INFORMATICA, 2020, Vol. 31, No. 3, 459–479

DOI: https://doi.org/10.15388/20-INFOR408

System-Assigned Passwords: The Disadvantages of the Strict Password Management Policies

Boštjan BRUMEN
University of Maribor, Faculty of Electrical Engineering and Computer Science, Smetanova 17, Si-2000 Maribor, Slovenia
e-mail: bostjan.brumen@uni-mb.si

Received: December 2018; accepted: February 2020

Abstract. After Morris and Thompson wrote the first paper on password security in 1979, strict password policies have been enforced to make sure users follow the rules on passwords. Many such policies require users to select and use a system-generated password. The objective of this paper is to analyse the effectiveness of strict password management policies with respect to how users remember system-generated passwords of different textual types – plaintext strings, passphrases, and hybrid graphical-textual PsychoPass passwords. In an experiment, participants were assigned a random string, passphrase, and PsychoPass passwords and had to memorize them. Surprisingly, no one has remembered either the random string or the passphrase, whereas only 10% of the participants remembered their PsychoPass password. The policies where administrators let systems assign passwords to users are not appropriate. Although PsychoPass passwords are easier to remember, the recall rate of any system-assigned password is below the acceptable level. The findings of this study explain that system-assigned strong passwords are inappropriate and put unacceptable memory burden on users.

Key words: passwords, passphrases, security, human memory, mnemonics, authentication.

1. Introduction

Suppose you just bought a brand new car – on average you would spend a bit more than $36.000 in the USA (Buehler and Mrasek, 2018) – and when you would like to open the door and start the engine for the first time, the car would ask you to come up with a password – hopefully "unique and hard to crack"; this was the actual advice given to LinkedIn users after the breach (Popkin, 2012). You would be lucky if you got an advice that your password should be at least 8 characters long with mixed lower and upper case letters and at least one number and a symbol. Furthermore, the car would ask each new driver to do so before they first used the car. Every time one would like to drive the car (or even just open the door), he or she would have to enter the password. Clearly, the car's security would be determined by the weakest password. Luckily, the cars are not protected by passwords, or else much more than nearly $6 billion would be lost to motor vehicle thefts at the rate of 237.4 per 100,000 inhabitants as estimated by FBI (2018), compared to $16,8 billion lost due to identity frauds (Pascual *et al.*, 2018) at the estimated rate of 5,127 per 100,000 inhabitants. The computer industry is sometimes compared to

the automobile industry (Gates, 1997), and becomes a source of numerous jokes. Security is no joke, even when such a comparison is made. Weak passwords have led to much more serious breaches, exposing millions of users and/or causing billions in damages, and have sometimes led to deaths (Jones, 2017). The history of password-related problem pre-dates the seminal paper written by Morris and Thompson (1979) – it goes way back to mid-1960s and to the CTSS operating system exposing all the passwords as a daily welcome message (Corbató, 1991).

The following is a historical list of sample breaches that are originating from weak passwords or password management policies. The list is far from being complete; it only gives a glimpse into the variety, scope and damages done by hacking into passwords:

- In 1978, Stanley Rifkin obtained the electronic transfer code for the Security Pacific Bank and used the code to transfer $13 million from Security Pacific to his Swiss bank account (Tom, 1991; Zviran and Haga, 1999).
- In 1986, a group of German hackers penetrated dozens of military, government, and commercial computer systems by cracking passwords of legitimate users and system administrators. They were looking for military information that could be sold to the Soviet Union (Stoll, 1988, 1989).
- In April 1994, two English teenagers penetrated several systems through the Air Force's Rome (New York) Laboratory. Among others, they obtained all of data stored on the Korean Atomic Research Institute system and deposited it on Rome Lab's system. Initially it was unclear whether the Korean systems belonged to North Korea or South Korea. The concern was that if it was North Korea, the North Koreans would think the logical transfer of the storage space was an intrusion by the US Air Force, which could be perceived as an aggressive act of war (USA, 1996).
- In November 1998, Robert Morris, Jr., a student at Cornell University created what later became known as the first computer worm distributed via the Internet. It contained a bug that caused it to propagate itself far faster than Morris intended. While no known alteration or destruction of data occurred, the program filled all available memory space on infected computers, bringing them to a grinding halt. The cost of clearing memory space and restarting systems was estimated at US$ 100 million. A key element of the Internet worm involved attempts to discover user passwords. It exploited the tendency of users to choose easy-to-remember passwords and used lists of words, including the standard online dictionary, name lists, and combinations of four-digit numbers, as potential passwords (Seeley, 1989; Spafford, 1989; Zviran and Haga, 1999).
- In June 2005, the hackers broke into CardSystems' database. The company did not encrypt any of users' information. The names, accounts numbers, and verification codes of more than 40 million card holders were stolen and exposed (Krim and Barbaro, 2005; Sahadi, 2005).
- An intrusion into TJX's payment system took place in July 2005, but was not detected until mid-December 2006. Between 45,6 and 94 million credit and debit card numbers were stolen (Pereira, 2007; Vijayan, 2007a, 2007b) and the cost of data breach is estimated at US$ 256 million (Kerber, 2007).
- In April 2011, the Sony Playstation Network outage has affected 77 million users and the costs are estimated at more than US$171 million (Hachman, 2011; Sangani, 2011).

- The LinkedIn password leak in June 2012 has exposed more than 6,5 million users (Kamp, 2012; Kirk, 2012; Popkin, 2012).
- In April 2013, the hackers have obtained personal information of 50 million LivingSocial's users (Acohido, 2013).
- In 2017, the largest U.S. credit bureau, Equifax, suffered a breach that exposed the personal data of 143 million people, including Social Security numbers. It was among the worst breaches on record because of the amount of sensitive information stolen (Gressin, 2017).

A comprehensive list of breaches since 2005 can be found at Privacy Rights Clearinghouse (PRC, 2018).

A typical survey evaluating the generation and use of passwords revealed that users have several password uses and the average password has more than one application. Two thirds of passwords are designed around one's personal characteristics, with most of the remainder relating to relatives, friends or lovers. Proper names and birthdays are the primary information used in constructing passwords, accounting for about half of all password constructions. Almost all respondents reuse passwords, and about two thirds of password uses are duplications. Passwords have been forgotten by a third of respondents, and over half keep a written record of them (Brown *et al.*, 2004).

It seems that nothing has been learnt and changed in the course of almost 50 years. Most researchers claim that users and their passwords are the weakest link (Adams and Sasse, 1999; Adams *et al.*, 1997; Notoatmodjo, 2007; Sasse *et al.*, 2001; Tam *et al.*, 2009), although the basic and the most relied-upon security mechanism in information systems continues to be the ability to authenticate the identity of a user. The passwords used to be (Loch *et al.*, 1992; Tzong-Chen and Hung-Sung, 1996; Zviran and Haga, 1990) and still are the main method of authentication (Creese *et al.*, 2013; Egelman *et al.*, 2013; Lee *et al.*, 2013), although research continues on more sophisticated methods of authentication, see e.g. Al-Hudhud *et al.* (2014), Hölbl *et al.* (2008, 2010, 2012), Jiang *et al.* (2013), Kuo *et al.* (2006), Liaojun *et al.* (2013). Some novel solutions are even improvements of concepts well known to the automobile industry (i.e. car keys) (Grosse and Upadhyay, 2013); others are based asymmetric cyphers (Sakalauskas and Mihalkovich, 2017), on certificateless key encapsulations (Gao *et al.*, 2017; Wu *et al.*, 2018), ID-based cryptography (Meshram *et al.*, 2017), or image-based encryption (Khan *et al.*, 2017).

