University of Dhaka

Computer Science and Engineering

Device New Technique for a Stronger Yet Memorable Textual Password for Smart Phone

By:
Md. Faruk Hossain
Roll: 84
Md. Mizanur Rahman
Roll: 60

Supervisor:
Dr. Sarker Tanveer Ahmed Rumee,
Assistant Professor.
Computer Science and Engineering,
University of Dhaka.

January 2, 2019

Abstract

Authentication is one of the primary way to keep personal information secure. Textual passwords is the most common way for this process. To make this process more secured we can analyze the concept of password for mass users. The analysis includes how the password concept varies from user to user depending on the age, educational qualification, technological knowledge and keyboard layouts structure in smart phone. The survey will be done with appropriate questionnaires which will provide mass data on the users password pattern. Depending on the information provided by the users there will be inference about how textual password can be made more secure in smart phone and introduce a new layout model which will influence user to create strong password.

Contents

1 Introduction

Information Systems security is one of the biggest challenges facing society's technological age. Information Systems have become an integral part of everyday life in the home, businesses, government, and organizations. Therefore, security of the information has become a prime concern. Authentication, being an important subfield of security, received much attention among usable security researchers. Many authentication schemes have been proposed to keep a balance between usability and security, like drawing a doodle or identifying a spot on Google Maps [38, 45, 115](hoque uta). However, textual passwords came out to be the simplest and cost effective authentication process [11](hoque uta). As a result, textual password-based authentication scheme still remains the most favorable form of user authentication on the Web, and there is little chance in the near future that the scenario might change [55](hoque uta).

However, textual password-based authentication is not the ultimate solution since security is a prime concern here. A good password need to support two conflicting requirements at the same time: being "easy to remember" and "hard to guess" [120](hoque uta). Extensive prior work has examined how password composition policies affect password strength and usability on laptops and desktops (e.g., [39, 45, 48])(chi2016). But, electronic device landscape has changed significantly over the last decade. Mobile devices, such as smartphones and tablets, have become very popular and are now used not only for calling and sending text messages, but also for email, web surfing, social networking, and banking [18](chi2016). Most of these activities use textual password-based authentication for security concern. Unfortunately, due to the limitation of virtual key size and the navigation tradeoff between keyboard pages, text entry on smartphone is time consuming and error prone [29, 37, 42](chi2016). A study by Jakobsson et al. reported that password entry on handsets frustrates users due to the lack of coverage, small screen size [60](hoque uta). Prior work suggests that this problem has important effects on the usability and security of text passwords generated from smartphones [24, 51](chi2016). That implies that the passwords need to be difficult to guess. Attackers can steal the databases of the hashed passwords and then these passwords can be cracked with trillions of guesses.(e.g., [3, 5, 21, 36])(chi2016). This can be pretty damaging because people generally use passwords with minor modification for different websites and accounts.[20](chi2016). There has been major study on the textual passwords on the context of laptops and desktops while the study on the passwords generated from the smartphone is yet to be focused. Thus an important question is raised regarding the research: "What will be the device new technique for the smartphone to generate stronger yet memorable password?" From general speculation it can be said that a good password is the combination of letters, digits and special symbols. But inserting digits and symbols between the letters is not as straightforward as tradition laptop or pc keyboard. For example in iphone default keyboard layout for accessing digits after the letters requires extra shift key press where is for the traditional laptop or pc layouts both the digits and letters are accessible at the same time. That means no extra effort is required for the traditional layouts but from smartphone generating a strong password is less comfortable

In this paper, we compare the strength and usability of the textual passwords generated from the computer layouts with different current keyboard layout of smartphones. We have used commonly used smartphone layouts for the statistical analysis. We investigate the strength and the usability drawback due to the limitation of the keyboard screen size of the smartphones. We found that a new prototype for the keyboard can make the passwords generated from the smartphones more stronger and usable.
Our first work was to closely compare the strength of the textual passwords generated from the currently used keyboard layouts. We find how the password strength varies for computer and different smartphone keyboard layouts. With the recent advancement of internet and technology people now use smartphone for logging in important websites or personal accounts. To ensure the clarity of the data we implemented a utility website named "Blood Bank". Users can create personal accounts here where privacy is maintained. We analyzed the textual password provided by the 50 clients of the websites with having their permission taken for the thesis purpose. We make the comparative analysis of the entropy of the passwords generated from the different layouts. For making the evaluation of the data more significant we run different statistical test on the data.
The goal of our second work was to compare the usability of the keyboard layouts. For this we measured the typing speed of the passwords generated from the computer layouts and different smartphone layouts. This gives the idea of what will be the best entry interface keeping the fact the password must be strong. We calculate the error rate and analyze the keystroke time

for different keyboard size. 10 random people with different hand size used different layouts from which the calculation was made. This ensures the comfortable key density for the keyboard prototype which is going to be proposed.

