Lund University School of Economics and Management

Department of Informatics
October 2013

Authentication with Passwords and Passphrases

- *Implications on Usability and Security*

Authors: Dan Andersson
Dan Saedén

Course: INFC40 / Information Systems Security
Examiner: Anders Svensson

Abstract

This article aims to explore the implications on usability and security when using passwords and passphrases as an authentication method for information systems. The result shows that neither passwords nor passphrases offer a big enough benefit for one to be recommended in front of the other. Many factors affect usability and security and they tend be inversely related. Practitioners should aim to design security policies that are actually used rather than too strict policies that end up being circumvented by the users.

Table of Contents

1. Introduction

Passwords have been employed for user authentication since the invention of the first time-sharing systems in 1960 (Denning 1992). It is a simple and practical system, well understood by both users and administrators. But passwords have many documented problems, and better forms of authentication are available (Orman 2013). Despite this, passwords remain the dominant form of identity authentication in computer systems (Inglesant & Sasse, 2010). A good password should be *easy to remember but hard to guess* (Bosworth & Summers, 2004). In other words it should be usable and secure. There is however an apparent trade-off between this usability and security, where techniques to increase security tend to decrease the usability and vice versa (Haga & Zviran, 1992). Passphrases, a term originally coined by Porter (1982), have been proposed as an enhancement of passwords. Proponents argue that passphrases are superior to passwords both in terms of usability and security strength, but empirical evidence to support these claims is scarce (Bauer, Christin, Cranor, Kelley, Komanduri, Mazurek, Shay, Vidas & Ur, 2012a). This article study how passwords and passphrases relate to each other. It examines their respective weaknesses and strengths with regard to usability and security. It also looks at usability and security themselves, to see how they influence each other and the people who use them.

2. Research problem

The authors of this paper seek to explore the implications on usability and security, when using passwords and passphrases as an authentication method for information systems.

3. Objectives

- To see how passphrases relate to passwords and how they each affect security and usability.
- To seek out how usability and security affect each other and the user in the context of password/passphrase authentication.

4. Review of literature and related work

4.1 Passwords and passphrases

A password is a sequence of characters from a pool of allowed characters, used to authenticate a user (Bosworth & Summers, 2004). A password can have any length and content, but the traditional computer password is short, 5-16 characters, and consists of random characters and symbols. In contrast, a *passphrase* consists of typically 3-4 natural language words, concatenated with or without spaces, to form a sort of sentence (Bauer et al, 2012a). Aids such as grammatical rules and selection of words with personal meanings may further help memorization of the passphrase (Kini, Jha & Rao, 2013). A passphrase is thus a kind of password, and the distinction between the two is not crystal clear. This article follows the example of Bauer et al (2012a) and uses the word *secret* as a general term covering both passwords and passphrases to avoid confusion.

With passphrases being a subset of passwords, environments with a password policy can usually change to a passphrase policy without infrastructure changes, provided that the system software does not limit the length or content of passwords (Bauer et al, 2012a).

4.2 Security

4.2.1 Creating secrets

Both passwords and passphrases can be system generated or selected by the user (Bauer et al, 2012a). A combination of the two is also possible. A system generated secret is created and assigned to the user by the information system in accordance with policy. Policy rules can be designed to increase security as well as usability factors such as memorability. System generated secrets are typically stronger, but perceived by users as being harder to remember (Čapek, Hub, Myšková & Roudn, 2010). A weakness of system generated secrets is that the secret must somehow be shared with the intended user in such a way that is it not disclosed to or intercepted by someone else (Gollmann 2011).

Allowing users to decide secrets themselves often leads to weak or predictable secrets (Čapek et al, 2010, Blocki, Komanduri, Procaccia & Sheffet, 2013) but users seem to prefer self-selected secrets to system generated ones (Haga & Zviran, 1992). Users often pick secrets related to their life or popular culture (Bosworth & Summers, 2004). Co-workers and other associates tend to use similar strategies when selecting secrets (Orman 2013). This makes it possible to predict a secret by examining the personality of a user or even from just looking at a person's desk. Dictionaries, exposed password lists and sourcing the Internet for content such as popular movie titles have been shown to be effective ways to guess user-chosen secrets in automated attacks (Herley, Mitzenmacher & Schechter, 2010). Imposing constraints on the composition may countervail weak secrets, but may lead to user frustration if too strict, with users coming up with creative ways to circumvent the restrictions, thus weakening the security (Herley et al, 2010).

