MementoKey: *Keeping Passwords in Mind*

Bongkeum Jeong
ITI/LARSyS, M-ITI, University of Madeira
Funchal, Madeira, Portugal
bongkeum.jeong@m-iti.org

Chris Csikszentmihalyi
ITI/LARSyS, M-ITI, University of Madeira
Funchal, Madeira, Portugal
csik@m-iti.org

Dulce Pacheco
ITI/LARSyS, M-ITI, University of Madeira
Funchal, Madeira, Portugal
dulce.pacheco@m-iti.org

Alexander Vallat
Imperial College
London, United Kingdom
mementokey@alex.vallat.name

Junwu Park
ITI/LARSyS, M-ITI, University of Madeira
Funchal, Madeira, Portugal
upop-junwu.park@m-iti.org

ABSTRACT

In this paper, we introduce a novel system of password generation, MementoKey, consisting of private words that exist only in a user's memory and a corresponding set of public (non-secret) words that will facilitate users' recall of the private words, which they are associated with. We will demonstrate how MementoKey offers a useful alternative to existing options for storing passwords in password managers, or to using cryptographically weak, but memorable, passwords. We have conducted a user study to evaluate the word-association technique for recalling passwords, and the effectiveness

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland Uk

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3313066

of our prototype software training and checking system to guide the user successfully through the memorization process.

Our study involving 60 diverse participants indicates that our prototype can effectively lead users through a visualization and memorization technique to create a strong word-association memory between pairs of adjectives and nouns.

KEYWORDS

Cyber Security, Human and Computer Collaboration, Password manager, Passwords

INTRODUCTION

The limitations and difficulties of creating and remembering secure passwords are well known. Password recommendations are usually for a combination of at letters and numbers, with a minimum length of 8 (or sometime more). Many sites and services also recommend changing the password frequently [7]. More critical sites and services suggest the use of a password manager, but these have not been widely adopted [1].

This may be due to a combination of multiple factors. Users can be reluctant to trust their passwords to a cloud service, and may need to use passwords when they are not on their own device, or even on the internet. It only take one instance of needing a password and not having access to it to frustrate a user into using a (probably insecure) memorable password instead.

There have been many studies on how people choose and reuse passwords. Some studies analyze real passwords through leaked datasets [2, 4, 8, 10, 12] or browser plug-ins [5, 11] to figure out trends related to weak password and password reuse [6]. All this work has highlighted a number of issues, which are well known: secure passwords are difficult to remember, users have too many passwords, and have difficulty matching their passwords to accounts. These problems lead users to develop insecure coping mechanisms, such as picking passwords that are memorable but easy for attackers to guess, reusing passwords across multiple accounts, or writing passwords down [9]. Vulnerable passwords, which are set up to be easy to remember, pose a risk of being hacked at any time. However, these methods do not allow us to explain why users create bad password habits [6]. The present study proposes a design to address a number of problems that have been addressed in previous studies, and to overcome security vulnerabilities in the creation and use of passwords in a novel and more effective way.

Our prototype involves a guided process of generating and learning words to create a new password. A set of four word pairs is generated, and at the end of the process the user will have memorized one set of words to use as a password. Although the use of this new type of password system is initially more onerous than using an insecure memorable short password, the investment of the time necessary to memorize a strong password may be offset by the benefits of increased cyber security. Previous studies and cryptographic analysis have demonstrated that a password consisting of four randomly selected English words has significantly higher entropy (and therefore security) than the usual 8 characters-and-numbers recommendation. However, this only applies if the words are randomly selected, not grammatically related phrases [8]. Our study aims to demonstrate the possibility of also making these four-word passwords far more memorable than the alternative. Further work could be done in the future to quantify the effect on both memorability and security of increasing the number of words, to validate the optimal number to use as a balance between security and ease of memorization.

The study aims to validate the hypothesis that using a word association system of pairing an adjective with a noun will result in increased recall ability over simply trying to remember four unassociated words. Further, we aim to show that our word learning assistant guided training software will produce even greater improved recall compared to simply being shown word pairs and asked to memorize them. To that end, we split our participants into three groups. Group 1 is our control group, and will simply be asked to memorize four words. Group 2 will be shown four word pairs, and asked to memorize the second word in each pair, being shown the first as a reminder later. Group 3 will be taken through the full-guided learning process by our software to form strong associations between the paired words.

