that claims "stronger" authentication may lose customers to competitors who promote "usability" while remaining with the existing authentication mechanism. Therefore, it is not easy to convert everybody's opinion to adopt a new mechanism, such as graphical passwords, quickly and this again weakens the possibility of replacing the existing password mechanism.

Thirdly, it appears that organisations are in a difficult position when trying to determine a trade-off decision about known loss incidents (e.g. in the event of loss-related data) which are caused by weak password authentication versus the unknown costs of possible customer defection. This is due to lack of information obtained on the scale, frequency, nature and financial impact of password loss incidents, as well as information on the nature of adversaries. For instance, when password loss does occur, there are many possibilities that might be the cause, such as phishing, man-in-the-middle, social engineering or key-logging attacks, or even perhaps several combinations

of adversaries' attacks. Thus, organisations are seldom able to apportion the blame solely on the use of alphanumeric passwords to the extent that they need to be replaced with a new alternative mechanism such as graphical passwords. This is due to the fact that it is difficult to "solve" security issues without proper and reliable measurements of what the actual problem is, especially when the solutions are neither cheap nor easy.

Finally, after all the hype and publicity about the introduction of alternative mechanisms, the problem of traditional text-based passwords is probably not as large as imagined, and does therefore not require a totally new mechanism as a replacement. Besides proposals introducing alternative mechanisms, credits ought to be extended to efforts in finding means of improving the existing password mechanism. For example, at the beginning of this research, the idea of adopting persuasion strategies along-side personality study was investigated, in order to broaden understanding of users' compliance behaviour. Such effort requires minimal cost to management in comparison with adopting alternative technologies such as graphical passwords. Moreover, the results of this password guideline experimental study indicates that persuasion strategy and personality study can be utilised in an effort to improve users' compliance behaviour.

As a concluding remark to this final research question, alternative mechanisms such as graphical passwords have a long way to go before they are ready to become substitutes for the traditional, alphanumeric passwords. Nevertheless, it is undeniable that the graphical passwords scheme has a promising future as a mechanism that can be used to strengthen the existing mechanism, as demonstrated in the current implementation of two-factor authentication [140] and multi-factor authentication [154]. Summing up this final research question, the discussion thereon has indirectly provided a complete overview of the issues and countermeasures in the password authentication domain discussed throughout this thesis.

7.3 Research contributions

This section will discuss several contributions of this research work. First, this research has managed to balance its focus by investigating both non-technical and technical issues involving the password authentication domain. Throughout this research, the

findings of experimental studies have demonstrated that a focus on non-technical solutions is indeed as important as the technical solutions. As presented in the first half of this thesis, the combination of utilising a persuasion approach and personality study to improve compliance behaviour with password guidelines as a low cost solution can contribute to a significant outcome in terms of improving the issues facing the password authentication domain. Thus, this research has indirectly recognised the importance of human factors that commonly receive little attention from security practitioners.

Secondly, this research also considers technical solutions by introducing three novel defence techniques to increase resistance to shoulder surfing attacks as a common challenge facing graphical passwords. To the best of our knowledge, currently there is little research into shoulder surfing defences for graphical password systems, other than in these studies [115, 112, 37, 70]. In this research, three innovative techniques are proposed to provide shoulder surfing protection for DAS and BDAS systems. A well-known lesson in computer security is that, how security engineers expect to provide effective security, and what happens in reality, can differ greatly [197].

In order to evaluate our approach, all three techniques were implemented in a prototype version and two separate controlled laboratory experiments were conducted to evaluate both the security and usability of these techniques. These techniques do not aim to provide perfect shoulder surfing protection (e.g. to make passwords invulnerable to attacks with a camera, video recorder or equivalent electronic devices). Rather, the aim is to protect passwords from less dedicated attacks, those that can be carried out by human eyes alone. While attacks aided with a camera or the like can be a serious threat, casual human-based attacks may still pose real risks. It appears that the only feasible way of achieving a perfect shoulder surfing defence relies on zero-knowledge interaction, as demonstrated in [153]. However, it is an ongoing problem to make such an approach practicable for ordinary users.

Thirdly, all of the experimental studies that have been conducted have produced empirical evidence to support the applicability of the proposed countermeasures suggested here. The first experimental study has demonstrated that there is evidence to support the worthiness of considering persuasion strategies to present the information content of a password guideline. As persuasion strategies might increase compliance

behaviour among users, personality attributes will certainly help to heighten the effect of the strategies applied. This is especially applicable for organisations which commonly include personality assessments for their employees, as a better compliance rate can be obtained if appropriate persuasion strategies are applied. Moreover, this study has initiated a foundation platform for other researchers to explore further the use of persuasion in conjunction with personality study to improve compliance behaviour with password guidelines.

The second and third experimental studies have also provided empirical evidence to support the applicability of the proposed defence techniques both from security and usability perspectives. This takes into account that the literature of several similar works [112, 37] failed to conduct appropriate evaluation studies and thus the applicability of their proposed mechanisms remains unproved. Although the proposed defence techniques have only been implemented and tested with the Draw-A-Secret (DAS) prototype, the findings were found to be applicable for most other schemes in its category; thus, only slight or minor modification is needed to suit other schemes alike.

Fourthly, the discussion that has been provided in this thesis has highlighted the most common issue facing the password authentication domain and the proposed countermeasures that have been suggested are practical in nature. Moreover, it requires minimal cost to be implemented. The research questions raised in this research are valid and relevant, and the countermeasures proposed and tested have taken into account both theoretical and practical considerations.

Finally – this research is exploratory in nature, having no intention to support or refute any existing theories or practice. However, it does open up a new platform for more research to be conducted in the near future. This research also does not attempt to provide an ultimate solution to the existing issues, but instead opens possible avenues to be investigated. In our opinion, a piece of good research will not provide a silver bullet to an issue but instead creates more opportunity for interested parties to collaborate in an effort to improve the existing proposed countermeasures. The next subsection provides some discussion on possible future work relevant to this research.

7.4 Future work

As mentioned previously, this research creates some opportunities for future work to be conducted. With regards to the password guidelines study, it will be interesting to conduct an experimental study in a workplace environment, involving employees in a particular organisation. Several other contributing factors, such as the security culture and elements of punishment or surveillance in the workplace might yield a totally a different finding. Also worth further research is verifying the target domain for password use, as the level of security for passwords might differ according to the level of protection required. Thus, it may be worth, for example, involving users who want to create a password that involves financial accounts in a comparison with those who require a password for an ordinary email account.

Initial findings on the personality study indicate that relationships do exist between personality attributes and the persuasion strategies applied, as measured by password strength. Therefore, it is conjectured that another prospect for future research is to extend this particular finding by looking into persuasion profiles in relation to individual differences. There is an existing study which investigates this issue with regards to the online business domain, focusing on an online book purchasing system which adapts its recommended books according to user preferences [102]. It is therefore interesting to investigate further how a similar scenario can be implemented in the password domain, perhaps by suggesting appropriate advice or guidelines that can most likely influence certain individuals according to their personal characteristics.

With regards to expanding the proposed defence techniques, an immediate endeavour that can be carried out is to investigate ways to improve the defence techniques to provide perfect shoulder surfing protection (i.e. to make passwords invulnerable to attacks armed with a camera, video recorder or equivalent electronic devices). This is an interesting research field as the challenge of balancing security and usability remains. It is also worthwhile combining the existing solutions (e.g.: haptic-based input) with our proposed techniques to see how both mechanisms might improve the current protection against shoulder surfing attacks.

7.5 Summary

This final chapter concludes the whole research project by revisiting the research questions and providing a broad discussion on each one. This chapter also highlights several contributions of this research, followed by recommendations for possible future work to be carried out.

REFERENCES

REFERENCES

[1] Ahmed, F., Campbell, P., Jaffar, A., Alkobaisi, S., & Campbell, J. 2010. Learning & Personality Types: A Case Study of a Software Design Course. *Journal of Information Technology Education Innovations in Practice, 9,* 237-252.

[2] Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes, 50,* 179-211.

[3] Aluja, A., Garcia, O., Rossier, J., & Garcia, L. F. (2005). Comparison of the NEO-FFI, the NEO-FFI-R and An Alternative Short Version of the NEO-PI-R (NEO-60) in Swiss and Spanish Samples. *Personality and Individual Differences, 38,* 591-604.

[4] .Amzer Privacy Protector Shield for HTC. Retrieved Feb, 11, 2011, from http://www.cellsavers.co.uk/acatalog/Privacy_Screen-Protectors.html

[5] Andrews, J. C., & Shimp, T. A. (1990). Effects of Involvement, Argument Strength and Source Characteristics on Central and Peripheral Processing in Advertising. *Psychology & Marketing, 7,* 195-214.

[6] Archer, R. P. 2006. *Forensic Uses of Clinical Assessment Intruments*. Erlbaum Associates, Mahwah: New Jersey.

[7] Arteaga, S. M., Kudeki, M., & Woodworth, A. 2009. Combating Obesity Trends in Teenagers Through Persuasive Mobile Technology. *ACM SIGACCESS Accessibility and Computing Newsletter*. http://surf-it.soe.ucsc.edu/sites/default/files/woodworth_report.pdf

[8] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. 2010. Smudge Attacks on Smartphone Touch Screen. In Proceedings of *The 4th USENIX Conference on Offensive Technologies (WOOT'10),* Washington, DC, August 2010, USENIX Association Berkeley, CA, USA, 1 – 7.

[9] Bandura, A., Grusec, J. E., & Menlove, F. L. 1967. Vicarious Extinction of Avoidance Behaviour. *Journal of Personality and Social Psychology, 5*, 16-23.

[10] Barrick, M. R., & Mount, M. K. 1991. The Big Five Personality Dimensions and Job Performance: A Meta-Analysis. *Personality Psychology, 44*, 1-26.

[11] Benoit, W. L. 1987. Argument and Credibility Appeals in Persuasion. *Southern Speech Communication Journal 52*, 181-197.

[12] Benoit, W. L. 1998. Forewarning and Persuasion. In *Persuasion Advances Through Meta-Analysis*, M. Allen & R. W. Preiss, Ed. Hampton Press, Cresskil: NJ, 139-184.

[13] Benoit, W. L. 2012. Persuasion. Retrieved March, 1, 2012, from http://www.cios.org/encyclopedia/persuasion/index.htm

[14] Bettinghaus, E. P., & Cody, M. J. 1987. *Persuasive Communication* (4th ed.). Holt, Rinehart & Winston, New York: NY.

[15] Beutler, L. E., Malik, M., Talebi, H., Fleming, J., & Moleiro, C. 2004. Use of Psychological Test/Instruments for Treatment Planning. In *The Use of Psychological Testing for Treatment Planning and Outcomes Assessment*, M. E. Maruish, Ed. Erlbaum Associates, Mahwah, NJ: 111-146.

[16] Bicakci, K. 2008. Optimal Discretization for High-Entropy Graphical Passwords. In Proceedings of *The 23rd International Symposium on Computer and Information Sciences (ISCIS'08)*, Turkey, Istanbul, October 27 – 29, 2008, IEEE Computer Society, 1 – 6.

[17] Biddle, R., Chiasson, S., & Oorschot, P. C. V. 2011. *Graphical Passwords: Learning from the First Twelve Years.* School of Computer Science, Carleton University.TRNo.TR11-01. http://www.scs.carleton.ca/shared/research/tech_Reports/2010/TR-11-01%20Chiasson.pdf

[18] Birget, J.-C., Hong, D., & Memon, N. 2003. *Robust Discretization With An Application to Graphical Passwords.* Cryptology ePrint Archive. R. 2003/168 Ed. http://clam.rutgers.edu/~birget/grPssw/robDiscr.pdf

[19] Blonder, G. 1996. Graphical Passwords. United States Patent 5559961.

[20] Borg, J. 2007. *Persuasion - The Art of Influencing People* (2nd Ed.). Pearson, Prentice Hall, Harlow: England.

[21] Braden, J. P. (2003). Psychological Assessment in School Settings. In *Handbook of Psychology:Assessment Psychology*, I. B. Weiner, J. R. Graham & J. A. Naglieri, Ed. Hoboken, NJ: Wiley, 261-290.

[22] Briggs, P. & Olivier, P. 2008. Biometric Daemons: Authentication via Electronic Pets. In Proceedings of *The Conference on Human Factors in Computing Systems (CHI'08),* Florence, Italy, April 5 – 10, 2008, USENIX Association Berkeley, CA, 2423-2432.

[23] Brostoff, S., Inglesant, P., & Sasse, M. A. 2010. Evaluating The Usability and Security of a Graphical One-Time PIN Systems. In Proceedings of *The 24th BCS Conference on Human Computer Interaction*, Dundee, Scotland, September 6 – 10, 2010, British Computer Society Swinton, UK, 88 – 97.