The most natural question is: why we have so many password-related breaches? The answer is relatively simple: passwords need to be as long and as complex as possible to render guessing, dictionary and brute-force attacks prohibitively expensive and time consuming; yet at the same time passwords need to be memorable and simple to support user experience.

One of the basic principles of security (Stallings, 2006) states: (1) a password scheme is said to be computationally secure if the cost of breaking it exceeds the value of the protected information, or (2) the time required to break the password exceeds the useful lifetime of the information. Today, costs for building a cracking machine are relatively low (in the range of ∼US$1000, see e.g. Gosney, 2018) and thus quite affordable, not to mention the possibility that a rouge individual or organization may have millions of interconnected machines at her disposal.

The time required for breaking the password is all we can count on. Let us assume that the useful lifetime of a stored information is 60 years, which is a typical assumption for medical data (Brumen *et al.*, 2013). Under this assumption, a safe password today would be made of at least nine characters from upper and lowercase letters, numbers and symbols, but it would not be safe in 10 years from now. Thus, 10- or more character passwords are required today to be safe tomorrow as well, confirming findings by Egelman *et al.* (2013). However, some authors argue, based on the entropy principle, that passwords shall be at least 15 characters long with entropy similar to that of 3DES or AES (StClair *et al.*, 2006); this claim needs to be taken with caution as other authors give evidence that the notion of password entropy does not provide a valid metric for measuring the security of a password (Weir *et al.*, 2010).

When we come to 10 (or more) characters to remember, they constitute a much larger corpus than is the capacity of a human memory, where the well-known 7 ± 2 principle applies (Miller, 1956). Human memory, in addition, is temporally limited (short-term) when it comes to memorizing sequences (Johnson, 1991). For this reason good passwords that are consisting of an abundant number of randomly selected characters are doomed: the users will either forget them (Florencio and Herley, 2007) or write them down (insecurely), or both (Yan *et al.*, 2000, 2004; Zviran and Haga, 1993).

Starting from the findings of first research on users' role in password security almost two decades ago (Adams and Sasse, 1999; Sasse *et al.*, 2001; Tam *et al.*, 2009) and by misunderstanding the concept of 'users are weakest link', administrators and security professionals tried to minimize the impact of the weakest links (users) by trying to force them into using safe, system-assigned passwords. When administrators have been setting the password management policies, they had a notion that users are their enemies (Adams and Sasse, 1999) and that they pose a security threat that needs to be controlled, ignoring warnings that the actual password management needs to balance between convenience and security (Tam *et al.*, 2009).

This work contributes to understanding of the impact of strict password management policies to usability and memorability of such passwords. Namely, previous research has predominantly dealt with memorability and/or usability of user-generated passwords, see e.g. Biddle *et al.* (2011), Cipresso *et al.* (2012), De Angeli *et al.* (2005), Keith *et al.* (2007), Nelson and Vu (2010), Vu *et al.* (2007), Wiedenbeck *et al.* (2005), Woods and Siponen (2018), Yan *et al.* (2000, 2004).

The rest of the paper is organized as follows: the next sub-section presents the state of the art in the field by review of related works and is followed by a presentation of PsychoPass method; the articulated research question concludes this introductory section. In Section 2, we present the research method and in Section 3, the results. We conclude the papers with discussion and final remarks in Section 4.

1.1. *Related Work*

User authentication schemes are based on the following principles (or combinations thereof): "what you know", "what you are" and "what you have" (Pfleeger and Pfleeger,

Table 1
Textual password creation schemes.

Principle	Advantages	Disadvantages	Source
Personal characteristics, e.g. birthdate, names, pets, addresses, etc.	Easy to remember	Easy to crack, easy to guess	(FIPS, 1985; Morris and Thompson, 1979; Zviran and Haga, 1999)
Cognitive, a randomly selected set of personal questions which only an authorized user can answer correctly	High recall rate	Easy to guess by family and friends	(Brostoff, 2004; Kuo *et al.*, 2006)
Pass-sentences and pass-phrases	Memorable, cracking resistant	Inappropriate for mobile use, inconvenient, useless for repeated use	(Brostoff, 2004; Spector and Ginzberg, 1994)
Randomly generated pronounceable passwords	Memorable, brute force cracking resistant	Vulnerable to a special dictionary attack	(Ganesan *et al.*, 1994; Gasser, 1975)
Mnemonic, a memorable phrase (e.g. first letters of a sentence)	Memorable, brute force cracking resistant	Vulnerable to a special dictionary attack	(Kuo *et al.*, 2006; Nelson and Vu, 2010; Zviran and Haga, 1990)

2003; Stallings, 2006). "What you know" is based on secrecy known only to an authorized user, "what you are" is based on a user's physical characteristics (e.g. retina image, fingerprint) – also called biometrics, whereas "what you have" is based on possession of an extra token, such as a single/multi-factor cryptographic device, single/multi-factor one-time password device, out-of-band devices or simply look-up secrets. In this paper we study the "what you know" principle-based authentication scheme.

The "what you know" principle-based authentications relies on passwords of two types: textual and graphical ones (Davis *et al.*, 2004; Suo *et al.*, 2005). In this paper we deal with textual passwords and do not take into the account the graphical ones because they require a different user interface (Suo *et al.*, 2005) and hence are not the focus of our study.

The strongest passwords by far are those randomly selected, but they are at the same time the hardest to remember and thus subject to unsafe practices (Pfleeger and Pfleeger, 2003). There are several "what-you-know" alternatives to a (nearly) random long textual password. We briefly list them in Table 1.

Orthogonal to the works on different textual password generating and management schemes are contributions that deal with password metrics, principally meters that show users how strong their password might be (Bishop and Klein, 1995; Egelman *et al.*, 2013; Weir *et al.*, 2010). It was shown empirically (Weir *et al.*, 2010) and mathematically (Verheul, 2006) that Shannon entropy value is not useful when determining the strength of a password creation policy, and other policies need to be used. Common advices on minimum password length and character set requirements provide against online attacks (Weir *et al.*, 2010). Yet, by observing these requirements, users tend to forget passwords and/or write them down, usually in an insecure location (Zviran and Haga, 1999). Writing down a password is not a bad practice itself, as pointed out by Bruce Schneier: "*. . .if only users*

wrote [*a password*] *down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet*" (Schneier, 2005).

Complementary to our work are also contributions dealing with users' compliance to different password creation policies (Adams and Sasse, 1999; Adams *et al.*, 1997; Sasse *et al.*, 2001; Weirich and Sasse, 2001) and how the users can improve the password security and memorability under such policies in place (Vu *et al.*, 2007). General observation is that users tend to choose bad passwords due to inexistent policies or try to comply with them with minimal effort (Dell'Amico *et al.*, 2010; Gehringer, 2002; Tam *et al.*, 2009; Vu *et al.*, 2007; Weir *et al.*, 2010). All users need a sound piece of advice and an explanation why passwords need to be strong and how to achieve it (Cox, 2012; Davinson and Sillence, 2010; Horcher and Tejay, 2009; Sasse *et al.*, 2001; Weigel and Hazen, 2014; Workman *et al.*, 2008).

