Samu Turunen

# USER EXPERIENCE AND THE SECURITY OF GRAPHICAL PASSWORDS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
28.5.2015

# TIIVISTELMÄ

Turunen, Samu
User Experience and the security of graphical passwords
Jyväskylä: Jyväskylän yliopisto, 2015, 32 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Woods, Naomi

Graafiset salasanat ovat lupaava vaihtoehto alfanumeeriselle autentikaatiolle. Älypuhelinten ja muiden korkea resoluutioisten kosketusnäytöllisten laitteiden määrä on kasvussa ja alfanumeeriset salasanat ovat kehitetty alun perin näppäimistölle syötettäviksi. Tarkkuutta vaativa kirjoittaminen ei tällöin ole välttämättä käyttäjälle kaikkein mielekkäintä. Graafisia ja alfanumeerisia salasanoja on tutkittu muistin toiminnan sekä käytettävyyden näkökulmasta. Tutkielma on tehty kirjallisuuden pohjalta käyttäen apuna erilaisia tieteellisia julkaisuja sisältäviä tietokantoja, kuten IEE Explore ja ACM Digital Library -tietokantoja.

Tutkielman tarkoituksena oli kuvata ja tutkia tieteellisten artikkeleiden avulla alfanumeeristen ja graafisten salasanojen muistamista sekä käytettävyyttä, sekä löytää hyviä ja huonoja puolia salasanojen käyttäjille. Tutkimuksessa havaittiin, että graafisten salasanojen muistaminen on yleensä helpompaa kuin alfanumeeristen salasanojen. Kuitenkin käyttäjän oma sisäinen motivaatio on useimmin esteenä kunnolliselle salasanan käytölle.

Asiasanat: graafinen salasana, alfanumeerinen salasana, tietoturvallisuus, käytettävyys, käyttäjäkokemus, muisti

# ABSTRACT

Turunen, Samu
User experience and the security of graphical passwords
Jyväskylä: University of Jyväskylä, 2015, 32 p.
Information Systems, Bachelor's Thesis
Supervisor: Woods, Naomi

Graphical passwords are a promising substitute to alphanumeric authentication. While the amount of high resolution touchscreen hand held devices is rising, the alphanumeric password was originally developed for a keyboard. Authentication process demands great precision and it may not be the most convenient way for the user. In this thesis, alphanumerical and graphical passwords are discussed in terms of memorability and convenience and how does convenience effect with memorability. Thesis is based on a literature review conducted trough academic article databases such as IEEE Explore and ACM Digital Library.

Among the principle findings of this research is that graphical authentication is more easy to remember than alphanumeric authentication. However, the suprising finding was how much the convenience of the authentication scheme effects the motivation of using a decent password.

Keywords: graphical passwords, alphanumerical passwords information security, convenience, user experience, memory

## FIGURES

Figure 1 Human memory: a proposed system by Atkinson & Shiffinr (1968, p. 113).12

**SISÄLLYS**

TIIVISTELMÄ
ABSTRACT
FIGURES

1 INTRODUCTION6

2 USER SATISFACTION AND SECURITY8

3 ALPHANUMERICAL PASSWORDS10
3.1 Memory11
3.2 Usability and convenience15

4 GRAPHICAL PASSWORDS17
4.1 Memory18
4.2 Usability and convenience20

5 ALPHANUMERICAL VERSUS GRAPHICAL PASSWORD23

6 SUMMARY & CONCLUSION27

REFERENCES29

# 1 INTRODUCTION

People use different kinds of sensitive services which need authentication every day. Sensitive services can vary from personal online banking to corporate databases ([1]Chiasson, Van Oorschot & Biddle, 2006); Chiasson et al., 2006; Renaud et al., 2013; Vu, 2007). Authentication is needed to ensure privacy and that the user has the right to access the database or service. While the number of online services increase, so does the need for authentication. Hence, users have to use more and more passwords in everyday life. With a large number set of different passwords to remember, this causes the user's memory to have a heavy burden (Chiasson et al. 2006). Traditionally, passwords have been alphanumeric passwords, that include characters, special characters and numbers, e.g. "psad"#!cS2".(Suo et al., 2005.) To and to avoid unauthorized access, security policies impose strength (combination of letters, numbers and special characters) and advise that every password should be unique. However, this burdens the user's memory even more, because remembering random passwords is rather difficult for most users, even though there are mnemonic-tactics to ease the burden. (Nelson & Vu, 2010; Vu, 2007.) Therefore, to ease this burden, there has been an increase in the development of graphical passwords in the past few year.

This thesis focuses on the user experience and convenience of graphical passwords and how the user satisfaction correlates with memorability. Does the user remember his or her password if the level of convenience is higher? Previous studies of graphical passwords have covered the usability and memorability. In 1968, Paivio et al. published a paper in which they described how pictures are easier to remember and recall than word - picture superiority effect. In 2007, Chiasson et. al. suggested that graphical passwords reduce the memory burden on users and therefore graphical passwords would decrease the use of unsafe practices, adopted in order to cope with the difficulties of recalling passwords. In addition,

graphical passwords could lead to larger password spaces (Chiasson, 2007). Their research suggested that the password space with graphical passwords is larger than with traditional alphanumeric passwords, which is important because the larger the password space is, the bigger is the number of possible passwords.