Finally based on the previous works and our statistical analysis on the entropy and the usability measurement we propose a new keyboard layout for android smartphone. We also ensure based on the significant data analysis that the proposed layout will increase the strength and usability of the textual passwords generated.

2 Background and Related works:

According to prior research, passwords generated from smartphones are more vulnerable to guessing attacks[50](chi2016). Previous research speculated that smartphone generated passwords are significantly weaker when the attacker can made more than 10^{16}guesses.(chi2016).
In this section we review the prior work on textual passwords generated from smartphone, the alternatives of textual passwords, password entry methods etc.

2.1 Textual passwords on smartphone devices

Prior research of Zezschwitz et al. has found that textual passwords generated from smartphones contains less symbols and special characters.They analyzes on how and why mobile phones makes it difficult to enter passwords and what are the security issue due to this.[chi 2016-50].on the contrast we focus on the variation of the strength and usability in the existing keyboard patterns. Other studies had found that users who primarily work with traditional devices type passwords more slowly on mobile devices which influence password security [chi -2].Greene et al. evaluated the usability of complex, randomly generated passwords on mobile devices and found that entering the password on mobile devices increases the time to enter the password and the number of errors during password entry [chi -25].We also analyze the usability by calculating the error rate and the keystroke time on the customized layouts.Our proposed custom layout also provides a novel mechanism for inserting digits and special characters when constructing a password. It removes the burden of making an extra click when inserting digits/special characters in a password. Related works have mainly focused on improving the general typing speed on mobile phones.

2.2 Alternatives of textual passwords in smartphones

Alternative to textual passwords have been considered for authentication on mobile devices, such as graphical patterns [chi-51], fingerprint and face unlock mechanisms [chi-4], recognition-based graphical passwords [chi-16], authentication mechanisms that use the front and the back of mobile devices [chi-13], and authentication mechanisms that use all of these approaches [chi-43]. These authentication processes are promising but till now most of the websites use textual passwords for the authentication process.Due to the intensive growth of the smartphones people are using smartphones to access these websites . Therefore, quantifying and examining how best to tune the usability and security of text passwords on mobile devices remains an important topic

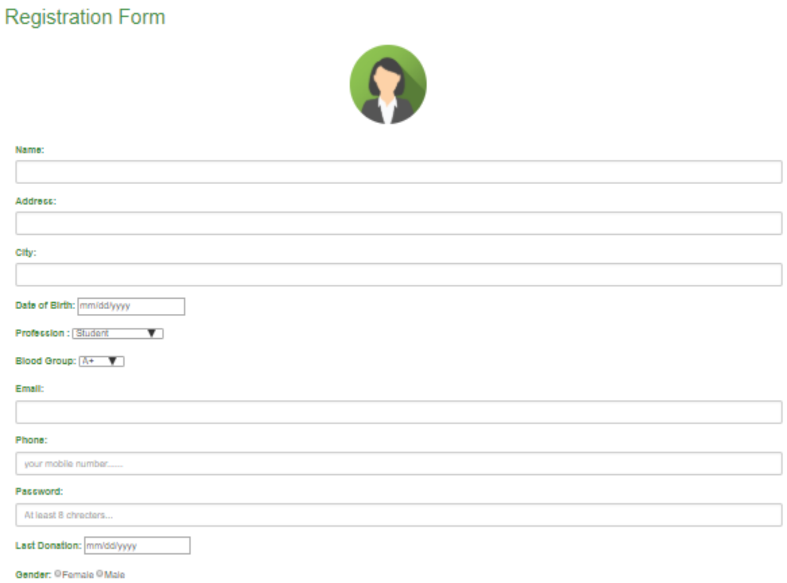
3 Thesis Objectives

1.A statistical analysis on the strength, usability and memorability of the commonly used layouts in smartphone and computer.
2.Since the password generated from the smartphone is significantly weaker because of keyboard layouts of smartphone influence to innovative new keyboard layout model for smartphone.
3.A comparative analysis on the strength, usability and memorability of the proposed layout and the commonly used layout.

