Rotate to Protect

Harshal Tupsamudre
TCS Research
Pune, India
harshal.tupsamudre@tcs.com

Sachin Lodha
TCS Research
Pune, India
sachin.lodha@tcs.com

Akhil Dixit
TCS Research
Pune, India
akhil.dixit@tcs.com

Manish Shukla
TCS Research
Pune, India
mani.shukla@tcs.com

Vijayanand Banahatti
TCS Research
Pune, India
vijayanand.banahatti@tcs.com

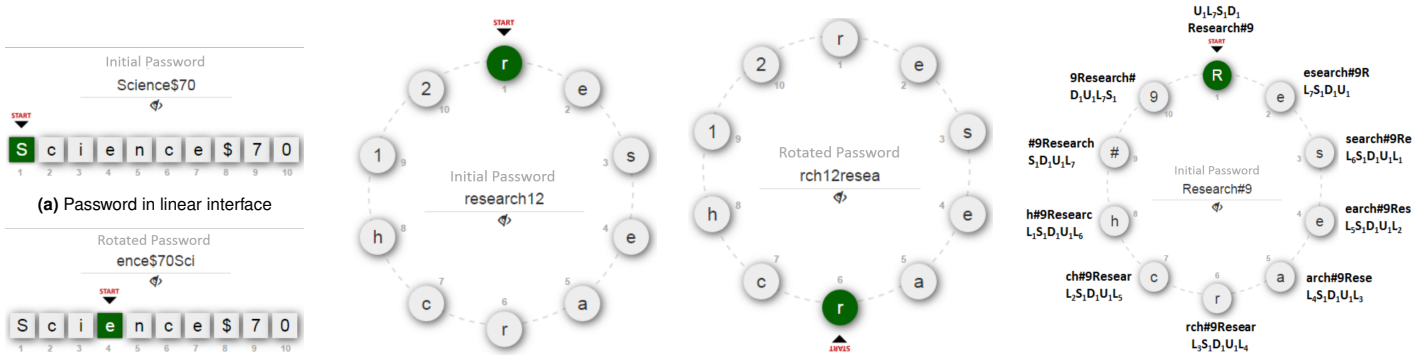
Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee. Poster presented at the 12th Symposium on Usable Privacy and Security (SOUPS 2016), June 22-24, 2016, Denver CO.

Abstract
Human-generated text passwords are vulnerable to statistical guessing attacks. The counter strategies either require building the entire system from scratch or need major rework and therefore cannot be adopted easily. In this paper, we demonstrate how a slight modification to login interface can influence users to create relatively secure text passwords. We develop two graphical interfaces, linear and circular, which allow users to rotate their text passwords by selecting a new starting point. To evaluate these interfaces, we conducted an experiment with 107 participants. We found that participants willingly chose new starting point to rotate their password which improved the guessing resistance by 8 times. Further, multiple cues helped participants recall their starting point in just one attempt. As both interfaces can be deployed as plugins,we encourage their use.

Author Keywords
Authentication; text passwords; usable security

ACM Classification Keywords
H.5.2 [User Interfaces]: Prototyping; K.6.5 [Security and Protection]: Authentication

Introduction
Human generated text passwords are drawn from a small space [8, 5, 6]. The utilized password space can be easily



(a) Password in linear interface

(b) Rotation using linear interface

(c) Password in circular interface

(d) Rotation with circular interface

(e) Rotation changes password and its structure

L - Lowercase Letters
U - Uppercase Letters
D - Digits
S - Symbols

Figure 1: (a) and (b) demonstrates the use of linear interface to rotate the *initial password* 'Science$70'. By default, the *initial password* is read from the node labelled 1 in a cyclic clockwise order (a). 'Science$70' can be rotated to 'ence$70Sci' by choosing the letter e (node 4) as new starting point (b). The password letters in the textbox and in the interface are masked by default and made visible only if user clicks on the eye button. Circular interface works similarly (c) and (d). The rotation operation not only changes the *initial password* but also changes its structure thus improving the utilized space (e).