[24] Brostoff, S., & Sasse, M. A. 2000. Are Passfaces More Usable Than Passwords? A Field Investigation. In Proceedings of *The Human Computer Interaction*, Sunderland, England, September 5 – 8, Springer, 405 – 424.

[25] Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. 2004. Generating and Remembering Passwords. *Applied Cognitive Psychology*, *18*, 641 - 651.

[26] Brunas-Wagstaff, J. 1998. *Personality: A Cognitive Approach*. Routledge, London / New York.

[27] Buchanan, T., Johnson, J. A., & Goldberg, L. R. 2005. Implementing a Five Factor Personality Inventory for Use on the Internet. *European Journal of Psychological Assessment, 21*,2, 116-128.

[28] Budd, K. S. 2005. Assessing Parenting Capacity in a Child Welfare Context. *Child and Youth Services Review, 27,* 4, 429-444.

[29] Burch, G. S. J., & Anderson, N. 2008. Personality as a Predictor of Work Related Behaviour and Performance: Recent Advances and Direstions for Future Research. In *International Review of Industrial and Organisation Psychology,* G. P. Hodgkinson & J. K. Ford, Ed. John Wiley & Sons Ltd., 261-305.

[30] Burger, J. M. 1993. *Personality* (3rd Ed.). Brooks/Cole Publishing Co., California: CA.

[31] Burger, J. M., Messian, N., Patel, S., Del Prado, A., & Anderson, C. 2004. What a Coincidence! The Effects of Incidental Similarity On Compliance. *Personality and Social Psychology Bulletin, 30*, 35-43.

[32] Burr, W. E., Dodson, D. F., & Polk, W. T. 2006. Electronic Authentication Guideline: National Institute of Standards and Technology.

[33] Bushnell, I. W. R. 2001. Mother's Face Recognition in Newborn Infants: Learning and Memory *Infant and Child Development, 10*, 67-74.

[34] Campbell, J., Ma, W., & Kleeman, D. 2006. Password Composition Policy: Does Enforcement Lead to Better Password Choices. In Proceedings of *The 17th Australian Conference on Information Systems*, Adelaide, Australia, December 6 – 8, Australian Association for Information System, 60 – 69.

[35] Carstens, D. S. R. P., Mc-Cauley, B., & DeMara, R. F. 2004. Evaluation of The Human Impact of Password Authentication Practices on Information Security. *Information Science Journal, 7*, 67-85.

[36] Chadwick, D. 1999. Smart Cards Aren't Always the Smart Choice. *Computer, 32, 12,* 142-143.

[37] Chakrabarti, S., Landon, G. V., & Singhal, M. 2007. Graphical Passwords: Drawing A Secret With Rotation as a New Degree of Freedom. In Proceedings of *The 4th IASTED Asian Conference on Communication Systems and Networks*, Phuket, Thailand, April 2 – 4, 2007, ACTA Press Anaheim, CA, USA, 114 -120.

[38] Chiasson, S., Forget, A., Biddle, R., & Oorschot, P. C. V. 2008. Influencing Users Towards Better Password: Persuasive Cued Click Points. In Proceedings of *The 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, Liverpool, UK, September 1 – 5, 2008, British Computer Society Swinton, UK, 121 – 130.

[39] Chiasson, S., Forget, A., Biddle, R., & Oorschot, P. C. V. 2009. User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. *International Journal of Information Security, 8* 387-398.

[40] Chiasson, S., Oorschot, P. C. V., & Biddle, R. 2007. Graphical Password Authentication Using Cued Click-Points. In Proceedings of The *12th European Symposium On Research In Computer Security (ESORICS)*, Dresden, Germany, September 2007, Springer-Verlag, 359 – 374.

[41] Cialdini, R. B. 1988. *Influence Science and Practice* (2nd ed.). Pearson, Boston.

[42] Cialdini, R. B. 2001. Harnessing the Science of Persuasion *Harvard Business Review*, 72-79.

[43] Cialdini, R. B., & Trost, M. R. 1998. Social Influence: Social Norms, Conformity and Compliance. In *The Handbook of Social Psychology* (4th ed), D. T. Gilbert, S. T. Fiske & G. Lindzey, Ed. Boston: Mc-Grawhill, 151-192.

[44] Cohen, J. 1992. A Power Primer. *Psychological Bulletin*, 112, 1 (1992), 155-159.

[45] Costa, P. T., & McCrae, R. R. 1995. Domain and facets: Hierarchical Personality Assessment using the Revised NEO Personality Inventory. *Journal of Personality Assessment, 64*, 21-50.

[46] Couger, J. D., Zawacki, R. A., & Opperman, E. B. 1979. Motivation Levels of MIS Managers Versus Those of Their Employees. *MIS Quarterly, 3*(3), 47-56.

[47] Crano, W. D., & Prislin, R. 2006. Attitudes and Persuasion. *Annu. Rev. Psychol., 57*, 345-374.

[48] Cranor, L. F. 2008. A Framework for Reasoning About the Human in the Loop. In Proceedings of *The 1st Conference on Usability, Psychology and Security*, San Francisco, CA, April 14, 2008, USENIX Association Berkeley, CA, USA, 1 – 15.

[49] Cunha, A. D. D., & Greathead, D. 2007. Does Personality Matter?: An Analysis of Code-Review Ability. *Communications of the ACM 50*(5), 109-112.

[50] Danchev, D. (2008). DIY Phishing Kits Introducing New Features. *ZDNet* Retrieved Jan, 12, 2012, from http://blogs.zdnet.com/security/?p=1104

[51] Davis, D., Monrose, F., & Reiter, M. 2004. On User Choice in Graphical Password Schemes. In Proceedings of *The 13th USENIX Security Symposium*, San Diego, CA, USA, August 9 – 13, 2004, USENIX Association, 151 – 164.

[52] De Angeli, A., Conventry, L., Johnson, G., & Renaud, K. 2005. Is A Picture Really Worth A Thousand Words? Exploring the Feasibility of Graphical Authentication Systems. *International Journal of Human-Computer Studies, 63*, 128-152.

[53] De Luca, A., Weiss, R., & Drewes, H. 2007. Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN Entry. In Proceedings of *The 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces (OzCHI'07),* Adelaide, Australia, November 28 – 30, 2007, ACM New York, NY, USA, 199 – 202.

[54] Deutsch, M., & Gerard, H. B. 1955. A Study of Normative and Informational Social Influences Upon Individual Judgement. *Journal of Abnormal and Social Psychology, 51*, 629-636.

[55] Dewhurst, S. A., & Conway, M. A. 1994. Pictures, Images and Recollective Experience. *Journal of Experimental Psychology: Human Learning, Memory and Cognition 20*(5), 1088-1098.

[56] Dhamija, R., & Perrig, A. 2000. Deja Vu: A User Study Using Images for Authentication. In Proceedings of *The 9th Conference on USENIX Security Symposium,* Denver, Colorado, US, August, 14 – 17, 2000, USENIX Association Berkeley, CA, USA, 4 – 4.

[57] Digman, J. M. (1990). Personality Structure: Emergence of the Five Factor Model *Annual Reviews Psychology 41*, 417-440.

[58] Dirik, A. E., Memon, N., & Birget, C. J. 2007. Modelling User Choice in the PassPoints Graphical Password Scheme. In Proceedings of *The 3rd Symposium on Usable Privacy and Security,* Pittsburgh, PA, US, July 18 – 20, 2007, ACMPress New York, NY, US, 20 – 28.

[59] Driskell, J. E., Salas, E., Goodwin, F. F., & O'shea, P. G. 2006. What Makes a Good Team Player? Personality and Team Effectiveness. *Group Dynamics, Theory, Research and Practise, 10*(4), 249-271.

[60] Dunphy, P., Nicholson, J., & Olivier, P. 2008. Securing Passfaces for Description. In Proceedings of *The 4th Symposium on Usable Privacy and Security*, Pittsburgh, PA, US, July 23 – 25, 2008, ACMPress New York, NY, US, 24 – 35.

[61] Dunphy, P., & Yan, J. 2007. Do Background Images Improve "Draw A Secret" Graphical Passwords? In Proceedings of *The 14th ACM Conference on Computer and Communications Security,* Alexandria, VA, US, Oct 29 – Nov 2, 2007, ACMPress New York, NY, USA, 36 – 47.

.

[62] Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. 2009. A Comprehensive Study of Frequency,Interference and Training of Multiple Graphical Passwords. In Proceedings of *The 27th International Conference on Human factors in Computing Systems*, Boston, MA, USA, Apr 4 – 9, 2009, ACMPress New York, NY, USA, 889 – 898.

[63] Fazio, R. H., Powell, M. C., & Williams, C. J. 1989. The Role of Attitude Accessibility in The Attitude-to-Behaviour Process. *Journal of Consumer Research, 16*, 280-288.

[64] Feldt, R., Angelis, L., & Samuelson, M. 2008. Towards Individualized Software Engineering: Empirical Studies Should Collect Psychometrics. In Proceedings of *The 2008 International Workshop on Cooperative and Human Aspects of Software Engineering*, Leipzig, Germany, May 13, 2008, ACMPress New York, NY, USA, 49 -52

[65] Fishbein, M., & Ajzen, I. 1975. *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*. Addison Wesley, Reading: MA, USA.

[66] Florencio, D., & Herley, C. 2007. A Large-Scale Study of Web Password Habits. In Proceedings of *The 16th International Conference on World Wide Web*, Banff, Alberta, Canada, May 8 – 12, 2007, ACMPress New York, NY, USA, 657 – 666.

[67] Fogg, B. J. 1998. Persuasive Computers: Perspectives and Research Direction. In Proceedings of *The Conference on Human Factors in Computing Systems (CHI' 98)*, Los Angeles CA USA, April 18 – 23, 1998, ACM Press/Addison-Wesley Publishing Co. New York, NY, USA, 225 – 232.

[68] Forget, A., Chiasson, S., Oorschot, P. C. V., & Biddle, R. 2008. Improving Text Passwords through Persuasion. In Proceedings of *The Symposium on Usable Privacy and Security (SOUPS'08)*, Pittsburgh, PA, USA, July 23 – 25, 2008, ACMPress, New York, NY, USA, 1 – 12.

[69] Forget, A., Chiasson, S. & Biddle, R. 2010. Shoulder Surfing Resistance With Eye-Gazed Entry in Cued-Recall Graphical Passwords. In Proceedings of The *Conference on Human Factors in Computing Systems (SIGCHI)*, Atlanta, GA, USA, ACMPress, New York, NY, USA, 1107-1110.

[70] Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. 2008. YAGP: Yet Another Graphical Password Strategy. In Proceedings of *The Annual Computer Security Applications Conference*, Anaheim, California, USA, December 8 – 12, 2008, IEEE Computer Society Washington, DC, USA, 121 – 129.

[71] Gao, H., Ren, Z., Chang, X., & Aickelin, U. 2010. A New Graphical Password Scheme Resistant to Shoulder Surfing. In Proceedings of *The International Conference on CyberWorlds*, Singapore, October 20 – 22, 2010, IEEE Computer Society, 194 – 199.

[72] Goldberg, J., Hagman, J., & Sazawal, V. 2002. Doodling Our Way to Better Authentication. In Proceedings of *The Human Factors in Computing Systems*, Minneapolis, Minnesota, USA, ACMPress New York, NY, USA, 868 – 869.

[73] Goldberg, L. R. 1990. An Alternative "Description of Personality": The Big Five Factor Structure. *Journal of Personality and Social Psychology, 59*, 1216-1229.

[74] Goldberg, L. R. 1992. The Development of Markers for the Big-Five Factor Structure. *Psychological Assessment, 4*(1), 26-42.

[75] Golofit, K. 2007. Click Passwords under Investigation. In Proceedings of *The 12th European Symposium on Research in Computer Security*, Dresden, Germany, September 24-26, 2007, Springer-Verlag Berlin, Heidelberg, 343 – 358.

[76] Gosling, S. D., Rentfrow, P. J., & Swann Jr., W. B. 2003. A Very Brief Measure of The Big-Five Personality Domains. *Journal of Research in Personality 37*, 504-528.

[77] Govindarajulu, N. S., & Madhvanath, S. 2007. Password Mangement Using Doodles. In Proceedings of *The 9th International Conference on Multimodal Interfaces*, Nagoya, Aichi, Japan, November 12 – 15, 2007, ACM New York, NY, USA, 236 – 239.

[78] Grawmeyer, B., & Johnson, H. 2011. Using Multiple Password: A Week to a View. *Interacting With Computers, 23*(3) 256-267.