This thesis will first look at the theory of remembering and convenience alphanumeric and graphical passwords, then it will examine and compare the differences of alphanumeric and graphical passwords. After the comparison, the results for the research questions: "How does the user experience effect on the security of graphical passwords?" and "How does the aspect of convenience effect with the memorability and hence the security of passwords?" will be discussed in the discussion.

.

# 2 USER SATISFACTION AND SECURITY

In 2013, Almuairfi et al. divided passwords in three different categories: what does the user know, what does the user have and what the user-comprises. User's knowledge refers to alphanumeric passwords. What the user is, or comprises of, refers to biometrical attributes like fingerprints and iris-scanning. And what the user has is based on devices, e.g. key-tokens and keys. None of these authentication schemes are perfect nor without their problems. (Almuairfi, 2013).
In the year 2000, Chiasson et. al., suggested some of the ways in which the lack of the user satisfaction and acceptance can affect a lack of security. Schaub et al. (2013) also suggested that 50% of smartphone users do not use password or passphrase to prevent unauthorised use on their mobile phone, as users felt the security measures too burdensome. In 2011, Mihajlov and Jerman-Blažič suggested that when the authentication becomes and increasingly burdens, the users will attempt to avoid it.

Many studies have shown that users have a problem with remembering long, complex random passwords. (Chiasson et al., 2009; Nelson & Vu, 2010; Wiedenbeck et al., 2005.) This is due the limitations of long term memory (LTM), and the recall of irregular passwords is more difficult, than say, using real words which are found in dictionary (Wiedenbeck et al., 2005). Hence, as the complexity of remembering passwords rise, the user satisfaction falls which can lead to a lack of security. For example, Stobert and Biddle (2013) demonstrated that to ease their memory burden, users tended to write down their passwords in plain text which compromised security.

Ultimately, the usability of authentication affects the user satisfaction (De Angeli et al., 2005; Sasse et al., 2001**)**. Lack of user satisfaction may lead to compromised security if users neglect password policies by, e.g. writing down their passwords. To ease the memory burden of multiple, complex

passwords, researchers have introduced several alternative authentication methods e.g. graphical passwords. (Blonder, 1996; Chiasson et al., 2007; Wiedenbeck et al., 2005).

# 3 ALPHANUMERICAL PASSWORDS

Alphanumerical password are the most common authentication mechanism (Hafiz et al., 2008; Renaud et al., 2013). These passwords consists from normal letters (capitals and lowercase), special characters and numbers. By combining these elements together, an alphanumerical password can be made. When creating passwords, the service includes password policies that impose a set of rules that direct the user to include certain amounts of alphanumerical characters and symbols.
In this chapter, alphanumerical passwords will be discussed, first, in terms of memory, then second, in terms of usability and convenience

## 3.1 Memory

The creation of a password is a complicated matter. This section reviews several factors known to influence the human memory and their implications for password memorability and recall. (Brown et al., 2004.)

The amount of different passwords is presented by the RSA's (2005) in a survey. It reported that over 25% of users manage more than 13 work-related passwords. Adams & Sasse (1999) suggested that creating a unique and strong password is a burdening process that increases the cognitive load, which does not ease the situation of users.

Referring to Atkinson and Shiffrin's model (1968), it described the basic architecture of memory system (Figure 1). This model is used to attain better understanding about how human memory operates. These researchers suggested that there are three different types of memory storages: sensory stores, short-term store (STM) and long-term store (LTM). Sensory stores holds information from external inputs, e.g. visual stimulation. The information is stored for a very short period of time, which it is then lost or disseminated to the short-term store. The information is processed in the short term store, which has limited capacity, before being disseminated to long time store, The LTM has unlimited capacity and information can be recalled after a considerable long periods of time. (Atkinson & Shiffrin, 1968).
The SMT-model describes the learning and recall processes of passwords. The difficulties with learning can be described with SMT-model: after the passwords has been passed from sensory store to the STM, the memory item should be processed to be passed to LTM. If the memory item is not processed enough or at all, it will not be encoded and enteedr the LTM. Hence, it can not be recalled. (Atkinson & Shiffrin, 1968.) When passwords are created, they are received by sensory store and processed, learned and encoded in STM. While the creator of password processes the new memory item, it will be encoded and sent to LTM. (Atksinson &, Shiffrin, 1968; Brown et al., 2004).