Structure	Count (Percent %)
L_6	3,987,911 (12.47%)
L_7	2,738,042 (8.56%)
L_8	2,469,702 (7.72%)
D_6	2,278,924 (7.12%)
Total	11,474,579 (35.87%)

Table 1: Top 4 password structures in 32 million Rockyou dataset.

Password	Count (Percent %)
123456	2,90,729 (0.91%)
12345	79,076 (0.25%)
123456789	76,789 (0.24%)
password	59,462 (0.18%)
Total	506,056 (1.58%)

Table 2: Top 4 passwords in 32 million Rockyou dataset.

demonstrated using the concept of password structure [13]. Password structure is an ordered sequence that captures passwords composition using 4 alphabets L, U, D and S, *e.g.*, the structure L_6 represents 6 length lowercase passwords and the structure L_6D_2 represents 8 length passwords with 6 lowercase followed by 2 digits.

The number of n length password structures is 4^n, however the analysis of real-world password data reveals that most of these structures are never used. For instance, top 20 structures constitute about 70% of 32 million Rockyou passwords [4]. Moreover, these popular structures are simple ones and are of the form L_n, D_n, $L_{n-k}D_k$ (Table 1). Still worse, only few passwords within these structures are actually preferred. For instance, the password *123456* in D_6 is used by 290,729 Rockyou users (Table 2). And if other alphabets like uppercase letters or symbols are used, they are placed at predictable positions [9]. Clearly user choices are heavily biased towards fewer passwords and password structures, and therefore vulnerable to guessing attacks.

Contribution. *Our objective is to facilitate password creation from different password structures and improve the utilized space without affecting the usability.* We observed that permuting a password string not only changes the password but also changes its structure. Further, research shows that graphical passwords perform better on memorability front, but less on theoretical security and deployment front when compared to text passwords [3, 2]. *In this work, we consider rotation operation, a kind of permutation, which is also human-computable. We combine the benefits of both textual and graphical worlds and develop two alternative graphical interfaces, linear and circular, to help users create and remember rotation-based text passwords. Rotation improves the space utilization by tapping into the uncommon text passwords and their structures.*

As the user types her password in a conventional textbox, simultaneously the linear interface organizes every letter in a discrete node, further arranging these nodes in a linear fashion (Fig.1a). In the case of circular interface, letters are

	Linear	Circular
Gender		
Male	57.69%	52.73%
Female	42.31%	47.27%
Age		
20-25	51.92%	54.55%
26-30	15.38%	14.55%
31-35	15.38%	16.36%
36-40	9.62%	5.45%
≥ 41	7.69%	9.09%
Profession		
Students	26.92%	34.55%
Engineer	32.69%	27.27%
Researcher	28.85%	23.64%
Other	11.54%	14.54%
#Participants	52	55

Table 3: Participant demographics. All students were from non-CS/IT.

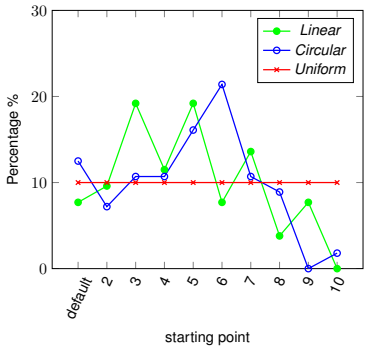


Figure 2: Distribution of starting points chosen in the study.

$$Entropy\ H = \sum_{i=1}^{n} p_i \cdot log_2(1/p_i)$$

arranged in a circular fashion (Fig.1c). By default, this *initial password* is read from the node labelled 1 in a clockwise direction. Both interfaces allow users to click on a new node to change the starting point of their *initial password*. The *rotated password* is obtained by reading the *initial password* from the new starting point in a clockwise direction (Fig.1b,1d). This *rotated password* is finally sent to the server. During login, the user is provided the same interface where she just needs to enter the *initial password* and then click on the starting point to perform rotation.

Science behind Circular Interface. Both interfaces are interactive and encourage users to rotate their passwords. However, the circular interface has some inherent advantages as compared to the linear.

1. Visual Psychology. People find curved object more aesthetic [1] and prefer symmetry [10]. The circular interface is designed with these preferences in mind.