[79] GrIDsure. 2009. Retrieved December, 5, 2011, from http://www.gridsure.com

[80] Groenewold, G., Bruijn, B., and Bilsborrow, R. 2006. Migration of the Health Belief Model (HBM): Effects of Psychosocial and Migrant Network Characteristics on Emigration Intentions in Five Countries in West Africa and the Mediterranean Region. In Proceedings of the *Population Association of America 2006 Annual Meeting*, Los Angeles, CA, March 30 - April 1, 2006, 1 – 25.

[81] Hadyn, D. E., Bruce, V., & De Schonen, S. 1992. The Development of Face Processing Skills. *Philosophical Transactions: Biological Sciences, 335*, 105 - 111.

[82] Hafiz, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. 2008. Towards Identifying Usability and Security Features of Graphical Password in Knoweldge Based Authentication Technique. In Proceedings of *The Second*

Asia International Conference on Modelling & Simulation, Kuala Lumpur, Malaysia, May 13 – 15, 2008, IEEE Computer Society, 396 – 403.

[83] Hale, J. L., Householder, B. J., & Greene, K. L. 2002. The Theory of Reasoned Action In *The Persuasion Handbook: Developments In Theory and Practice*, J. P. Dillard & M. Pfau Ed. Thousand Oaks: CA: Sage, 259-286.

[84] Halko, S., & Kientz, J. A. 2010. Personality and Persuasive Technology: An Exploratory Study on Health-Promoting Mobile Applications. *PERSUASIVE LNCS 6137*, 150-161.

[85] Hanny, J. E., Arisholm, E., Engvik, H., & Sjoberg, D. I. K. 2010. Effects of Personality on Pair Programming. *IEEE Transactions on Software Engineering*, *36*(1), 61-80.

[86] Hayashi, E., & Christin, N. 2008. *Use Your Illusion: Secure Authentication Usable Anywhere*. In Proceedings of *The 4th Symposium on Usable Privacy and Security*, Pittsburgh, PA, USA, July 23 – 25, 2008, ACMPress New York, NY, USA, 35 – 45.

[87] Hedrick, A.M. 1990. The Effects of Piracy in Foreign Markets on U.S. Business. *Journal of International Studies, 21*, 4.

[88] Heider, F. 1946. Attitudes and Cognitive Organization. *Journal of Psychology, 21*, 107-112.

[89] Heider, F. 1958. *The Psychology of Interpersonal Relation*. Hillsdale, NJ: Lawrence Erlbaum Associates.

[90] Herath, T., & Rao, H. R. 2009. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems, 18*, 106-125.

[91] Herley, C. 2009. So Long and No Thanks for the Externalities: The Rational Rejection of Security Advices by Users. In Proceedings of *The 2009 Workshop on New Security Paradigms* Workshop Oxford, UK, September, 8-11, 2009, ACMPress New York, NY, USA, 133 – 144.

[92] Herley, C., Oorschot, P. C. V., & Patrick, A. S. 2009. Passwords: If We're So Smart, Why Are We Still Using Them? In Proceedings of *The 13th International Conference on Financial Cryptography & Data Security*, Accra Beach, Barbados, February 23–26, 2009, Springer-Verlag, 230 – 237.

[93] Hoonakker, P., Bornoe, N., & Carayon, P. 2009. Password Authentication from Human Factors Perspective: Results of a Survey among End-Users. In Proceedings of *The 53rd Annual Meeting of The Human Factors and Ergonomics Society*, San Antonio, Texas, US, October 19 – 23, 2009, 459 – 463.

[94] Hough, L. M., & Furnham, A. 2003. Use of Personality Variables in Work Settings. In *Handbooks of Psychology: Industrial and Organizational Psychology*, I. B. Weiner, W. C. Borman, D. R. Ilgen & R. J. Klimoski, Ed., Hoboken, NJ: Wiley, 131-170.

[95] Hovland, C. I., Janis, I. L., & Kelley, H. H. 1953. *Communication and Persuasion: Psychological Studies of Opinion Change*. New Heaven: CT: Yale University Press.

[96] Huang, C.-Y., Ma, S.-P., & Chen, K.-T. 2011. Using One-time Passwords to Prevent Passwords Phishing Attacks. *Journal of Network and Computer Applications, 34*(4), 1292-1301.

[97] Jayanti, R.K. & Burns, A.C. 1998. The Antecedents of Preventive Healthcare Behaviour: An Empirical Study. *Journal of the Academy of Mraketing Science, 26, 1,* 6-25.

[98] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. 1999. The Design and Analysis of Graphical Passwords. In Proceedings of *The 8th USENIX Security Symposium* Washington, DC, August 23 – 26, 1999, USENIX Association, 1 – 14.

[99] John, O. P., Naumann, L. P., & Soto, C. J. 2008. Paradigm Shift to the Integrative Big-Five Trait Taxonomy: History, Measurement and Conceptual Issues. In *Handbook of Personality: Theory and Research,* O. P. John, R. W. Robins & L. A. Pervin, Ed. New York, NY: The Guilford Press, 114-158.

[100] John, O. P., & Srivastava, S. 1999. The Big Five Trait Taxonomy: History, Measurement and Theoretical Perspectives. In *Handbook of Personality: Theory and Research,* L. A. Pervin & O. P. John, Ed., New York: The Guilford Press, 102-138.

[101] Johnston, A. C. & Warkentin, M. 2010. Fear Appeals and Information Security Behaviours: An Empirical Study, *MIS Quarterly, 34, 3*, 549-566.

[102] Kaptein, M., & Eckles, D. 2010. Selecting Effective Means to Any End: Futures and Ethics of Persuasion Profiling. In Proceedings of *The 5th International Conference PERSUASIVE 2010*, Copenhagen, Denmark,

[103] Karlins, M., & Abelson, H. I. 1970. *Persuasion: How Opnions and Attitudes are Changed* (2nd ed.). Springer Publishing Company, Inc, New York.

[104] Kasschau, R. A. 1980. *Personality Theories,* Englewood Cliffs, NJ.

[105] Kline, S. L., & Clinton, B. L. 1998. Developments in Children's Persuasive Message Practices. *Communication Education 47*, 120-136.

[106] Komanduri, S., Shay, R., Kelly, P. G., Mazurek, M. L., Bauer, L., Christin, N., . . . Egelman, S. 2011. Of Passwords and People: Measuring the Effect of Password-Composition Policies. In Proceedings of *The Human Factors and*

Computing Systems, Vancouver, BC, Canada, May 7 – 12, 2011, ACMPress New York, NY, USA, 2595-2604.

[107] Kukkonen, O. H., & Harjumaa, M. 2008. Towards Deeper Understanding of Persuasion in Software and Information Systems. In Proceedings of *The First International Conference on Advances in Computer-Human Interaction*, Sainte Luce, Martinique, February 10- 15, 2008, IEEE Computer Society Washington, DC, USA, 200 – 205.

[108] Langer, E. J., Blank, A., & Chanowitz, B. 1978. The Mindlessness of Ostensibly Thoughtful Action: The Role of "Placebic" Information in Interpersonal Interaction. *Journal of Personality and Social Psychology*, *36*(6), 635-642.

[109] LeBlanc, D., Chiasson, S., Forget, A., & Biddle, R. 2008. *Can Eye Gaze Reveal Graphical Passwords?* In Proceedings of *The 4th Symposium on Usable Privacy and Security (SOUPS'08),* Pittsburgh, PA, US, July 23 – 25, 2008, ACMPress New York, NY, USA, 1- 2.

[110] Lewis, J. R., & Sauro, J. 2006. When 100% Really Isn't 100%: Improving the Accuracy of Small-Sample Estimates of Completion Rates. . *Journal of Usability Studies, 3*(1), 136-150.

[111] Lin, C.-L., Sun, H.-M., & Hwang, T. 2001. Attacks and Solutions on Strong-Password Authentication. *IEICE Trans. Commun., E84-B*(9), 2622-2627.

[112] Lin, D., Dunphy, P., Olivier, P., & Yan, J. 2007. Graphical Passwords & Qualitative Spatial Relations. In Proceedings of *The Symposium on Usable Privacy and Security (SOUPS'07),* Pittsburgh, PA, USA, July18 – 20,2007, ACMPress New York, NY, USA, 161 – 162.

[113] Maetz, Y., Onno, S., & Heen, O. 2009. Recall-A-Story: A Story-telling Graphical Password System. In Proceedings of *The Symposium On Usable*

Privacy and Security(SOUPS'09), Mountain View, CA, USA, July 15 -17, 2009, ACMPress NewYork, NY, USA, 27 – 28.

[114] Maio, G. R., & Olson, J. M. 2000. *Why We Evaluate: Functions of Attitudes*. Lawrence Erlbaum Associates, Mahwah: New Jersey.

[115] Malek, B., Orozco, M., & El-Saddik, A. 2006. Novel Shoulder Surfing Resistant Haptic-based Graphical Password. In Proceedings of The *EuroHaptics Conference*, Paris, France, July 3 – 6, 2006, Springer Verlag, 1-6.

[116] Man, S., Hong, D., & Matthews, M. 2003. A Shoulder Surfing Resistant Graphical Password Scheme - WIW. In Proceedings *The International Conference on Security and Management (SAM'03)*, Las Vegas, Nevada, June 23 – 26, 2003, CSREA Press, 1 – 6.

[117] McConochie, W. A. 2012. Assessment Testing and Self Discovery, from http://www.testmasterinc.com/tests/bfi/

[118] McCrae, R. R., & Costa, P. T. 1989. Reinterpreting the Myers-Briggs Type Indicator from the Perspective of the Five-Factor Model of Personality. *Journal of Personality, 57*(1), 17- 40.

[119] McCrae, R. R., & John, O. P. 1992. An Introduction to the Five Factor Model and Its Application. *Journal of Personality 60*(2), 175-215.

[120] McGuire, W. J. 1968. Personality and Susceptability to Social Influence. In *Handbook of Personality Theory and Research*, E. F. Borgatta & W. W. Lambert, Ed., Chicago: Rand McNally, 1130-1187.

[121] McMillan. 2006. 'Rock Phish' Blamed for Surge in Phishing. *InfoWorld* Retrieved Jan, 10, 2012, from http://www.infoworld.com/article/06/12/12/HNrockphish_1.html

[122] Milburn, M. A. 1991. *Persuasion and Politics: The Social Psychology of Public Opinion*. Brooks/Cole, Pacific Grove: California.

[123] Milgram, S. 1974. *Obedience to Authority: An Experimental View*. New York: Harper & Row.

[124] Miller, G. R. 1980. On Being Persuaded: Some Basic Distinctions. In *Persuasion: New Directions in Theory and Research*, M. E. Roloff & G. R. Miller, Ed., Sage, Beverly Hills: California, 11-28.

[125] Miller, N. D. A., & Stafford, M. R. 1999. An International Analysis of Emotional and Rational Appeals in Services vs Goods Advertising. *Consumer Marketing, 16*, 42-57.

[126] Monrose, F. 1999. *Towards Stronger Authentication.* Doctor of Philosophy, New York University.

[127] Moriarty, T. 1975. Crime, Commitment and the Responsive Bystander. *Journal of Personality and Social Psychology, 31*, 370-376.

[128] Murray, J. B. 1990. Review of research on the Myers-Briggs Type Indicator. *Perceptual and Motor Skills, 70*, 1187-1202.

[129] Nelson, D. L., Reed, V. S., & Walling, J. R. 1976. Pictorial Superiority Effect. *Journal of Experimental Psychology Human Learning and Memory, 2*(5), 523-528.

[130] Ng, B-Y., Kankanhalli, A. & Xu, Y. 2009. Studying Users' Computer Security Behaviour: A Health Belief Perspective. *Journal of Decision Support System, 46*, 815 - 825.

[131] Nutbeam, D. & Harris, E. 2004. *Theory in a Nutshell: A Practical Guide to Health Promotion Theories*. McGraw-Hill, Sydney, Australia.

[132] O'Keefe, D. J. (1990). *Persuasion: Theory and Research*. Sage, New Park: California.

[133] Olsen, J. C., & Marshuetz, C. 2005. Facial Attractiveness is Appraised in a Glance. *Emotional, 5*, 498-502.

[134] Oorschot, P.C.V, Salehi-Abari, A. & Thrope, J. 2010. Purely Automated Attacks on PassPoints-Style Graphical Passwords. *IEEE Trans. Info. Forensics and Security, 5, 3*, 393- 405.

[135] Oorschot, P. C. V., & Thrope, J. 2011. Exploiting Predictability in Click-Based Graphical Passwords. *Journal of Computer Security, 19*, 669-702.