With respect to password management policies, the U.S. National Institute of Standards and Technology published a draft Guide to enterprise password management, publication NIST 800-118 (Scarfone and Souppaya, 2009), which defines four authentication assurance levels (AAL). For each level, several password management policy elements must be implemented. These elements address a) the required password length, b) required type and number of used character sets (e.g. lower/uppercase letters, numerals, special characters), c) password composition restrictions, d) password change frequency, e) technical password management (related to storing and transmitting of passwords), f) password management restrictions, and g) password origin.

A strict password management policy in the mentioned NIST publication using the above factors could be implemented as follows: (a) a minimum 8 characters; (b) type: at least upper and lower case plus one numeral or a special symbol and at least three of those; (c) composition restrictions: no biographic elements and no dictionary words; (d) frequency: password change frequency (at least every 12 months); (e) technical password management: no stored passwords allowed, only salted hashes, no password transmission over insecure networks; (f) management restrictions: password reuse not allowed, writing down of passwords not allowed, deriving passwords from other passwords is not allowed; and (g) password origin: *system-assigned*.

We can see many of these requirements nowadays implemented in many web pages and services: a minimum 8-character, mixed upper and lowercase plus numeral plus special character, not in a dictionary password. Most of the elements can be system-controlled by imposing a set of rules and measures, except the element c) where system cannot control if a user has included her biographic elements into the password. The only way to control this is to use the g) element: passwords are generated and assigned by a system. Yet, the element on management restriction (f), the part that prohibits writing down of passwords, completely relies on a user (Scarfone and Souppaya, 2009) and is very hard to implement, despite abundant training of users.

Despite the fact that the NIST 800-118 (Scarfone and Souppaya, 2009) was a draft, it was widely adopted and implemented in authentication schemes. Recent NIST standard 800-63B (Grassi *et al.*, 2017) still has some elements from the previous draft, including the requirement for an 8-character password. However, it has moved away from requiring

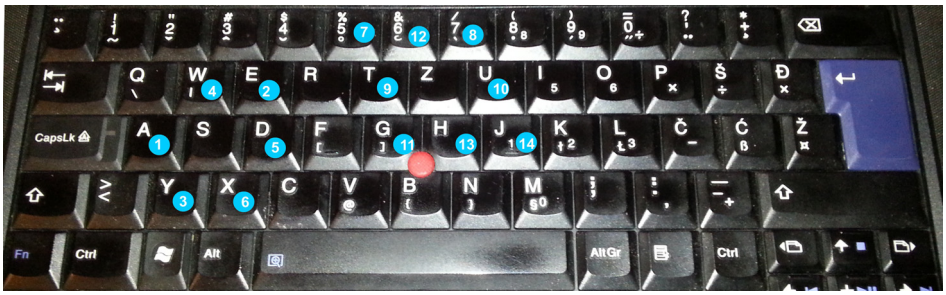

Fig. 1. A circle and a square on keyboard producing a strong password.

Table 2
Password result of the visual representation from Fig. 1 using PsychoPass.

Sequence #:	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Shift (sh)/alt-gr (al) used		Sh		Al		sh	sh		sh		al			sh
Resulting character:	a	E	y	|	d	X	%	7	T	u	]	6	h	J

system-assigned passwords. Nevertheless, many system and/or security administrators implemented strict password management policy by having system-generated passwords for users, believing they have solved the problems of password composition, password reuse and passwords deriving from other passwords.

1.2. *PsychoPass Method*

Here, we briefly present a hybrid method for generating textual passwords proposed by Cipresso and colleagues (Cipresso *et al.*, 2012). It was improved by authors in Brumen *et al.* (2013). The method is considered hybrid because it generates string passwords, whereas the underlying principle is graphic (visual) representation of the produced string on a keyboard. While randomly generated textual strings (e.g. 'aEy|dX%7Tu]6hJ') and passphrases (e.g. 'SunNy69sCReen' are straightforward, we present the PsychoPass method in more detail.

"*The idea of PsychoPass is that a password can be created, memorized and recalled by just thinking of an action sequence instead of a word or string of characters*" (Cipresso *et al.*, 2012). With PsychoPass method, a user creates a password based on visual location of keys, not the key values themselves. Figure 1 depicts a visual circle and a square (actually a rhombus) on the keyboard using blue numbered dots. The keys that draw the circle are A-W-E-D-X-Y, and the keys that draw the square are 5-6-7-T-U-G-H-J.

However, the improved PsychoPass method requires the use of SHIFT and ALT-GR keys and that the keys that are not always adjacent to each other in the sequence. Suppose that key #1 is pressed without SHIFT or ALT-GR, key #2 is pressed in combination with shift key, and so on, as given in Table 2 (please note that SI-Slovenian keyboard layout is used).

Table 3
Password result of the visual representation from Fig. 1 using PsychoPass, shifted one.

Sequence #:	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Shift (sh)/alt-gr (al) used		Sh		Al		sh	sh		sh		al			sh
Resulting character:	s	R	x	E	f	C	&	8	Z	i	h	7	j	K

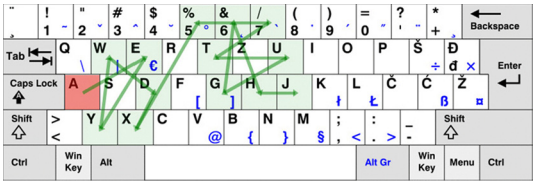

Fig. 2. A representation of password »aEy|dX%7Tu]6hJ«.

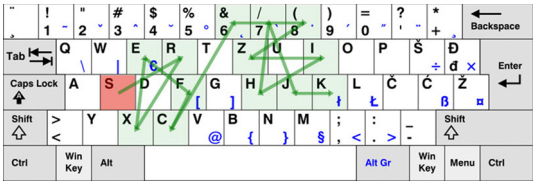

Fig. 3. A representation of password »sRxefC&8Zih7jK«.

The password representing the circle and the square in Fig. 1 would read »aEy|dX%7Tu]6hJ«. Interestingly, the very same shapes, if shifted one key to the right on a keyboard, would yield another password, namely »sRxefC&8Zih7jK«, as shown in Table 3.

The representations of passwords »aEy|dX%7Tu]6hJ« and »sRxefC&8Zih7jK« are shown in Fig. 2 and Fig. 3, respectively.

The user thus memorizes a password based on its visual representation (action sequence) and additionally when to press SHIFT or ALT-GR.

It may seem that the password produced (e.g. »aEy|dX%7Tu]6hJ«) is totally random (with $75^{14} = 178.179.480.135.440.826.416.015.625 = 1{,}78\text{E}{+}26$ different combinations, brute force attack would take some 5, 6E+9 years), but in reality it is not so. The total number of different combinations using the improved PsychoPass method is $n_k b^{le-1}$, where n_k is the number of different characters on the keyboard from where the sequence can start, b is the number of possible next keys, and le is the length of the produced sequence. At the beginning, we have some 45 keys on a keyboard ($n_k = 45$) for selecting the key as the starting point and for the first character of the password (the "A" is chosen in example from Table 2). From there on, each keyboard key has (at most) 8 first neighbours (plus the key itself), so in each step only one out of 9 combinations ($b = 9$) could have been used. However, we can choose any key as the next in the sequence. For the sake of simplicity (and the speed of input), let us suppose we select only the first or the second neighbour (key distance is 1 or 2); that is q, w, s, x, and y are one key distance from "a" on the key-

board whereas 1, 2, 3, e, d, and c are two key distances away. Additionally, each of these keys can be used in combination with SHIFT or ALT-GR, each producing different result. This way the base b is increased from original $b = 9$ to $b = 54$ (Brumen *et al.*, 2013). All in all, there are $45^1 \cdot 54^{13}$ (= 1.493.933.931.608.915.411.066.880 = 1,4E+24) different passwords of length 14, although PsychoPass passwords of length 10 are sufficient today (Brumen *et al.*, 2013) and those of length 11 should be sufficiently safe in ten years from now. A detailed discussion on the strength of the psychopass passwords can be found in Brumen and Černezel (2014).