2. Multiple Cues. Along with the verbal cues (numbers), the circular interface also provides spatial cues to recall the starting point [11].

3. Metaphor. The circular interface is designed to stimulate human intuition and is heavily inspired by an analog clock, a real-world metaphor [7]. Due to the ubiquity of clock, users with different skills can easily interact with this interface.

4. Screen Space. Linear interface occupies more space than the circular. This factor is important especially on mobile devices as they have a small space. If a linear interface can arrange at most x letters on a screen, the circular interface can arrange at most $\pi \cdot x$ letters on the same screen.

5. Scalability. The circular interface can be easily extended to perform permutations other than rotations, for instance, by drawing graphical patterns.

Experimental Study

We recruited 111 participants within the organization through the use of internal mailing lists. The demographics of 107 participants who completed the study is shown in Table 3. 52 of these participants were assigned to condition A (linear interface) and 55 were assigned to condition B (circular interface). The study was conducted in a lab in a controlled environment during January 2016. All participants were compensated with a pen, diary and chocolate worth $2.

Procedure. We asked participants to imagine that they are creating a new email account. Further, they were requested to not to write down their password. The experiment was conducted in the following two phases.

Creation (Day 1). Participants were asked to create at least 8 length password. We refer to this as *initial password*. The *initial password* was then arranged using either linear or circular interface. Participants could use this interface to choose a new starting point and rotate their *initial password*. However, performing rotation was not mandatory and participants could submit their *initial password* as it is.

Recall (Day 4). 72 hours later, we invited participants for recall. Participants entered their *initial password* which was then arranged using the same interface assigned during creation phase. Next, participants performed rotation by clicking on the starting point chosen during creation. Finally, we captured participants' sentiments using a short survey.

Uncertain Starting Points

Even though the rotation operation was not mandatory, 92.3% of the participants in linear condition and 87.5% in circular condition rotated their *initial password*. The distribution of starting point choices is shown in Fig.2. As the average password length in the study was 10, we consider first 10 positions only. In both conditions, participants starting point choices were quite distinct. To gauge the uncertainty due to varied choices, we use the entropy measure H. The entropy due to selection of 10 different starting positions in linear interface and circular interface is 3.02 and $2.99\ bits$ respectively (ideal is $log_2(10) \approx 3.32\ bits$). *Thus,*

Login	Linear	Circular
Attempt 1	92.31%	94.55%
Attempt 2	5.77%	3.63%
Successful	98.08%	98.18%
Avg Attempts	1.06	1.04
#Participants	52	55

Table 4: Login attempts of successful participants during recall phase.

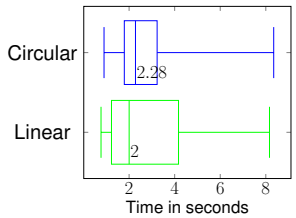


Figure 3: Starting point recall time.

O-R Pairs	Guess Description	$\frac{G^R}{G^I}$
30	$G^I = G^R = \infty$	–
30	$G^R = \infty$	∞
32	$G^I << G^R$	2^{16}
4	$G^I > G^R$	$1/2^4$
96		

Table 5: Comparing the guessing resistance of initial (O) and rotated (R) passwords using CMU's PGS. ∞ indicates unguessable using PGS.

the guessing resistance is improved by a factor of $2^3 = 8$.

Usability Results

We emphasize that our system is simply an add-on to existing text-based password systems. It provides users with an option to select a different starting point for their passwords. Hence, we focus only on the data pertaining to starting point chosen by participants and report the resulting usability and security benefits due to new starting points.

Login Attempts. During recall, on wrong password entry, participants were asked to enter both *initial password* and starting point again. Further, only 2 failed attempts were allowed. Memorability was quite good as *98% participants in both linear and circular conditions successfully recalled their starting point in just 1.06 and 1.04 trials respectively.*

Creation Time. During creation phase, most participants explored various starting points to rotate their *initial password*. However, the time required to choose starting point using the linear interface (median 11.52s) is 1.57 times high as compared to that of circular interface (median 7.32s).

