Analysis of the Security and Memorability of the *Password Card*

Peter Mayer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
peter.mayer@secuso.org

Alexandra Kunz
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
alexandra.kunz@secuso.org

Melanie Volkamer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
Privacy and Security Research Group
Karlstad University
melanie.volkamer@secuso.org

ABSTRACT

Choosing and remembering secure passwords poses a problem to users. The *password card* is a proposal intended to help users to cope with this problem. It is a paper card with a grid of random letters, numbers, and symbols, on which users choose a starting point and a walk of adjacent cells. The characters on the traversed cells form the new password. We analyze the security and memorability of passwords created this way. We find that users mostly choose predictable walks and starting points. At the same time, memorability of the passwords seems low. Thus, the password card seems to fail in helping users to choose and remember secure passwords.

1 INTRODUCTION

While text passwords are the most widely used authentication scheme, choosing and remembering hard to guess text passwords is a challenge for users [8]. Proposals trying to help users to cope with this problem include electronic means (i.e. password managers [6]) and analog means (i.e. means to securely take notes of passwords such as securely stored password logbooks [4]). While there exists a vast amount of literature examining the security (e.g. [5]) and the usability (e.g. [3]) of password managers, the security and usability of analog means are an uncharted area.

The goal of this work is to evaluate the security and memorability claims of one specific analog means: the *password card*. It is a paper card (roughly the size of a credit card), with a grid of random letters, numbers, and symbols. To create a password, users choose a starting point and then a walk of adjacent cells (see fig. 1).

We evaluated the security and memorability of this solution in a user study with 30 participants. Our results indicate that the most popular walks chosen by the participants are straight horizontal lines and that the starting points are not randomly dispersed on the grid. At the same time, memorability of the passwords seems low.

2 THE PASSWORD CARD

The password card was proposed to help users choosing and remembering secure text passwords [7]. It consists of a grid filled with letters, numbers, and symbols (see fig. 2). The grid's coordinates are the letters A-Z for the x-axis and the numbers 1-12 for the y-axis. As the letters, numbers, and symbols in the grid are the same for all users, losing the password card does not pose an availability problem and the card does not need to be kept secret.

To create a password with the password card, the user chooses a starting point and then creates a walk of adjacent cells in the grid with a length of at least 8. The characters traversed in that walk form the new password (see fig. 1 for an example). Usage instructions are printed on the card below the grid and on its back.

3 METHODOLOGY

To evaluate the security and memorability of passwords created with the password card, we conducted a user study. The study meets all requirements of our university's ethics commission. Participants were recruited on the street and by word of mouth. Overall 30 participants were recruited for the study. Each participant received 5€ as compensation. The study's procedure comprised five phases and took overall about 20 minutes for each participant:

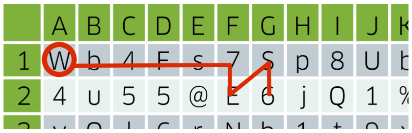
Phase 1: The participants received a brief introduction to the password card. Then, they were given a password card to familiarize themselves with it (including reading the information on its back).

Phase 2: After familiarization with the password card, the participants received a first questionnaire. In this questionnaire the participants were asked if they had already known the password card before the study, and if so, whether they also use it.

Phase 3: Having answered the first questionnaire, the participants were asked to create passwords for the three purposes "primary e-mail", "online banking", and "online forum" by using the password card. Each password was created using a separate paper password card one after the other. The participants were instructed to create the passwords according to the instructions on the card, i.e. choosing a starting point and creating a walk containing at least eight characters. The participants marked the starting point with a circle and the walk with a line through the respective grid cells (as shown in fig. 1). Then, the cards were collected.