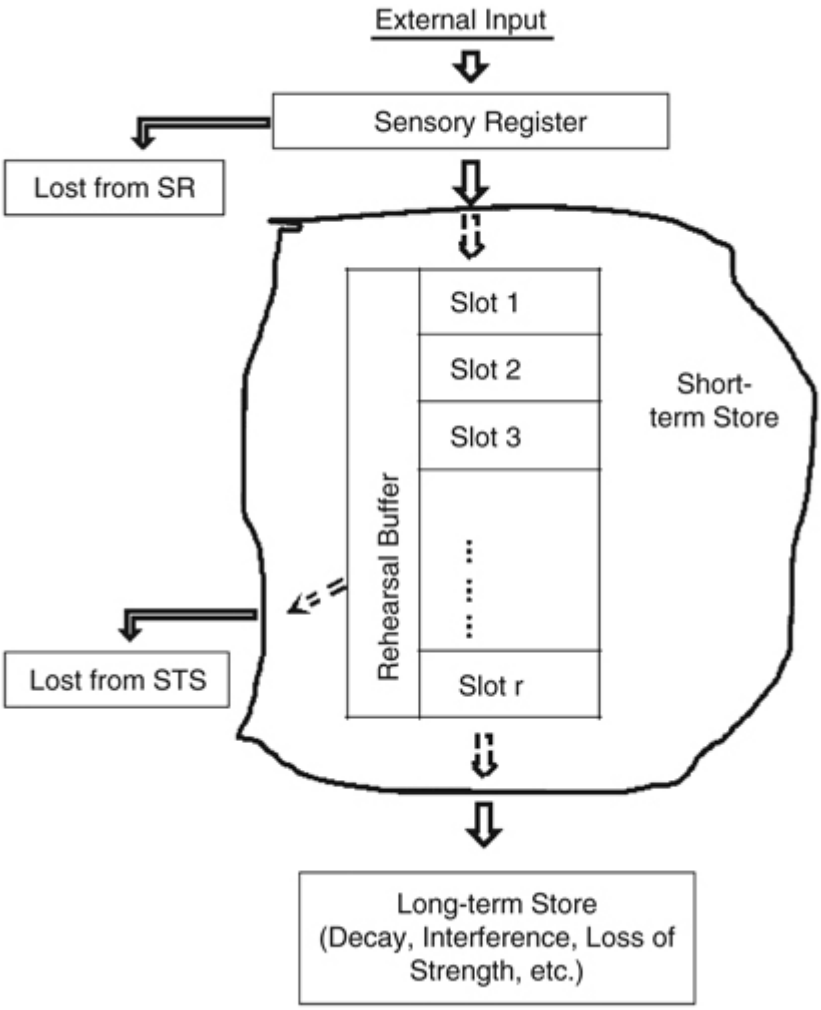


Figure 1 Human memory: a proposed system by Atkinson & Shiffrin (1968, p. 113).

One memory phenomenon is the Generation Effect: it proposes that information created within one's own mind is more memorable then if it is just presented to ourselves. In termes of passwords, users remember passwords they create from their own mind than computer-generated ones. (Sasse et al., 1999; Slamecka & Graf, 1978). ~~Sasse et. al. (1999)~~ Ergo, users tend not to write down their passwords as often, when the user has created them, compared with system-generated passwords.

Brown et al. (2004) suggests that the creation of a password is often made in hurry and with no meaning and no opportunity for rehearsal, which may lead to a poor recall rate. Due the lack of rehearsal, the memory trace may not reach long-term memory and the recall will become impossible. Short-term memory is able to store information for about 15-30 seconds. The longer the information stays in short-term memory, the possibility that the information will enter the long-term memory, which leads to better recall rate. (Atkinson & Shiffrin, 1968; Zhang et al., 2009.)

Another memory phenomenon is memory interference. Interference describes a situation where one memory item disturbs recalling another memory item (Underwood & Postman, 1960). Similar information increases the interference effect. Retroactive interference is high if a new learned item, e.g. a new name, disrupts and earlier learnt item. (Underwood & Postman, 1960.) Proactive interference is high when two different memories comes from same stimulus and it is low when stimulus are not alike. In 2009, Zhang et al. showed that a new password for known service is difficult to recall. These researchers pointed out that the memory trace of older password interferences recalling current item, and this illustrates proactive interference. Vu et al. (2007) suggests that every new memory item associated with the same service leads to increased proactive interference. Hence, with an increasing amount of passwords to remember, effects the recall of passwords: "As memory load increases, the number of forgotten items increases (Neath, 1998; Vu et al., 2007).

The memorability of passwords can also be improved: firstly Vu, 2007; Craik and Lockhart, 1972; Jacoby and Craik, 1979, showed in their research that increased depth of processing increases password recall. According to these researchers this is caused due to the amount of connections between memory items, which has the possibility to create more retrieval paths for recalling.
Second way to improve the recall rate of password is mnemonics. By this technique the user can encode items better to increase memorability (Vu et al. 2007; Neath, 1998.), by making an organizational scheme. Because of the depth of processing, mnemonics work as they improve the connection of items for when they are needed to be recalled (Vu et al., 2007). For example "m,1aNib7 becomes 'Me, I am NOT impressed by SevenofNine')", these random characters have meaning, but only for the user (Sasse et al., 2001). This mnemonic technique is more effective when user is allowed to provide their own, because of the generation effect (Atkinson & Raugh, 1975). Furthermore, Sasse et al., 2001 and Hasket, 1984 suggested that these mnemonics work well with heavily used passwords. Another type of mnemonics is presented by Horcher (2009), who suggested that a passphrase, which consists from abbreviation of a sentence and would be meaningful only for the author, would help to preserve the security. While the user has to process an abbreviation in working memory, the probability of the item entering the LMT rises. Hence the recall rate is better. (Atkinson & Shiffrin, 1968; Horcher, 2009)._Another technique to improve recall rate is chunking (Nelson & Vu, 2010 ; Vu et al. 2007). By chunking this thesis refers to technique in which user forms a string, e.g. IMSTILLYOUNGANDALIVE, with 20 letters, which "compresses" information into more manageable form. Hence the summary is needed to

remember, not the whole passage. This could help users to remember long, unique passwords. (Ausubel, 1960; Nelson & Vu, 2010.)
Thirdly the frequency of using the password effects the recalling process: using the password regularly helps the long term memory to store the password more easily and more securely. If passwords are not used often they are subject to decay, as the passwords fades away from the long term memory. (Wiedenbeck et al. 2005.)