Recall Time. During recall phase, participants used interface cues to recall their starting point. As a consequence, the time required to recall starting point in both conditions is less. *The median recall time in linear condition is 2.00s and in circular condition is 2.28s* (Fig.3).

Acceptability. In the post-experiment survey, *90% of the participants in both conditions agreed that interface is easy to use*. When asked about their starting point selection strategy, 35.42% participants in linear condition reported choosing a letter, 35.42% chose the node number and 29.16% chose starting point based on the perceived complexity of the rotated password. In circular condition, 27.08% participants chose letter, 18.75% chose node number, 18.75% chose node position (spatial) and 35.41% chose rotational version based on the perceived complexity. Also, no one reported writing down their password.

Security Results

96 out of 107 participants rotated their initial password *by choosing new starting point. The resulting entropy of 3 bits slows down dictionary attacks by a factor of 8.* To gauge the security improvements due to rotation against real-world attacks, we submitted all 96 initial-rotated (I-R) password pairs to CMU's Password Guessing Service (PGS) [12]. We measured the security of all 96 pairs against 4 different attack strategies, namely John the Ripper, Hashcat, Markov model and Probabilistic Context Free Grammar. We define the guessing resistance G^p of a password p as the minimum number of guesses required to crack p using any of these 4 attack strategies. The PGS results are summarized in Table 5. *30 out of 96 password pairs were unguessable (∞). In other 30 pairs,* initial passwords *were guessed but their rotated counterparts remained unguessable. While in 32 pairs, the security of rotated passwords was much greater (2^{16} times) than their initial versions. Of all 96 pairs, only 4 rotated passwords were weaker than the initial ones.*

Deployment. Our interfaces are easy to deploy on any platform. Websites can add them to their existing web-pages or they can be implemented at client side as a plug-in feature in standard web browsers. Whenever user enters password on a website, the interface comes into action and facilitates users to rotate their passwords.

Conclusion

In this work, we showed how a simple design change can influence users to create relatively secure text passwords. The use of our interfaces facilitates password creation from different structures and improves the resulting password distribution. The usability results indicate that both interfaces are intuitive and easy to use. Due to different rotation strategies of participants the security is also increased by 8 times. Further, our proposed idea is just a simple add-on and therefore can be easily adopted by existing systems.

REFERENCES

1. Moshe Bar and Maital Neta. 2006. Humans prefer curved visual objects. *Psychological science* 17, 8 (2006), 645–648.

2. Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)* 44, 4 (2012), 19.

3. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP '12)*. IEEE Computer Society, Washington, DC, USA, 553–567. DOI: http://dx.doi.org/10.1109/SP.2012.44

4. Ron Bowes. 2007. Passwords. Website. (12 March 2007). Retrieved May 20, 2016 from https://wiki.skullsecurity.org/Passwords.

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, NY, USA, 657–666. DOI: http://dx.doi.org/10.1145/1242572.1242661

6. Zhigong Li, Weili Han, and Wenyuan Xu. 2014. A Large-Scale Empirical Analysis of Chinese Web Passwords. In *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA, 559–574.

7. Theo Mandel. 1997. *The Elements of User Interface Design*. John Wiley & Sons, Inc., NY, USA, Chapter The Golden Rules of User Interface Design, 5.1–5.28.

8. Robert Morris and Ken Thompson. 1979. Password Security: A Case History. *Commun. ACM* 22, 11 (Nov. 1979), 594–597. DOI: http://dx.doi.org/10.1145/359168.359172

9. Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, NY, USA, Article 2, 20 pages. DOI: http://dx.doi.org/10.1145/1837110.1837113

10. Paul J Silvia and Christopher M Barona. 2009. Do people prefer curved objects? Angularity, expertise, and aesthetic preference. *Empirical studies of the arts* 27, 1 (2009), 25–42.

11. Endel Tulving and Shirley Osler. 1968. Effectiveness of retrieval cues in memory for words. *Journal of experimental psychology* 77, 4 (1968), 593.

12. Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, and Richard Shay. 2015. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. In *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C., 463–481.

13. 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. DOI: http://dx.doi.org/10.1109/SP.2009.8