A mnemonic phrase-based password is where users select a memorable phrase and then use one character from each word, commonly the first, to construct a password (Cranor, Kuo & Romanosky, 2006). Personal variations on letter casing and replacing letters with symbols can further make the password more complex. This creates a seemingly random password that is still easy for the user to remember. However, a majority of users will select popular phrases when making up mnemonic passwords (Cranor et al, 2006). This could be exploited by attackers that source popular phrases and convert these to mnemonics passwords for use in dictionary attacks (Cranor et al, 2006). If users are taught to avoid such common phrases, mnemonics offer an alternative to passwords that can improve memorability and security (Čapek et al, 2010).

If users are allowed to choose their own secrets, a security meter can help them create stronger secrets (Bauer, Christin, Cranor, Kelley, Komanduri, Lee, Maass, Mazurek, Passaro, Shay, Ur & Vidas, 2012b). Security meters provide a visual cue to the user on the strength of the secret while entering it, nudging them in the right direction. Bauer et al (2012b) show that stringent security meters make users spend more time on entering secrets, resulting in stronger security. There is however no universal scale for security meters on how to interpret the security of a secret.

4.2.2 Compromising secrets

Passwords and passphrases do not authenticate a particular user; they only imply that a user knows the secret (Gollmann, 2011). An attacker that obtains a secret will thus be able to pose as the real owner. There are a variety of ways attackers use to do this.

In a brute force attack, the attacker does an exhaustive search through all possible values in the search space in order to eventually find the correct secret. The numbers of possible combinations increase exponentially with length of the secret, making brute force attacks on longer secrets infeasible. Today this "exponential wall" appears at around 6-8 characters, depending on hardware and used symbol set (Ars Technica 2013). Attackers can optimize their cracking software by using character frequency tables that match the innate properties of languages (Cranor et al, 2006) and use pre-calculated data from lookup tables (Bosworth & Summers, 2004). Using long secrets and choosing symbols from a large character set are effective ways of increasing search space and thus improving the protections against brute force attacks.

Thanks to their increased length, passphrases have an innate resistance to brute force attacks. But passphrases have a strong relationship with grammatical structures of languages and commonly used words (Orman 2013) and their strength does not increase uniformly with length making them vulnerable to dictionary attacks (Kini et al, 2013). A longer passphrase is therefore not necessarily stronger that a shorter password.

A dictionary attack is similar to a brute force attack, but tests word combinations instead of character combinations (Herley et al, 2010). Lists of common words are used to reduce the search space and thus time needed to crack a secret, which also allows guessing much longer secrets. Word lists can be sourced from text corpuses such as dictionaries, electronic book repositories, websites with user generated content and pop culture lists such as movie names, just to name a few (Čapek et al, 2010, Ars Technica 2013). These words can further be mutated with common variations, such as grammatical rules, spelling errors, capitalizations and so forth to form comprehensive dictionaries (Cranor et al, 2006, Kini et al, 2013). Protection against dictionary attacks involves avoiding words and word sequences that can be found in word lists or derived therefrom.

Leaked password lists from hacked online services have given new insights into how people construct their secrets, which can be used to create rules for cracking software (Ars Technica 2013). A typical password Th0ma$_1956 might seem secure to the user, but can be broken down to a rule set such as *first name + separator + birth year, try casing variations on first letter, try common letter-to-symbol substitutions, make separator optional.* This rule set would be able to find similarly constructed secrets such as john1967 and M4ry-1999. Another source for constructing rules is to look at organizational password policies (Ars Technica 2013). This kind of knowledge in combination with text corpuses and statistical guessing allows crackers to construct highly efficient dictionary attacks, even against long secrets (Herley et al, 2010).

A common user pattern is to construct secrets by using a real words and appending a number of random characters before or after this word. Such secrets can be cracked by a hybrid attack, combining a dictionary attacks with a brute force attack mimicking this pattern (Ars Technica 2013).