4 Methodology

4.1 First phase

As we are interested in a device new technique which will increase the strength of textual passwords generated from smartphone while keeping the usability concern least, we need to analyze the current keyboard layouts of the smartphones as well as the computers. For this the first phase of our work include the comparison of the current layouts. We need to collect data from the users to check how the strength of the textual passwords varies in input constraint devices like smartphones. The development of network and technology has made the smartphone a part and parcel of our life. Now for signing up an account in online social , commercial websites people are using smartphones. Therefore the textual passwords are being generated for registration purpose. To make the analysis more significant our first challenge is to ensure the sample data be more realistic. For this , We made an utility website named “Blood Bank”. This is a website for making the blood donation process more user friendly.



Registration Form

Name:

Address:

City:

Date of Birth: mm/dd/yyyy

Profession : Student ▼

Blood Group: A+ ▼

Email:

Phone: your mobile number.......

Password: At least 8 chrocters...

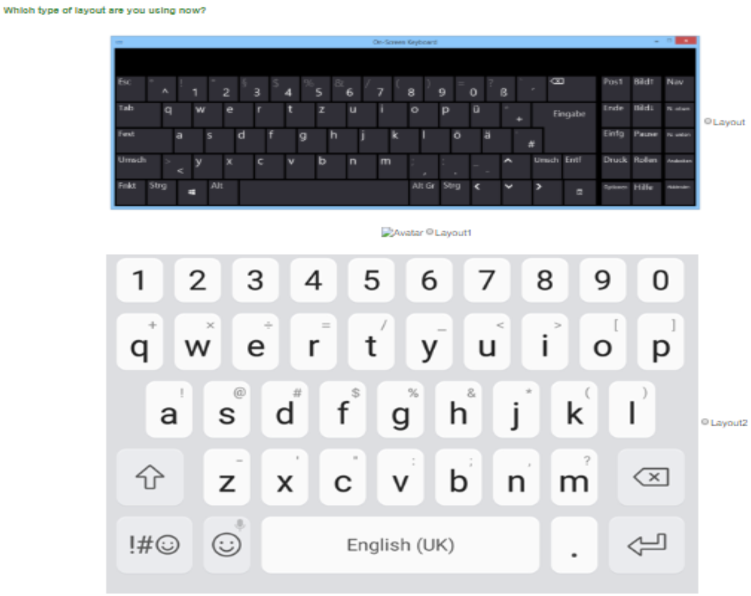
Last Donation: mm/dd/yyyy

Gender: ○Female ○Male

Figure 1: Registration form for different keyboard layout analysis.

Users can create their own profile where he can seek for a specific blood

group and available donors. There are sensitive personal data whose security is ensured by us. We used HTML, PHP, javascript for the implementation of the website.
Here , the user will register in the website with all the required information. To ensure the security of the data the authentication system is textual passwords . Since we are interested in the keyboard layouts the users are using we add some commonly used layouts sample. After giving all the information the users choose what type of keyboard he/she is using.



Which type of layout are you using now?

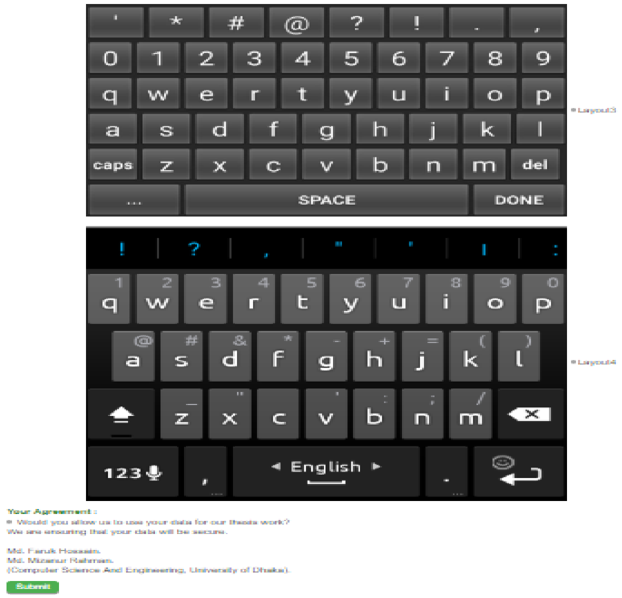
○ Layout

Avatar ○ Layout1

○ Layout2

Figure 2: Choosing own layout type.

Here , the first layout resembles the commonly used traditional keyboard of desktops or laptops. If the users give input from desktops or laptops this option is clicked. The second layout is common layout which is used in most of the android smartphones.



