Pass-Roll and Pass-Scroll: New Graphical User Interfaces for Improving Text Passwords

Harshal Tupsamudre*, Akhil Dixit†, Vijayanand Banahatti* and Sachin Lodha*
*TCS Research, Pune
Email: firstname.lastname@tcs.com
†UC Santa Cruz
Email: akadixit@ucsc.edu

***Abstract*—The user interface for inputting text-based passwords has been the same for past 40 years. Today, technology enables the development of intuitive, interactive and responsive interfaces that can help users in creating and remembering more secure passwords. In this paper, we exploit the power of modern-day technologies and develop two novel interfaces, (i) linear one called as Pass-Scroll and (ii) circular one called as Pass-Roll. These graphical interfaces allow users to perform rotation operation by choosing a new starting point for their passwords. Consequently, the security of a $\mathbf{n}$ length password can be potentially improved by $\mathbf{\log_2(n)}$ bits.**

To evaluate Pass-Roll and Pass-Scroll interfaces we conduct two user studies, one in the laboratory and the other on CrowdFlower. Both studies show that users willingly take advantage of these interfaces and choose a new starting point to rotate their password. We find that users' choices are quite diverse and multiple cues associated with the interfaces help users to recall their starting point in just one attempt. Moreover, our interfaces require no server-side changes and can be easily implemented as browser extensions.

I. Introduction

Textual passwords remain the most popular authentication method on the internet despite several shortcomings. A plethora of security studies [22], [28], [42] show that users choose predictable passwords even for relatively important accounts [21], [27]. Passwords are generally short and created using dictionary words including names, dates and keyboard patterns [33], [40]. Further, the set of operations performed by most users on their passwords is limited to appending digits or symbols and placing capital letters in the beginning [38], [41] which leads to a predictable password structure.

However, a recent study [36] investigated the users' perception of password security and found that in most cases users' understanding of what features make a secure password was consistent with the performance of current password cracking tools. For instance, users correctly recognized that adding digits or symbols in the middle of a password is a more secure behaviour rather than adding them at the end while placing a capital letter in the middle is more beneficial than placing it at the beginning. Thus, despite having correct understanding about password security, users often create simple passwords.

As passwords chosen by users are predictable, they are vulnerable to guessing attacks. Depending on whether guessing is carried out *remotely* or *locally*, these attacks are broadly classified into two categories, *online attacks* and *offline attacks*. In online attack, guessing is performed against an account on a *remote* website using internet. The online attacker exploits the fact that a handful of passwords are very popular among users, *e.g.*, the password *123456* was used by around 1% (290,731) of Rockyou account owners [23]. Recently, Bonneau [14] found that an optimal online attacker who could manage just 10 popular guesses on a large-scale website such as Yahoo can compromise around 1% passwords.

In offline attack, the attacker steals the database containing passwords of all registered users of a website. Nowadays, the breach of a password database is not an uncommon event. In the past few years, millions of passwords have been stolen from prominent websites including Yahoo, LinkedIn, Hotmail, Twitter, Sony, Adobe and many others [10]. To thwart such attacks, passwords are generally protected using a one-way hash function and long random salts [6]. However, since guessing is carried out *locally*, the offline attacker can try potentially infinite number of hashed guesses against any account.

Just as *popular passwords* are vulnerable to online attacks, *popular password structures* are vulnerable to offline attacks. We refer to a string derived using the alphabet set $\alpha = \{L, U, D, S\}$ as *password structure*, where L, U, D, S denote lowercase letters, uppercase letters, digit and special characters respectively. Basically, password structure is an ordered sequence that captures the composition of a password using four alphabets L, U, D and S, e.g., L_8 represents 8 length passwords such as *princess* composed entirely of lowercase letters while L_6D_2 represents 8 length passwords such as *monkey12* composed of 6 lower letters followed by 2 digits.

The number of n length password structures composed using 4 character classes, namely lowercase, uppercase, digit and special character is 4^n, however, the analysis of real-world password data reveals that most of these structures are never used. For instance, the top 20 password structures in the Rockyou dataset [7] comprise nearly 70% of the passwords. Moreover, these popular structures are simple ones and are of the form L_n, D_n, $L_{n-k}D_k$ and $U_1L_{n-k-1}D_k$. Clearly

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23004

users' choices are heavily biased towards fewer passwords and password structures which makes them susceptible to guessing attacks.

In this paper, we explore the viability of password entry interfaces that allow users to craft passwords with less predictable password structures. The need for user-centric interfaces for solving security problems has been emphasized many times in the past [18], [43]. However, the design of usable and creative interfaces in the context of textual passwords has remained largely an unexplored area. Today, technology enables the development of intuitive, interactive and responsive interfaces that can help users in creating and remembering more secure passwords. We think that password entry interfaces should influence users to perform more secure operations on their passwords. More diverse set of operations on passwords imply more guessing effort.

One such operation is a permutation. We observed that permuting a password string not only changes the password but also changes its structure. In this work, we focus on rotation, a kind of permutation, because of the following reasons.

- Rotation is not a popular operation among users. For instance the password *princess* is one of the most popular password in the Rockyou dataset [7] and was used by 33,291 Rockyou users. However, as shown in Table I, most of the rotational variants of *princess* in the dataset remain unused (count 0). On the other hand, adding an extra digit at the end of a password is a very common operation [38], [41]. For instance, the password *princess* and all its one digit variants are already present in the Rockyou dataset (Table I). If the user selects *princess* as her password, influencing her to append an extra digit will not improve the utilised space, since such password variants would have already been taken by other users of the website. Therefore, rotation improves the space utilisation while appending a digit does not.

TABLE I: Frequency of *princess* along with its rotational and extra-digit variants in the Rockyou dataset.

Point	Password	Count
0	princess	33,291
1	rincessp	0
2	incesspr	0
3	ncesspri	0
4	cessprin	4
5	essprinc	0
6	ssprince	0
7	sprinces	0

Digit	Password	Count
	princess	33,291
1	princess1	5,187
2	princess2	683
3	princess3	391
4	princess4	252
5	princess5	266
6	princess6	145
7	princess7	410
8	princess8	224
9	princess9	204

- Rotation also improves the space utilization by tapping into uncommon password structures. For instance, if the user selects the password as *monkey12* and rotates it to *nkey12mo*, the structure also changes from L_6D_2 to $L_4D_2L_2$. In the Rockyou dataset the number of passwords that belong to the structure L_6D_2 is 923,989 while the number of passwords that belong to the structure $L_4D_2L_2$ is 4,279. Thus, the resulting structure $L_4D_2L_2$ is less predictable than the original structure L_6D_2.
- Rotation is a human-computable operation. If the rotation tool is not available, then the rotated variant can be generated easily if the user remembers the initial password and the point around which the initial password is rotated.