[136] Pahnila, S., Siponen, M., Mahmood, A. 2007. Employees' Behaviour Towards IS Security Policy Compliance. In Proceedings of *The* 40th *Hawaii International Conference on System Sciences, 2007, IEEE, Hawaii*, IEEE Computer Society Washington, DC, USA, 156 – 166.

[137] Paivio, A. 1991. Dual Coding Theory: Retrospect and Current Status *Canadian Journal of Psychology, 45*(3), 255-287.

[138] Paivio, A. 2006. *Mind and Its Evolution: A Dual Coding Theoretical Approach*. Psychology Press, Mahwah: New Jersey.

[139] Palmer, D. (2012). Why Do People Say Yes? The 6 Weapons of Influence Retrieved March, 1, 2012, from http://www.fripp.com/blog/why-do-people-say-yes-the-6-weapons-of-influence/

[140] Passfaces Corporation. 2009. The Science Behind Passfaces, December 27, 2011, from http://www.passfaces.com/enterprise/resources/white_paper.htm.

[141] Perloff, R. M. 2008. *The Dynamics of Persuasion - Communication and Attitudes in the 21st Century* (3rd ed.). Routledge Taylor & Francis Group, New York.

[142] Peslak, A. R. 2006. The Impact of Personality on Information Technology Team Project. In Proceedings of *The 2006 Conference on Computer Personnel Research: Forty Four Years of Computer Personnel Research: Achievements, Challenges & the Future (ACM SIGMIS CPR)*, Claremont, California, USA, April 13 – 15, 2006, ACMPress New York, NY, USA, 273-279.

[143] Petty, R. E., & Cacioppo, J. T. 1984. The Effects of Involvement on Responses to Argument Quantity and Quality: Central and Peripheral Routes to Persuasion. *Journal of Personality and Social Psychology, 46*, 69-81.

[144] Petty, R. E., & Cacioppo, J. T. 1986. The Elaboration Likelihood Model of Persuasion. In *Advances in Experimental Social Psychology*, L. Berkowitz, Ed., Academic Press, New York, 123-205.

[145] Proctor, R. W., Lien, M. C., Vu, K. P. L., & Schultz, E. E. 2002. Improving Computer Security for Authentication of Users: Influence of Proactive Password Restrictions. . *Behaviour Res. Methods, Instruments & Computers, 34*, 163-169.

[146] Rammstedt, B., & John, O. P. 2007. Measuring Personality in One Minute or Less: A 10 Item Short Version of the Big Five Inventory in English and German. *Journal of Research in Personality, 41*, 203-212.

[147] Richards, G. 1996. *Putting Psychology in Its Place: An Introduction from a Critical Historical Perspective*. Routledge, London/New York.

[148] Rogers, R.W. 1975. A Protection Motivation Theory of Fear and Attitude Change. *Journal of Psychology, 91*, 93 – 114.

[149] Rogers, R.W. 1983. Cognitive and Physiological Process in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In Cacioppo, J. & Petty, R. (Eds.), Social Psychophysiology New York: Guilford Press.

[150] Rosenstock, I. 1974. Historical Origins of the Health Belief Model. *Health Education Monographs, 2, 4.*

[151] Rosenstock, I. 1966. Why People Use Health Services. *Milbank Memorial Fund Quarterly, 44, 3*, 94-127.

[152] Rosselli, F., Skelly, J. J., & Mackie, D. M. 1995. Processing Rational and Emotional Messages: The Cognitive and Affective Mediation of Persuasion. *Journal of Experimental Social Psychology, 31*, 163-190.

[153] Roth, V., Richter, K., & Freidinger, R. 2004. A PIN-Entry Method Resilient Against Shoulder Surfing. In Proceedings of *The 11th ACM Conference on Computer and Communications Security*, Washington, DC, US, October 25 – 29, 2004, ACMPress New York, NY, USA, 236 – 245.

[154] Sabzevar, A. P., & Stavrou, A. 2008. Universal Multi-Factor Authentication Using Graphical Passwords. In Proceedings of *The 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, Bali, Indonesia, November 30 – December 3, 2008, IEEE Computer Society, 625-632.

[155] Salehi-Abari, A., Thrope, J., & Oorschot, P. C. V. 2008. On Purely Automated Attacks and Click-Based Graphical Passwords. In Proceedings of *The Annual Computer Security Application Conference (ACSAC)*, Anaheim, California, USA, IEEE Computer Society Washington, DC, USA, December 8 – 12, 2008, 111 – 120.

[156] Salleh, N., Mendes, E., Grundy, J., & Burch, G. S. J. 2010. An Empirical Study of the Effects of Conscientiousness in Pair Programming using the Five-Factor Personality Model. In Proceedings of *The 32nd ACM/IEEE International Conference on Software Engineering (ICSE'10)*, Cape Town, South Africa, May 2 – 8, 2010, 577 – 586.

[157] Sasse, M. A., Brostoff, S., & Weirich, D. 2001. Transforming The 'Weakest Link' - A Human/Computer Interaction Approach to Usable Security and Effective Security. *BT Technology Journal, 19*(3), 122 - 131.

[158] Saucier, G. 1994. Mini-Markers: A Brief Version of Goldberg's Unipolar Big-Five Markers. *Journal of Personality Assessment, 63*(3), 506-516.

[159] Saucier, G. 2002. Orthogonal Markers for Orthogonal Factors: The Case of The Big Five. *Journal of Research in Personality, 36,* 1-31.

[160] Schultz, E. E., Proctor, R. W., Lien, M.-C., & Savendy, G. 2001. Usability and Security: An Appraisal of Usability Issues in Information Security Methods. *Computers and Security 20*(7), 620–634.

[161] Sfetsos, P., Stamelos, I., Angelis, L., & Deligiannis, I. 2009. An Experimental Investigation of Personality Types Impact on Pair Effectiveness in Pair Programming. *Empirical Software Engineering, 14*, 187-226.

[162] Shay, R., Komanduri, S., Kelly, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., . . . Cranor, L. F. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviours. In Proceedings of *The Symposium on Usable Privacy and Security (SOUPS'10)*, Redmond, WA, USA, ACMPress, New York, NY, USA, July 14 – 16, 2010, 14 – 34.

[163] Shepard, R. 1967. Recognition Memory for Words, Sentences and Pictures *Journal of Verbal Learning and Verbal Behaviour, 6*, 156-163.

[164] Shropshire, J., Warkentin, M., Johnston, A. & Schmidt, M. (2006). Personality and IT Security: An Application of the Five Factor Model. In Proceedings of *The Americas Conference on Information Systems (AMCIS)*, Acapulco, Mexico, AIS Electronic Library, August 4 – 6, 2006, 3443 – 3449.

[165] Sobrado, L., & Birget, J. C. 2002. Graphical Passwords *The Rutgers Scholar* (Vol. 4).

[166] Srivastava, S. 2012. Personality and Social Dynamics Lab, from http://pages.uoregon.edu/sanjay/bigfive.html

[167] Standing, L. 1973. Learning 10,000 Pictures. *Quarterly Journal of Experimental Psychology 25*(2), 207-222.

[168] Standing, L., Conezio, J., & Haber, R. 1970. Perception and Memory for Pictures: Single-Trail Learning of 2500 Visual Stimuli. *Psychonomic Science, 19*(2), 73-74.

[169] Summers, W. C., & Bosworth, E. 2004. Password Policy; The Good, The Bad and The Ugly. In Proceedings of *The Winter International Symposium on Information and Communication Technologies*, Cancun, Mexico, January 5 – 8, 2004, ACMPress New York, NY, USA, 1- 6

[170] Suo, X., Zhu, Y., & Owen, G. S. 2005. Graphical Passwords: A Survey. In Proceedings of *The 21st Annual Computer Security Applications Conference*, Tucson, Arizona, USA, December 5 – 9, 2005, IEEE Computer Society Washington, DC, USA, 463 - 472.

[171] Suo, X. 2006. A Design and Analysis of Graphical Password. Master's thesis. College of Arts and Sciences, Georgia State University.

[172] Sutton, S. 1998. Predicting and Explaining Intentions and Behaviour: How Well Are We Doing? *Journal of Applied Social Psychology, 28*, 1317-1338.

[173] Tao, H. 2006. *Pass-Go: A New Graphical Password Schemes.* University of Ottawa, Canada.

[174] Tao, H., & Adams, C. 2008. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *International Journal of Network Security, 7*, 273-292.

[175] Tari, F., Ozok, A. A., & Holden, S. H. 2006. A Comparison of Perceived and Real Shoulder-surfing Resistant Risks between Alphanumeric and Graphical Passwords. In Proceedings of *The Second Symposium on Usable Privacy and Security* (SOUPS' 06), Pittsburgh, PA, USA, July 12 – 14, ACMPress New York, NY, USA, 56-66.

[176] Taylor, S. E., & Thompson, S. C. 1982. Stalking The Elusive "Vividness" Effect. *Psychological Review, 89*, 155-181.

[177] Teague, J. 1998. Personality Type, Career Preference and Implications for Computer Science Recruitment and Teaching. In Proceedings of *The 3rd Australasian Conference on Computer Science Education (ACSE' 98)*, Brisbane, Queensland, Australia, July 8 – 10, 1998, ACMPress, 155 – 163.

[178] .The Password Meter. Retrieved May, 12, 2012, from http://www.passwordmeter.com/

[179] Thrope, J., & Oorschot, P. C. V. 2004. Towards Secure Design Choices for Implementing Graphical Passwords. In Proceedings of *The 20th Annual Computer Security Applications Conference (ACSAC'04),* Tucson, Arizona, USA, December 6 – 10, 2004, IEEE Computer Society Washington, DC, USA, 50 – 60.

[180] Thrope, J., & Oorschot, P. C. V. 2007. Human-seeded Attacks and Exploiting Hot-spots in Graphical Passwords. In Proceedings of *The 16th USENIX Security Symposium on USENIX Security Symposium*, Boston, MA, August 6 – 10, 2007, USENIX Association, US, 103 – 118.

[181] Towhidi, F., Abdul Manaf, A., Mohd. Daud, S., & Lashkari, A. H. 2011. *The Knowledge Based Authentication Attacks*. In Proceedings of *The International Conference on Wireless Network (ICWN'11)*, Las Vegas, Nevada, US, July 18 – 21, 2011, CSREA Press, 649 – 653.

[182] Valentine, T. 1999. Memory for Passfaces After a Long Delay: Goldsmiths College University of London.

[183] Vance, A., Suponen, M., & Pahnila. S. 2009. *How Personality and Habit Affect Protection Motivation*. In Proceedings of *The Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP'09)*, Phoenix, AZ, USA, December 15 – 19, 2009, IEEE Computer Society Washington, DC, USA,1 – 14.

[184] Varenhorst, B. 2004. Passdoodles: A Lightweight Authentication Method: MIT Research Institute.

[185] Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., & Cook, J. 2007. Improving Password Security and Memorability to Protect Personal and Organisational Information. *International Journal of Human-Comp. Studies, 65*, 744-757.

[186] Walker, L. R., and Thomas, K. W. 1982. Beyond Expectancy Theory: An Integrative Motivational Model from Health Care. *Academy of Management Review, 7, 2*, 187-194.

[187] Weiner, I. B. 2004. Rorschach Assessment: Current Status. In *Comprehensive Handbooks of Psychological Assessment: Personality Assessment*. M. Hersen, M. J. Hilsenroth & D. L. Segal Ed., John Wiley & Sons, Hoboken: New Jersey.

[188] Weiner, I. B., & Greene, R. L. 2008. *Handbook of Personality Assessment*. Hoboken, NJ: John Wiley & Sons, Inc.

[189] Weinshall , D., & Kirkpatrick, S. 2004. *Passwords You'll Never Forget, But Can't Recall*. In Proceedings of *The Conference on Human Factors and Computing Systems*, Vienna, Austria, April 24 – 29, 2004, ACMPress, New York, NY, USA, 1399 – 1402.

[190] Weirich, D., & Sasse, M. A. 2002. Pretty Good Persuasion: A First Step towards Effective Password Security in The Real World. In the *Proceedings of the 2001 Workshop on New Security Paradigms Workshop,* Cloudcroft, New Mexico, September 10 -13, 2001, ACMPress, New York, NY, USA, 137 – 143.

[191] Wessels, P. L., & Steenkamp, L. P. (2007). Assessment of Current Practices in Creating and Using Passwords as a Control Mechanism for Information Access. *South African Journal of Information Management, 9,* 1-14.

[192] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. 2005. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *International Journal of Human-Computer Studies, 63,* 102-127.

[193] Wiener, J. L., & Mowen, J. C. 1986. Source Credibility: On the Independent Effects of Trust and Expertise. In *Advances in Consumer Research,* R. J. Lutz, Ed., Association for Consumer Research, Provo, UT, 306-310.