The Atkinson's and Shiffrin's (1968) SMT-model describes well the learning and recall processes with alphanumeric strings. Problems with interference and the limited space of STM are limiting factors for encoding the memory item for the LTM. The amount of processing in STM, e.g. creation of password or mnemonics, effects on the memorability by increasing the probability of memory item entering the LTM.

## 3.2 Usability and convenience

The user is often faced with a dilemma when trying to secure their passwords (Brown et al., 2004). Firstly, they have to consider the capability of their memory, when creating a secure yet memorable password, and their ability to remember password (Zhang et al. 2009). Secondly, they have to weigh up, what is convenient, in term of time and mental effort it takes to create, learn and recall passwords (Grawemeyer & Johnson, 2011). Darren et al., (2004) found that authentication only slows the users down, and their motivations lie with, for example, getting their work done as fast as possible. They suggested that this may lead users to become at risk of damaging their companies or their own digital goods (Monrose & Reiter, 2004). Another study (Brown et al., 2004) showed that two thirds of passwords are guessable from one's personality, attributes or relatives or other close people.
Brown et al. (2004) said "So we are faced with a continuing dilemma in personal password construction between security and convenience: fool the password hacker and you are likely to fool yourself."

In 2001, Horowitz estimated that 20% of users had a note on their monitor with their password written on it, to ease the burden of recall.

Writing passwords down is considered an insecure password behavior that violates security policies. Many security policies across different services do not ease memory burden of creating and recalling passwords. Some policies forces the user to have special characters and numbers and other services do not accept special characters (Vu et al. 2007). For example, in the University of Massachusetts, security policy requires a password with a certain amount of numbers, letters and other symbols (Shay et al., 2007). From the users' perspective enforcing the creation of strong passwords via complicated rules or guidance does not ease the burden of learning a new password (Chiasson et al. 2006).Therefore, as the amount of services grows, users tend to not make new login credentials but reuse the same, already familiar credentials to cope with their memory burden (Gaw & Felten, 2006). In the situation where the user is forced to change their password, the user's frustration can multiply. The distraction from current goals, e.g. work or leisure, and the criteria of password policies can reduce the satisfaction and motivation to create and learn a password. (Marquadson, 2012).
Adams & Sasse (1999) argued that users are able to remember only five unrelated passwords. Ergo, to cope, users tend to write down or reuse their passwords rather than trying to remember them, further ignoring security policies. Even though, the difference of policies can have a differentiating effect, which helps the user to differentiate one service from

another and lower the interference; Zhang et al. (2009) proposed that the interference (retro- and proactive) from different passwords is a major challenge to recall multiple-password. To cope, users use account-related passwords. In 2009 Chiasson et al. showed that 40% of text passwords were clearly associated with the name of the account. They wrote also that several studies have shown that users tend to have easy-to-guess alphanumeric passwords for multiple accounts. In 2006, Gaw and Felten accounted a research and suggested that users tend to reuse their passwords, pointing out that while the number of different services rises, the risk of password reuse grows cumulatively. This leads to a large risk, compromising the security of the accounts, because the same login credentials are often in different services. (Gaw & Felten, 2006.)

The memorability of alphanumerical passwords have a clear effect on the usability and use and complexity of alphanumerical passwords. The effort used in creation of a unique strong password does correlate the memorability; the more mental effort used in learning-phase, the better the memory item is encoded in LTM. The users do have problems with strong, unique alphanumeric passwords but they have developed security compromising coping strategies e.g. writing down and reuse.
Having defined what is meant by memorability, usability and convenience in terms of alphanumerical passwords, I will now move on to discuss these topics in therms of graphical passwords.

# 4 GRAPHICAL PASSWORDS

Chiasson et al., in 2009, summed up the function of graphical passwords: "graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope."

It is necessary to clarify exactly what is meant by graphical password. De Angeli et al. (2005) uses the term 'graphical authentication' to refer to the idea of replacing the recall of alphanumerical password by recognition of pictures. Furthermore, De Angeli et. al. (2005) divided graphical authentication to three subcategories: Cognometrics, Locimetrics and Drawmetrics. The Cognometric term is defined by Real User Corporation (2004) as the measurement of innate cognitive abilities of the human brain, e.g. face recognition. With locimetric systems the identification mechanisms requires a unique image with a target point to identificate. Drawmetric systems lies between biometric and graphical mechanisms for they require the user to redrawn pre-drawn the outline of a drawing (De Angeli et al., 2005).

In this chapter, graphical passwords will be discussed in terms of memory, usability, convenience and how convenience effects recall.

## 4.1 Memory

To recall a memory item, the information must be first, learnt. The Atkison and Shiffrin (1968) memory theory: Stages of Memory Theory (SMT), referred earlier in this literature review, has been used by many researchers to gain greater understanding and demonstrate the learning and recall process of pictures, and hence graphical authentication.

Based on De Angeli et al. (2005) categorization of graphical passwords, Stobert and Biddle (2013) categorized graphical passwords in terms of the recall process: free recall-based (drawmetric), cued recall-based (locimetric) and recognition-based (cognometric) graphical passwords.