1.3. *Research Question*

The research question is as follows: what is the impact of a strict password creation policy on the convenience and memorability of different system-assigned passwords? We expect that users will spend less time entering passphrases, followed by random and psychopass. In terms of memorability, we expect that approximately 25% of participants will remember their assigned passwords after one week (Zviran and Haga, 1993).

2. Method

We conducted an experiment where a group of second year computer science students ($n = 45$) at University of Maribor, Faculty of Electrical Engineering and Computer Science (Slovenia, Europe) was using a specially developed web tool, available on-line. The experiment was designed so that each participant was given three different types of passwords. First, a password was system-generated by using eight randomly selected characters from a pool of upper and lowercase letters, numbers and special symbols (hereinafter referred to as random password). The pool consisted of the following characters: »a b c č d e f g h i j k l m n o p q r s š t u v w x y z ž A B C Č D E F G H I J K L M N O P Q R S Š T U V W X Y Z Ž 0 1 2 3 4 5 6 7 8 9 ! $? _ -. #«, in total 75. The total number of possible combinations is $75^8 = 1.001.129.150.390.625 = 1E+15$ combinations.

Next, the system created a password by using concatenations of words and symbols and/or numbers (pass-phrase password). Here, each password was created by using a 6-letter word (mixed upper and lowercase letters), concatenated by two digits, and followed again by a 6-letter word, totaling 14 characters. The words were chosen randomly by the system from a custom built dictionary of Slovenian 6-lettered words which were in turn obtained from On-line dictionary of Slovenian Words (SASA, 2013). There are 22.093 different 6-letter words out of total 354.205 different words in the on-line dictionary. Each 6-letter word can appear in $2^6 = 64$ different forms if lower and uppercase letters are used. The total number of possible combinations is thus $22.093 \cdot 2^6 \cdot 10^2 \cdot 22.093 \cdot 2^6 = 199.926.025.830.400 = 1{,}9E{+}14$ combinations.

Finally, a password was created by the system using the improved PsychoPass method (referred to as a psychopass password). The length of the password ($le = 11$ characters) and the base (9 keys combined with shift; $b = 18$) were set so that the total number

of combinations would be comparable to the previous two, i.e. $n_k b^{le-1} = 45 \cdot 18^{10} = 160.671.025.198.080 = 1{,}6\text{E}{+}14$ combinations.

It can be noted that the strength of a random password is of one order of magnitude higher than the other two. However, 7-character random password would yield ∼1E+13 combinations, one order of magnitude lower. We decided for the 8-character password to have the length of the password higher and more comparable to 14 and 11 characters in pass-phrase and psychopass passwords, respectively. Additionally, length 8 is typical (Dell'Amico *et al.*, 2010) and also endorsed by recent standards, e.g. NIST 800-63B (Grassi *et al.*, 2017).

Each consenting participant was assigned a username and an initial password that were sent to her or him by email prior to the beginning of the experiment. The experiment itself first took place in a classroom where the participants were explained the outline and the purpose of the experiment. They were also told that the passwords need to be memorized not only for the day of the experiment but for a longer period and that they should not write down the password; for this reason the participants had to put away bags, papers, pens and even mobile devices prior to entering the experiment room and for the entire duration of the experiment. After the presentation phase, the participants moved without their belongings to a computer room. This way we controlled that the participants could not write down or else store their assigned passwords. After the experiment the participants entered a classroom for lectures, further delaying them from access to their belongings for one hour.

When a participant has logged in to the experimental web page, the system has displayed a randomly generated password. If the participant did not like the assigned password, an alternative was offered. This way we emulated a strict password policy which does not allow a user to create her own weak password but may choose from several alternatives offered by the system. Once the password was accepted, the user was re-typing the assigned password back to the system for two minutes for the random and pass-phrase, and for five minutes for the psychopass password. The allowed time for entering the repetitions was determined in the testing phase of the web page. The selected password with additional data was stored in a database with user's details. The additional data included the measured time needed for typing the password and whether the re-types of the password were successful or not.

The experiment continued in one week. This time it was measured only if a participant had remembered any of the assigned passwords. The participant had a possibility to enter the password correctly three times only (simulating a real-world lockout). If she or he did not remember it, the system had it displayed for the user's reference, and marked a failure.

2.1. *Data Collection and Processing*

The data from the experiment and its web page were collected in a database. For each user a login username and password were initially stored. Additionally, the time taken to enter each password was measured for all the participants. The measurement of time started with the first keystroke and ended when the ENTER key was pressed. The data on successful password recall was collected as well.

From the collected data we removed 5 users' entries because they did not complete all three tests or they did not enter some of the passwords correctly at least once in the first phase. The final dataset contains data from 40 users.

2.2. *Hypotheses*

First, we checked for the usability of the passwords in terms of the time needed for the input. We compare the times needed to enter the password in the system at two points of the first part of the experiment, the first time entry and last time entry. First time entry was recorded when participants first repeated the system-assigned password, and last time entry was recorded at the end of 2- and 4-minute interval for random/passphrase and psychopass, respectively.

We expect that the mean times needed to enter a password at the beginning and at the end will significantly differ across the groups. At the beginning, we expect that it will be the easiest (shortest times) to enter a passphrase compared to the other two groups. At the end, we expect that cognitive-based methods (psychopass, passphrase) will require less time to enter the password compared to a randomly selected password.

The primary experimental hypotheses are the following:

- Hypothesis 1: $H1_0$: $\mu_D = 0$; the mean times for the first time entering a password are the same for random, passphrase and psychopass passwords.
  - Alternative hypothesis 1: $H1_a$: $\mu_D \neq 0$; the mean times for the first time entering a password are different for random, passphrase and psychopass passwords.
- Hypothesis 2: $H2_0$: $\mu_D = 0$; the mean times for the last time entering a password are the same for random, passphrase and psychopass passwords.
  - Alternative hypothesis 1: $H2_a$: $\mu_D \neq 0$; the mean times for the last time entering a password are different for random, passphrase and psychopass passwords.

In case $H1_a$ holds ($H1_0$ is rejected) we shall test the following hypotheses, which are actually pairwise comparisons to see where the differences are coming from:

- Hypothesis 1A-1_0: $\mu_D = 0$; the mean times for the first time entering a random and psychopass password are the same.
  - Alternative hypothesis 1A-1_a: $\mu_D \neq 0$; the mean times for the first time entering a random and psychopass password are different.
- Hypothesis 1A-2_0: $\mu_D = 0$; the mean times for the first time entering a random and passphrase password are the same.
  - Alternative hypothesis 1A-2_a: $\mu_D \neq 0$; the mean times for the first time entering a random and passphrase password are different.
- Hypothesis 1A-3_0: $\mu_D = 0$; the mean times for the first time entering a passphrase and psychopass password are the same.
  - Alternative hypothesis 1A-3_a: $\mu_D \neq 0$; the mean times for the first time entering a passphrase and psychopass password are different.