We anticipate that Group 2 will demonstrate improved recall over Group 1, which will indicate that simply being shown two words together is enough for one of those words to act as a prompt to assist recall in the other, even without specific training or techniques to forge a strong word association. Further, we anticipate that Group 3 will demonstrate improved recall over both Groups 1 and 2, which will validate the effectiveness of the software-led "Learn Words" system to create and reinforce a strong, long-lasting word association between an adjective and noun pairs.

The experimental protocol involved checking the recall of the participants after an interval of one hour following memorization, one day, one week, and finally one month. Everyone who participated in the experiment had personally reported some history of failing to remember their user name or password when attempting to access previously registered accounts after long periods.

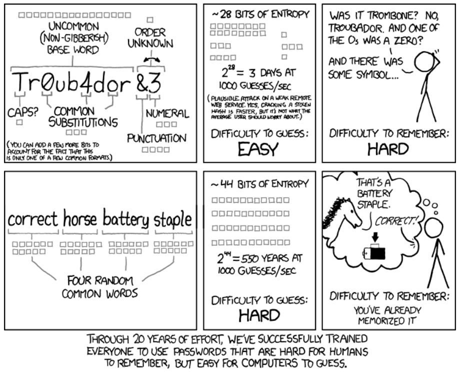

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Figure 1: xkcd 936 - Password Strength

CRYPTOGRAPHIC SECURITY

In this brief paper we will not be presenting a full cryptographic analysis of the security of a four word password compared to an 8-character one. Other studies have already addressed this area [3], and it has even begun to pass into (semi-) public awareness (Figure 1, a popular webcomic).

It is worth emphasizing that multi-word pass-phrase passwords are only cryptographically strong when the words are randomly generated - allowing the user to choose their own words weakens the security significantly [8]. For this reason, MementoKey does not allow users to choose their own words, but instead concentrates on assisting the user with memorizing words that have been randomly generated.

Naturally a longer traditional password (16 characters or greater) would represent even greater cryptographic security, however at that length it is unrealistic to expect users to memorize them (if truly randomly generated), and instead is the domain of password manager software.

PROTOTYPES

In this section, we present the current MememtoKey prototype design. The use of the prototype begins with the creation of a new password after entering a username and a site name on the main screen. A list of word pairs of adjectives and nouns are generated. The adjectives form the public key are used as a memento to aid recall of the nouns, which are the private key. After the private keywords have been memorized, they are discarded. They are never recorded or stored, and once the page has been closed are irretrievable.

The public keywords, however, can always be re-obtained simply by providing the username and site name. The key words are derived by hashing these, so no cloud or local storage is required âĂŞ no user-specific password database is maintained. For the sake of the study, we plan to have a dictionary of 1,024 adjectives to pick from for the Public key, and around 5,000 noun words for the Private key.

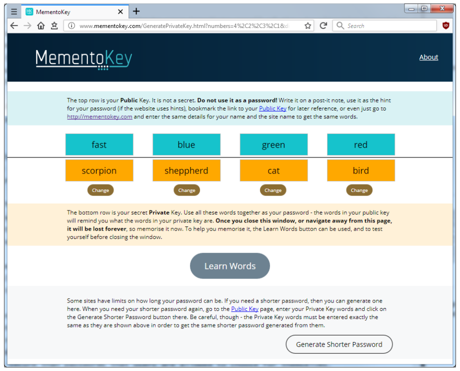
The system places a total of eight-word boxes in the center of the screen, showing the public words in the top four blue boxes and the private words in the bottom four pink boxes. The public key in the blue boxes at the top helps you remember the private key just below it (Figure 2).

Although it is important for security that the words be randomly generated, rather than user-selected, we do provide a "Change" button to allow the user to reject any of the words and replace it with another randomly generated one. This is intended in case the user doesn't know the meaning of the word, or would be unable to spell it, or finds it offensive or otherwise undesirable in any way.

The aim of the process is to create the passwords that will only exist in the user's memory, so to assist with this a "Learn Words" process is provided to guide the user through the word-association method of memorization (Figures 3 and 4).

The Learn Words process offers step-by-step instructions. In the first step, the system shows an adjective and a noun together, for example, a "web keyboard", and asks you to visualize this as a funny image. When this picture is clear, we can move on to the next stage.