To clarify further the terms "recall" and "recognition" are used solely to mean as Hollingworth (1913) referred: recalling and recognition are processes where information is retrieved from memory. When the context is provided, the specific focus generates the phenomena of recall. Recognition occurs when the process of remembering the contextual information while the focus is provided. The process of recall is generally divided to cued recall and free recall. In cued recall, the subject is afforded with a cue which provides assistance in retrieval of the correct memory item. In free recall, the subject has no cues to aid remembering.

Many researches have found that recognition is almost always superior to recall and several theories attempt to explain this difference (Hollingworth, 1913).

Anderson and Bower (1972) proposed the generate-recognize theory. After the user has learnt an item, the information is in long-term memory and the user attempts to recall or recognize the learnt item. In this theory, there are two phases to retrieve the memory of a word: firstly, in the generate phase, the search is located in long term memory and a list of candidate words is formed. In the second phase (recognize phase), the words of the list is evaluated to see if the desired word is located in the list. Because the recognition does not need the first phase, the amount of time and effort is less needed. The benefits of cued-recall (locimetric) can also be explained with generate-recognize theory: a cue helps to create the candidate list and aid to recognize the needed word from the list. (Stobert & Biddle, 2013).

Another theory of memory retrieval is presented by Tulving and Thompson (1973). The encoding specificity theory explains that he processed information, at the time of storage, can be used as cues. Hence,

if semantic information is processed at the same time as learning, then the same semantic information can be used as retrieval cue if the subject encodes the semantic linking between these items during the learning process. (Stobert & Biddle, 2013).

A major difference between generate-recognize and encoding specificity theories is that generate-recognize theory is far more complex because it is two-phased. Since recall has generation and decision phases, the recognition is more simple in that it only require the decision. Unlike in the generate-recognize theory, the encoding specificity theory suggests the retrieval of a memory item is an automated and simple process and in which the complexity emerges only in the process of encoding (Stobert & Biddle, 2013).
For users, images (and therefore graphical passwords) tend to be easier to remember. One explanation for this is provided by, Paivio et. al (1968) who argued in dual coding theory that the brain has separate ways to remember visual and verbal information; the processed images are encoded visually and furthermore, they are translated also in verbal form. By these researchers, the picture superiority effect occurs when users remember images. The researchers argued that the effect occurs because images are dual processed: images are not only encoded visually, they are also processed and translated to a verbal format and hence remembered semantically. (Paivio et al., 1968). The user's cognitive capabilities do not affect this phenomenon (Bower et al., 1975).

The pictory superiority effect of Paivio et al. (1968) has a huge impact in the Atkinsons and Shiffrins STM-theory by suggesting that pictures are double encoded when moved to LTM. In next, graphical passwords are discussed in terms of practice.

## 4.2 Usability and convenience

This review focuses on three common approaches to authenticate with graphical passwords: the recognition-based and recall-based authentication.

In practice, the recall-based authentication is based on authentication, by selecting different pre-selected locations on a picture. By this way, the sequence of selected points on an image is the password. (Blonder, 1996). PassPoints is another authentication recall-based scheme suggested by Wiedenbeck et. al., (2005b). This is where the users can click any location of the picture. In PassPoints, the clicks are not meant to be pixel-perfect since the system has invisible tolerance squares around the selected point. Invisible tolerance squares are the pre-appointed area around the selected point, which is treated like the selected point. This eases the authentication. (Wiedenbeck et al. 2005b).

One issue with these click-based authentication schemes is that users tend to select same locations and hence creating guessable hot-spots (Dirik et al., 2007; Thorpe and Van Oorschot, 2007). Chiasson et al. (2009) showed that in this cued-recall (locimetric) graphical authenticationm users will often use geometric and symmetrical patterns, which also reduces the level of security. To eschew these easy guessable passwords, some schemes guides users to select better passwords during the password creating stage, by highlighting a random area of the image where the user is obligated to select the clicking point. This technique prevents users from reusing passwords and using symmetric pattern. (Chiasson et al., 2009.) While using recall-based (locimetric) schemas, clickable graphical password, the invisible tolerance squares play a major role. The tolerance is important to set carefully, because high tolerances might lead to many false positives, and therefore the system may be more vulnerable. Too low tolerance might lead to large number of false negatives, which may lead to compromised user satisfaction and therefore neglected security policy. (Suo et al., 2009.) Davis et al. (2004) showed that the size of tolerance square impacts the memorability of password. For example, 10x10 sized tolerance square in PassPoint-schema forces user to remember the details of the password point carefully. They pointed out that this detailed memory might decay over time without regular use, let alone at the situation when the user has multiple different graphical passwords which may cause interference. (Davis et al., 2004.)

A free recall-based (drawmetric) authentication scheme is suggested by Jermyn et al. (1999), where the user draws a free form on a grid. This Draw-A-Secret (DAS) authentication improves memorability when users are allowed to create their own passwords. Unfortunately, users tend to draw symmetric forms, which decreases the potential, vast password space. While the password space is decreased, the amount of

unique passwords falls which leads to reduced security. (Thorpe & Van Oorschot, 2004)

The recognition-based (cognometric) authentication is based on the sequence of images that are preselected by the user. The user recognizes pictures from given series which includes distraction pictures, for example PassFaces has one pre-selected picture and several distraction pictures. (Mihajlov, Jerman-Blažič, 2011; Real User Corporation, 2004). The leverage of recognition is used by displaying every possible choice to the user, and the user has to recognize the correct candidate (Stobert & Biddle, 2013). Davis et al. (2004) shows that the user's choice is highly affected by the attractiveness of the faces and the race and gender. This makes the PassFaces passwords more guessable (Hafiz et al., 2008).