A. Contribution

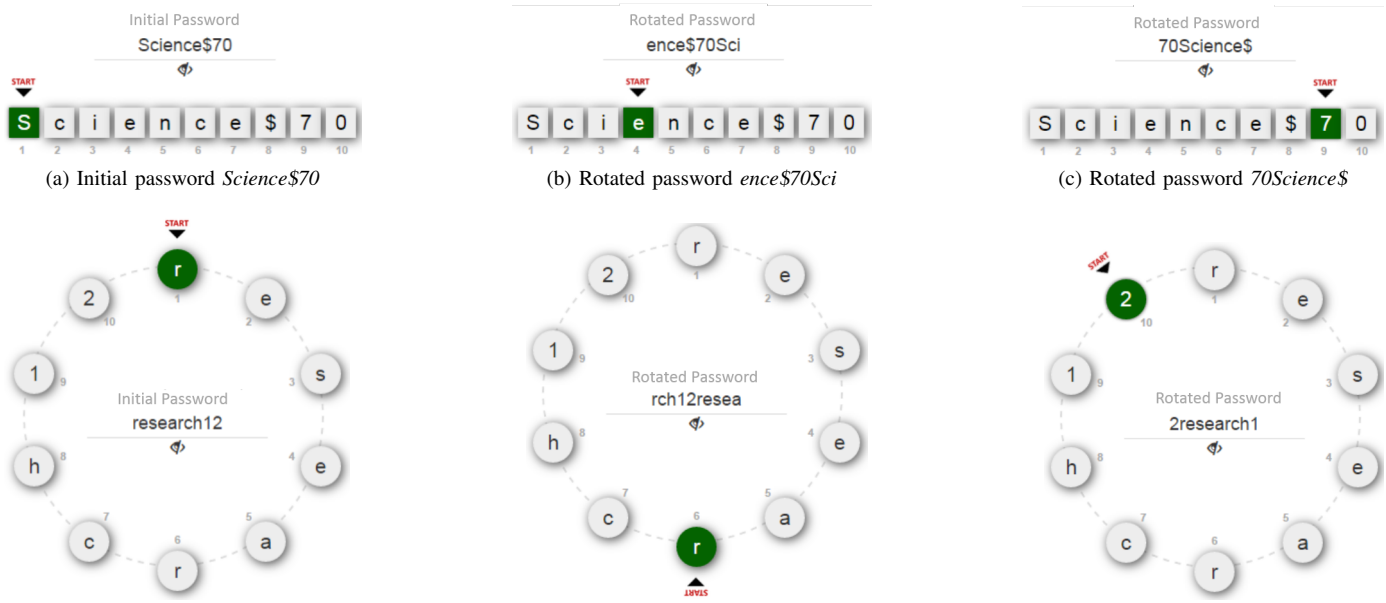
The purpose of our work is to facilitate the password creation from different password structures and to improve the space utilisation without compromising on usability. To achieve this goal, we equip users with a tool that enables them to rotate their passwords. We draw upon the ideas of graphical user interfaces to help users to create and remember rotation-based text passwords. Prior research suggests that most graphical password schemes perform better on memorability front, but less on theoretical security and deployment front when compared to textual passwords [15], [13]. We combine the benefits of both textual and graphical worlds and develop two alternative graphical interfaces, (i) linear one referred to as *Pass-Scroll* and (ii) circular one referred to as *Pass-Roll*.

As the user types her password in a conventional textbox, *Pass-Scroll* simultaneously organizes every character in a discrete node, further arranging these nodes in a linear fashion (Fig.1a). In case of *Pass-Roll*, characters are arranged in a circular fashion (Fig.1d). We refer to this password as *initial password*. By default, the initial password is read from the node labelled 1 in a (cyclic) clockwise direction. Both interfaces allow users to click on any node to choose a new starting point for their password. The rotated password is obtained by reading the initial password from the new starting point in a clockwise direction (Fig.1b, 1e). This rotated password is finally sent to the server.

For instance, if the user selects *Science$70* as her initial password (Fig.1a) and employs *Pass-Scroll* to choose the node 4 (letter 'e') as the new starting point then the initial password is rotated to *ence$70Sci* (Fig.1b). During login, the same interface is provided where the user enters her initial password *Science$70* and then clicks on the starting point 4 (letter 'e') to produce the rotated version *ence$70Sci*. Therefore, the user has to remember the initial password and new starting point to obtain her rotated password.

Due to rotation, the resulting password becomes more distinct and relatively more resistant to online guessing attacks. Rotation also improves the total number of password structures thereby making offline attacks more expensive (Fig.2). All of this is achieved with a small change in the interface and minimal increase in the cognitive load. Both interfaces provide users with multiple cues (verbal, spatial) to recall the new starting point. Further, these interfaces require *no server-side changes* and can be easily deployed as browser plugins.

Study and Results. We evaluated both *Pass-Scroll* and *Pass-Roll* interfaces by performing two studies. The first study was conducted in a controlled laboratory setting and the second study was conducted using the online crowdsourcing platform CrowdFlower [1]. The laboratory study was completed by 107 participants and the online study was completed by 195 participants. The results reveal that users willingly take advantage of our interfaces and choose a new starting point to rotate their password. The diverse starting point choices of participants on their minimum eight length password improved guessing resistance by at least $log_2(8) = 3$ bits. Also, most participants were able to recall their starting point in just one attempt.



(a) Initial password *Science$70* (b) Rotated password *ence$70Sci* (c) Rotated password *70Science$*

(d) Initial password *research12* (e) Rotated password *rch12resea* (f) Rotated password *2research1*

Fig. 1: (a), (b) and (c) demonstrates the use of *Pass-Scroll* to rotate the *initial password* **Science$70**. (a) By default, the *initial password* **Science$70** is read from the node labelled 1 in cyclic clockwise order. (b) **Science$70** can be rotated to **ence$70Sci** by choosing character 'e' (node 4) as the new starting point. (c) To obtain **70Science$**, one has to select character '7' (node 9) as the starting point. The characters of a password in the input textbox and in the interface are masked (hidden) by default and made visible only if the user clicks on eye button. *Pass-Roll* works similarly (d), (e) and (f).

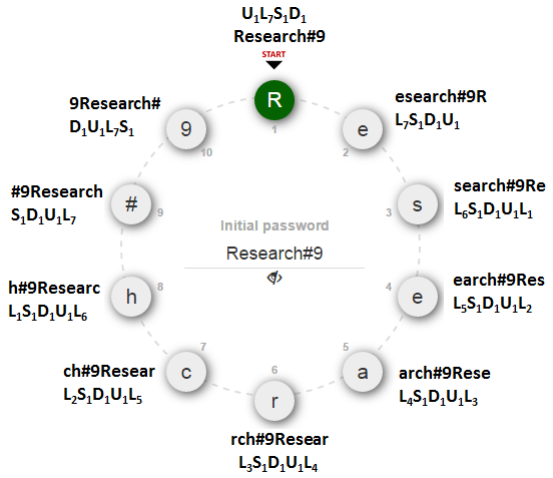


Fig. 2: The figure shows the initial password **Research#9** and its 9 rotated variants. Rotation not only changes the initial password but it also changes the structure. Selecting different starting points distributes the popularity of password **Research#9** among its rotated variants and thus provides better security against online attacks. Selecting different starting points also distributes the popularity of structure $\mathbf{U_1L_7S_1D_1}$ among its variants and increases the effort of offline attacks. The passwords and their structures are displayed only for understanding purpose and are not part of the interface.

II. Science behind Interfaces

Both *Pass-Scroll* and *Pass-Roll* interfaces are designed to influence users to rotate their passwords. Specifically, these interfaces have the following characteristics.

Interactive. To encourage the exploration of different starting points by users, we designed interfaces to be interactive. On clicking any node, both interfaces provide explicit feedback to the user in the form of a rotated password (Fig.1b, 1e). The rotated password in turn should motivate the user to choose a new starting point and thus set a more complex password. Further, to ensure security against shoulder-surfing attacks, the password is masked (hidden) by default and is made visible only if the user clicks on eye button.

Cues. According to psychological research [11], [34] the information can be remembered more reliably with the help of different cues. To assist users in recalling a new starting point during subsequent logins, both interfaces associate a number (verbal cue) with each character (node) of a password. The node containing the first character of a password is labelled 1 while the node containing the last character is labelled with the password length n (Fig.1). Users can thus remember the node number and click on the associated starting point to obtain their rotated password. Apart from verbal cues, the circular interface also provide users with spatial cues (position of nodes) to recall the starting point of their password.

Contextual Information. The encoding specificity theory [35] postulates that the contextual information plays an important role during recall. According to this theory, recall is better if the information available during encoding is also available during retrieval. The interface (information) available during password creation is also available during login which help users in retrieving the starting point from their memory.

Metaphor. Both linear and circular interfaces are designed with users in mind and aim to simulate human intuition. While the linear design is a natural extension of conventional password entry interface, the circular design is heavily inspired by rotary dial phone, a real-world metaphor [26]. Hence, we think that users with different skills can easily interact with both interfaces.

III. Laboratory Experiment

To assess the usability and security of our interfaces, we conducted a pilot study in a controlled laboratory environment during January 2016. The objectives of this study were three-fold, (a) to examine the influence of *Pass-Scroll* (linear) and

Pass-Roll (circular) interfaces on users, (b) to measure the resulting security improvements due to rotation and (c) to determine the usability of these rotation interfaces. We recruited 111 participants within our organization, of which 107 participants completed the study. We conducted the experiment in two phases, namely, creation and recall. The usability and security results were published in SOUPS'16 [8]. In summary, we found that participants willingly chose new starting point to rotate their minimum 8 length passwords which improved guessing resistance by a factor of 8. Further, multiple cues helped most participants to recall their starting point in just one attempt.