[194] Wolfe, J. M. 2000. *Visual Attention*. Academic Press, San Diego: California.

[195] Woodhouse, S. 2007. Information Security: End User Behavior and Corporate Culture. In Proceedings of *The 7th IEEE International Conference on Computer and Information Technology (CIT'07),* Fukushima, Japan, October 16 – 19, 2007, IEEE Computer Society Washington, DC, USA, 767-774.

[196] Xu, H., Rosson, M. B., & Carroll, J. M. 2007. Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View. In Proceedings of *The Symposium On Usable Privacy and Security (SOUPS'07),* Pittsburgh, PA, US, July 18 – 20, 2007, ACMPress, New York, NY, USA, 1-5.

[197] Yan, J., Blackwell, A., Anderson, R., & Grant, A. 2004. Password Memorability and Security: Empirical Results. *IEEE Privacy & Security, 2*(5), 25-31.

[198] Zey, M. 1998. *Rational Choice Theory and Organizational Theory: A Critique*. Sage Publication, Inc., London: UK.

[199] Zhang, L., & McDowell, C. W. 2009. Am I Really At Risk? Determinants of Online Users' Intention to Use Strong Passwords. *Journal of Internet Commerce, 8*, 180-197.

[200] Zhou, J. & Deng, R. On The Validity of Digital Signature. *Computer Communication Review (ACM SIGCOMM), 30, 2,* 29-34.

[201] Zurko, M. E. 2005. User-Centered Security: Stepping Up to the Grand Challenge. In Proceedings of *The Annual Computer Security Application Conference*, Anaheim, California, USA, December 5 – 9, 2005, IEEE Computer Society Washington, DC, USA, 188 – 202.

LIST OF APPENDICES

LIST OF APPENDICES

Appendix A:

Materials related to Password Guidelines Experimental Work

i) Recruitment email

Hello,

My name is Haryani and I am PhD student at School of Computing Science. As part of my PhD work, I am planning to invite people to help me with a small computer experiment which only takes about 25 – 30 minutes. The experiment does not require any specific computing skills so please don't hesitate to participate. It should be fun and knowledgeable to get involved in my experiment.

The experiment will take place from **Mon-Fri (930am - 4pm) starting on the 31 October 2011 onwards. Each person will be allocated a 30 minutes slot.**

On top of that, you will also receive **£5 (cash)** for your time and effort in participating.

If you are interested in helping out, please email me at (**n.h.zakaria@ncl.ac.uk**)and I will allocate a slot for you to come to my office at **Claremont Tower** (**Room 10.04**).

I really hope you can come and participate so really looking forward to hear from you soon!

Many thanks.

N.Haryani Zakaria
Room 10.04 Claremont Tower
School of Computing Science
Newcastle University

ii) Consent form

SCHOOL OF COMPUTING SCIENCE
FACULTY OF SCIENCE, AGRICULTURAL & ENGINEERING
NEWCASTLE UNIVERSITY

Participant Consent Form

Name of Study:
PASSWORD GUIDELINES
Purpose:
The purpose of this study is to :
1) investigate the effectiveness of different types of persuasion strategies embedded in the password guidelines.
2) investigate participants' personality using Big Five Inventory (BFI) personality framework to see its' relationship with certain types of persuasion strategies embedded into the password guidelines.

Procedure:
If you agree to be in this study, you will be asked to do the following:
1. Fill in consent form and complete the BFI personality test.
2. You need to create a password email account. During the password creation, you are highly encouraged to refer to the password guideline given. **Please do not use any password that you had used for your other accounts. It is important to note that you are not required to reveal your password to the experimenter nor your password is collected by the system.**
3. Once you completed the task, you will be given a short break and will be asked to re-login again sometimes later using the same password you have created.
4. Then you will be asked to complete short questionnaires.
5. Finally you will receive your experiment remuneration from the experimenter before you leave the room.

The total time required to complete the study should be approximately 15 - 20 minutes. You will receive £5 of free printing credits for participating.

Benefits/Risks to Participant:
Participants will be informed about the importance of using good (stronger) password for better protection of their accounts.
Voluntary Nature of the Study/Confidentiality:
Your participation in this study is entirely voluntary and you may refuse to complete the study at any point during the experiment, or refuse to complete any task which you are uncomfortable. You may also stop at any time and ask the researcher any questions you may have. Your student number will never be connected to your results instead; it will only be used for providing compensation for your participation. We will use serial numbers instead, for identification purposes. Information that would make it possible to identify you or any other participants will never be included in any sort of report. The data will be accessible only to those working on the project.

Contacts and Questions:
At this time you may ask any questions you may have regarding this study. If you have questions later, you may contact the person conducting the study, Haryani Zakaria via email at n.h.zakaria@ncl.ac.uk Questions or concerns about institutional approval should be directed to Ms Jo Mayne, Deputy Head of Administration at the Faculty of Science, Agricultural & Engineering, Newcastle University via email joanne.mayne@ncl.ac.uk or call her at 0191 222 5923.

Statement of Consent:
I have read the above information. I have asked any questions I had regarding the experimental procedure and they have been answered to my satisfaction. I consent to participate in this study.
Name of Participant_____Date: _____
Signature of Participant:_____Age:_____
(**Note:** You must be 18 years of age or older to participate in this study. Let the experimenter know if you are under 18 years old.)

Thank you for your participation!

iii) The Big Five Inventory (BFI) personality test form

The Big Five Inventory (BFI)

This 44-item test was developed by Oliver P. John, Ph.D. and V. Benet-Martinez in 1998. It provides a score for each of the Big Five personality traits (**Conscientiousness**, **Agreeableness**, **Emotional Stability**, **Extroversion** and **Openness**).

Instructions:
For each statement below, please indicate the extent to which you **agree or disagree with that statement**. It's important that you respond to all statements.

Num.	Questions	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
1)	Is talkative					
2)	Tends to find faults with others					
3)	Does a thorough job					
4)	Is depressed, blue					
5)	Is original, comes up with new ideas					
6)	Is reserved					
7)	Is helpful and unselfish with others					
8)	Can be somewhat careless					
9)	Is relaxed, handles stress well					
10)	Is curious about many different things					
11)	Is full of energy					
12)	Starts quarrels with others					
13)	Is a reliable worker					
14)	Can be tense					
15)	Is ingenious, a deep thinker					
16)	Generates a lot of enthusiasm					
17)	Has a forgiving nature					
18)	Tends to be organised					
19)	Worries a lot					
20)	Has an active imagination					

Num.	Questions	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
21)	Tends to be quiet					
22)	Is generally trusting					
23)	Tends to be lazy					
24)	Is emotionally stable, not easily upset					
25)	Is inventive					
26)	Has an assertive personality					
27)	Can be cold and aloof					
28)	Perseveres until the task is finished					
29)	Can be moody					
30)	Values artistic, aesthetic experiences					
31)	Is sometimes shy, inhibited					
32)	Is considerate and kind to almost everyone					
33)	Does things efficiently					
34)	Remains calm in tense situations					
35)	Prefers work that is routine					
36)	Is outgoing, sociable					
37)	Is sometimes rude to others					
38)	Makes plans and follows through with them					
39)	Get nervous easily					
40)	Likes to reflect, play with ideas					
41)	Has few artistic interests					
42)	Likes to cooperate with others					
43)	Is easily distracted					
44)	Is sophisticated in art, music or literature					

~Thank you for your cooperation ~

Please leave your email _____ if you interested to know the result of your BFI personality test.

iv) Scoring the BFI Scales

BFI scale scoring: Reverse score the items labelled “R” and compute scale scores as the mean of the following items:

Personality traits	Number of questions	Scores metric
Extraversion	8 items	1, 6R, 11, 16, 21R, 26, 31R, 36
Agreeableness	9 items	2R, 7, 12R, 17, 22, 27R, 32, 37R, 42
Conscientiousness	9 items	3, 8R, 13, 18R, 23R, 28, 33, 38, 43R
Neuroticism	8 items	4, 9R, 14, 19, 24R, 29, 34R, 39
Openness	10 items	5, 10, 15, 20, 25, 30, 35R, 40, 41R, 44

**Note that the items numbered with R needs a inversion on the score.*

v) The instructions for participants

Creating new university login account

The ISS (Information System & Services) Department of Newcastle University wants all the students to create a new login account to replace the existing one. This new login account provides access to important online services including university email, course registration, access to your personal data storage and many others. Due to staff and resources limitation, ISS department is taking this opportunity to invite student (batch by batch) to create their new login account in order to:

- Provide better assistance to all students
- Avoid crowding and speed up the procedures
- Allow effective communication and avoid any confusion

If you require any assistance please do not hesitate to talk and discuss with the experimenter.

***Please read thru the guidelines given to you as a reference, before you start creating the new login account.**

Thank you.

vi) **The password guidelines for participants in the control group**

Please refer to the guideline below to create your password.

The way to set a password:

- Password does not contain all or part of the users account name
- Password is at least 8 characters long
- Password is not “password” or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$”*etc.)

vii) **The password guidelines for participants in the rational group**

Why good password is important...?

The fact that it is hard to convince people about how vulnerable their passwords are, is common. So, how would one actually breach your personal security? The answer is quite simple. Here's the logic - You probably use the same password for different accounts, right? Your Banks probably have good decent security, so hackers would possibly not put them as their first attempt. However, other less important sites like the online newspaper site you visit every morning, an online forum you frequent or site you've visited for some free interesting articles might not be as well prepared. So those are the ones the hackers would work on. But you must be wondering how do hackers know which bank you use and what your login ID is for the sites you frequent? The cookies in your Web browser's cache have it all. By paying particular attention to the difference between using only lowercase characters and using all possible characters (uppercase, lowercase, and special characters (like @#$%^&*) - adding just one capital letter and one asterisk would significantly prolong the time for hackers to crack your password!

Please refer to the guideline below to create your password.

The way to set a password:

- Password does not contain all or part of the users account name
- Password is at least 8 characters long
- Password is not "password" or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$"*etc.)

viii) **The password guidelines for participants in the emotional group**

Why good password is important...?

Imagine your account being hacked - the hackers could temper with your major computer systems or carry out illegal activities using your account! It is even worse, if you use the same password for other accounts as well - they can easily obtain your private information something as valuable as your banking stuff! As alarming as these might sound to you, these are all common incidents that could possibly happen to computer users who do not care much about their password choice. It is frustrating to know that most people don't think hackers would target them personally. However, cases have been reported that the hackers get their hands on a database and just go through the list without personally knowing anyone - looking for financial data or just playing around with people's information. Although, it is understood that perfect security is impossible, we can at least give the hackers a tougher job to crack our password if we choose them properly.

Please refer to the guideline below to create your password.

The way to set a password:

- Password does not contain all or part of the users account name
- Password is at least 8 characters long
- Password is not "password" or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$"*etc.)

ix) **The password guidelines for participants in the social proof group**

Why good password is important...?

The hackers have developed a whole range of sophisticated tools to get to your personal data. Sometimes hackers do not have to work hard to obtain your password. With the current trend of mostly everyone having a social networking account such as Facebook, hackers can obtain their victims' password more easily as we normally choose our password from something that is personal and yet easy for us to remember. While having account (such as Facebook) being hacked is the last thing that we would wished for, the consequences could be damaging. For instance, the hackers would be able to impersonate you to post ridiculous message status to all your network of friends and this will affect your image. As a university student, you do not want to be popular because of your bad image among your colleagues of friends by having a wrong choice of password! Indeed, somebody having a good password, not only protect their personal information but also their good reputation.

Please refer to the guideline below to create your password

The way to set a password:

- Password does not contain all or part of the users account name
- Password is at least 8 characters long
- Password is not "password" or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$"*etc.)

x) **The password guidelines for participants in the commitment & consistency group**

Why good password is important...?

Everyone agrees that good passwords are important but not many actually use them! If you understood the importance of password and willing to comply by creating a strong password for your email account, we highly recommend that you state your commitment by signing the form below and return it to the experimenter. By doing so, you have put yourself in the right position of complying with good security behaviour which should deserve a praised and we thank you for your commitment.

"Preventive measures can easily be taken and never once allow yourself to become their victims! It can simply be done by avoiding common mistakes made by other people when creating passwords."

(Name)_____ID Number:_____

I am committed to protect myself and my university account by creating stronger password.

Signature:_____ Date:_____

**This form will be hand over to the ISS department as a proof of your commitment and will be kept in record.*

Please refer to the guideline below to create your password.