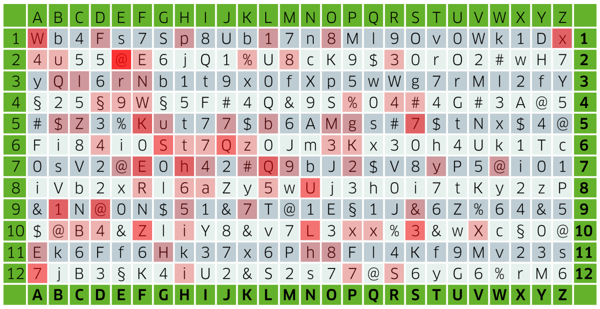
Phase 4: As distraction after creating the passwords, the participants answered a second questionnaire, including questions regarding demographic data (e.g. age, gender) and further questions regarding the use of the password card (e.g. whether they would use it in the future). Answering it took about 5-10 minutes.

Phase 5: Lastly, participants were asked whether they remembered the three passwords they created before. To verify whether the participants' perception of the extend to which they remembered the passwords is correct, the participants had to mark their passwords on three empty password cards analogously to phase 3. Then, the participants were asked about their choice of passwords (i.e. starting points and walks). Finally, they were informed about the purpose of the study and received their compensation.



	A	B	C	D	E	F	G	H	I	J	K
1	W	b	4	F	s	7	S	p	8	U	b
2	4	u	5	5	@	E	6	j	Q	1	%

Figure 1: An example for a walk in the password card corresponding to the password "Wb4Fs7ES6".



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	W	b	4	F	s	7	S	p	8	U	b	1	7	n	8	M	l	9	O	v	0	W	k	1	D	x	1
2	4	u	5	5	@	E	6	j	Q	1	%	U	8	c	K	9	$	3	0	r	O	2	#	w	H	7	2
3	y	Q	l	6	r	N	b	1	t	9	x	0	f	X	p	5	w	W	g	7	r	M	l	2	f	Y	3
4	§	2	5	§	9	W	§	5	F	#	4	Q	&	9	S	%	0	4	#	4	G	#	3	A	@	5	4
5	#	$	Z	3	%	K	u	t	7	7	$	b	6	A	M	g	s	#	7	$	t	N	x	$	4	@	5
6	F	i	8	4	i	0	S	t	7	Q	z	0	J	m	3	K	x	3	0	h	4	U	k	1	T	c	6
7	0	s	V	2	@	E	0	h	4	2	#	Q	9	b	J	2	$	V	8	y	P	5	@	i	0	1	7
8	i	V	b	2	x	R	l	6	a	Z	y	5	w	U	j	3	h	0	i	7	t	K	y	2	z	P	8
9	&	1	N	@	0	N	$	5	1	&	7	T	@	1	E	§	1	J	&	6	Z	%	6	4	&	5	9
10	$	@	B	4	&	Z	l	i	Y	8	&	v	7	L	3	x	x	%	3	&	w	X	c	§	0	@	10
11	E	k	6	F	f	6	H	k	3	7	x	6	P	h	8	F	l	4	K	f	9	M	v	2	3	s	11
12	7	j	B	3	§	K	4	i	U	2	&	S	2	s	7	7	@	S	6	y	G	6	%	r	M	6	12
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	

Figure 2: Heatmap of all the starting points chosen by the participants in our study.

4 RESULTS

The sample was relatively even distributed with respect to gender (13 male, 17 female participants). The age of the participants ranged from 19 to 70 years with a mean of 34.2 years.

4.1 Security

The security of the passwords created with the password card depends on whether (a) the starting points are randomly dispersed on the grid and (b) the walks are not predictable.

To investigate the dispersion of starting points, we use the spatial $J(r)$ statistic as proposed for security analysis in [2], where r is the radius around each point considered for the dispersion. $J(r)$-values close to 1 represent a random distribution of the starting points (as would be desirable for password security). $J(r)$-values below 1 indicate clustering. $J(r)$-values above 1 indicate spatial regularity. With $J(2) = 0.785$, the starting points seem to be somewhat clustered. The heatmap in Figure 2 illustrates the dispersion. The answers regarding the participants reasons for choosing the starting points shed further light on this result. The coordinates of the starting points were often chosen taking semantics from the account: "*For the starting point for the bank password I chose 'B' and '9' because it's for the bank and my account number starts with a '9'*" (p3), "*For the banking password I chose a random cell with a dollar sign in it and for the email a cell with an '@' sign*" (p6). Other participants used personal information or personal experience to choose the starting points: "*To choose the coordinates I chose the first letter of my name and a number from my date of birth*" (p18), "*I chose as coordinate for the email password my lucky number*" (p13). However, others stated to have chosen completely random starting points.