Limitations. While the laboratory study results suggest that both *Pass-Scroll* (linear) and *Pass-Roll* (circular) interfaces are effective, based on the feedback we received in the SOUPS'16 conference, we learned that our experimental setup had few limitations.

- The laboratory experiment was conducted in the organization with a tech-savvy crowd. Further, the experiment was controlled and conducted in the presence of an instructor. Therefore, it is not very much clear if an average user can use these interfaces without requiring any training and support.
- The recruitment method in the laboratory study was restricted to employees working in the organization which may have resulted in a selection bias.
- The usability and security data collected from the tech savvy employees is unlikely to be representable and thus, the results of the laboratory experiment may not be generalizable to a larger population.
- Participants knew about the two-step password creation process before the study began. However, recent research [32] suggests that if users are aware of multi-step password creation process before selecting their passwords then they choose weaker (initial) password in the first step which might negatively impact the overall security of the password. In the study, we did not verify whether our interfaces influence users to rotate their password when they are not aware of the rotation step in advance.
- Also, we did not use a standard feedback survey such as System Usability Scale (SUS) questionnaire [9] to capture the users' perception about the usability of our systems.

We try to address several of these limitations by performing an online experiment using the CrowdFlower platform [1]. The details of the experiment are sketched in the next section.

IV. Online Experiment

We followed the experimental methodology as described by Komanduri *et al.* in [24]. We advertised our study on CrowdFlower as a two-part "brief study" with a bonus opportunity. We required participants to be at least 18 years old level-3 performers [2]. A total 228 participants were recruited satisfying the age and performance level criteria of which 195 completed the study. Participants were assigned randomly to either *Pass-Scroll* condition or *Pass-Roll* condition. The experiment began in August 2016 and lasted for 10 days.

A. Study Overview

The study was conducted in two phases, namely *creation* and *recall*. We asked participants to imagine that they are creating a new email account. We requested them to behave as if this were their real email account. Participants were compensated with 10 cents for completing the *creation phase* and 20 cents for completing the *recall phase*. The overall contributor satisfaction for our task was 4.4 out of 5. The online experiment differed from the laboratory experiment in various ways. Most importantly, in the online setup, participants were not aware of the rotation step while choosing their password. The detailed procedure is given below.

(1) **Creation Phase (Day 1).**

(i) Participants were shown a consent form which briefed them about surveys conducted in the study. After reading it, participants were required to click a check box indicating their consent to participate in the study.

(ii) After getting consent, participants were requested to provide a username for creating a new email account.

(iii) Subsequently, participants were asked to create a minimum 8 length password (there was no limit on maximum length) to protect their new email account. We refer to this password as *initial password*. Upon failing to meet the minimum length requirement, participants were informed accordingly and instructed to retry.

(iv) After getting an acceptable password, participants were informed about the rotation step. They were shown snapshots (similar to Fig.1) illustrating the use of the assigned interface (*Pass-Scroll* or *Pass-Roll*). Further, in the instructions, we emphasized that the rotation step is not mandatory and can be skipped. Since we informed participants about the rotation step after the creation of initial password, we can therefore verify whether participants get influenced to use our interfaces when they are not aware of the two-step password creation process in advance.

(v) The initial password from step (ii) was then arranged using either *Pass-Scroll* or *Pass-Roll*, as per the interface assigned to participants. All characters in the discrete nodes as well as in the text box were masked (hidden) with asterisk and made visible only if participants clicked on eye button (Fig.1). As depicted in Fig.1a and Fig.1d, the first character is the default starting point of the password. Participants were free to choose a new starting point (or keep the default one) and rotate their initial password. *Note that performing rotation was not mandatory and participants could submit their initial password as it is*.

(vi) After the submission of password, participants were asked to fill a short survey that captured their demographics and sentiments about password creation. The survey questions along with their responses are listed in appendix A.

(vii) Later, we had a verification round where participants were required to provide their initial password and use the interface to click on the starting point (if any) selected during creation. We gave participants a maximum of five attempts before showing their initial password and start point. Finally, we displayed a code to participants which they had to submit on CrowdFlower to receive their payment. We also told them that they would be contacted to complete the remaining study, but we did not mention when we would do so.

(2) **Recall Phase (Day 4).** 72 hours later, we invited participants to complete the *recall phase*. There were no practice sessions between creation and recall phases. This setup enabled us to measure the recall efficiency when the password was not used for a while. *Recall phase* had the following 3 steps.

(i) Participants were asked to enter their initial password.

(ii) This initial password was then arranged using the same interface provided during the *creation phase*. Next, participants used the interface to select their starting point (if any) to rotate the initial password. Again, we gave participants a maximum of five attempts before showing their initial password and starting point.

(iii) Finally, participants were requested to fill a short survey that captured their strategy for choosing a new starting point, their password storage behaviour during the online study and their sentiments towards the assigned interface. The survey questions along with their responses are listed in appendix B. To capture the perceived usability of our systems, we also requested participants to answer the SUS questionnaire (appendix C). Upon completion of the survey, we made the remaining payment to participants using the CrowdFlowers' API.

B. Demographics

Of 228 participants who enrolled for the online study, 219 participants completed the *creation phase*, 203 participants returned for the *recall phase* and 195 completed the entire study. *We concentrate on the usability and security results pertaining to these 195 participants only.* Participants belonged to 34 different nationalities and their demographics are shown in Table II. Of 195 participants who completed the study, 100 participants had been randomly assigned to *Pass-Scroll* (linear) condition and the remaining 95 participants had been assigned to *Pass-Roll* (circular) condition. Most of the participants were below the age of 41 years and had a graduate degree in a non-CS field. We found no statistically significant difference in age, gender, technical experience or educational level between conditions (chi-square test, $p > 0.05$).

V. Security Results

In the experiment, we asked participants to create a minimum 8 length password. We did not impose any character set restriction on the password composition. Further, the rotation step was optional. The basic statistics of passwords created using *Pass-Scroll* and *Pass-Roll* conditions are given in Table III. The median password length across both conditions is 11. When faced with the minimum length requirement, users typically create password using lowercase letters and digits, and avoid the use of uppercase letters and symbols [22], [24], [25]. We observed similar password composition in our study (Table III). Note that rotating a password neither affects its length nor its composition. However, as illustrated in Fig.2 rotation does affect the password structure.

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

TABLE II: Participant demographics in the online experiment.

	Pass-Scroll	*Pass-Roll*
Gender		
Male	76.00%	64.21%
Female	24.00%	35.79%
Age		
20-30	38.00%	41.05%
31-40	32.00%	35.79%
≥ 41	30.00%	23.16%
Profession		
Computer-related	29.00%	27.37%
Other	66.00%	66.32%
No answer	5.00%	6.31%
Education		
Associate	17.00%	14.74%
Bachelors	59.00%	46.32%
Masters	21.00%	34.74%
Other	1.00%	2.10%
No answer	2.00%	2.10%
#Participants	100	95

TABLE III: Table shows the number of participants in each condition followed by the median password length and median number of each character classes per password.

Condition	Participants	Length	L	U	D	S
Pass-Scroll	100	11	6	0	4	0
Pass-Roll	95	11	7	0	3	0

A. Uncertain Starting Points.

Even though participants were not aware of the two-step password creation process in advance, 76% (76/100) of the participants in *Pass-Scroll* condition and 66.32% (63/95) participants in *Pass-Roll* condition rotated their initial password. The starting point choices of participants in both conditions were quite diverse. As the median password length was 11, we consider the first 11 starting positions only. The probability distribution of these 11 starting point choices is given in Table IV. We gauge the amount of randomness in the distribution using the entropy measure H.

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

The entropy due to the selection different starting positions for minimum 8 length passwords using *Pass-Scroll* and *Pass-Roll* interfaces is 3.17 and 3.04 bits respectively (ideal entropy is $log_2(11) \approx 3.46$ bits). Thus, guessing resistance is improved by at least a factor of $2^{3.04} \approx 8.22$. The most popular non-default starting point choice on both *Pass-Scroll* and *Pass-Roll* interfaces is 7.