○ Layout3

○ Layout4

Your Agreement :

○ Would you allow us to use your data for our thesis work?
We are ensuring that your data will be secure.

Md. Faruk Hossain.
Md. Mizanur Rahman.
(Computer Science And Engineering, University of Dhaka).

Submit

Figure 3: User agreement .

Layout 3 and 4 are the other two commonly used keyboards for smartphones. Users check the options and choose the layout type which mostly resembles to their own keyboards. Since the data is being used for the research purposes we make this transparent to the users who are giving the permission for using the data

4.2 Second phase

From the first phase of the data collection and analysis we get that the addition of extra row of symbols or digits make the textual passwords generated from the smartphone more strong and usable. To check how the strength and the usability varies due to addition of extra rows of digits and symbols we develop a customized android keyboard prototype. We use android studio for the development of the customized keyboard prototype.

This keyboard protoype is used in the prior comparison analysis of the existing keyboards. We get from the calculative analysis that the entropy of the textual passwords increases .

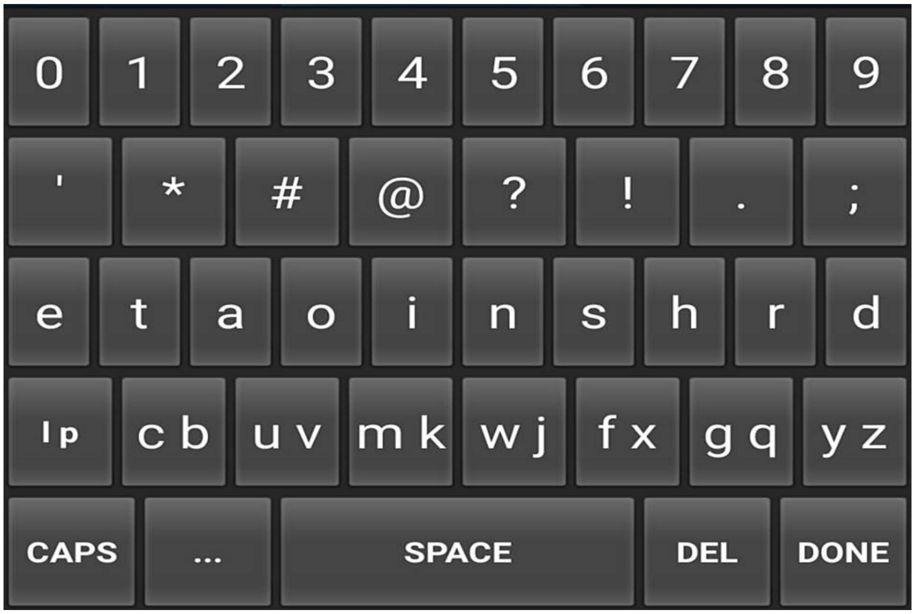


Figure 4: User agreement .

4.3 Third phase

Entropy and usability are two conflicting issue while the textual passwords are formed. The new layout increases the entropy but it must keep the usability of the generated passwords. For This reason in our third work we check the usability of the customized layout. For analysis purpose we develop 11 keyboard layouts for analysis of error rate and key stroke. The width of the screen is chosen to be 7 cm which is for moderate smartphones. Then for different length we find the change of error rate and key stoke per unit time. This gives the optimal keyboard density which is required to be maintained while adding extra rows of symbols and digits.

5 Result

In this section, we shall be describing the entropy analysis among the keyboard layouts and try to find the motives. We also try to find the relation between the error rate and key density on a keyboard for smartphone.

5.1 Entropy Analysis

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability[1]. But we have calculated the entropy value using Shannon entropy[2].

$$Entropy, E = L * log_2 N$$

where, L is the length of the password and N is the size of character. The character size is the sum of the sizes of different character types, Specifically;

- Lowercase Letters: 26
- Upparcase Letters: 26
- Digits: 10
- Symbols: 92

The calculation of entropy has been plotted in the following page where the box plot describe how the entropy are distributed and the entropy table show the means of entropy from different layout.