The way to set a password:

- Password does not contain all or part of the users account name
- Password is at least 8 characters long
- Password is not "password" or a deviation thereof or left blank
- Password must contain characters from three of the following categories;
  - English uppercase characters (A….Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!£@~%$"*etc.)

xi) The metrics for the measurement of the password strength scores

Additions	Formula Counts
Number of characters	+ (n*4)
Uppercase letters	+((len–n)* 2)
Lowercase letters	+((len–n)* 2)
Numbers	+ (n*4)
Symbols	+ (n*6)
Middle numbers or symbols	+ (n*2)
Requirements	+ (n*2)
Deductions	**Formula Counts**
Letters only	-n
Numbers only	-n
Repeat characters (case insensitive)	-
Consecutive upper case letters	-(n*2)
Consecutive upper case letters	-(n*2)
Consecutive numbers	-(n*2)
Sequential letters (3+)	-(n*3)
Sequential numbers (3+)	-(n*3)
Sequential symbols (3+)	-(n*3)

xii) The metrics for the measurement of the password compliance scores

Additions	Formula Counts
Not contain username	+5
Contain username	-5
At least 8 characters	+5
Less than 8 characters	-5
Not the using the word “password”	+5
Using the word “password”	-5
Contain at least three of the following: • A-Z • a-z • Numbers • Symbols	(*x*) characters * 5

**Note that the minimum score for compliance = 30 and <30 indicates non-compliance*

xiii) **The questionnaires for participants in the control group**

For each of the following question, please tick (✓) the box that best applies to you.

1) Age group:

	Less than 18 years
	18 – 25 years
	26 – 35 years
	36 – 45 years
	46 – 55 years
	More than 55 years

2) Gender:

	Male
	Female

3) a) Current course/degree:

	Undergraduate (BSc, BA etc.)
	Postgraduate (MSc, MA, PhD etc.)

b) Faculty:

	Science, Agriculture and Engineering (SAgE)
	Humanities & Social Sciences (HaSS)
	Medical Sciences

4) Experience of using computers (in number of years):

	0 – 5 years
	6 – 10 years
	More than 10 years

5) Is the password that you have just created one that you have used in the past?

	Yes
	No
	Something similarity to another password that I have used before

6) How did you choose your password?

	Meaningful detail (e.g. name, date, street, registration number)
	Combination of meaningful details (e.g.Jack1234, 15Apr97)
	Pronounceable password (e.g. cusoon, one4all)
	Using the first letter from each word in a special phrase (e.g. “My pet is call Tom” to create the password mpicT)
	Random combination of characters (e.g. Qcar&67*)

Others, please specify: _____

7) If you had to rely on your memory alone, how likely are you able to remember this password within:

1 week from now?		**1 month from now?**	
	Very likely		Very likely
	Likely		Likely
	Neither likely nor unlikely		Neither likely nor unlikely
	Unlikely		Unlikely
	Very unlikely		Very unlikely

xiv) **The questionnaires for participants in the rational, emotional and social proof group**

For each of the following question, please tick (✓) the box that best applies to you.

1) Age group:

	Less than 18 years
	18 – 25 years
	26 – 35 years
	36 – 45 years
	46 – 55 years
	More than 55 years

2) Gender:

	Male
	Female

3) a) Current course/degree:

	Undergraduate (BSc, BA etc.)
	Postgraduate (MSc, MA, PhD etc.)

b) Faculty:

	Science, Agriculture and Engineering (SAgE)
	Humanities & Social Sciences (HaSS)
	Medical Sciences

4) Experience of using computers (in number of years):

	0 – 5 years
	6 – 10 years
	More than 10 years

5) Is the password that you have just created one that you have used in the past?

	Yes
	No
	Something similarity to another password that I have used before

6) How did you choose your password?

	Meaningful detail (e.g. name, date, street, registration number)
	Combination of meaningful details (e.g.Jack1234, 15Apr97)
	Pronounceable password (e.g. cusoon, one4all)
	Using the first letter from each word in a special phrase (e.g. "My pet is call Tom" to create the password mpicT)
	Random combination of characters (e.g. Qcar&67*)

Others, please specify: _____

7) If you had to rely on your memory alone, how likely are you able to remember this password within:

1 week from now?		**1 month from now?**	
	Very likely		Very likely
	Likely		Likely
	Neither likely nor unlikely		Neither likely nor unlikely
	Unlikely		Unlikely
	Very unlikely		Very unlikely

8) Do you think the advice on "Why Password is important?" have persuaded you to create better (stronger) password?

	Very likely
	Likely
	Neither likely nor unlikely
	Unlikely
	Very unlikely

xv) **The questionnaires for participants in the commitment & consistency group**

For each of the following question, please tick (✓) the box that best applies to you.

1) Age group:

	Less than 18 years
	18 – 25 years
	26 – 35 years
	36 – 45 years
	46 – 55 years
	More than 55 years

2) Gender:

	Male
	Female

3) a) Current course/degree:

	Undergraduate (BSc, BA etc.)
	Postgraduate (MSc, MA, PhD etc.)

b) Faculty:

	Science, Agriculture and Engineering (SAgE)
	Humanities & Social Sciences (HaSS)
	Medical Sciences

4) Experience of using computers (in number of years):

	0 – 5 years
	6 – 10 years
	More than 10 years

5) Is the password that you have just created one that you have used in the past?

	Yes
	No
	Something similarity to another password that I have used before

6) How did you choose your password?

	Meaningful detail (e.g. name, date, street, registration number)
	Combination of meaningful details (e.g.Jack1234, 15Apr97)
	Pronounceable password (e.g. cusoon, one4all)
	Using the first letter from each word in a special phrase (e.g. "My pet is call Tom" to create the password mpicT)
	Random combination of characters (e.g. Qcar&67*)

Others, please specify: _____

7) If you had to rely on your memory alone, how likely are you able to remember this password within:

1 week from now?		**1 month from now?**	
	Very likely		Very likely
	Likely		Likely
	Neither likely nor unlikely		Neither likely nor unlikely
	Unlikely		Unlikely
	Very unlikely		Very unlikely

8) Do you think showing off your commitment by signing and submitting the form has persuaded you to create better (stronger) password?

	Very likely
	Likely
	Neither likely nor unlikely
	Unlikely
	Very unlikely

xvi) **The participants' distribution list**

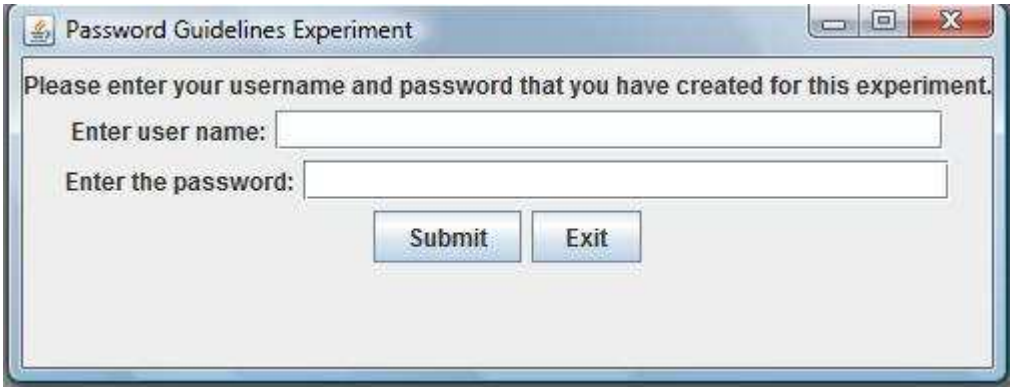
No.	User ID	Group	No.	User ID	Group
1	User001	R	47	User047	E
2	User002	E	48	User048	SP
3	User003	SP	49	User049	C&C
4	User004	C&C	50	User050	C
5	User005	C	51	User051	R
6	User006	R	52	User052	E
7	User007	E	53	User053	SP
8	User008	SP	54	User054	C&C
9	User009	C&C	55	User055	C
10	User010	C	56	User056	R
11	User011	R	57	User057	E
12	User012	E	58	User058	SP
13	User013	SP	59	User059	C&C
14	User014	C&C	60	User060	C
15	User015	C	61	User061	R
16	User016	R	62	User062	E
17	User017	E	63	User063	SP
18	User018	SP	64	User064	C&C
19	User019	C&C	65	User065	C
20	User020	C	66	User066	R
21	User021	R	67	User067	E
22	User022	E	68	User068	SP
23	User023	SP	69	User069	C&C
24	User024	C&C	70	User070	C
25	User025	C	71	User071	R
26	User026	R	72	User072	E
27	User027	E	73	User073	SP
28	User028	SP	74	User074	C&C
29	User029	C&C	75	User075	C
30	User030	C			
31	User031	R			
32	User032	E			
33	User033	SP			
34	User034	C&C			
35	User035	C			
36	User036	R			
37	User037	E			
38	User038	SP			
39	User039	C&C			
40	User040	C			
41	User041	R			
42	User042	E			
43	User043	SP			
44	User044	C&C			
45	User045	C			
46	User046	R			

xvii) The interfaces of the prototype for password guidelines experiment

(a) The interface for users to choose whether to sign-up account, login or exit

(b): The main interface to create login account

(c): The interface shown after successfully created an account



(d): The main login interface

(e): The interface shown to indicate login successful

(f): The interface shown to indicate login failure

Appendix B:

Materials related to Security Evaluation of the Proposed Defence Techniques for Recall-based Graphical Password

i) Recruitment email

Hi,

My name is Haryani and I am PhD student at School of Computing Science. As part of my research work, I am planning to test the security of visual password system (no knowledge of computer security nor visual password system is required).

Therefore, I need people to help me out with this test. The test takes only 15 minutes and should be fun to do. I will be able to compensate your time with free 200 pages of printing credits.

The test would take place at Room 10.04 Claremont Tower on 14th - 18th February 2010. I will be there from 930am till 530pm and you can choose to come between this hour to try out the test.

For more information, please do not hesitate to email me (n.h.zakaria@ncl.ac.uk) or call me at 0191 222 5405.

Many thanks

Haryani Zakaria
Room 10.04 Claremont Tower
School of Computing Science
Newcastle University

Personal Website: http://www.cs.ncl.ac.uk/people/n.h.zakaria

ii) Consent form

SCHOOL OF COMPUTING SCIENCE
FACULTY OF SCIENCE, AGRICULTURAL & ENGINEERING
NEWCASTLE UNIVERSITY

Participant Consent Form

Name of Study:
SHOULDER SURFING RESISTANT TO DRAW-A-SECRET (DAS) GRAPHICAL PASSWORD

Purpose:
The purpose of this study is to discover which defence technique is the best among the three being proposed.

Procedure:
If you agree to be in this study, you will be asked to do the following:
1. You need to try your very best to capture the passwords drawn by the experimenter on the PDA screen.
2. Observe the experimenter carefully as she draws her passwords (3 different passwords in total) as you will only have one chance to do this and no repetition is allowed.
3. You are allowed to take notes on your observations.
4. After the three drawn passwords completed, please reproduce the passwords by drawing them on the (5x5) grid lines provided to you.

The total time required to complete the study should be approximately 15 minutes. You will receive 200 pages (worth of £2) of free printing credits for participating.

Benefits/Risks to Participant:
Participants will learn about the Draw A Secret graphical passwords and it's security protection as this will be beneficial for computer security knowledge. Possible risks include frustration caused by not being able to capture any of the observed passwords.

Voluntary Nature of the Study/Confidentiality:
Your participation in this study is entirely voluntary and you may refuse to complete the study at any point during the experiment, or refuse to complete any task which you are uncomfortable. You may also stop at any time and ask the researcher any questions you may have. Your student number will never be connected to your results instead; it will only be used for providing compensation for your participation. We will use serial numbers instead, for identification purposes. Information that would make it possible to identify you or any other participants will never be included in any sort of report. The data will be accessible only to those working on the project.

Contacts and Questions:
At this time you may ask any questions you may have regarding this study. If you have questions later, you may contact the person conducting the study, Haryani Zakaria via email at n.h.zakaria@ncl.ac.uk. Questions or concerns about institutional approval should be directed to Ms Jo Mayne, Deputy Head of Administration at the Faculty of Science, Agricultural & Engineering, Newcastle University via email joanne.mayne@ncl.ac.uk or call her at 0191 222 5923.

Statement of Consent:
I have read the above information. I have asked any questions I had regarding the experimental procedure and they have been answered to my satisfaction. I consent to participate in this study.

Name of Participant_____Date: _____
Signature of Participant _____Age:_____
(Note: You must be 18 years of age or older to participate in this study. Let the experimenter know if you are under 18 years old.)

Thank you for your participation!

iii) Introduction to The Draw-A-Secret (DAS) scheme

Draw-A-Secret (DAS) scheme is a graphical password that allows you to draw your passwords on grid lines. An example of DAS password is shown in Figure 1.