TABLE IV: Distribution of starting points chosen in the online study.

Point	*Pass-Scroll*	*Pass-Roll*
1 (default)	24.24%	35.96%
2	12.12%	5.62%
3	5.05%	4.49%
4	9.09%	6.74%
5	9.09%	7.87%
6	7.07%	7.87%
7	14.14%	10.11%
8	6.06%	6.74%
9	8.08%	4.49%
10	1.01%	7.87%
11	4.04%	2.25%

B. Simulating Rotation on Rockyou Dataset.

To get an elaborate view of security achieved due to rotation, we apply our findings on the real-world password data. Specifically, we use 11 length passwords from the Rockyou dataset [7] and demonstrate the effect of rotating these passwords against guessing attacks. There are more than 1.16 million 11 length Rockyou passwords (866,012 distinct) composed using 13,052 distinct password structures. Suppose that the linear interface *Pass-Scroll* was used on the Rockyou website to help users rotate their password and its use resulted in the starting point distribution as shown in Table IV. In other words, we take 11 length passwords from the Rockyou dataset and simulate the use of *Pass-Scroll* by randomly rotating each password according to the starting point distribution obtained from the online experiment (Table IV). We analyse the security improvements of the resulting rotated Rockyou dataset against both online and offline guessing attacks. We repeat the experiment 1000 times and report only the average values as the standard deviation was very small.

- **Online Resistance.** Originally, the string *christopher* with 3,438 occurrences was the most frequent 11 length password in the Rockyou dataset. After simulating the use of *Pass-Scroll*, *christopher* remains the most popular password, however its frequency is reduced to 835. Table V illustrates how *Pass-Scroll* distributes the popularity of *christopher* among its rotated variants. The strings such as *hristopherc*, *ristopherch* that were originally unused (count 0) in the Rockyou dataset are better utilised after performing rotation. Similar improvements occur due to the use of *Pass-Roll* as well.

  A typical strategy to falter online attacks is to limit the number of failed attempts to, say 3. Originally, the online attacker could compromise $3,438+2,868+2,429=8,735$ accounts by trying the top three 11 length guesses on the Rockyou website (Table VI). However, after using *Pass-Roll*, the frequency of the top 3 passwords is reduced as all rotated variants are now more uniformly distributed. Consequently the attacker can now compromise $835+689+597=2,121$ Rockyou accounts, 4.12 times less than the original. Also, due to rotation, the number of distinct 11 length Rockyou passwords increased from 866,012 to 1,003,389 (15.86% improvement). Thus, the use of rotation interfaces offers much better security against online guessing attacks.
- **Offline Resistance.** We classify password structures into two categories, *simple* and *complex*. The password structure composed of a single character class such as $L_{11}, D_{11},$, U_{11} and S_{11} is called simple while the password structure composed of at least 2 character classes is called complex, *e.g.,* L_9D_2. We discuss the offline security improvements for these two categories separately.
  - *Simple.* If the structure of a password is simple then performing rotation operation does not affect its structure, however it does improve the distribution of resulting passwords (more uniform). Simple password structures are very popular in the Rockyou dataset. Nearly 387,521 distinct (with repetitions 593,673) Rockyou passwords are composed using simple password structures, L_{11}, D_{11}, U_{11} and S_{11}. After simulating the use of *Pass-Scroll* on simple Rockyou passwords, the number of distinct passwords increased to 469,178 (21.07% improvement).

TABLE V: The effect of *Pass-Scroll* and *Pass-Roll* interfaces on the popularity of password **christopher** and its rotated variants in the Rockyou dataset.

Password	*Original*	*Pass-Scroll*	*Pass-Roll*
christopher	**3,438**	**835**	**1,234**
hristopherc	0	439	209
ristopherch	0	166	129
istopherchr	0	327	244
stopherchri	0	303	279
topherchris	3	232	305
opherchrist	0	519	351
pherchristo	0	185	181
herchristop	0	285	173
erchristoph	0	27	251
rchristophe	0	123	85
Total	3,441	3,441	3,441

TABLE VI: The effect of *Pass-Scroll* and *Pass-Roll* interfaces on the efficiency of online attacker with 3 guessing attempts on the Rockyou website.

Popular	*Original*	*Pass-Scroll*	*Pass-Roll*
christopher	3,438	835	1,234
harrypotter	2,868	689	1,008
12345678910	2,429	597	847
Total	8,735	2,121	3,089

TABLE VII: The effect of *Pass-Scroll* and *Pass-Roll* interfaces on the frequency of password structure $\mathbf{L_9D_2}$ and its rotated variants in the Rockyou dataset.

Structure	*Original*	*Pass-Scroll*	*Pass-Roll*
L_9D_2	**108,227**	**26,660**	**39,503**
$L_8D_2L_1$	507	14,266	7,345
$L_7D_2L_2$	580	6,307	5,367
$L_6D_2L_3$	881	11,552	8,743
$L_5D_2L_4$	1,420	11,058	9,986
$L_4D_2L_5$	1,291	8,594	9,693
$L_3D_2L_6$	572	16,292	11,615
$L_2D_2L_7$	279	7,125	7,352
$L_1D_2L_8$	159	9,387	6,027
D_2L_9	4,980	2,908	10,959
$D_1L_9D_1$	849	5,596	3,155
Total	119,745	119,745	119,745

TABLE VIII: The effect of *Pass-Scroll* and *Pass-Roll* interfaces on the frequency of 11 length distinct simple and complex passwords in the Rockyou dataset.

Password	*Original*	*Pass-Scroll*	*Pass-Roll*
Simple	387,521	469,178	464,344
Complex	478,491	534,211	531,022
Total	866,012	1,003,389	995,366
Structures	13,052	18,347	18,137

  - *Complex.* Originally, L_9D_2 with 108,227 occurrences was the most frequent 11 length complex password structure in the Rockyou dataset. After simulating the use of *Pass-Scroll*, L_9D_2 still remains the most popular complex password structure, however, its frequency is reduced to 26,660. If the initial password has a complex structure (at least two character classes) then performing rotation operation also affects its structure (Fig.2). Table VII illustrates how *Pass-Scroll* distributes the popularity of L_9D_2 among its rotated variants. The password structures such as $L_2D_2L_7$, $L_1D_2L_8$ which were originally underutilised in the Rockyou dataset are now better utilised due to rotation.

    Further, after using *Pass-Scroll*, the number of 11 length complex structures increased from 13,052 to 18,347 (40.67% increase). Similar improvements occur due to *Pass-Roll* as well. Thus, rotation not only makes the structure distribution more uniform but it also improves the number of distinct structures which results in better

security against offline attacks. Also, originally the offline attacker [42] could recover about 60% of the complex Rockyou passwords by exploring the top 10 complex password structures. After simulating the use of *Pass-Scroll* on the Rockyou dataset, the attacker could recover only 26% passwords from the top 10 complex password structures (Fig.3). These improvements are considerable given that users just have to tweak and remember the new starting point of their password.

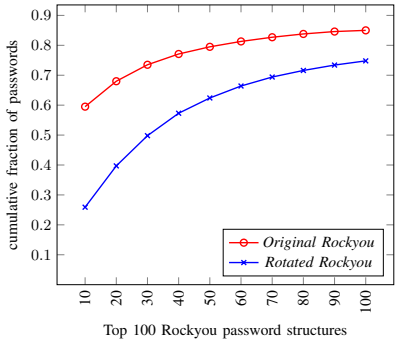


Fig. 3: Comparing the distribution of 11 length passwords in the top 100 complex password structures of original and rotated (*Pass-Scroll*) Rockyou dataset.

Thus, due to uncertain starting point choices, rotated passwords are now more distinct and therefore more resistant to online guessing attacks. Rotation also improves the number of password structures and therefore offers more resistance to offline guessing attacks.