Brute force and dictionary methods are typically offline attacks. In an offline attack the attacker has obtained direct access to the password file or system to mount the attack against. Online attacks, on the other hand, submit login attempts to operational systems, where security features and network latencies work as limitations, making it impossible or unfeasible to guess the secret. (Gollmann 2011)

Besides technical attacks, social engineering attacks are possible (Chantler & Broadhurst, 2006). Psychological tricks can be used to manipulate users into revealing their secrets. Typically the attacker takes advantage of human behavior to first build a trust relationship with the victim, and then exploit this relationship. A simple example could be calling a random user and claim to be from the IT department, explaining that the system is about to break and that you urgently need the users credentials so you can fix it. The unsuspecting user feels obligated to help and reveals his or her secrets, despite breaking security policies. Other forms of non-technical attacks include eavesdropping on users (shoulder surfing), going through the trash for useful information (dumpster diving), looking for post-it notes at common places at or around the desktop, physical visits impersonating someone like a repair technician or delivery guy, or simply learning enough about a person to be able to guess their secret (Chantler & Broadhurst, 2006). Related to social engineering are phishing emails and spyware (Gollmann 2011).

Protection against social engineering mostly involves security awareness for all user, because strong secrets will not offer protection against these kinds of attacks (Inglesant & Sasse, 2010). The security policy should address social engineering. Users need proper training to learn the value their data and recognize attacks. Organizations should be aware that the majority of attacks originate from within the organization (Gollmann 2011), such as employees seeking financial gain or disgruntled employees seeking revenge (Chantler & Broadhurst, 2006). Making security awareness a recurring theme, for example in a newsletter section, helps maintaining users awareness which may otherwise be lost shortly after training sessions (Chantler & Broadhurst, 2006).

4.2.3 Policies

It is absolutely necessary for an organization to have a security policy, to make users aware of its rules and to enforce its usage (Bosworth & Summers, 2004). The policy should be a living document that is updated to reflect the current situation, published in a visible way. Acceptance of the policy is tightly connected to the organizational culture and management commitment.

The password/passphrase policy should contain composition rules and recommendations, such as minimum length, character variations and avoidance of dictionary and pop culture words (Bosworth & Summers, 2004). Usage rules include how often secrets must be changed, policy on re-using passwords and number of failed login tries before locking an account. Additionally the document can instruct users on how to manage secrets, such as rules against writing down secrets and to never share it with anyone, and defence against social engineering attempts (Chantler & Broadhurst, 2006). Besides user centric rules, technical and management should also be addressed, for example how and where secrets are stored in the systems, software requirements, personnel responsibilities and how to manage user accounts. Different systems manage material of variably sensitivity, which should be reflected in the policy (Biddle, Chiasson, Forget & van Oorschot, 2008). The policy needs to take into consideration legacy systems that may not support the desired rules due to technical limitations (Biddle et al, 2008), such as Unix system that limit passwords to 8 characters (Gollmann 2011).

Since attackers can use statistical guessing to quickly crack the most popular user-selected passwords, Herley et al (2010) suggest skipping complex creation policies and instead allow any password as long as it is not an already popular password. Information on password popularity would be sourced from large Internet sites. The researchers argue that this approach can increase both security and usability, although the popularity lists would have to be protected from being obtained or queried by attackers who could otherwise use the information therein to improve their dictionaries with actual data. Additionally, notifying users that they are using weak passwords would serve an educational benefit.

Policy makers need to be aware of current trends and vulnerabilities. Because password cracking is a complex and highly mathematical subject, not understanding the inner workings may lead to recommendations that appear to *look* more secure than they actually are (Kini et al, 2013, Blocki et al, 2013).

4.3 Usability

Usability is a software quality. A user interface should achieve its specified goal effectively, efficient and with user satisfaction (Čapek et al, 2010). This means in terms of authentication in information systems, that a user should be able to with ease authenticate his or hers identity to the system. This is however not always the case. There are several usability factors to take into account when an information system relies on secrets as the main authentication method. This section focuses on two such usability factors; memorability errors and typographical errors. Studies have shown that different password and passphrase policies can affect the usability of the authentication and thereby affect the users' perception of the system in whole (Keith, Shao, & Steinbart, 2009). This could in turn affect the users' compliance to other security policies and by that result in a security risk. Thus Keith et al (2009) states that it is key to take usability into account when designing policies.