In case $H2_a$ holds ($H2_0$ is rejected) we shall test the following hypotheses, which are actually pairwise comparisons to see where the differences are coming from:

- Hypothesis 2A-1_0: the mean times for the last time entering a random and psychopass password are the same.
  - Alternative hypothesis 2A-1_a: the mean times for the last time entering a random and psychopass password are different.
- Hypothesis 2A-2_0: $\mu_D = 0$; the mean times for the last time entering a random and passphrase password are the same.
  - Alternative hypothesis 2A-2_a: the mean times for the last time entering a random and passphrase password are different.
- Hypothesis 2A-3_0: $\mu_D = 0$; the mean times for the last time entering a passphrase and psychopass password are the same.
  - Alternative hypothesis 2A-3_a: the mean times for the last time entering a passphrase and psychopass password are different.

Second, we were interested whether the recall rate at the second stage of the experiment is somehow connected to the password type. Here, the hypothesis is as follows:

- Hypothesis 3: $H3_0$: the recall rate is not associated with the password type.

Alternative hypothesis 3: $H3_a$: the recall rate depends on the password type.

2.3. *Statistical Analysis*

The data sets containing measurements of time needed to enter a password for the first time and for the last time in a given time-frame for three different groups of measurements (group 1: random, group 2: passphrase, group 3: psychopass) were analysed using 3-way ANOVA and independent samples t-test for the differences in means. We considered differences to be significant at the $\alpha < 0.05$ level.

We used the Bonferroni correction to counteract the problem of multiple comparisons in t-tests (Abdi, 2007). The correction is based on the idea that if an experimenter is testing n dependent or independent hypotheses on a set of data, then one way of maintaining the family-wise error rate is to test each individual hypothesis at a statistical significance level of $1/n$ times what it would be if only one hypothesis were tested. We would normally reject the null hypothesis if $P < 0.05$. However, by performing three pairwise comparisons (passphrase-random, passphrase-psychopass, random-psychopass) Bonferroni correction requires a modified rejection threshold for P, $P < (0.05/3) < 0.0167$.

SPSS version 25 (IBM Corporation, Armonk, NY, USA) was used for analysis.

3. Results

3.1. *Results Part I*

First, we calculated the descriptive statistics for the data obtained. The results are shown in Table 4 where the times are listed in milliseconds.

Table 4
Descriptive statistics for experimental data, time to enter the password.

		N	Mean	Std. deviation	Std. error	95% Confidence interval for mean		Minimum	Maximum
						Lower bound	Upper bound		
first_time	random	40	17387,25	13826,064	2186,093	12965,46	21809,04	3481	60866
	passphrase	40	16894,18	10169,751	1607,979	13641,73	20146,62	7680	67295
	psychopass	40	30327,85	14929,805	2360,609	25553,07	35102,63	7797	83947
	Combined	120	21536,43	14443,180	1318,476	18925,71	24147,14	3481	83947
last_time	random	40	10010,18	16905,091	2672,930	4603,66	15416,69	2763	112728
	passphrase	40	11210,08	6557,797	1036,879	9112,79	13307,36	3919	31178
	psychopass	40	11086,38	7549,515	1193,683	8671,92	13500,83	3018	35659
	Combined	120	10768,88	11257,245	1027,641	8734,04	12803,71	2763	112728

Table 5
Results of ANOVA tests.

		Sum of squares	df	Mean square	F	Sig.
first_time	Between Groups	4642211670,950	2	2321105835,475	13,456	**0,000**
	Within Groups	20181835238,375	117	172494318,277		
	Total	24824046909,325	119			
last_time	Between Groups	34843575,200	2	17421787,600	0,135	0,873
	Within Groups	15045497409,925	117	128593994,957		
	Total	15080340985,125	119			

Next, we tested for the differences in means of times needed to enter each password at the beginning and at the end of the experiment (tested for $H1_0$ and $H2_0$). We used the ANOVA test. The results are shown in Table 5.

The results show that the hypothesis $H1_0$ needs to be rejected at $P = 0{,}000$ (see Table 5, row 1) which is lower than any reasonable threshold. It means that there are significant differences among groups regarding the mean time to enter the password.

On the other hand, the hypothesis $H2_0$ cannot be rejected: the mean times to enter any password at the end of the first part of the experiment were not statistically significantly different from each other at $P = 0{,}837$ (see Table 5, row 2).

Since $H1_0$ was rejected, we tested the additional hypotheses ($1A\text{-}1_0$, $1A\text{-}2_0$, and $1A\text{-}3_0$) to see which pairs are comparable. As mentioned, multiple (=3) comparisons were performed, so Bonferroni adjustment was used. The results are given in Table 6.

The results show that mean times to enter the first passphrase and psychopass passwords are statistically significantly different at any reasonable threshold. The same holds for the random-psychopass pair. The hypotheses $1A\text{-}1_0$ and $1A\text{-}3_0$ need to be rejected at $P = 0{,}000$ while the hypothesis $1A\text{-}2_0$ cannot be rejected.

3.2. *Results Part II*

The second part of the experiment was implemented after one week from the first part. Here, the participants were asked by the system to enter each of the three previously as-

Table 6
Results of multiple comparisons, Bonferroni adjusted.

Dependent variable	(I) group	(J) group	Mean difference (I-J)	Std. error	Sig.*	95% Confidence interval	
						Lower bound	Upper bound
first_time	random	passphrase	493,075	2936,787	1,000	−6640,05	7626,20
		psychopass	−12940,600*	2936,787	**0,000**	−20073,73	−5807,47
	passphrase	random	−493,075	2936,787	1,000	−7626,20	6640,05
		psychopass	−13433,675*	2936,787	**0,000**	−20566,80	−6300,55
	psychopass	random	12940,600*	2936,787	**0,000**	5807,47	20073,73
		passphrase	13433,675*	2936,787	**0,000**	6300,55	20566,80

* The mean difference is significant at the 0,05 (and at Bonferroni adjusted 0,0167) level.

Table 7
The results of the second part of the experiment: remembered vs. not remembered by password type.

	Random	Passphrase	Psychopass
Did not remember	40	40	36
Did remember	0	0	4
Total	*40*	*40*	*40*

Table 8
Results of Chi-Square test.

	Value	df	Asymp. sig. (2-sided)
Pearson chi-square	8,276	2	**0,016**
Likelihood ratio	9,068	2	**0,011**
N of valid cases	120		

signed passwords. The three-times-and-out system policy was enforced, meaning users had to be successful within three trials. The results – how many participants (of total $n = 40$) remembered their assigned passwords – are presented in Table 7.

The results show that 10% of the participants completing both part of the experiment were able to remember their psychopass password after one week, but no one remembered the random or passphrase-based password. Of all those that have remembered, they were successful only on the third try. Our means to control the password write-down were proven successful. Otherwise, if a participant were able to somehow write down the password, she would have entered it correctly on the first try, not on the third.

We have checked whether the better results in remembering the psychopass passwords are due to chance or is there a systematic reason behind the ease of recall. The chi-square (χ^2) test for independence, also called Pearson's chi-square test or the chi-square test of association, was used to discover if there is a relationship between the categorical variables describing recall ('yes/no') and password type ('random/passphrase/psychopass'). The result of the test is presented in Table 8.

We can see here that $\chi^2 = 8{,}276$, $P = 0{,}016$. This tells us that there is a statistically significant association (at $\alpha < 0{,}05$ level) between password type and recall; that is, dif-

ferent types of passwords are not equally likely to be remembered and hence, psychopass passwords are easier to remember.