- **Password Strength.** Weir *et al.* [41] proposed a method to compute the strength of human-generated passwords using the probabilities of password structures and their components. These probabilities are learned from the breached password databases [10]. According to their model, if the password structure is popular (highly probable) then the password is more vulnerable to offline attacks. For instance, L_9D_2 is the most popular 11 length complex structure in the Rockyou dataset. If the user creates a new password using this structure, then its probability will be relatively high, making it susceptible to offline attacks. Since, rotation modifies the structure of a password, users can now utilise rare (less probable) password structures such as $L_1D_2L_8$ and create much stronger passwords.

C. Practical Attacks using PGS

The distribution of human-generated passwords is highly skewed (biased) [23], [14]. Our rotation interfaces attempt to reduce this skewness by distributing the frequency of a password among its rotational variants. Reducing the skew results in a relatively more uniform distribution which increases the effort of guessing attacks. We demonstrate this by considering 11 length passwords that were used by at least 10 users on the Rockyou website. In other words, we focus on 11 length passwords from the Rockyou dataset [7] having frequency count of at least 10. There are 4,502 such passwords shared by total 163,439 users. After simulating the use of Pass-Scroll (Table IV), the number of distinct passwords increased from 4,502 to 35,086 ($\sim$8 times). Prior to performing rotation, the attacker could crack passwords of 163,439 users within just 4,502 guesses but after performing rotation and assuming that the rotation is incorporated in the guessing strategy, the attacker could compromise only 21,097 accounts within 4,502 guesses. To crack passwords of all 163,439 users, the attacker needs at least 35,086 ($\sim$8 times more) guesses. Thus, the use of our interfaces results in a decreased efficiency even if the rotation strategy is considered in guessing (online and offline) attacks.

Of 195 participants who completed the online study, 139 chose a new starting point to rotate their *initial password*. To gauge the security improvements due to rotation against current password cracking strategies, we submitted all 139 initial-rotated (I-R) password pairs to CMU's Password Guessing Service (PGS) [39]. We measured the security of all 139 pairs against four different attack strategies, namely, John the Ripper (JTR), Hashcat, Markov model and Probabilistic Context Free Grammar (PCFG). We define guessing resistance G^p of a password p as the minimum number of guesses required to crack p using any of these four attacking strategies.

$$G^p = min(G^p_{JTR}, G^p_{Hashcat}, G^p_{Markov}, G^p_{PCFG}) \quad (2)$$

where G^p is the minimum number of guesses required to crack the password p and, G^p_{JTR}, $G^p_{Hashcat}$, G^p_{Markov} and G^p_{PCFG} are the number of guesses required to crack p using JTR, Hashcat, Markov model and PCFG respectively. For instance, if the number of guesses required to crack the password *monkey* using JTR, Hashcat, Markov model and PCFG is 70, 50, 40 and 30 respectively, then $G^{monkey}_{min} = 30$. If the password p is not guessable by any of the attacking strategy, then we assign $G^p = \infty$.

TABLE IX: Comparing guessing resistance of initial and rotated passwords (created in the online experiment) using PGS.

Initial-Rotated	Description	$\frac{G^{rotated}}{G^{initial}}$
66 (47.48%)	$G^{initial} = G^{rotated} = \infty$	-
16 (11.52%)	$G^{rotated} = \infty$	∞
46 (33.09%)	$G^{initial} << G^{rotated}$	2^{22}
11 (7.91%)	$G^{initial} > G^{rotated}$	$1/2^3$
139		

The PGS results are summarized in Table IX. 66 out of 139 initial-rotated (IR) password pairs were not guessed by any of the strategies, *i.e.* $G^{initial} = G^{rotated} = \infty$. Therefore, we focus on the remaining 73 initial-rotated password pairs.

- In 16 of these 73 pairs, initial passwords were guessed by at least one attacking strategy but the corresponding rotated passwords remained unguessable, *i.e.* $G^{rotated} = \infty$.
- In the remaining 57 pairs, both initial and rotated passwords were guessable. 11 of these initial passwords were nearly 2^3 times stronger than their rotated counterparts while the remaining 46 initial passwords were very weak (2^{22} times on an average) as compared to their rotated counterparts.
- Thus, changing the starting point improved the practical security as 16+46 = 62 out of 73 initial-rotated password pairs have more guess-resistant rotated passwords than the corresponding initial ones.

VI. Usability Results

Now, we investigate the usability of *Pass-Scroll* and *Pass-Roll* interfaces. Specifically, we examine dropout rates, password creation, storage behaviour, memorability, efficiency and

the sentiments of participants. While discussing dropout rates we consider all 228 participants who registered for the study and for the remaining discussion, we concentrate only on the 195 participants who completed the study.

A. Study Dropout

A total 228 participants enrolled for the online study of which 115 were randomly assigned to *Pass-Scroll* condition and the remaining 113 were assigned to *Pass-Roll* condition. 219/228 (96.05%) participants completed the password *creation phase*. After 72 hours, 203/228 (89.04%) participants returned for the *recall phase* and 195/228 (85.53%) completed the entire study. The details are given in Table X.

98.26% (113/115) participants in *Pass-Scroll* condition and 93.81% (106/113) participants in *Pass-Roll* condition completed the *creation phase* while 86.96% (100/115) participants in *Pass-Scroll* condition and 84.07% (95/113) participants in *Pass-Roll* condition completed the *recall phase*.

TABLE X: Dropout rates in the online experiment.

	Creation (Day 1)		**Recall (Day 4)**	
Condition	Enrolled	Created	Returned	Completed
Pass-Scroll	115	113 (98.26%)	105 (91.30%)	100 (86.96%)
Pass-Roll	113	106 (93.81%)	98 (86.73%)	95 (84.07%)
Total	228	219 (96.05%)	203 (89.04%)	195 (85.53%)

B. Password Creation

The study required participants to create at least 8 characters (initial) password. Of 195 participants who completed the study, 13 failed to comply with this minimum length requirement. However, after displaying the policy, all 13 participants created valid password in the following attempt. Then, in the next step, participants were provided with an option to rotate their password using one of our interfaces.

Sentiments. To capture participants' sentiments about password creation process we included two questions in the survey (appendix A). The first question was pertaining to the password creation difficulty and the second was about the fun element. 53% participants in *Pass-Scroll* condition disagreed that password creation was difficult and 31% remained neutral. While in *Pass-Roll* condition, 65.26% participants disagreed and 18.95% remained neutral. Moreover, 81% participants in *Pass-Scroll* condition agreed that password creation was fun and the remaining 19% were neutral. Similarly, 75.79% participants in *Pass-Roll* condition agreed about fun and 20% stayed neutral. *Therefore, most participants did not find it difficult to create password using our interfaces and the entire process was fun.*

Real Behaviour. To understand the real-world password creation behaviour of participants, we asked participants if they would have used a similar password provided in this study for their real email account (appendix B). 48% of the participants in *Pass-Scroll* condition and 42.11% in *Pass-Roll* condition confirmed that nothing would have changed and they would have behaved no differently for creating their real account. Similar results were observed when Fahl *et al.* [21] investigated the ecological validity of online and laboratory password studies by comparing the study passwords of participants with their real university passwords. The authors found that 46% of the passwords from the online study and 49% of the passwords from the laboratory study were fully representative of the participants actual passwords.

C. Cues

76 participants (of 100) in *Pass-Scroll* condition and 63 participants (of 95) in *Pass-Roll* condition chose a new starting point to rotate their password. When asked about their starting point selection strategy, 30.27% participants in *Pass-Scroll* condition reported choosing a character, 25% chose a node number, 43.42% chose starting point randomly based on the perceived complexity of the rotated password and the remaining 1.31% reported choosing some other strategy. While in *Pass-Roll* condition, 31.75% participants reported choosing a character, 25.39% chose a node number, 31.75% chose the rotated version of the initial password randomly and the remaining 11.11% chose some other strategy.

D. Memorability

The use of rotation interfaces improved guessing resistance by at least a factor of 8. To evaluate the usability-security trade-off due to the use of our interfaces, we focus on data pertaining to starting points only. We measure memorability in terms of:

- number of users who successfully recalled starting point of their password during the *recall phase* and
- average login attempts required for successful recall of the starting point.