4.3.1 Typographical errors

Typographical errors when entering a password or passphrase is one of the more common authentication errors. The error occurs when a user remembers the password or passphrase but wrongly types it in the system. The most common causes to typographical errors is when users press one or several keys wrong or miss a key completely on the keyboard (Keith et al, 2009). One factor that contributes to this type of error is that passwords are often masked by the system to protect the secret from eavesdropping. This graphical user-interface behavior complicates the user's ability to confirm that he or she has entered the correct password. The user can therefore usually only confirm that the right amount of characters has been entered. Some devices such as smartphones, however, let the user see the last entered character for a split second before it gets masked. When the entered secret is compared to the secret stored in the information system, most systems only let the user know that he or she entered the wrong secret. Either the system grants the user access or some sort of error message is displayed letting the user know that the authentication failed. (Keith et al, 2009)

The number of characters in the password or passphrase has been linked to the risk for typographical errors. The more characters the secrets consists of, the higher the risk. Thus it is argued that usage of passphrases, that are usually longer than regular passwords, will increase the risk of typographical errors. However the Keith et al (2009) study can only partially confirm that passphrases result in more typographical errors than regular passwords. At the same time other studies on this subject claim that there is a direct link between passphrases and increased risk of typographical errors. Keith et al also did an earlier study which states that there is a measurable difference in the amount of typographical errors at first between regular passwords and passphrases, but that this small measured difference almost disappears after 4 weeks when the passphrase user got more used to using passphrases (Keith, Shao & Steinbart, 2007).

Keith et al (2009) states that automatic activation and word processing mode (WPM) are two factors that affect typographical errors. Some research states that a password or passphrase can become so learned that the user does not have to collect the characters from memory. Instead the user remembers the patterns of entering the secret. The risk of typographical errors decreases when a user reaches this level of familiarization with a secret, because the mind does not need to interpret the secret from characters in memory to actual keystrokes on the keyboard. To reach this state of automatic activation the password or passphrase needs to be structured very similar to regular words or sentences that are used on a daily bases. Keith et al (2009) calls this "Word Processing Mode", WPM. In their study they show that passwords or passphrases which conform to WPM decrease the risk of typographical errors. An example of this could be the passphrase "Th1$Pa$$W0rd1$My$3cretThatN00n3Kn0ws", which does not conform to WPM because the characters S, O, E and I have all been replaced with resembling special characters. Consequently, without taking security issues into consideration, passphrases should be similar in structure to what would be typed in a word processing document. Then the users can use their word processing skills when entering a secret and thus lower the risk of typographical errors. (Keith et al, 2009)

4.3.2 Memory related errors

To authenticate themselves with a secret, user must either retrieve the secret from its memory or from some other stored space such as a piece of paper or password management software (Keith et al, 2007). This section will cover the problems related to memorizing a secret and retrieving it when authentication is necessary.

When an employee for example is given login credentials to the company's intranet, they are often required to memorize the credentials by heart, because physically storing the secret is for the most part not compliant with most companies' security policies (Keith et al 2009). To memorize the secret the user needs to work or use the secret for an extended period of time to transfer the secret from short-term memory to long-term memory. How long this transfer period lasts is individual and can differ widely depending on the user's ability to memorize data as well as the composition and length of the secret itself. Gollmann (2011) argues that once a user has been assigned a secret, he or she should write secret down many times to ease the transition from short-term to long-term memory. Once stored in long-term memory, the mind does not require the secret to be used as often to stay in the individual's memory. (Keith et al 2009)

When memorizing a secret, the mind breaks up the secret in different pieces. How big these pieces are varies, but studies show that a piece can consist from one character up to whole phrases. The sizes of the pieces are determined by how familiar the mind is with the different parts of the secret. (Keith et al 2009) Take for instance the password "iloveyou22". The mind could e.g. break up this password in two pieces. The first phrase "I love you" is very common and it should be easy for the user to relate to this phrase. Thereby this phrase could be stored as one piece in the mind together with another piece for "22", which e.g. could represent the house number where the user's partner lives. It is important to note that the process of breaking up secrets into different pieces is highly individual and can differ widely between users (Keith et al 2009).