In the second step of Learn words, the system checks your immediate recall of the visualization by asking you to pick, from a small set of multiple choice words, the correct noun that matches the adjective. In the final step, the user must type the noun correctly into a free-entry textbox, with no multiple-choice options available (Figure 4). Throughout the process, learning steps and checking


MementoKey
www.mementokey.com/GeneratePrivateKey.html?numbers=4%2C2%2C3%2C1&d
Search
MementoKey
About

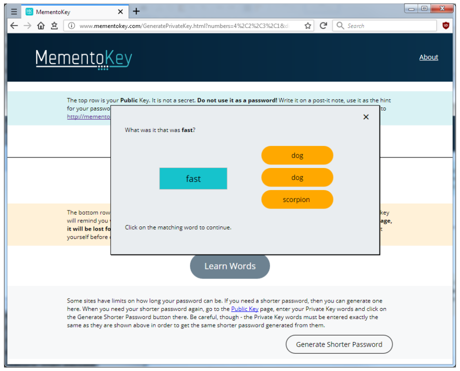
The top row is your **Public** Key. It is not a secret. **Do not use it as a password!** Write it on a post-it note, use it as the hint for your password (if the website uses hints), bookmark the link to your Public Key for later reference, or even just go to http://mementokey.com and enter the same details for your name and the site name to get the same words.

fast	blue	green	red
scorpion	sheppherd	cat	bird
Change	Change	Change	Change

The bottom row is your secret **Private** Key. Use all these words together as your password - the words in your public key will remind you what the words in your private key are. **Once you close this window, or navigate away from this page, it will be lost forever**, so memorise it now. To help you memorise it, the Learn Words button can be used, and to test yourself before closing the window.

Some sites have limits on how long your password can be. If you need a shorter password, then you can generate one here. When you need your shorter password again, go to the Public Key page, enter your Private Key words and click on the Generate Shorter Password button there. Be careful, though - the Private Key words must be entered exactly the same as they are shown above in order to get the same shorter password generated from them.

Figure 2: Pairs of private and public words for memorization


MementoKey
www.mementokey.com/GeneratePrivateKey.html?numbers=4%2C2%2C3%2C1&d
Search
MementoKey
About

The top row is your **Public** Key. It is not a secret. **Do not use it as a password!** Write it on a post-it note, use it as the hint for your passwo … to http://memento…

What was it that was **fast**?

Click on the matching word to continue.

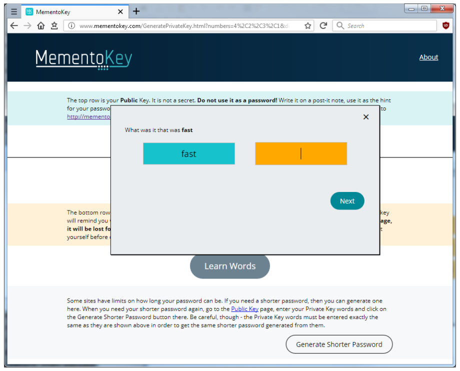
The bottom row … key will remind you … **age, it will be lost fo**… yourself before …

Some sites have limits on how long your password can be. If you need a shorter password, then you can generate one here. When you need your shorter password again, go to the Public Key page, enter your Private Key words and click on the Generate Shorter Password button there. Be careful, though - the Private Key words must be entered exactly the same as they are shown above in order to get the same shorter password generated from them.

Figure 3: Word learning assistant with a multiple choice question

steps are interspersed for each of the four words, with the system backtracking to re-check the words that the user previously had difficulty with.

Once the user has demonstrated accurate learning of the word pairs, the association of words from the public key to the private key is complete and can function as a password that the real computer users will use.


MementoKey
www.mementokey.com/GeneratePrivateKey.html?numbers=4%2C2%2C3%2C1&d
Search
MementoKey
About
fast
Next
Learn Words
Generate Shorter Password

The top row is your **Public** Key. It is not a secret. **Do not use it as a password!** Write it on a post-it note, use it as the hint for your passwo to http://memento

What was it that was **fast**

The bottom row key will remind you **age,** **it will be lost fo** t yourself before

Some sites have limits on how long your password can be. If you need a shorter password, then you can generate one here. When you need your shorter password again, go to the Public Key page, enter your Private Key words and click on the Generate Shorter Password button there. Be careful, though - the Private Key words must be entered exactly the same as they are shown above in order to get the same shorter password generated from them.

Figure 4: Word learning assistant with a free-entry question

USER STUDY

The sample set was divided into three groups, consisting of one control group, one intermediate group, and one experimental group. 20 people were allocated for each group.

Group 1 was not offered the public words, but only shown the four private words to memorize as their password. Group 2 was shown both the public and private words, but given no further assistance than informing them that the public words would be available to them as a reminder. Group 3 were given access to the full word-learning assistant described in the previous section.