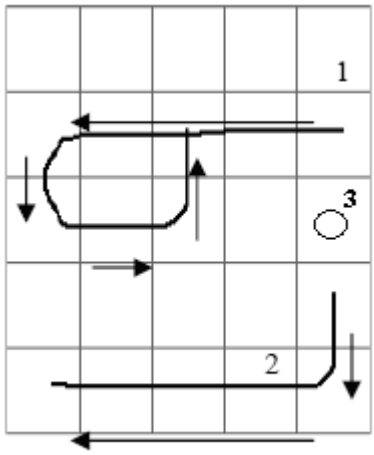


Figure 1: An Example of DAS Password

Based Figure 1, in order for the password to be accepted by the system, the following structures have to be maintained:

1) Number of stroke – 3 (as label above)
2) Order of the stroke (in the correct sequence)
2) Direction of the stroke – as shown by the arrows

It is important to note the following:

1) The system **DOES NOT** allow:
   i) **tracing grid** ii) **crossing corners** iii) **drawing lines too near the grid**

2) If a stroke is drawn inside one cell (i.e.: the 3rd stroke), direction of the stroke is not important.

*Please ask the facilitator if you are unsure of how to construct a DAS password. A quick demonstration of the prototype will be shown to you.

iv) The explanation provided to the participants on the three proposed defence technique

DECOY STROKE DEFENCE TECHNIQUE

The following is a description of how decoy stroke defence technique works. Figure 1 shows an example of original DAS password scheme. In figure 2, the decoy stroke (in dark brown color) will start to appear as you start to draw your stroke. Please refer to a short demo shown to you by the experimenter.

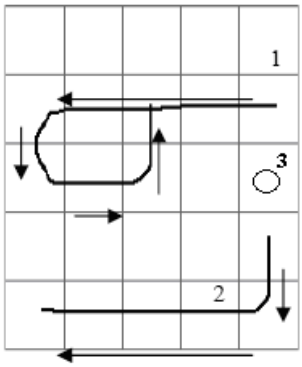


Figure 1: DAS Password (without defence activated)

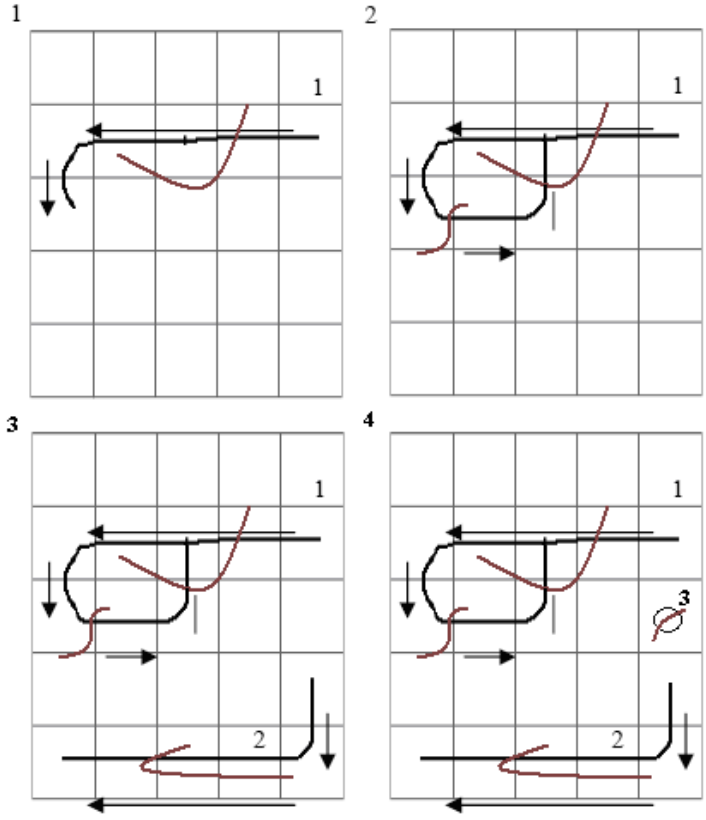


Figure 2: Example of display for DAS Password (defence activated)

DISAPPEARING STROKE DEFENCE TECHNIQUE

The following is a description of how disappearing stroke defence technique works. Figure 1 shows an example of original DAS password scheme. In figure 2, the stroke will stay for a short while before it disappears. Please refer to a short demo shown to you by the experimenter.

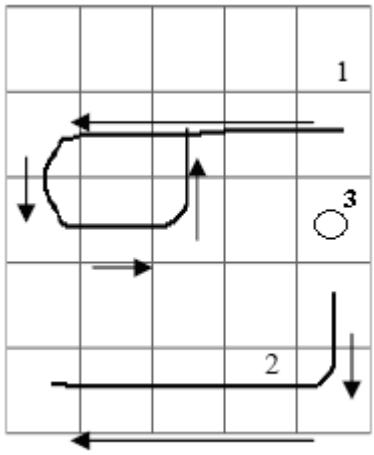


Figure 1: DAS Password (without defence activated)

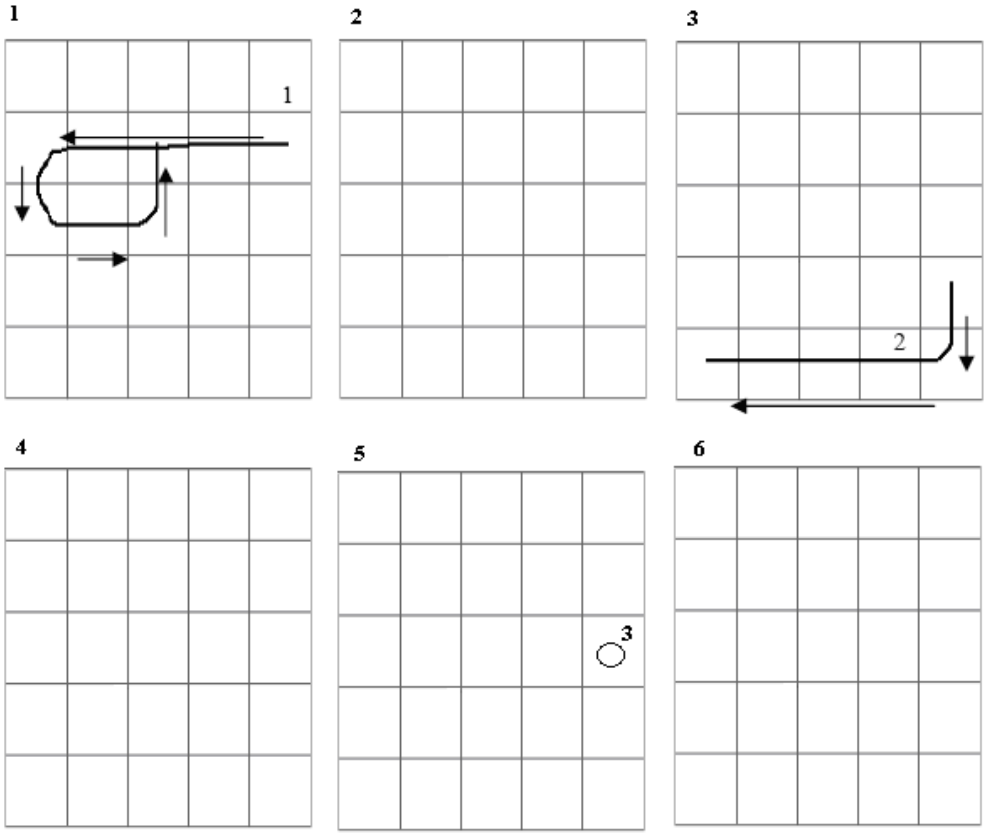


Figure 2: Example of display for DAS Password (defence activated)

LINE SNAKE DEFENCE TECHNIQUE

The following is a description of how line snake defence technique works. Figure 1 shows an example of original DAS password scheme. In figure 2, the stroke is disappearing as it is being drawn. Please refer to a short demo shown to you by the experimenter.

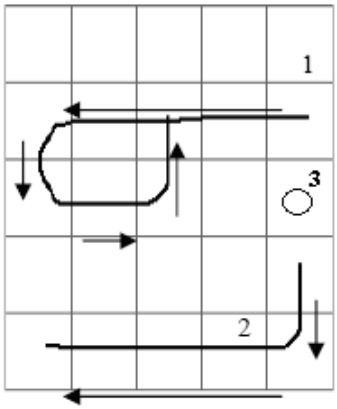


Figure 1: DAS Password (without defence activated)

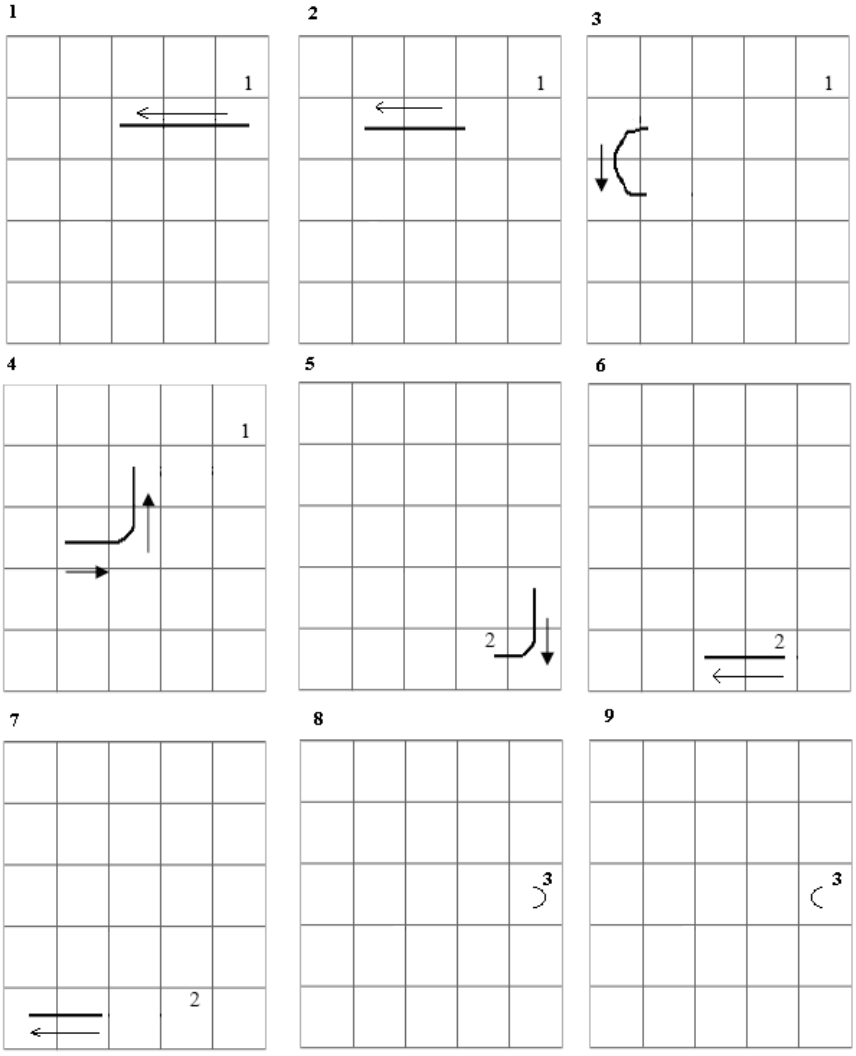


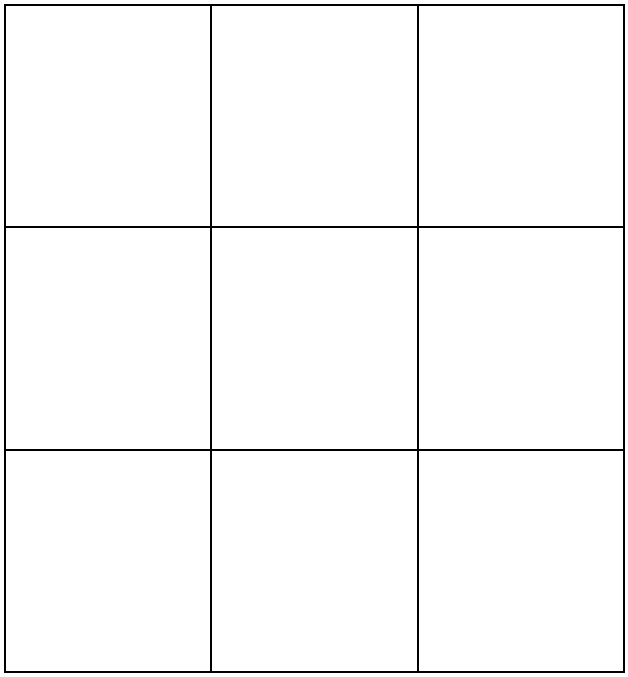
Figure 2: Example of display for DAS Password (defence activated)

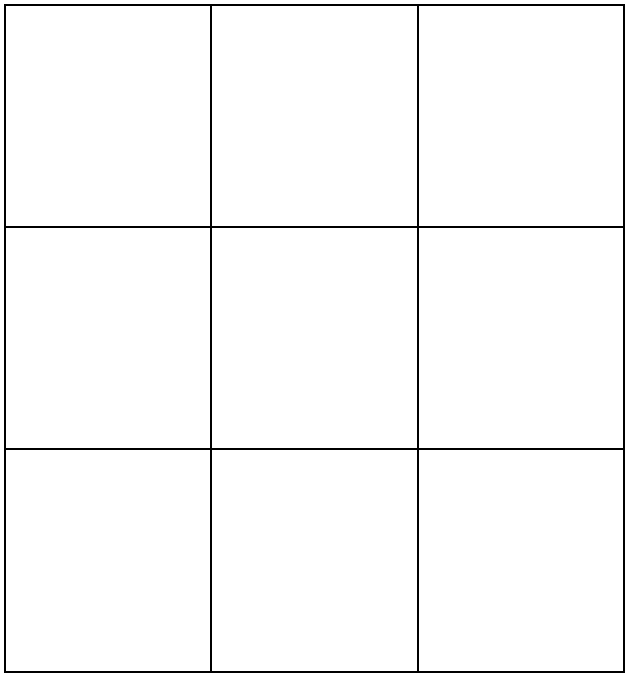
v) Instructions given to participants

What's your TASK?