Mihajlov and Jerman-Blažič (2013) argued that usable graphical passwords generally have smaller password space compared to alphanumeric passwords, which means that there is less unique combinations of graphical passwords than alphanumeric passwords. Stobert et al. (2010) suggested that by forcing the users to have longer passwords and hence enhance the password space, it would affect the memorability and the usability of the system. On the orher hand, Stober et al. (2010) found that the theoretical password space for graphical passwords, with is less clickable points, is approximately the same password space than longer alphanumeric passwords. The effective password space refers to the set of passwords that users tend to create and use (Stober et al., 2010).

The Persuasive Cued Click-Points (PCCP) (Chiasson et al., 2008.) is a promising alternative graphical authentication method, in where user selects different clickable points from given area of the picture. It is suggested to reduce the hotspots and patterns; the effective password space increases near to the theoretical password space. (Chiasson et al., 2008.) If the theoretical password space of PCCP is matched to that of alphanumeric passwords, the effective password space of this graphical password schema is at least larger than the space of alphanumeric passwords. (Stober et al. 2010.)

From the user's perspective, the problem of interference does not vanish while using graphical password when compared with alphanumeric password. Wiedenbeck et al. (2005) hypothesized that if the user is forced to authenticate with one image and two or more sets of password points for two or more different systems, the situation would likely generate interference. These researchers argued that the interference would emerge from the difficulty to link the right set of password points with the right service. Also, the picture in itself could arouse interference by content, e.g.

if the picture's similar objects confuse the user to select wrong object for the certain service. To avoid this, using different image for different password might reduce the interference. The variety of images increase the amount of images to remember, which may lead problems to connect the right image with the right system (Wiedenbeck et al. 2005). The choice of image has also an influence on the success rate of authentication by graphical passwords (Chiasson et al., 2007).

Authentication with graphical passwords is suggested to be less burdening process than authentication with alphanumerical passwords due the retrieval and recognition processes are faster and lighter than with alphanumerical passwords. The for human memory, remembering pictures is natural and this phenomena is exploited by a vast set of different kind of graphical authentication methods.
Graphical passwords are a promising technology in the field of authentication but not problem free. The advantages and problems with graphical passwords are discussed in the next section, where graphical passwords are compared with alphanumerical passwords.

# 5 ALPHANUMERICAL VERSUS GRAPHICAL PASSWORD

The advantages and weaknesses of alphanumerical and graphical passwords are discussed in this section. How does the recall-process differ in alphanumerical authentication from graphical authentication and how does their convenience effect on security. This is really important issue as users are more concerned about remembering their passwords than securing the information within the used service. Hence, users tend to adopt poor password behaviors such as writing passwords down and, reusing or using slightly changed passwords to cope with multiple passwords and remembering them. (Grawemeyer & Johnson, 2011.)

Alphanumerical passwords have a clear advantage to graphical passwords, as they have been around for over 30 years, and users are familiar with them. (Hafiz et al., 2009; Morris & Thompson, 1979; Renaud et al., 2013). Hence, with graphical passwords are facing the problems of new technology: users are forced to learn a new authentication schema. E.g. users do have developed a behaviour to help them to remember alphanumeric passwords. ([2]Chiasson et al., 2009.) Even though, the elaborate techniques, such as the passphrases and mnemonics, can increase the security and memorability of alphanumeric passwords, passphrases often result in login failures; although they also suggest that these errors reduce over time (Keith et al., 2007).

Wiedenbeck et al. (2005) argued that creating a PassPoints -graphical password was fast and easy, and the recall over weeks was as successful as alphanumeric passwords. On the other hand, Suo et al. (2005) conducted a survey where a major complaint from the users was that the registration and login processes were too slow. This issue was strong in recognition-based (cognometric) authentication, where the user had to select images from large selection. During the login-phase, users are

forced to scan through a large set of images to recognize the right pictures, which users may find time-consuming and a frustrating process. This process may lead to a lack of satisfaction in-convenient (Renaud et al., 2009; Suo et al., 2005). This lack of user satisfaction may cause problems, because it can lead to neglecting security policies and hence result in compromised security (Suo et al., 2005).

However, the login time should be compared to the time and effort of resetting the password. If the graphical password needs much less often resetting due the better memorability, longer login time might be acceptable. The benefits compared with the issues of time consuming and convenience might be worth the effort (Renaud et al. 2009). Therefore, the decision of which authentication method, alphanumerical or graphical, is used should be considered carefully, examining the details of the situation and application, hence the systems are not isolated from the real world (Renaud et al. 2009). Wiedenbeck et al. (2005) suggested that with small screens, the creation and use of graphical passwords have problems, as the small screen constricts using the authentication schema. They argue that people with motor issues may not feel satisfaction while using graphical authentication, which uses clicking an accurate point, especially with small screens. Personal desktop computers and laptops do have a keyboard and mouse, which negates this authentication issue. Keyboards are convenient with typing alphanumeric passwords, and mobile devices traditionally do not have one, which, alongside smaller screens, limits variety of alphanumeric passwords. Hence, inconvenience with keyboard-based authentication schemes, governs favorability for graphical authentication with mobile devices. (Renaud et al. 2009.)