4. Discussion and Conclusion

Passwords are the Achilles' heel of modern computing as they are mostly at users' responsibility. The computer community has not made a very much needed shift in password management for almost 40 years. It seems nothing has changed since Robert Morris and Ken Thompson wrote the seminal paper on (UNIX) password security in 1979: the passwords are still the main method of authentication (Creese *et al.*, 2013; Egelman *et al.*, 2013; Lee *et al.*, 2013; Loch *et al.*, 1992; Tzong-Chen and Hung-Sung, 1996; Zviran and Haga, 1990) and the users and their passwords remain the weakest link (Adams and Sasse, 1999; Adams *et al.*, 1997; Notoatmodjo, 2007; Sasse *et al.*, 2001; Tam *et al.*, 2009), and based on the data on numerous breaches, they are still weak and vulnerable to various attacks.

It was observed that most common password creation policies remain vulnerable to off-line attacks and that external password creation policies need to be enforced (Weir *et al.*, 2010), mainly due to a subset of users selecting passwords that (barely) comply with the password policy. For example, a password policy may require the use of mixed uppercase and lowercase letters, at least one symbol and one digit, but the »*PassWord!1*« is nevertheless a weak one.

System and/or security administrators have tried to avoid weak users' passwords by introducing very strict password management policies requiring users to pick and use a system-assigned password. This way they have (inadvertently?) put users to very high memory loads and at the same time, because users tend to write passwords down, to inacceptable security practices and risks.

We designed an experiment where we tested how such strict password management policies reflect in users memorizing their system-assigned passwords.

We first tested the times needed to enter a password produced by three different methods: random, passphrase and psychopass. At the beginning of the experiment, when users typed-in the passwords for the first time, the easiest (and the fastest) password to enter was passphrase, followed by random and psychopass with mean times of 16.894,18, 17.387,25 and 30.327,85 seconds, respectively. The mean times of passphrase and psychopass passwords and of random and psychopass are statistically significantly different at any reasonable threshold, while the pair random-passphrase is not. This finding partially confirms our expectations: the mean times did differ, and the passphrase was easiest (fastest) to enter.

However, at the end of entering (learning) of passwords, the mean times for entering various passwords are not statistically significantly different from each other. This was a surprise, meaning that the users were in average able to enter the PsychoPass-generated password as quickly as the other two. Additional surprise was that the average time to enter any password was around 10 to 11 seconds, although they were of different lengths: 8, 14, and 11 characters for random, passphrase and psychopass, respectively.

None of the participants remembered neither the random string nor passphrase password. However, 4 participants out of 40 (10%) did remember their psychopass password. There is a statistically significant association ($P = 0.016$) between password type and recall, that is the psychopass passwords are easier to remember. This result needs to be taken with a word of caution: they may be *easier* to remember than others, yet they are still difficult to remember.

As a side effect, we found several advantages of the PsychoPass method. First, the main advantage of the method seems to be the memorability of the password, yet this needs to be checked under more lax security policies. Second, a psychopass password looks like a randomly generated one and hence, the attackers cannot recognize it as such. Third, the passwords are currently resilient to dictionary attacks as there are no known dictionaries built and the currently available are useless. Fourth, the method enables the password reuse: the same visual effect can produce several different passwords by just shifting the starting point of the first key. For each of different authentication services a user only needs to know the starting key for a particular service; the visual sequence is always the same. Thus, an attack that would repeat a compromised password on a different service would fail. Further research is needed to show the perceived benefits of the method in settings where users may create their own passwords.

It is true that the PsychoPass method performed better than the other two in terms of memorability and was just as good in terms of usability (speed of typing/entering), however, the results also show that the achieved threshold of 10% is way below expected and previously measured by Zviran and Haga (1993). However, in their research the authors did not control for the password write-down, and hence 23% of their participants 'remembered' the system-assigned (random) password. In our experiment, no one remembered their random password, hence one can conclude that memorability in Zviran and Haga's research can be attributed to write-down effect mainly. Other studies confirm that up to 50% of users write down their passwords (Vu *et al.*, 2007).

Our findings raise a serious question on applicability of strict password management policies not allowing the users to select their own passwords. It is true that system-assigned passwords are hard (or close to impossible) to break using brute force or dictionary attacks, but at the same time users forget them. An adversary who knows the details of password management policy would simply not use brute force or dictionary attacks, but other available means (e.g. shoulder surfing, workplace browsing, garbage shifting, stealing of notes, etc.).

The password management policy implementation is not an easy task. Users should not be considered as an uneducated and ignorant enemy. In many cases system/security administrators can be their own worst enemies. Tightening restriction in one field may open up a new hole in an unexpected way and area. A sound password management policy today needs to implement a dictionary checking and also probabilistic checking (e.g. Markov models based, grammar based, or a combination) to prevent weak passwords.

Acknowledgements. Additional thanks goes to Mr. Renato Ivačič for his help in the experiment phase and implementing the application support.

Funding

The author acknowledges the financial support from the Slovenian Research Agency (research core funding No. P2-0057, project funding No. V5-1725), and from University of Maribor (http://www.um.si, core funding).

References

Abdi, H. (2007). The Bonferonni and Šidák corrections for multiple comparisons. In: Salkind, N.J. (Ed.), *Encyclopedia of Measurement and Statistics*. SAGE Publications, Inc., Thousand Oaks, CA, USA.

Acohido, B. (2013). ANALYSIS: why LivingSocial disclosed huge data theft. *USA Today, April 30*.

Adams, A., Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. https://doi.org/10.1145/322796.322806.

Adams, A., Sasse, M.A., Lunt, P. (1997). Making passwords secure and usable. In: *People and Computers XII*. Springer London, London, pp. 1–19. Chapter 1.

Al-Hudhud, G., Abdulaziz Alzamel, M., Alattas, E., Alwabil, A. (2014). Using brain signals patterns for biometric identity verification systems. *Computers in Human Behavior*, 31(0), 224–229. https://doi.org/10.1016/j.chb.2013.09.018.

Biddle, R., Mannan, M., van Oorschot, P.C., Whalen, T. (2011). User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Information Forensics and Security*, 6(3), 970–979. https://doi.org/10.1109/TIFS.2011.2116781.

Bishop, M., Klein, D.V. (1995). Improving system security via proactive password checking. *Computers & Security*, 14(3), 233–249. https://doi.org/10.1016/0167-4048(95)00003-Q.

Brostoff, A.S. (2004). *Improving Password System Effectiveness*. PhD Thesis, Department of Computer Science, University College London. Doctor of Philosophy, University of London, London, UK.

Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6), 641–651. https://doi.org/10.1002/acp.1014.

Brumen, B., Černezel, A. (2014). Brute force analysis of PsychoPass-generated passwords. In: *37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 26–30 May 2014.

Brumen, B., Heričko, M., Rozman, I., Hölbl, M. (2013). Security analysis and improvements to the PsychoPass method. *Journal of Medical Internet Research*, 15(8), e161. https://doi.org/10.2196/jmir.2366. PMID: 23942458.

Buehler, B., Mrasek, N. (2018). Average new-car prices rise nearly 4 percent for January 2018 on shifting sales mix. Retrieved from https://mediaroom.kbb.com/2018-02-01-Average-New-Car-Prices-Rise-Nearly-4-Percent-for-January-2018-on-Shifting-Sales-Mix-According-to-Kelley-Blue-Book. Accessed: 2018-10-09. Archived by WebCite® at http://www.webcitation.org/7329ILsmT.