Earlier research has shown that the human mind can normally memorize up to 5-9 pieces in a set. Recent research has however lowered this number to 3-5. These limitations could affect users that have been given a random generated password which they cannot relate to and could result in the user's mind needing to use more pieces for fewer characters. (Keith et al

2009) This seems to be in line with what Haga & Zviran (1992) claim, who argue that user-selected secrets are easier to remember for users than system generated.

The research on passwords and passphrases has not given a conclusive results on which facilitates the user's ability to memorize a secret the most. Keith et al (2009) claim in their recent research that passphrases result in less memory related authentication errors than regular passwords. On the other hand Keith et al (2007) claim in their earlier research that there is no measurable difference in memorability between passwords and passphrases. However they concluded in both research that passphrases are still quite a foreign concept for most users, which results in lower user satisfaction.

4.3.3 Improving usability

The literature suggests various ways that can improve usability.

Repeatedly entering secrets, especially more complex secrets such as long passphrases, is impractical and an interruption that may reduce productivity and lead to user frustration (Cranor et al, 2006). Single sign-on solutions may alleviate this. A single sign-on can replace multiple secrets with only one and thus reduce the memory load for the user. It can also replace the need to actively log on to many individual services (Glassman, Tam & Vandenwauver, 2010). Users often have to remember a large number of passwords. AlFayyadh, Jøsang, Klevjer & Thorsheim (2012) suggest that users should be allowed to write down their passwords in order to take away the fear of forgetting passwords. Password management software installed on the local computer can provide similarly usability benefits. The risk of single sign-in solutions and password manager software is however the master secret being compromised (AlFayyadh et al, 2012).

The risk of a secret being compromised increases with its age, but users rarely change their secrets unless forced to (Inglesant & Sasse, 2010). Many policies thus require users to change their secrets at intervals, but Inglesant & Sasse argues that the advantage of frequently changing secrets is marginal. If this is still required though, users should be warned one day in advance in preparation (Glassman et al, 2010). Changes should not be made just before weekends or holidays since lack of use makes the secrets harder to remember (Gollmann 2011).

In a study by Bauer et al (2012a) the authors saw that users made more spelling errors when entering passphrases that when entering passwords. This was alleviated by the researchers by employing automatic error corrections, such as allowing different ordering of words, allowing typos or visual cues when errors were typed. Using such corrections the error rate of passphrases was made comparable to passwords.

4.4 The human perspective

Computer security is a people problem (Gollmann 2011). When security policies have been established by the organization for an IT-system, it's up to the users to comply with them (Keith et al 2009). Haga & Zviran (1992) has shown that different policies for secrets have direct effects on the usability of the system. There is an apparent trade-off between usability and strong security, where techniques to increase security tend to decrease the usability and vice versa (Haga & Zviran, 1992). When the usability is affected negatively by security policies, the users may bypass or try to trick the system's control mechanisms to achieve higher usability (Keith et al 2009). Biddle et al (2008) states that this kind of behavior from the users could be rooted in a growing frustration caused by the large number of secrets a user needs to remember to be able to access different IT-systems. A business user could be required to remember up to 15 secrets at one time (Mulligan & Elbirt, 2005). Often users only see authentication as an obstacle that needs to be bypassed to access the desired information (Inglesant & Sasse, 2010). An example of this can be when users are aware of the security policies but tries to figure out the weakest secret that still complies with the policy. (Inglesant & Sasse, 2010, Bauer et al, 2012b, Chantler & Broadhurst, 2006). The secret may comply technically, but the intentions of the policy are lost (Keith et al 2009).