During the creation of a password, mnemonics can add meaning for password and hence improve the recall rate. Using images with mnemonics, had a higher recall rate than with alphanumerical passwords with mnemonics. (Nelson & Vu, 2010). However, Keith et al. (2007) investigated that passphrases resulted more often to login failure due typographical errors than plain text passwords, but also suggested that these errors reduce over time.

In the terms of memory load of alphanumerical and graphical passwords, Stobert and Biddle (2009) reported that with recall based graphical passwords, users wrote their passwords down to cope with the burden of recalling the password more often than with recognition based schemas. This problem lies also with alphanumeric passwords, as Stobert and Biddle (2013) suggested in other studies that users write their alphanumeric passwords down to ease the burden.

For users, changing a password is annoying. Creating and learning a new password increases the cognitive load for the user. Users' goals are rarely focused on creating passwords, hence they tend to reuse old passwords, to avoid learning a unique and new passwords. (Grawemeyer & Johnson,

2001.) Remembering a large set of different, unique passwords is difficult in both authentication schemas (Chiasson et al., 2007; Davis et al., 2004; Gaw & Felten, 2006). Changing a password may cause interference, especially if the user is forced to remember a large set of passwords (Vu et al., 2007.)

Interference occurs in both authentication schemes, and can decrease security, hence while going through their mental password list and trying every password they remember e.g. the risk of recording the password increases (Chiasson et al. 2006). Inference in graphical passwords may happen when the same image is used for two different graphical passwords, e.g. when using same picture for two or more sets of PassPoints Another problem with interference is if the content of two different images are too similar; similar objects might confuse the user to select wrong password for right service (Wiedenbeck et al. 2005). Interference with alphanumerical and graphical passwords emerges when old or new password (retro- or proactive interference) confuses the user (Underwood & Postman, 1960; Zhang et al. 2009). For graphical passwords, interference can be avoided by selecting a different image to authenticate, if the images differ enough. Hence, the context of authentication may lead to less interference (Wiedenbeck et al., 2005). While with the alphanumerical passwords the login context may stay the same, (in the assumption that users use unique, non-account-related passwords) which may lead to interference with recalling the password (Hollingworth, 1913; Zhang et al., 2009).

As mentioned previously, the memorability and recall rate can be improved: firstly, increasing the depth of processing, which increases the recall rate in both authentication schemas (Vu, 2007: Craik and Lockhart, 1972; Jacoby and Craik, 1979).

The mnemonics can be used in graphical and alphanumeric passwords. Nelson and Vu (2010) suggests in their research that image-based mnemonic techniques were more successful than text-based mnemonics. For text-based mnemonics, the problem occurred when users had to remember which letter was lower- or uppercase and where in the password digits and special characters should be. (Nelson & Vu, 2010.) These researchers also point out that a lot of alphanumeric and graphical passwords were based on personal information, which can be a security problem. Yet, mnemonics do not expel the problem of remembering multiple passwords (interference). Matching right password to the right account is still a problem. (Zhang et al., 2009.) This section has analysed the advantages and drawbacks of alphanumerical and graphical passwords. The next part of this paper will discuss the results of the comparison.

# 6 SUMMARY & CONCLUSION

While the amount of hand held devices with high resolution touch screens are rising, the niche for graphical authentication improves. Also, with the amount of online and digital services rising, there is a need for safe, convenient and fast authentication (Brown et al., 2004). Many researches point out that alphanumeric passwords are not easy to recall, and hence users try to cope with the burden on their memory by e.g. writing passwords down in plain text (Brown et al., 2004; Hafiz et al., 2008; Renaud et al., 2013).

In this thesis the Atkinsons and Shiffrins (1968) Stages of Memory Theory was used to describe the functions of the human memory. Thise theory, alongside with The picture superiority effect (Paivio et al., 1968) described the basic advantage of graphical passwords, the dual coding and the issues of alphanumerical passwords.

Alphanumerical passwords have been in use for approximately 30 years. Users have developed several coping strategies to ease the burden of recalling passwords, e.g. reusing the password, mnemonics and password managers. Rehearsal and password training (processing the information in short term memory) have been successful to improve the recall rate of alphanumeric passwords by increasing the probability of information entering the long term memory. For users, to remember long, nonsense passwords is not easy; remembering strings of irrelevant, random characters, and burdens the users' memory, as creating more than one password increases the cognitive load.

With graphical passwords the recall and recognition rate seems to be higher. This is due the Picture Superiority effect (Paivio et al., 1968), by dual coding images and words, helps the memory item to move to LTM, and hence

the retrieving of graphical passwords is less burdening for the user. (Paivio et al., 1968; Stobert & Biddle, 2013.)

For users, the authentication only slows them down from distracting them from their main task, work or leisure. Hence, the authentication process should be fast and convenient. The LTM does not have capacity limits and hence, the limits of recalling or recognizin passwords is only limited by the users skills of retrieving the memory item. The recognition with graphical passwors was suggested to be faster than recalling (Anderson & Bower, 1972).