Cipresso, P., Gaggioli, A., Serino, S., Cipresso, S., Riva, G. (2012). How to create memorizable and strong passwords. *Journal of Medical Internet Research*, 14(1), e10. https://doi.org/10.2196/jmir.1906. PMID: 22233980.

Corbató, F.J. (1991). On building systems that will fail. *Communications of the ACM*, 34(9), 72–81. https://doi.org/10.1145/114669.114686.

Cox, J. (2012). Information systems user security: a structured model of the knowing–doing gap. *Computers in Human Behavior*, 28(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003.

Creese, S., Hodges, D., Jamison-Powell, S., Whitty, M. (2013). Relationships between password choices, perceptions of risk and security expertise. In: *Human Aspects of Information Security, Privacy, and Trust. First International Conference, HAS 2013, Held as Part of HCI International 2013*, Las Vegas, NV, July 2013, Vol. 8030. Springer, pp. 80–89.

Davinson, N., Sillence, E. (2010). It won't happen to me: promoting secure behaviour among Internet users. *Computers in Human Behavior*, 26(6), 1739–1747. https://doi.org/10.1016/j.chb.2010.06.023.

Davis, D., Monrose, F., Reiter, M.K. (2004). On user choice in graphical password schemes. In: *The USENIX 2004 Security Symposium*.

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. https://doi.org/10.1016/j.ijhcs.2005.04.020.

Dell'Amico, M., Michiardi, P., Roudier, Y. (2010). Password strength: an empirical analysis. In: *The INFOCOM, 2010 Proceedings IEEE*.

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., Herley, C. (2013). Does my password go up to eleven? The impact of password meters on password selection. In: *Proceedings of the 2013 SIGCHI Conference on Human Factors in Computing Systems*, April 27–May 2, Paris, France.

FBI (2018). *Motor Vehicle Theft, Uniform Crime Report. Crime in the United States, 2017*. US Department of Justice – Federal Bureau of Investigation, Washington, DC, USA. Retrieved from https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/motor-vehicle-theft.pdf.

FIPS (1985). *PUB 112 Password Usage*. National Institute of Standards and Technology.

Florencio, D., Herley, C. (2007). A large-scale study of web password habits. In: *The Proceedings of the 16th International Conference on World Wide Web*.

Ganesan, R., Davies, C., Atlantic, B. (1994). A new attack on random pronounceable password generators. In: *Proceedings of the 17th {NIST}-{NCSC} National Computer Security Conference*, Baltimore, MD, USA.

Gao, W., Wang, G.L., Chen, K.F., Wang, X.L. (2017). Generic construction of certificate-based signature from certificateless signature with provable security. *Informatica*, 28(2), 215–235. https://doi.org/10.15388/Informatica.2017.127.

Gasser, M. (1975). *A Random Word Generator for Pronounceable Passwords, MTR-3006, ESD-TR-75-97, AD-A017676*. MITRE Corporation, Bedford, Mass.

Gates, B. (1997). Speech delivered at COMDEX 1997. http://web.archive.org/web/20090114203618/http://www.microsoft.com/presspass/exec/billg/speeches/1997/comdex97.aspx Accessed: 2014-10-20. Archived by WebCite® at http://www.webcitation.org/6JBczPMqN.

Gehringer, E.F. (2002). Choosing passwords: security and human factors. In: *2002 International Symposium on Technology and Society (ISTAS'02)*.

Gosney, J.M. (2018). 8x Nvidia GTX 1080 Ti Hashcat Benchmarks. https://gist.github.com/epixoip/ace60d09981be09544fdd35005051505/. Archived by WebCite® at http://www.webcitation.org/70yRle0jv.

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz N.B., Danker J.M., Choong Y.-Y., Greene K.K., Theofanos, M.F. (2017). *NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management*. Retrieved from Gaithersburg, MD, USA.

Gressin, S. (2017). *The Equifax Data Breach: What to Do*. Federal Trade Commission, Washington, DC.

Grosse, E., Upadhyay, M. (2013). Authentication at scale. *Security & Privacy*, 11(1), 15–22, https://doi.org/10.1109/MSP.2012.162.

Hachman, M. (2011). PlayStation Hack to Cost Sony $171 M; Quake Costs Far Higher. Retrieved from http://www.pcmag.com/article2/0,2817,2385790,00.asp. Accessed: 2014-01-30. Archived by WebCite® at http://www.webcitation.org/6N0tPpBte.

Hölbl, M., Welzer, T., Brumen, B. (2008). Improvement of the Peyravian–Jeffries's user authentication protocol and password change protocol. *Computer Communications*, 31(10), 1945–1951. https://doi.org/10.1016/j.comcom.2007.12.029.

Hölbl, M., Welzer, T., Brumen, B. (2010). Two proposed identity-based three-party authenticated key agreement protocols from pairings. *Computers & Security*, 29(2), 244–252. https://doi.org/10.1016/j.cose.2009.08.006.

Hölbl, M., Welzer, T., Brumen, B. (2012). An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences*, 78(1), 142–150. https://doi.org/10.1016/j.jcss.2011.01.002.

Horcher, A.-M., Tejay, G.P. (2009). Building a better password: the role of cognitive load in information security training. In: *IEEE International Conference on Intelligence and Security Informatics, 2009, ISI'09*.

Jiang, P., Wen, Q., Li, W., Jin, Z., Zhang, H. (2013). An anonymous user authentication with key agreement scheme without pairings for multiserver architecture using SCPKs. *The Scientific World Journal*. https://doi.org/10.1155/2013/419592. Article ID 419592.

Johnson, G.J. (1991). A distinctiveness model of serial learning. *Psychological Review*, 98(2), 204–217. https://doi.org/10.1037/0033-295X.98.2.204.

Jones, S.N. (2017). Having an affair may shorten your life: the ashley Madison suicides. *Georgia State University Law Review*, 33(2), 6.

Kamp, P.-H. (2012). LinkedIn password leak: salt their hide. *ACM Queue*, 10(6), 20. Available online at http://queue.acm.org/detail.cfm?id$=$2254400&ref=fullrss. Accessed: 2252013-2254410-2254420. Archived by WebCite® at http://www.webcitation.org/2254406JBdHEdhy.

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. https://doi.org/10.1016/j.ijhcs.2006.08.005.

Kerber, R. (2007, August 15). Cost of data breach at TJX soars to $256 m. *Boston Globe*.

Khan, J.S., Khan, M.A., Ahmad, J., Hwang, S.O., Ahmed, W. (2017). An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes. *Informatica*, 28(4), 629–649. https://doi.org/10.15388/Informatica.2017.149.

Kirk, J. (2012). How Charles Dickens Helped Crack Your LinkedIn Password. *PCWorld*, June 8, 2012.

Krim, J., Barbaro, M. (2005). 40 million credit card numbers hacked. *The Washington Post*, June 18, 2005.

Kuo, C., Romanosky, S., Cranor, L.F. (2006). Human selection of mnemonic phrase-based passwords In: *The Proceedings of the Second Symposium on Usable Privacy and Security*, July 12–14, Carnegie Mellon University, Pittsburgh, PA, USA.

Lee, C.-C., Liu, C.-H., Hwang, M.-S. (2013). Guessing attacks on strong-password authentication protocol. *International Journal of Network Security*, 15(1), 64–67.

Liaojun, P., He, L., Pei, Q., Wang, Y. (2013). Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard. Shanghai, China. In: *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, Shanghai, China.