Storage. Depending on whether participants reported storing their password or not, we classify participants into two categories, *storage* and *no-storage*. 49/100 (49%) participants in *Pass-Scroll* condition reported not storing their password and therefore belong to *no-storage* category while the remaining 51/100 (51%) reported storing their password on various mediums such as paper (27%), computer (19%), phone (2%), password manager (1%), browser (1%) and belong to *storage* category. 55/95 (57.89%) participants in *Pass-Scroll* condition belong to *no-storage* category while the remaining 40/95 (42.11%) participants reported storing their password on various mediums such as paper (20%), computer (18.95%), phone (1.05%), password manager (1.05%), browser (1.05%) and belong to *storage* category.

We report the memorability results for both categories separately. During recall, on wrong password entry, we asked participants to enter both *initial password* and starting point again. We did not inform participants if the entered initial password or starting point was wrong. Further, at most five failed attempts were allowed.

Recall Success. Memorability was good as *93.88% of the no-storage participants in Pass-Scroll condition and 98.18% in Pass-Roll condition successfully recalled their starting point in just 1.30 and 1.15 trials respectively (Table XI).*

Failed Attempts. After investigating failed login attempts of *no-storage* participants, we found that most of them chose a new starting point to rotate their initial password during creation but during recall they submitted their initial password with the default starting point *i.e.* without performing rotation. About 57% of the participants who required more than one attempt in both conditions failed due to this reason.

Another major cause of failed attempts particularly with

Pass-Scroll interface was due to confusing the actual starting point with its neighbouring points. For instance, if the participant chose node x as a new starting point for their initial password I during creation then during recall they mistook neighbouring nodes $x-1$ or $x+1$ as their actual starting point x. We attribute these failure to the linear layout of *Pass-Scroll* interface which do not provide spatial cues. 35.71% of the *no-storage* participants in *Pass-Scroll* condition who required more than one attempt for successful recall were baffled by nodes in the neighbourhood of actual starting point.

TABLE XI: The average login attempts and median recall time of successful participants in the *recall phase*.

	No-storage		**Storage**	
	Pass-Scroll	*Pass-Roll*	*Pass-Scroll*	*Pass-Roll*
Attempt 1	35 (71.43%)	49 (89.09%)	41 (80.40%)	29 (72.50%)
Attempt 2	8 (16.33%)	3 (5.45%)	3 (5.88%)	4 (10.00%)
Attempt 3	3 (6.12%)	2 (3.64%)	3 (5.88%)	4 (10.00%)
Successful	46 (93.88%)	54 (98.18%)	47 (92.16%)	37 (92.50%)
Avg attempts	1.30	1.15	1.19	1.32
Recall time	3.03s	2.75s	4.58s	3.66s
#Participants	49	55	51	40

E. Efficiency.

We measure efficiency in terms of:

- time required to choose the starting point of the password during the *creation phase* and
- time required to recall the starting point of the password during the *recall phase*.

Creation Time. During creation, participants explored various starting points to rotate their *initial password*. Participants who used *Pass-Scroll* interface tried 2.39 starting points on an average while those who used *Pass-Roll* interface tried 2.54 starting points on an average before settling on the final starting point. As a consequence, the time required to choose the starting point using *Pass-Scroll* and *Pass-Roll* is 17.71s and 15.40s respectively.

Recall Time. During recall, a large proportion of participants in both *Pass-Scroll* (50%) and *Pass-Roll* (55.79%) conditions selected their starting point without viewing their initial password in plaintext. This data suggests that the spatial and verbal cues provided by our interfaces were helpful. *The median recall time in Pass-Scroll condition for no-storage category participants is 3.03s while in Pass-Roll condition it is 2.75s.*

We note that users typically take more time to login on graphical interfaces as compared to entering textual passwords [13]. For instance, graphical-based *PassFaces* system [5] in which the user recognizes a pre-selected face among a set of 9 decoy faces arranged in a 3X3 grid takes 4.0s on an average to complete one round. There are total 5 rounds in *PassFaces* which require about 20.0s [16], [19]. Another instance *PassPoints* [44] in which users recall a sequence of 5 points on a pre-selected image requires about 24.25s on an average (a single point requires 4.85s) even after practicing for ten times. On the other hand in *Pass-Scroll* and *Pass-Roll* interfaces, we present users with $l \geq 8$ discrete nodes (where l is textual password length) arranged in either linear or circular fashion and ask them to recall a single pre-selected node (starting point) which takes at most 3.03s without any practice sessions.

F. Acceptability

In the post-experiment survey, *90% of the participants in both Pass-Scroll and Pass-Roll conditions agreed that interface is easy to use*. Further, *more than 93% of the participants in both conditions preferred our systems over the existing conventional text-based password system.*
Also, *the average SUS score of the Pass-Scroll and Pass-Roll systems turned out to be 70.65 and 70.47 respectively. The systems with the SUS score of 70 are considered to be good [12]. We think that these results are encouraging considering the fact that participants were not trained to use our systems.*

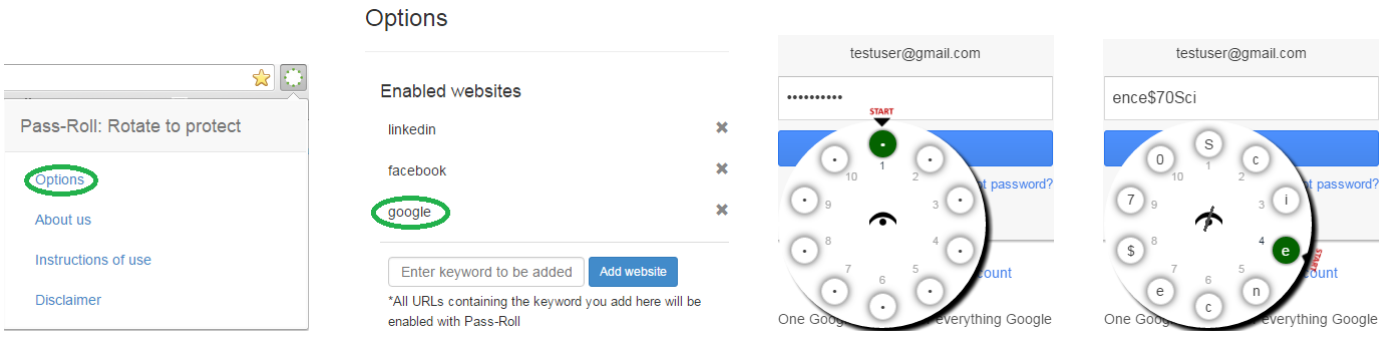
VII. Limitations

Our study does not include a control group without interface, thus our usability comparisons are informal. One control condition could be to allow users to choose a password and then ask them to extend it with a digit. However, appending a digit is already a common operation among users [38]. Further, the real-world password data shows that users do not choose digits randomly. After analysing the minimum 8 length passwords terminating with a digit in the Rockyou and Yahoo datasets [7], we found that 58.14% of the Rockyou passwords and 59.69% of the Yahoo passwords end with digit '1'. Consequently, the entropy due to choosing a digit (0-9) at the end of a password in the Rockyou and Yahoo datasets is 2.21 bits ($2^{2.21} = 4.63$) and 2.17 bits ($2^{2.17} = 4.50$) respectively. These entropies are less than 3.04 bits ($2^{3.04} = 8.22$) and 3.17 bits ($2^{3.17} = 9$) obtained due to the use of *Pass-Roll* and *Pass-Scroll* rotation interfaces in the online experiment.

More than 95% of the participants in our study were educated and may have better memory than average, which could positively influence the usability results. Further, only 195 participants completed the study and with a larger population we might be able to observe further patterns. However, the purpose of this study was to determine whether *Pass-Scroll* and *Pass-Roll* interfaces influence users to rotate their password. As the experimental data indicates, most participants used our interfaces to rotate their password. Also, we did not find any statistically significant difference in the usability results of *Pass-Scroll* and *Pass-Roll* interfaces.