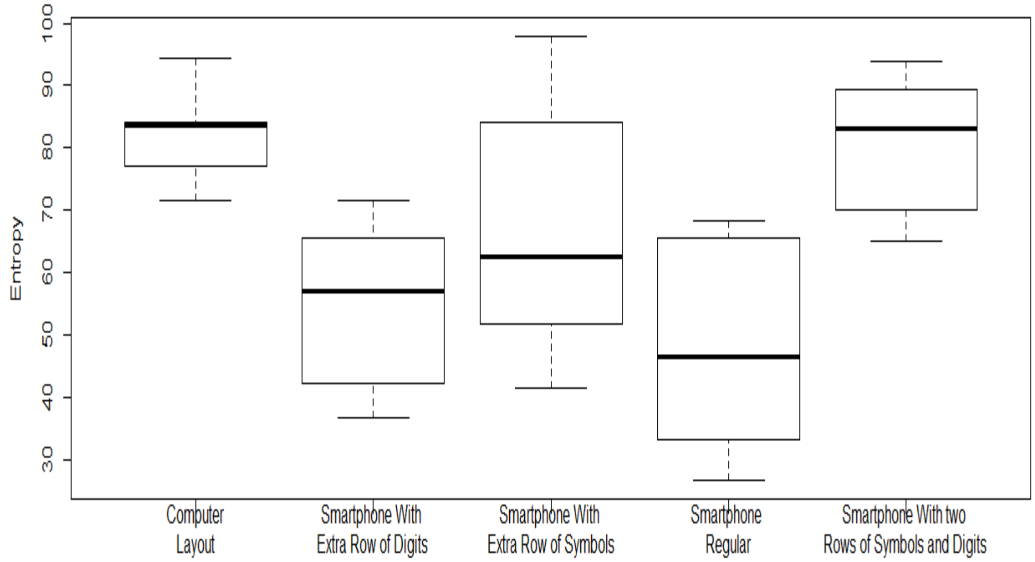


Figure 5: Entropy in different keyboard layouts.

From the above box plot[Figure 1], it is clear that the distribution of entropy of all layout are not normal. It would not be wise to compare the means to determine which layout is superior. Because Mean is very sensitive to the extreme value. So, we analysis the entropy using variance comparison. One of the powerful variance analysis is one-way analysis of variance known as ANOVA test.

5.1.1 ANOVA test

For ANOVA test, we first calculate Sum of Squre Between classes (SSB) and Sum of Squre Within class (SSW) from the entropy table.

Entropy Table					
Keyboard Layout	Computer Layout	Smartphone Layout With Extra Row of Digits	Smartphone Layout With Extra Row of Symbols	Smartphone Layout With Extra Two Rows of Symbols and Digits	Smartphone Regular layout
Number of Users	n[1]=10	n[2]=10	n[3]=10	n[4]=10	n[5]=10
Mean	$\overline{e[1]} = 82.04$	$\overline{e[2]} = 54.10$	$\overline{e[3]} = 66.39$	$\overline{e[4]} = 81.25$	$\overline{e[5]} = 48.34$

$$TotalUser, N = \sum_{i=1}^{5} n[i] = 50$$

$$GrandTotal, G = \sum_{i=1}^{5} \sum_{j=1}^{10} E[i][j] = 3321.38$$

Where, E[i][j] means ${}_jth$ number of entropy value of ${}_ith$ layout.

$$GrandMean, \overline{e} = G/N = 3321.38/50 = 66.43$$

$$SST = \sum_{i=1}^{5} \sum_{j=1}^{10} (E[i][j] - \overline{e})^2 = 17340.27$$

$$SSB = \sum_{i=1}^{5} (\overline{e} - \overline{e[i]})^2 = 9426.85$$

$$SSW = \sum_{i=1}^{5} \sum_{j=1}^{10} (E[i][j] - \overline{e[i]})^2 = 7913.42$$

Now, we shall make a ANOVA table (for Number of User: N, Numbers of Layout : k) using the SSB and SSW value.

Anova Table (N=50, K=5)				
Source of Variation	Degrees of Freedom (DF)	Sum of Squres (SQ)	Mean Squres, MS = SQ/DF	F Value
Between Classes	k-1 = 4	SSB = 9426.85	MSb=2356.71	13.40
Within Classes	N-k = 45	SSW = 7913.42	MSw=175.85	

**Means significant at 1% lavel.

From the F value table,
F(4,45) = 3.757 for 1% significance > sample F value.
So, we can tell with 99% confidence that at least there are two means which have significant difference. To identify this we shall use Least Significant Differences (LSD).

5.1.2 LSD test

From anova table,
Error variance, $EMS = N - K = 45$
For LSD calculation, we need to estimate a quantity called standard error (SE) for difference of any two means of entropy.

$$SE = \sqrt{(MSw * 2)/Numberofobservationperlayout} = \sqrt{(175.85 * 2)/10} = 5.93$$

This standard error (SE) value will be used to get the Least Significant Differences (LSD). To make the difference clear, we shall find two LSD value using t at 0.05 and 0.01 and named those as LSD5 and LSD1.

$$LSD = SE * t(k-1, N-k)$$

LSD at 5% Significance; $LSD5 = 11.86$
LSD at 1% Significance; $LSD1 = 16.01$

From this LSD values, we can determine which layout help to generate strong password.