As can be seen from the results in Figure 5, Group 1 demonstrated a marked decline in recall after each increasing interval. Group 2 performed better than Group 1, and Group 3 had the highest performance of all, maintaining high recall even after the one-month interval.

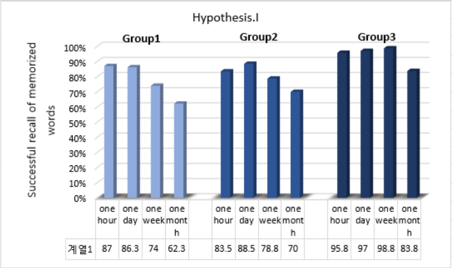


Figure 5: Results of password recall user testing study

CONCLUSIONS

The MementoKey prototype presents a usable system for generating passwords by randomly generated word pairs. These four-random-word passwords are of an equivalent entropy (and therefore cryptographic security) as a randomly generated password following usual password complexity rules, and are significantly more secure than passwords that users are allowed to choose for themselves.

Our user validation study supports the hypothesis that we can improve on previous work which simply presents random words for memorization by introducing word pairs and visual association.

FURTHER WORK

There are two areas of further work to pursue for this project. Firstly, formal cryptographic analysis of the strength of the generated passwords, based on the word-lists used. Secondly, more user studies are required to validate the real-world use of these passwords. Although the study we present in this paper demonstrates the initial viability of the concept, it will also be necessary to perform another guided study to investigate simultaneous memorization of multiple passwords, and a long term unguided study of real-world usage of memorized passwords by users. Finally, a variability study of the effect of number of words versus memorability and security would be useful to find the optimal balance to use.

ACKNOWLEDGMENTS

The LARSyS has been funding this project, UID/EEA/50009/2019. Acknowledgement to ARDITI-Agência Regional para o Desenvolvimento e Tecnologia under the scope of the Project M1420-09-5369-FSE-00000. Also supported by the Regional Development European Funds, for the Operational Program Madeira 14-20 (M1420-01-0145-FEDER-000002).

REFERENCES

[1] Nora Alkaldi and Karen Renaud. 2016. Why do people adopt, or reject, smartphone password managers? (2016).

[2] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP '12)*. IEEE Computer Society, Washington, DC, USA, 538–552. https://doi.org/10.1109/SP.2012.49

[3] Marco Antônio Carnut and Evandro Curvelo Hora. 2005. Improving the Diceware memorable passphrase generation system. In *Proceedings of the 7th International Symposium on System and Information Security. São José dos Campos: CTA/ITA/IEC*.

[4] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. *Proceedings 2014 Network and Distributed System Security Symposium* February (2014), 23–26. https://doi.org/10.14722/ndss.2014.23357

[5] Dinei Florencio and Cormac Herley. 2007. A Large-scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW '07)*. ACM, New York, NY, USA, 657–666. https://doi.org/10.1145/1242572.1242661

[6] Ameya Hanamsagar, Simon S. Woo, Chris Kanich, and Jelena Mirkovic. 2018. Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 570, 12 pages. https://doi.org/10.1145/3173574.3174144

[7] Bongkeum Jeong. 2017. Designing for Passwords. In *HCIK 2017*. HCIK, HCIK, Seoul.

[8] Ashwini Rao, Birendra Jha, and Gananand Kini. 2013. Effect of Grammar on Security of Long Passwords. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)*. ACM, New York, NY, USA, 317–324. https://doi.org/10.1145/2435349.2435395

[9] Elizabeth Stobert and Robert Biddle. 2014. A Password Manager That Doesn'T Remember Passwords. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14)*. ACM, New York, NY, USA, 39–52. https://doi.org/10.1145/2683467.2683471

[10] Rafael Veras, Christopher Collins, and Julie Thorpe. 2014. On the semantic patterns of passwords and their security impact. NDSS.

[11] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used Across Websites. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (SOUPS'16)*. USENIX Association, Berkeley, CA, USA, 175–188. http://dl.acm.org/citation.cfm?id=3235895.3235911

[12] Matt Weir, Sudhir Aggarwal, Breno de Medeiros, and Bill Glodek. 2009. Password Cracking Using Probabilistic Context-Free Grammars. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy (SP '09)*. IEEE Computer Society, Washington, DC, USA, 391–405. https://doi.org/10.1109/SP.2009.8