VIII. Deployment

In all our experiments, both *Pass-Scroll* and *Pass-Roll* systems operated in two steps. In the first step, the system gets an initial password from the participant and in the second step it arranges the initial password in either linear or circular fashion, thereby allowing the participant to choose (or recall) a starting point for their password. These two separate steps were constructed for study purpose to measure the time required to choose (or recall) new starting point more precisely. These two steps can be easily merged, for instance, as the user types characters of her password, the nodes can be generated and arranged in either linear or circular fashion on the fly. Users can then click on the starting point and finally submit the rotated password to the server.
Our interfaces require no server-side changes and can be easily deployed on the client-side as a browser plug-in. For demonstration purpose, we developed Pass-Roll [3] and Pass-Scroll [4] extensions for Google Chrome browser which can be



(a) Install *Pass-Roll* (b) Enable website (c) Use *Pass-Roll* (d) *Rotate to Protect*

Fig. 4: (a) *Pass-Roll* deployed as a Chrome browser extension. (b) The *Pass-Roll* plugin is enabled for Google website. (c) After enabling, it can be used to rotate the initial password. For instance in (d), the initial password **Science$70** is rotated to **ence$70Sci**. After clicking on submit button, **ence$70Sci** is sent to the Google server. In the figure, the password is displayed in plaintext for illustration purpose only. Also, note that *Pass-Roll* does not store users' passwords, it is used just to help users to rotate their passwords.

installed, enabled and used as follows. We give the procedure for *Pass-Roll*. *Pass-Scroll* can be used similarly.

(1) **Install.** Add *Pass-Roll* extension [3] from Chrome Store.
(2) **Enable.** Right click on the *Pass-Roll* icon located in toolbar and select *Options* menu from the drop-down list (Fig.4a). To enable a website for using *Pass-Roll*, specify any keyword from the its URL and then click on *Add website* button (Fig.4b). *Pass-Roll* is now ready to use.
(3) **Use.** The extension becomes active as soon as the user starts typing their password in the password field of the *Pass-Roll* enabled website. We suggest resetting the password of the newly enrolled website by choosing an initial password and a new starting point using *Pass-Roll* interface. Next, during login, the user can enter the initial password in the password field and use *Pass-Roll* to click on the starting point to generate the rotated version of their password (Fig.4c,d). Note that, *Pass-Roll* extension does not store any password-related information, it is used just to help users to rotate their passwords.

IX. Related Work

The password creation strategies of users have been well documented. In 1978, Morris and Thompson [28] analysed 3289 passwords and found that 86% of them are composed using lowercase letters and digits. Nearly 30 years later, Florencio and Herley [22] studied the passwords of 5 million users and reached the same conclusion. Recently, a large scale analysis of 100 million passwords by Li *et al.* [25] once again confirmed the dominance of lowercase letters and digits in the composition of passwords. Thus, in the past four decades, user behaviour has not changed much. The theoretical password space is enormous but the utilised space remains small.

Users choose easy to remember passwords which are also easy to guess. Various strategies have been proposed to counter guessing attacks. Most websites enforce stringent policies requiring passwords to be composed of at least one lowercase, uppercase, digit and symbol. However, research [33] shows that people use uppercase letters, digits, symbols at predictable positions which again results in underutilisation of the search space. Schechter *et al.* [31] suggested tracking the frequency count of every password using a count-min sketch data-structure and banning only those passwords that reach certain popularity threshold. However, such techniques require server-side changes. The password strength meters positively impact user choices during password creation [20], [37]. However, the currently deployed strength meters fail to capture the complexity of human-generated passwords [17].

To overcome the problems of textual passwords, various graphical schemes have been proposed [13]. Graphical passwords exploit humans' superior memory for recognizing and recalling visual information as opposed to verbal or textual information. According to dual-coding theory [29], [30] verbal (word-based) and non-verbal (image-based) memory are processed and represented differently in the brain. The storage of graphical information is a one-step process while the storage of textual information is a two-step process and therefore requires more effort. However, these graphical schemes cannot be incorporated by current websites without requiring major changes to their systems [15]. Our cued-based interfaces on the other hand can be easily deployed as browser plugins. Also, the theoretical security of the most graphical password schemes is much less than textual passwords [13]. In our work, we tried to improve the security of text passwords by taking advantage of users' memory for graphical information.

X. Conclusion

Password interface has been the same for the past four decades and so has been the password creation strategies of users. In this work, we demonstrated how a simple design change can influence users to create relatively secure text passwords. The *Pass-Scroll* and *Pass-Roll* interfaces provide users with more control and encourage users to perform rotation operation on their passwords. Both laboratory and online experiments show that these rotation interfaces are intuitive and can be used without any training. Further, the use of our interfaces on minimum 8 length passwords improved guessing resistance by at least 3 bits. Moreover, these interfaces require no server-side changes and can be easily deployed as browser extensions. Hence, we encourage their use.

Future Work. Today, a typical user has 25 password-protected online accounts [22]. Many users cope with multiple credentials by reusing the same password across different accounts. The next natural step would be to study whether such behaviour persists if the rotation interfaces are used on multiple websites. Also, a majority of participants (95%) in our experiments created their password using either desktop or laptop. It would be interesting to study the usability and security of *Pass-Scroll* and *Pass-Roll* systems on mobile phones and tablets.

REFERENCES

[1] "CrowdFlower," Website, retrieved 15 March, 2017 from https://www.crowdflower.com/.

[2] "Introducing Contributor Performance Levels!" Website, retrieved 15 March, 2017 from http://crowdflowercommunity.tumblr.com/post/80598014542/introducing-contributor-performance-levels.

[3] "Pass-Roll," Website, retrieved 15 March, 2017 from https://chrome.google.com/webstore/detail/pass-roll/finieofpmfjhijooekckemcmnlinkkbj?hl=en.

[4] "Pass-Scroll," Website, retrieved 15 March, 2017 from https://chrome.google.com/webstore/detail/pass-scroll/ffjkcnhkmdgkabcdabiacjfppgfncmjb?hl=en.

[5] "Passfaces: Two Factor Authentication for the Enterprise," Website, retrieved 15 March, 2017 from http://www.passfaces.com/.

[6] "Password Storage Cheat Sheet," Website, retrieved 15 March, 2017 from https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet.

[7] "Passwords," Website, retrieved 15 March, 2017 from https://wiki.skullsecurity.org/index.php?title=Passwords#Leaked_passwords.

[8] "Rotate to Protect," SOUPS'16, retrieved 15 March, 2017 from https://www.usenix.org/sites/default/files/soups16poster13-tupsamudre.pdf.

[9] "System Usability Scale," Website, retrieved 15 March, 2017 from https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[10] "World's Biggest Data Breaches," Website, retrieved 15 March, 2017 from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[11] J. R. Anderson and G. H. Bower, "Recognition and retrieval processes in free recall." *Psychological Review*, vol. 79, no. 2, p. 97, 1972.

[12] A. Bangor, P. Kortum, and J. Miller, "Determining what individual sus scores mean: Adding an adjective rating scale," *J. Usability Studies*, vol. 4, no. 3, pp. 114–123, May 2009. [Online]. Available: http://dl.acm.org/citation.cfm?id=2835587.2835589

[13] R. Biddle, S. Chiasson, and P. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.*, vol. 44, no. 4, pp. 19:1–19:41, Sep. 2012. [Online]. Available: http://doi.acm.org/10.1145/2333112.2333114

[14] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, ser. SP '12, 2012, pp. 538–552.

[15] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "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*, ser. SP '12, 2012, pp. 553–567.

[16] S. Brostoff and M. A. Sasse, *Are Passfaces More Usable Than Passwords? A Field Trial Investigation*. London: Springer London, 2000, pp. 405–424. [Online]. Available: http://dx.doi.org/10.1007/978-1-4471-0515-2_27

[17] X. D. C. D. Carnavalet and M. Mannan, "A large-scale evaluation of high-impact password strength meters," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 1:1–1:32, May 2015.

[18] L. Church and A. Whitten, "Generative usability: Security and user centered design beyond the appliance," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, ser. NSPW '09. New York, NY, USA: ACM, 2009, pp. 51–58. [Online]. Available: http://doi.acm.org/10.1145/1719030.1719038

[19] P. Dunphy, A. Fitch, and P. Olivier, "Gaze-contingent passwords at the atm," in *In 4th Conference on Communication by Gaze Interaction (COGAIN)*, 2008.