Regarding the walks used by the participants for their passwords, the vast majority is made up only of vertical or horizontal movements (83.3%). Walks with diagonal movements are the exception (16.7%). Also, the majority of walks (41.1%) do not change direction, i.e. are straight lines (23.3% horizontal, 10.0% vertical, 7.8% diagonal). Most of the horizontal and diagonal lines run from left to right. 22.2% of walks change direction only once (for details see fig. 3). Again the answers regarding the participants reasons for choosing their walks shed further light on this result. They center around considerations with respect to memorability: "*The characters in the grid are already random, therefore the walk does not need to be. So I chose a straight line because it's easier to remember.*" (p27), "*I chose a straight line because I can remember it more easily.*" (p4).

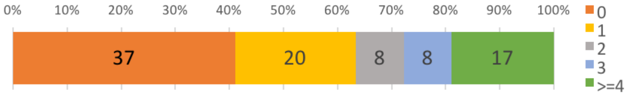


Figure 3: The frequencies with respect to the number of changes in direction in the walks chosen by the participants.

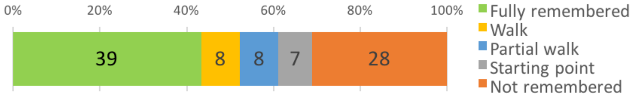


Figure 4: The frequencies with respect to what extend the participants remembered their passwords.

4.2 Memorability

The majority of passwords could not be reproduced by the participants in phase 5: only 43.3% of the passwords were fully remembered by the participants (see fig. 4 for details). Thereby, the participants perceived only for 58.9% of the passwords correctly, what they remembered about them (with respect to the categories from fig. 4). However, in contrast to the participants' assumptions that straight lines would be easier to remember, this does not seem to be the case. A Fisher's exact test failed to find a significant difference in whether the participant could remember their passwords between straight lines and other walks (FET: $p = 0.829$).

5 CONCLUSION

Our analysis of the security and memorability of the password card shows that memorability seems low, even after only 5-10 minutes. Also, we identify similar issues as security analyses of other approaches [1, 2]: (a) the starting points are not randomly dispersed in the grid and (b) most walks chosen in our study are straight lines or have just one directional change. Thus, the password card seems to fail in helping users to choose and remember secure passwords.

The next step in this work is to validate our results with a larger participant sample in an online study. Also, based on a larger sample of starting points and walks, a specialized guessing algorithm could be developed and evaluated.

REFERENCES

[1] Adam J Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Annual Computer Security Applications Conference*. ACM, 301–310.

[2] S Chiasson, E Stobert, A Forget, R Biddle, and P C van Oorschot. 2012. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE Transactions on Dependable and Secure Computing* 9, 2 (2012), 222–235.

[3] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *USENIX Security Symposium*. 1–16.

[4] Vijay Kothari, Ross Koppel, Jim Blythe, and Sean Smith. 2017. Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors. In *European Workshop on Usable Security*.

[5] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *USENIX Security Symposium*. 465–479.

[6] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C van Oorschot. 2012. Tapas: design, implementation, and usability evaluation of a password manager. In *Annual Computer Security Applications Conference*. 89–98.

[7] Reinhard Muth. 2013. Die Passwortkarte. https://www.dsin-blog.de/2013/08/20/die-passwortkarte/. (2013). Accessed: 2017-06-21.

[8] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords . In *Symposium on Usable Privacy and Security*.