Inglesant & Sasse (2010) states that when users bypass security policies, they often don’t have a clear understanding of the potential risks they expose the system to. This risk is too abstract for the users to care about, while the authentication barrier they want to overcome is real (Keith et al, 2007). Therefore it is imperative to take in account usability when designing authentication policies. If the policies are too strict they can backfire and user will try to find loopholes that can in some cases decrease the security (Keith et al 2009). Taking usability into account when designing policies can thus increase the security by aiding the user in doing the “right thing”. It is important for policy designers to realize that there should be a balance between security and usability in all policies, in order to design a secure and usable IT-system.

This balance between security and usability is unfortunately highly theoretical. The policies for an authentication method in an IT-system are usually based on the main goal of the system itself. Thus the security policies for commercial and non-commercial system often differ. Florêncio & Herley (2010) claim that some well-known e-commerce websites had relatively weak password policies, despite being some of the most attacked sites on the Internet. The commercial systems’ goal may be to produce an income for the organization, making the income is highly dependent on users logging in and using the system (Keith et al 2009). Biddle et al (2008) claim that a significant number of users will give up trying to create a secret if the security policies are too strict. Because of this the organization risk losing potential income to competitors with less stringent policies (Bauer, Christin, Cranor, Egelman, Kelley, Komanduri, Mazurek & Shay, 2011). Non-commercial IT-systems can be more security focused because the main goal of these systems is not to produce an income.

5. Proposed methodology

To try to answer the research problem the authors decided to rely on existing research in the field of information security. This decision was heavily rooted in the time constraint for the report. With the given time frame for the report, the authors drew the conclusion that they would not be able to realize a quantitative or qualitative study of academic quality. Instead the authors decided to do a literature study based on already existing published work.

5.1 Data collection

The material was selected by searching two different article databases search tools; LUBSearch and Google Scholar. LUBSearch is a database search tool available to all students registered on Lund University (Lund University Libraries 2013). Google Scholar on the other hand is a search tool provided free to anyone with an Internet connection by the company Google (Google Inc. 2013). The authors of this report have been unable to find any reliable information if Google Scholar is driven as a non-profit service within Google. Therefore the authors mainly used LUBSearch to locate reading material for the study. There was no predetermined number of maximum articles to be included in their report. Instead the focal point was to collect enough material to be able to answer the research problem. In addition to the academic articles, the authors also used the predefined course literature for the course; INFC40, Information Systems Security at Lund University - School of Economics and Management. The authors also stumbled upon a recently written article on a reputable website that covers technological news. This article gave fairly unique and up-to-date insight on how both password crackers and security experts work. Thus the information value of this article was deemed high enough to be included in this article. The authors also made an exception for this article in regards to the validation of its information. To balance this deficiency they agreed that this article would only be used to give insight in the current status of how secure different types of secrets are today and that it would not to be used to draw any conclusions that would affect the end result of this article.

5.1.1 Search criteria

When trying to locate reading material suitable to help answer the authors' research problem, a set of search criteria was predefined. The following keywords were used in various combinations with each other: usability, password, passphrase, security, information, system, computer, cracking. These keywords gave the authors a selection several thousand of articles to choose from. To reduce the selection the group decided to exclude material that was older than 1990. This action helped to actualize the selection so that only newer research was included.

5.1.2 Data validation

Critical thinking was always an important focus point for the authors. To answer the research problem the authors needed to rely on already reported studies and information. Thus it became important that the articles/studies that were to be included in this report were validated first. To validate sources of data, the authors agreed on a joint validation process. This validation process consisted of the following steps:

1. Does the author(s) of the source use references, in line with current academic requirements?
2. If the source is an article, has it been published in an academic paper?
3. If a study has been conducted:
    a. Is the study performed in such way that it can scientifically support the conclusions in that report?
4. Has the sources conclusions been cited in other work and therefore been validated by other researches?

These steps acted as an yardstick to help to set a standard for the authors of this report when collecting data to be able to answer the research problem.

5.2 Data processing

With the articles selected and validated the authors used the articles to highlight subjects that they thought were important for their research. These subjects got to be illuminated in the "Review of literature and related work" chapter and from that the authors drew their conclusions that were later detailed in the result chapter in the report. When different sources and studies contradicted each other on a subjected, the authors made a point out of always clarifying that the current research on the subject could not give a coherent picture of subject. By doing this the authors tried to always have an objective view on each subject so that the report maintained its academic quality.