1) You need to try your very best to capture the passwords drawn by the experimenter on the PDA screen.
2) **Observe** the experimenter carefully as she draw her passwords (three different passwords in total) as you will only have **one chance** to do this and **no repetition** is allowed.
3) However, you are **allowed** to take notes on your observations.
4) After the experimenter completed drawing the 3 passwords, please **reproduce** the passwords you've observed by **drawing** them on the (5x5) grid lines provided for you.

vi) Example of the 3x3 grid lines given to participants





Appendix C:

Materials related to Usability Evaluation of the Proposed Defence Techniques for Recall-based Graphical Password

i) Recruitment email

Hello & Good day,

My name is Haryani and I am PhD student at School of Computing Science. As part of my research work, I am planning to conduct a study to evaluate how user friendly my visual password system is. Therefore, I need some people to participate in the study (no knowledge of computer security nor visual password system is required).

The study takes approximately 30 minutes and should be fun to do. I will be able to compensate you with £10 for willingly to participate in the study.

The details of the study are as follows:

Date: 24th / 25th / 27th / 31st January and 1st /2nd February 2011
Time: 9am – 330pm
Venue: Room 808 Claremont Tower Building

If you are interested, please send me an email (n.h.zakaria@ncl.ac.uk) and I will arrange a slot for you.

Many thanks

N. Haryani Zakaria
Room 10.04 Claremont Tower
School of Computing Science
Newcastle University

Official Personal Website: http://www.cs.ncl.ac.uk/people/n.h.zakaria

ii) Consent form

SCHOOL OF COMPUTING SCIENCE
NEWCASTLE UNIVERSITY

Participant Consent Form

Name of Experiment:
USABILITY STUDY OF DISAPPEARING STROKE & LINE SNAKE TECHNIQUES FOR DRAW-A-SECRET (DAS) SCHEME

Purpose:
The purpose of this study is to evaluate the usability of **disappearing stroke** and **line snake techniques** for Draw-A-Secret (DAS) scheme.

Procedure:
1. You will be introduced to **DAS scheme**, **disappearing stroke** and **line snake techniques**.
2. Then you will be trained to use the prototype system.
3. You will be asked to login using the passwords used in your training phase for the three techniques (DAS scheme, disappearing stroke and line snake).
4. Some related questions will be asked at the end of the session.

The total time required to complete the study should be approximately 30 minutes.

Benefits/Risks to Participant:
Participants will learn more about DAS scheme and techniques relevant to it. No risks anticipated for this study.

Voluntary Nature of the Study/Confidentiality:
Your participation in this study is entirely voluntary and you may refuse to complete the study at any point during the experiment, or refuse to answer any questions with which you are uncomfortable. You may also stop at any time and ask the researcher any questions you may have. Your name will never be connected to your results or to your responses on the questionnaires; instead, a number will be used for identification purposes. Information that would make it possible to identify you or any other participant will never be included in any sort of report. The data will be accessible only to those working on the project.

Contacts and Questions:
At this time you may ask any questions you may have regarding this study. If you have questions later, you may contact the person conducting the study, Haryani Zakaria via email at n.h.zakaria@ncl.ac.uk. Questions or concerns about institutional approval should be directed to Ms Jo Mayne, Deputy Head of Administration at the Faculty of Science, Agricultural & Engineering, Newcastle University via email joanne.mayne@ncl.ac.uk or call her at 0191 222 5923.

Statement of Consent:
I have read the above information. I have asked any questions I had regarding the experimental procedure and they have been answered to my satisfaction. I consent to participate in this study.

Name of Participant_____Date: _____

Signature of Participant _____ Age: _____

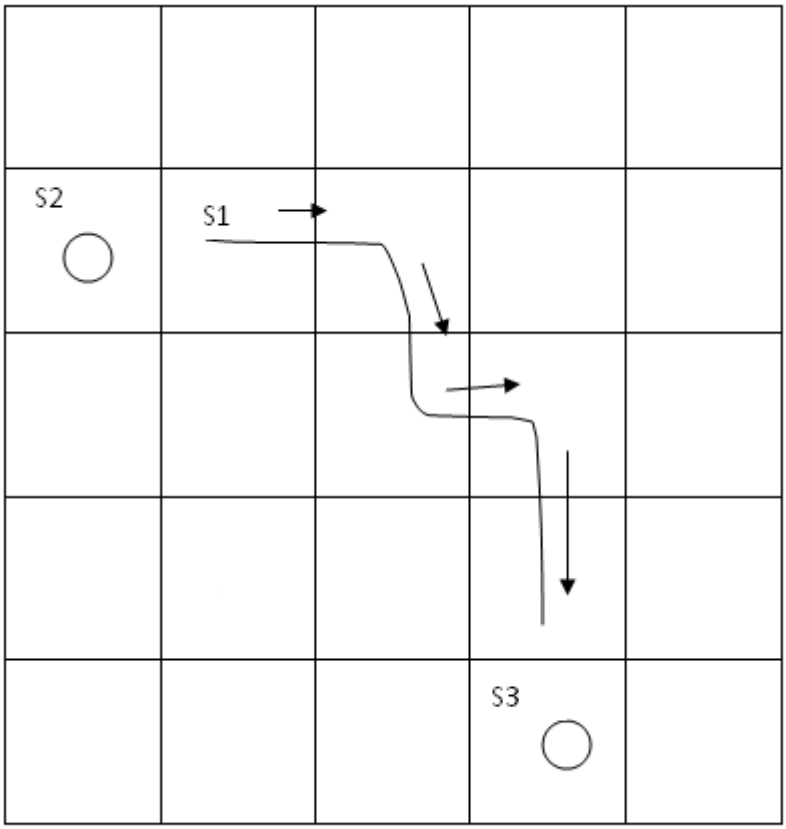
(**Note: You must be 18 years of age or older to participate in this study. Let the experimenter know if you are under 18 years old**.)

Thanks for your participation!

iii) **Example of graphical passwords used during the training session**

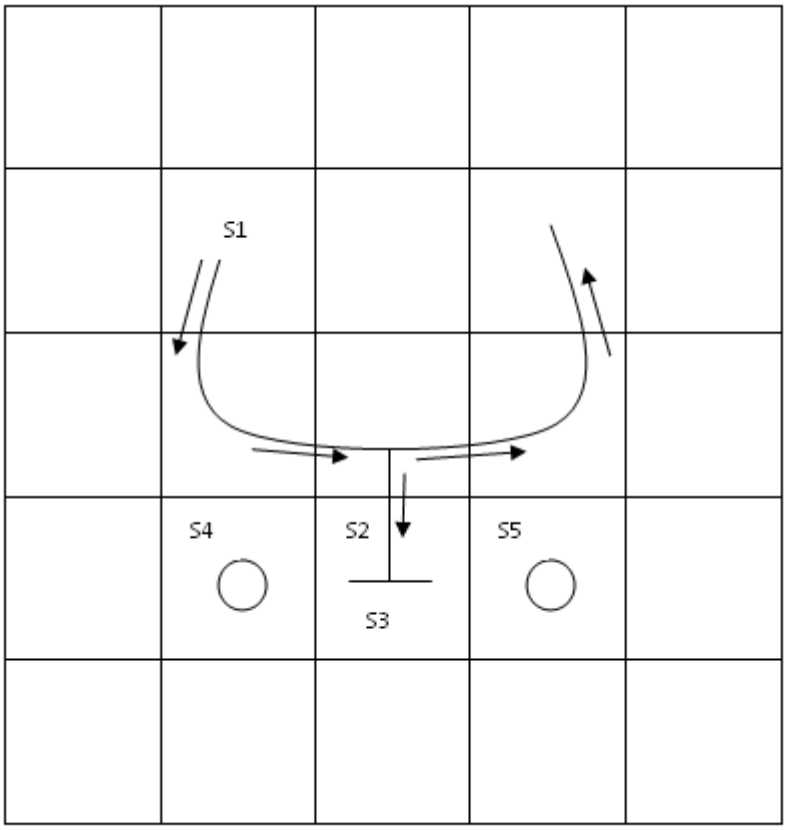
USERNAME: test1

GRAPHICAL PASSWORD NO. (1):



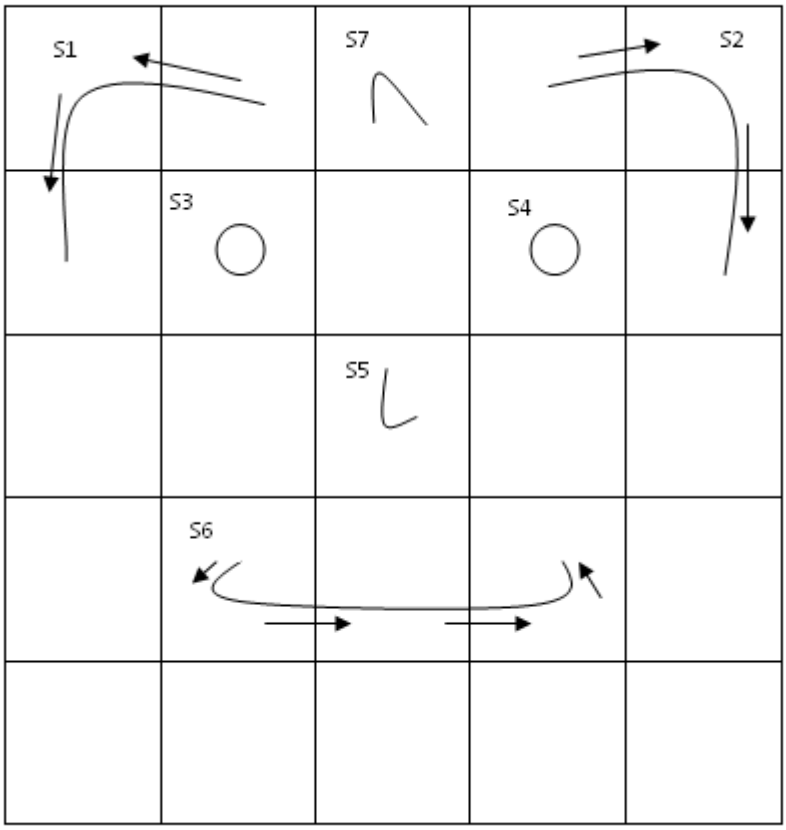
USERNAME: test2

GRAPHICAL PASSWORD NO. (2):



USERNAME: test3

GRAPHICAL PASSWORD NO. (3):



iv) **Questionnaires given to participants**

Categories		**DAS Scheme (undefended)**	**Disappearing Stroke**	**Line Snake**
Ease of use	**Very Easy**			
	Easy			
	Moderate			
	Difficult			
	Very Difficult			
Complexity	**Very Simple**			
	Simple			
	Moderate			
	Complex			
	Very Complex			
Confidence	**Very Low**			
	Low			
	Moderate			
	High			
	Very High			
Adoptability	**Very likely Yes**			
	Likely Yes			
	Not sure			
	Likely No			
	Very likely No			
Preference (rank them based on which you preferred most)				

Additional comments (option):

_____
_____
_____
_____