Loch, K.D., Carr, H.H., Warkentin, M.E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173–186. https://doi.org/10.2307/249574.

Meshram, C., Tseng, Y.-M., Lee, C.-C., Meshram, S.G. (2017). An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP. *Informatica*, 28(3), 471–484. https://doi.org/10.15388/Informatica.2017.139.

Miller, G.A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, 63(2).

Morris, R., Thompson, K. (1979). Password security: a case history. *Communications of the ACM*, 22(11), 594–597.

Nelson, D., Vu, K.-P.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. https://doi.org/10.1016/j.chb.2010.01.007.

Notoatmodjo, G. (2007). *Exploring the 'Weakest Link': a Study of Personal Password Security*. MSc thesis, The University of Auckland, New Zealand.

Pascual, A., Marchini, K., Miller, S. (2018). *2018 Identity Fraud: Fraud Enters a New Era of Complexity*. Retrieved from https://www.javelinstrategy.com/printpdf/58296.

Pereira, J. (2007). How credit-card data went out wireless door. *The Wall Street Journal*, 4.

Pfleeger, C.P., Pfleeger, S.L. (2003). *Security in Computing*. 3rd ed., Prentice Hall PTR, Upper Saddle River, NY, USA.

Popkin, H.A.S. (2012). LinkedIn confirms password leak, eHarmony has one, too. *ABC NEWS Technology*,

PRC (2018). Privacy Rights Clearinghouse. Chronology of Data Breaches. *Security Breaches 2005 – Present*. Retrieved from https://www.privacyrights.org/data-breaches. Accessed: 2018-10-09. Archived by WebCite® at http://www.webcitation.org/732CmnPm2.

Sahadi, J. (2005). 40M credit cards hacked. *CNN Money*, July 27, 2005.

Sakalauskas, E., Mihalkovich, A. (2017). Improved asymmetric cipher based on matrix power function resistant to linear algebra attack. *Informatica*, 28(3), 517–524. https://doi.org/10.15388/Informatica.2017.142.

Sangani, K. (2011). Sony security laid bare. *Engineering & Technology*, 6(8), 74–77. https://doi.org/10.1049/et.2011.0810.

SASA (2013). *On-Line List of Words in Slovenian language (Spletni Seznam Besed Slovenskega Jezika)*. Slovenian Academy of Sciences and Arts, Ljubljana, Slovenia. Retrieved from http://bos.zrc-sazu.si/sbsj.html. Accessed: 2014-10-20. Archived by WebCite® at http://www.webcitation.org/6JG7LCr5o.

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. https://doi.org/10.1023/A:1011902718709.

Scarfone, K., Souppaya, M. (2009). Guide to enterprise password management (draft). *NIST Special Publication*, 800, 118.

Schneier, B. (2005). *Write Down Your Password. Schneier on Security*, June 17, 2005.

Seeley, D. (1989). Password cracking: a game of wits. *Communications of the ACM*, 32(6), 700–703. https://doi.org/10.1145/63526.63529.

Spafford, E.H. (1989). Crisis and aftermath. *Communications of the ACM*, 32(6), 678–687. https://doi.org/10.1145/63526.63527.

Spector, Y., Ginzberg, J. (1994). Pass-sentence – a new approach to computer code. *Computers & Security*, 13(2), 145–160. https://doi.org/10.1016/0167-4048(94)90064-7.

Stallings, W. (2006). *Cryptography and Network Security: Principles and Practices*. 4th ed., Prentice-Hall, Upper Saddle River, NJ.

StClair, L., Johansen, L., Enck, W., Pirretti, M., Traynor, P., McDaniel, P., Jaeger, T. (2006). Password exhaustion: predicting the end of password usefulness. In: *Information Systems Security*. Springer, pp. 37–55.

Stoll, C.P. (1988). Stalking the wily hacker. *Communications of the ACM*, 31(5), 484–497. https://doi.org/10.1145/42411.42412.

Stoll, C.P. (1989). *The Cuckoo's Egg: Tracing a Spy Through the Maze of Computer Espionage*. Doubleday, New York, NY, USA.

Suo, X., Zhu, Y., Owen, G.S. (2005). *Graphical passwords: a survey*. In: *The 21st Annual Computer Security Applications Conference*, Tucson, AZ, USA.

Tam, L., Glassman, M., Vandenwauver, M. (2009). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3), 233–244. https://doi.org/10.1080/01449290903121386.

Tom, P.L. (1991). *Managing Information as a Corporate Resource*. 2nd ed., HarperCollins Publishers.

Tzong-Chen, W., Hung-Sung, S. (1996). Authenticating passwords over an insecure channel. *Computers & Security*, 15(5), 431–439. https://doi.org/10.1016/0167-4048(96)00004-1.

USA (1996). *Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, One Hundred Fourth Congress, Second Session*, May 22, June 5, 25, and July 16, 1996, Vol. 104. Government Printing Office, Washington, DC, USA.

Verheul, E.R. (2006). Selecting secure passwords. In: *Topics in Cryptology–CT-RSA 2007*. Springer, pp. 49–66.

Vijayan, J. (2007a). Scope of tjx data breach doubles: 94M cards now said to be affected. *Computerworld*, October 24, 2007.

Vijayan, J. (2007b). TJX data breach: at 45.6 M card numbers, it's the biggest ever. *Computerworld*, March 29, 2007.

Vu, K.-P.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65(8), 744–757. https://doi.org/10.1016/j.ijhcs.2007.03.007.

Weigel, F.K., Hazen, B.T. (2014). Technical proficiency for IS success. *Computers in Human Behavior*, 31(1), 27–36. https://doi.org/10.1016/j.chb.2013.10.014.

Weir, M., Aggarwal, S., Collins, M., Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In: *Proceedings of the 17th ACM Conference on Computer and Communications Security*, Chicago, IL, USA.

Weirich, D., Sasse, M.A. (2001). Persuasive password security. In: *CHI'01 Extended Abstracts on Human Factors in Computing Systems*.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N. (2005). PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1), 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010.

Woods, N., Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, 111, 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002.

Workman, M., Bommer, W.H., Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.

Wu, J.D., Tseng, Y.M., Huang, S.S., Chou, W.C. (2018). Leakage-resilient certificateless key encapsulation scheme. *Informatica*, 29(1), 125–155. https://doi.org/10.15388/Informatica.2018.161.

Yan, J., Blackwell, A., Anderson, R., Grant, A. (2000). *The Memorability and Security of Passwords: Some Empirical Results*. Cambridge, UK.

Yan, J., Blackwell, A., Anderson, R., Grant, A. (2004). Password memorability and security: empirical results. *IEEE Security & Privacy*, 2(5), 25–31. https://doi.org/10.1109/MSP.2004.81.

Zviran, M., Haga, W.J. (1990). Cognitive passwords: the key to easy access control. *Computers and Security*, 9(8), 723–736. https://doi.org/10.1016/0167-4048(90)90115-A.

Zviran, M., Haga, W.J. (1993). A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, 36(3), 227–237.

Zviran, M., Haga, W.J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, 15, 161–186.

B. Brumen received his doctor's degree in informatics, in 2004. He is an associate professor of informatics and tourism at University of Maribor. He was Secretary General (Provost) of University of Maribor for two consecutive terms between 2004 and 2011. Now he's serving as a dean of Faculty of Tourism. His research interests include data security and privacy, data analysis, automated learning, and technologies in tourism. He represents Slovenia in EU's Smart Specialisation platform "Digitalisation and Safety for Tourism".