6. Results

A passphrase is a form of password, where several natural language words are used instead of a shorter random sequence of characters. The distinction between the two is not crystal clear. A password system can mostly handle passphrases too, making the choice a matter of policy.

Secrets can be generated by the system or chosen by the user. User selected secrets tend to be less secure secrets and predictable in various ways. A security meter can help users choose a stronger secret. System generated secrets are generally more secure, but have less usability.

Attackers can compromise secrets in many ways. Offline brute force and dictionary attacks can crack even complex secrets today. Online systems are less vulnerable to such attacks, but through social engineering an attacker can compromise these too. There is no conclusive evidence that neither passwords nor passphrases offers better security than the other. They both have weaknesses that can be exploited, so their security depends on the composition and length, as well as the type of attack. Long secrets using made up words can protect against offline attacks, but not against social engineering, for which user awareness, attitude and education is essential.

Memory and typographical errors are the errors affecting usability the most when it comes to secrets. Users are more likely to enter passphrases wrong due to their sheer length. This difference tends to disappear as the users get more comfortable using passphrases. There is no evidence that user selected *passphrases* are easier to remember than user selected *passwords*. User selected *secrets* are however easier to remember than system generated *secrets*. Users also prefer to select their secrets themselves rather than being assigned system generated ones.

Usability and security can both be improved in various ways, but typically improving one will affect the other negatively. Strict policies can result in frustrated users that try to find ways to circumvent the mandated security. Different systems have different purposes and different security requirements. Thus policy makers should take into consideration both security and usability to find a suitable balance for the particular system.

7. Discussion

The goal of this study was to investigate passwords and passphrases in relation to usability and security. Intuitively passphrases appear to offer higher security because the general consensus is that longer secrets are most secure. However the results show that the difference between passwords and passphrases are not big enough to recommend either one. Usability and security are affected by many factors besides these two. Much security focus has been on composition and length, but these foremost protect against offline attacks, which are comparatively rare. Social engineering and insider attacks must also be considered. It can be argued that satisfied users doing the “right thing” are more important, because less strict policies that are actually used as intended are more secure than strict policies that are circumvented by the users. Practitioners should aspire to find a balance between security and usability in their systems. Their choices should be based on evidence, because password cracking is a complex subject where intuition cannot be trusted.

7.1 Limitations and suggested research

This study does not contain any original research and does not significantly contribute to current research. It is difficult to compare and value various sources in a correct way that does not color the end results. Further studies of interest would be to perform a qualitative study looking at how organizations value usability and security when designing password/passphrase policies for commercial and non-commercial systems.

8. Summary

This article aimed to explore the implications on usability and security when using passwords and passphrases as an authentication method for information systems. The objectives were to see how passphrases relate to passwords and how they each affect security and usability, and how security and usability affect each other.

To research this, the authors conducted a literature study on the current research. The literature mainly consisted of research articles that were found through searching the article databases LUBSearch and Google Scholar using relevant keywords. The collected articles were validated by using a predetermined validation method set by the authors.

The result showed that passphrases are a form of password that usually can replace passwords in information systems. They both have various weaknesses that can be exploited by attackers, and there is no conclusive evidence that either one offers better security than the other. Long secrets with made up words can protect against technical attacks, but not against social engineering, for which user awareness, attitude and education is essential. Passwords and passphrases effect on usability is unclear. Researchers have been able to measure small differences but the results are contradicting. They do however agree on that user-selected passwords or passphrases leads to better usability than system generated ones.

Usability and security can both be improved in various ways, but typically improving one will affect the other negatively. Strict policies can result in frustrated users that try to find ways to circumvent the mandated security. Different systems have different purposes and different security requirements. Thus policy makers should take in consideration both security and usability to find a suitable balance for the particular system.

In conclusion, neither passwords nor passphrases offered a big enough benefit to be recommended in front of the other. Usability and security tend to be inversely related. Practitioners should aim to design security policies that actually used rather than too strict policies that are circumvented by the users.