The convenience of graphical passwords are a significant factor, not only in remembering but in the motivation to use the password. It can therefore be assumed that the convenience has an effect to memorability, the more processing used in the creation of graphical password takes, the more likely the memory item will reach the LTM. The downside of graphical passwords lies on the convenience. (De Angeli et al., 2005; Stobert & Biddle, 2013) Users do have a 30 year history with alphanumerical passwords, and hence they have generated already mental models to create and remember alphanumeric passwords. Graphical passwords do have the burden of newcomer, and they need to be more effective and convenient than alphanumerical passwords to be a realistic substitute for alphanumeric passwords. The login time is in some schemas still too long, as well as at the creating phase. The clear advantage with recognition based graphical passwords is that the password is undemanding to remember. Another result in this literature review, is that if graphical password, or any authentication scheme, is not quick enough, the users do not use them.

Further research should be undertaken to investigate the convenience of motivation to use graphical passwords and how the login could be less time consuming and give more satisfaction for the user.

## REFERENCES


Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Mathematical and Computer Modelling, 58(1), 108-116.

Atkinson, R. C., & Raugh, M. R. (1975). An application of the mnemonic keyword method to the acquisition of a russian vocabulary. Journal of Experimental Psychology: Human Learning and Memory, 1(2), 126.

Atkinson, R. C., & Shiffrin, R. M. (1968). Human memory: A proposed system and its control processes. Psychology of Learning and Motivation, 2, 89-195.

Ausubel, D. P. (1960). The use of advance organizers in the learning and retention of meaningful verbal material. Journal of Educational Psychology, 51(5), 267.

Blonder, G. E. (1996). Graphical Password,

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641-651.

Chang, T., Tsai, C., & Lin, J. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems and Software, 85(5), 1157-1165.

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). Influencing users towards better passwords: Persuasive cued click-points. Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1, 121-130.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. Proceedings of the 16th ACM Conference on Computer and Communications Security, 500-511.

Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006). A usability study and critique of two password managers. Usenix Security, , 6

Chiasson, S., van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. Computer Security–ESORICS 2007 (pp. 359-374) Springer.

Craik, F. I., & Lockhart, R. S. (1972). Levels of processing: A framework for memory research. Journal of Verbal Learning and Verbal Behavior, 11(6), 671-684.

Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. USENIX Security Symposium, , 13 11-11.

De Angeli, A., Coventry, 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(1), 128-152.
Dirik, A. E., Memon, N., & Birget, J. (2007). Modeling user choice in the PassPoints graphical password scheme. Proceedings of the 3rd Symposium on Usable Privacy and Security, 20-28.
Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. Proceedings of the Second Symposium on Usable Privacy and Security, 44-55.
Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. Interacting with Computers, 23(3), 256-267. doi:http://dx.doi.org/10.1016/j.intcom.2011.03.007
Hafiz, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique. Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference On, 396-403.
Haskett, J. A. (1984). Pass-algorithms: A user validation scheme based on knowledge of secret algorithms. Communications of the ACM, 27(8), 777-781.
Hollingworth, H. L. (1913). Characteristic differences between recall and recognition. The American Journal of Psychology, , 532-544.
Horcher, A., & Tejay, G. P. (2009). Building a better password: The role of cognitive load in information security training. Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference On, 113-118.
Horowitz, A. S. (2001). Top 10 security mistakes. Computerworld, 35(28), p38.
Jacoby, L. L., Craik, F. I., & Begg, I. (1979). Effects of decision difficulty on recognition and recall. Journal of Verbal Learning and Verbal Behavior, 18(5), 585-600.
Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. Usenix Security,
Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. International Journal of Human-Computer Studies, 65(1), 17-28.
Marquardson, J. (2012). Password policy effects on entropy and recall: Research in progress.
Mihajlov, M., & Jerman-Blažič, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interacting with Computers, 23(6), 582-593.
Neath, I. (1998). Human memory: An introduction to research, data, and theory. Thomson Brooks/Cole Publishing Co.
Nelson, D., & Vu, K. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. Computers in Human Behavior, 26(4), 705-715. doi:http://dx.doi.org/10.1016/j.chb.2010.01.007

Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words? Psychonomic Science, 11(4), 137-138.
Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords? Computer Science and Information Systems (FedCSIS), 2013 Federated Conference On, 837-844.
Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.
Shay, R., Bhargav-Spantzel, A., & Bertino, E. (2007). Password policy simulation and analysis. Proceedings of the 2007 ACM Workshop on Digital Identity Management, 1-10.
Slamecka, N. J., & Graf, P. (1978). The generation effect: Delineation of a phenomenon. Journal of Experimental Psychology: Human Learning and Memory, 4(6), 592.
Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. Proceedings of the Ninth Symposium on Usable Privacy and Security, 15.
Stobert, E., Forget, A., Chiasson, S., van Oorschot, P. C., & Biddle, R. (2010). Exploring usability effects of increasing security in click-based graphical passwords. Proceedings of the 26th Annual Computer Security Applications Conference, 79-88.
Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical passwords: A survey. Computer Security Applications Conference, 21st Annual, 10 pp.-472.
Thorpe, J., & van Oorschot, P. C. (2007). Human-seeded attacks and exploiting hot-spots in graphical passwords. USENIX Security, , 7
Tulving, E., & Thomson, D. M. (1973). Encoding specificity and retrieval processes in episodic memory. Psychological Review, 80(5), 352.
Vu, K. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies, 65(8), 744-757.
Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005a). Authentication using graphical passwords: Effects of tolerance and image choice. Proceedings of the 2005 Symposium on Usable Privacy and Security, 1-12.
Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005b). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1), 102-127.
Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. Proceedings of the Working Conference on Advanced Visual Interfaces, 177-184.