[20] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?: The impact of password meters on password selection," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13, 2013, pp. 2379–2388.

[21] S. Fahl, M. Harbach, Y. Acar, and M. Smith, "On the ecological validity of a password study," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, USA: ACM, 2013, pp. 13:1–13:13. [Online]. Available: http://doi.acm.org/10.1145/2501604.2501617

[22] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*, ser. WWW '07, 2007, pp. 657–666.

[23] Imperva, "Consumer password worst practices," Website, March 2010, retrieved 15 March, 2017 from http://www.imperva.com/docs/WP_Consumer_Password_worst_Practices.pdf.

[24] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: Measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11, 2011, pp. 2595–2604.

[25] Z. Li, W. Han, and W. Xu, "A large-scale empirical analysis of chinese web passwords," in *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA, Aug. 2014, pp. 559–574.

[26] T. Mandel, *The Elements of User Interface Design*. New York, NY, USA: John Wiley & Sons, Inc., 1997, ch. The Golden Rules of User Interface Design, pp. 5.1–5.28.

[27] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur, "Measuring password guessability for an entire university," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 173–186. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516726

[28] R. Morris and K. Thompson, "Password security: A case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, Nov. 1979.

[29] A. Paivio, *Mind and its evolution: A dual coding theoretical approach*. Psychology Press, 2014.

[30] M. Sadoski and A. Paivio, "A dual coding view of imagery and verbal processes in reading comprehension." 1994.

[31] S. Schechter, C. Herley, and M. Mitzenmacher, "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks," in *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, ser. HotSec'10, 2010, pp. 1–8.

[32] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur, "A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2903–2912. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702586

[33] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: User attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10, 2010, pp. 2:1–2:20.

[34] E. Tulving and S. Osler, "Effectiveness of retrieval cues in memory for words." *Journal of experimental psychology*, vol. 77, no. 4, p. 593, 1968.

[35] E. Tulving and D. M. Thomson, "Encoding specificity and retrieval processes in episodic memory." *Psychological review*, vol. 80, no. 5, p. 352, 1973.

[36] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?" in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 3748–3760. [Online]. Available: http://doi.acm.org/10.1145/2858036.2858546

[37] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "How does your password measure up? the effect of strength meters on password creation," in *Proceedings of the 21st USENIX Conference on Security Symposium*, ser. Security'12, 2012, pp. 5–5.

[38] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "I added '!' at the end to make it secure: Observing password creation in the lab," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, Jul. 2015, pp. 123–140. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/ur

[39] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, "Measuring real-world accuracies and biases in modeling password guessability," in *24th USENIX Security Symposium (USENIX Security 15)*, Washington, D.C., Aug. 2015, pp. 463–481.

[40] R. Veras, C. Collins, and J. Thorpe, "On semantic patterns of passwords and their security impact." in *NDSS*, 2014.

[41] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "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*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 162–175. [Online]. Available:

http://doi.acm.org/10.1145/1866307.1866327
[42] M. Weir, S. Aggarwal, B. d. Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, ser. SP '09, 2009, pp. 391–405.
[43] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0," in *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, ser. SSYM'99. Berkeley, CA, USA: USENIX Association, 1999, pp. 14–14. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251421.1251435
[44] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon., "Authentication using graphical passwords: Basic results." in *11th International Conference on Human-Computer Interaction (HCI International)*, 2005.

APPENDIX

We give a list of survey questions that were asked to participants during study. We also list responses of participants in form of a tuple (x, y). The first part x of the response tuple belong to *Pass-Scroll* participants and the second part y belong to *Pass-Roll* participants.

A. Creation Phase Questionnaire

(1) Creating a password in this study was difficult?
  (a) Strongly Agree
  (4%, 6.31%)
  (b) Agree
  (12%, 9.47%)
  (c) Neutral
  (31%, 18.95%)
  (d) Disagree
  (31%, 31.58%)
  (e) Strongly Disagree
  (22%, 33.68%)

(2) Creating a password in this study was fun?
  (a) Strongly Agree
  (29%, 34.74%)
  (b) Agree
  (52%, 41.05%)
  (c) Neutral
  (19%, 20%)
  (d) Disagree
  (0%, 3.16%)
  (e) Strongly Disagree
  (0%, 1.05%)

(3) Your strategy to choose starting position for arriving at rotated password? (Only for participants who chose new starting point)
  (a) I chose node number as starting position
  (25%, 25.39%)
  (b) I chose character from my password as starting position
  (30.27%, 31.75%)
  (c) It was a random choice
  (43.42%, 31.75%)
  (d) Other
  (1.31%, 11.11%)

(4) On what sort of computer or device have you just entered your password?
  a) Tablet
  (1%, 1.05%)
  b) Desktop computer
  (55%, 56.85%)
  c) Smartphone
  (1%, 1.05%)
  d) Laptop computer
  (40%, 40%)
  e) I prefer not to answer
  (3%, 1.05%)
  f) Other
  (0%, 0%)

(5) Are you majoring in or do you have a degree or job in computer science, computer engineering, information technology, or a related field?
  (a) Yes
  (29%, 27.27%)
  (b) No
  (66%, 66.32%)
  (c) I prefer not to answer
  (5%, 6.31%)

(6) What is the highest level of education that you have completed?
  (a) High School Degree
  (0%, 0%)
  (b) Associate Degree
  (17%, 14.74%)
  (c) Bachelor's Degree
  (59%, 46.32%)
  (d) Master's Degree
  (21%, 34.74%)
  (e) Other
  (1%, 2.10%)
  (f) I prefer not to answer
  (2%, 2.10%)

(7) What is your gender?
  (a) Female
  (24%, 35.79%)
  (b) Male
  (76%, 64.21%)
  (c) I prefer not to answer
  (0%, 0%)

(8) How old are you?
(9) What is your nationality?

APPENDIX

B. Recall Phase Questionnaire

(1) Did you write down or store the password your created in this study? Please be honest, you get paid regardless and this will help our research.
  (a) I did not write down or store my password
  (49%, 57.89%)
  (b) I wrote down my password on paper
  (27%, 20.00%)
  (c) I stored my password on the computer
  (19%, 18.95%)
  (d) I stored my password on my phone or another electronic device
  (2%, 1.05%)
  (e) My password manager remembered my password
  (1%, 1.05%)
  (f) My browser remembered my password
  (1%, 0%)

(g) I prefer not to answer
(1%, 0%)
(h) Other
(0%, 1.05%)

(2) On what sort of computer or device have you just entered your password?
(a) Tablet
(2%, 0%)
(b) Desktop computer
(52%, 55.79%)
(c) Smartphone
(1%, 1.05%)
(d) Laptop computer
(45%, 42.11%)
(e) I prefer not to answer
(0%, 1.05%)
(f) Other
(0%, 0%)

(3) Consider the password you created for this study. If you were creating a password for your real email account under the same password-creation rules as used in this study, what would you have done differently? You may choose more than one.
(a) Nothing would have changed
(48%, 42.11%)
(b) I would have used more symbols
(20%, 22.11%)
(c) I would have used more uppercase letters
(9%, 18.95%)
(d) I would have reused a password, but did not reuse a password for this study
(8%, 4.21%)
(e) I would have used an easier-to-type password
(5%, 9.47%)
(f) I would have used an easier-to-remember password
(11%, 9.47%)
(g) I would have used a longer password
(14%, 8.42%)
(h) I would have used more digits
(7%, 10.53%)
(i) Other
(5%, 2.10%)

APPENDIX

C. SUS Questionnaire

SUS questionnaire comprises of the following 10 questions with responses measured on a five-point Likert scale (Strongly Agree to Strongly Disagree).

(1) I think that I would like to use this system frequently.
(2) I found the system unnecessarily complex.
(3) I thought the system was easy to use.
(4) I think that I would need the support of a technical person to be able to use this system.
(5) I found the various functions in this system were well integrated.
(6) I thought there was too much inconsistency in this system.
(7) I would imagine that most people would learn to use this system very quickly.
(8) I found the system very cumbersome to use.
(9) I felt very confident using the system.
(10) I needed to learn a lot of things before I could get going with this system.