9. References

B. AlFayyadh, A. Jøsang, H. Klevjer & P. Thorsheim (2012): Improving usability of password management with standardized password policies. In: 7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (7th Conference on Network and Information Systems Security) (SAR-SSI 2012)

L. Bauer, N. Christin, L. F. Cranor, S. Egelman, P. G. Kelley, S. Komanduri, M. L. Mazurek & R. Shay (2011): Of passwords and people: measuring the effect of password-composition policies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11).

L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, B. Ur & T. Vidas (2012b): How does your password measure up? the effect of strength meters on password creation. In: Proceedings of the 21st USENIX conference on Security symposium (Security'12).

L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas & B. Ur (2012a): Correct horse battery staple: Exploring the usability of system-assigned passphrases. In Proceedings of the Symposium On Usable Privacy and Security (SOUPS '12).

R. Biddle, S. Chiasson, A. Forget & P. C. van Oorschot (2008): Improving text passwords through persuasion. In: Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08).

J. Blocki, S. Komanduri, A. Procaccia & O. Sheffet (2013): Optimizing password composition policies. In: Proceedings of the fourteenth ACM conference on Electronic commerce (EC '13)

E. Bosworth & W. C. Summers (2004): Password policy: the good, the bad, and the ugly. In: Proceedings of the winter international synposium on Information and communication technologies (WISICT '04).

J. Čapek, M. Hub, R. Myšková & R. Roudn (2010): Usability versus security of authentication. In: International Conference on Communication and Management in Technological Innovation and Academic Globalization (COMATIA '10).

A. N. Chantler & R. Broadhurst (2006): *Social engineering and crime prevention in cyberspace*. Queensland University of Technology, Brisbane

L. F. Cranor, C. Kuo & S. Romanosky (2006): Human Selection of Mnemonic Phrase-based Passwords. In: Proceedings of the second symposium on Usable privacy and security (SOUPS '06).

P. J. Denning (1992): The Science of Computing: Passwords. *American Scientist*, Vol. 80, No. 2, pp. 117-120.

D. Florêncio & C. Herley (2010): Where do security policies come from? In: Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10).

M. Glassman, L. Tam & M. Vandenwauver (2010): The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, Vol 29 Issue 3, pp 233-244

Gollmann, D. (2011): *Computer Security*, 3 rd ed. John Wiley & Sons

W. J. Haga & M. Zviran (1992): A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, Vol. 36, No.3.

C. Herley, M. Mitzenmacher & S. Schechter (2010): Popularity is everything: a new approach to protecting passwords from statistical-guessing attacks. In: Proceedings of the 5th USENIX conference on Hot topics in security (HotSec'10).

P. G. Inglesant & M. A. Sasse (2010): The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10).

M. Keith, B. Shao, P. J. Steinbart (2007): The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies*, Volume 65, Issue 1, January 2007, pp 17-28.

M. Keith, B. Shao & P. Steinbart (2009): A Behavioral Analysis of Passphrase Design and Effectiveness. *Journal Of The Association For Information Systems*, Volume 10, Issue 2, pp 63-89.

G. Kini, B. Jha & A. Rao (2013): Effect of grammar on security of long passwords. In Proc. 3rd ACM Conf. Data and Application Security and Privacy (CODASPY '13).

J. Mulligan & A. J. Elbirt (2005): Desktop Security and Usability Trade-Offs: An Evaluation of Password Management Systems. *Information Systems Security*, Volume 14, Issue 2, pp 10-19.

H. Orman (2013): Twelve random characters: passwords in the era of massive Parallelism. *IEEE Internet Computing*, Vol. 17, No. 5, pp. 91-94.

S. N. Porter (1982): A password extension for improved human factors. *Computers & Security*, Vol 1, No 1, pp 54–56

9.1 Online references

Ars Technica (2013): *How the Bible and YouTube are fueling the next frontier of password cracking*, http://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking (visited on 2013-10-16)

Google Inc. (2013): *Google Scholar*, http://scholar.google.se/intl/en/scholar/about.html (Visited 2013-10-19)

Lund University Libraries (2013): *LUBsearch*, http://www.lub.lu.se/en/search/lubsearch.html (Visited 2013-10-19)