We, want to determine how computer layout differ from other layout with 95% confidence or 5% significance.

$$LSDmean(computerLayout) = SAMPLEmean(computerLayout) - LSD5$$

$$= 82.04 - 11.86$$

$$= 70.18$$

From the entropy table, we find that LSDmean(computer Layout) is greater than SAMPLEmean(Smartphone Regular Layout).But LSDmean(computer Layout) is not greater than SAMPLEmean(Smartphone layout with two Rows of Symbols and Digits).So, we can assert that computer layout is superior to smartphone regular layout but simillar to custom layout (Smartphone layout with two extra row of symbols and digits) with 95% confidence.
For overall comparison, we shall build a table named LSD table and use the short from of layout name.

Least significant Difference(LSD) Table			
Keyboard Layout(Short Form)	Sample Mean (CM)	LSD Mean 1% significance(LSD1)	LSD Mean 5% significance (LSD)
Computer Layout (CM)	82.04	66.03	70.18
Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	81.25	65.24	69.39
Smartphone Layout With Extra Row of Symbols (SPS)	66.39	50.38	54.53
Smartphone Layout With Extra Row of Digits (SPD)	54.10	38.09	42.24
Smartphone Regular layout (SP)	48.34	22.33	36.48

Finaly, we shall make a over all comparison among different keyboard layout. For this, we shall compare LSD mean with the sample mean of other layout. If The LSD mean is greater than the sample mean (SM) of any other layout then the layout is superior for entropy. Based on this information, we have built a comparison table using short name of keyboard layouts.

For 1% significant, Comparison table:

Comparison Table for 1% significance					
Keyboard Layout(Short Form)	Computer Layout (CM)	Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	Smartphone Layout With Extra Row of Symbols (SPS)	Smartphone Layout With Extra Row of Digits (SPD)	Smartphone Regular layout (SP)
Computer Layout (CM)	similar	similar	similar	CM	CM
Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	similar	similar	similar	SPSD	SPSD
Smartphone Layout With Extra Row of Symbols (SPS)	similar	similar	similar	similar	SPS
Smartphone Layout With Extra Row of Digits (SPD)	CM	SPSD	similar	similar	similar
Smartphone Regular layout (SP)	CM	SPSD	SPS	Similar	similar

From the above comparison table, each block define the comparison result between the two layouts of that row and collum. Let take the last row (Smartphone regular layout) of the table where the first block contain CM which means that computer layout is superior to smartphone regular layout. Second block contain SPSD which means Smartphone Layout With Extra Two Rows of Symbols is superior to smartphone regular layout for entropy. Also Smartphone Layout With Extra Row of Symbols is superior. But Smartphone Regular layout is similar to Smartphone Layout With Extra Row of Digits.
Finally we assert with 1% significant that both Computer Layout and Smartphone Layout With Extra Two Rows of Symbols and Digits are better for entropy than other layouts.Now we shall make another comparison table for 5% significant from the LSD table.

For 5% significant, Comparison table:

Comparison Table for 5% significance					
Keyboard Layout(Short Form)	Computer Layout (CM)	Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	Smartphone Layout With Extra Row of Symbols (SPS)	Smartphone Layout With Extra Row of Digits (SPD)	Smartphone Regular layout (SP)
Computer Layout (CM)	similar	similar	CM	CM	CM
Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	similar	similar	SPSD	SPSD	SPSD
Smartphone Layout With Extra Row of Symbols (SPS)	CM	SPSD	similar	SPS	SPS
Smartphone Layout With Extra Row of Digits (SPD)	CM	SPSD	SPS	similar	similar
Smartphone Regular layout (SP)	CM	SPSD	SPS	Similar	similar

Now, we serialize the layout according to their entropy supuriority for 5% significance:

- Computer Layout (CM), Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD).
- Smartphone Layout With Extra Row of Symbols (SPS)
- Smartphone Layout With Extra Row of Digits (SPD), Smartphone Regular layout (SP)

From the above analysis, it is clear that Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD) has a great impact over entropy than other smartphone layouts. But we have to take usability also on count.

5.2 Usability Analysis

Strength and usability are two conflicting requirements on the context of textual passwords generated from the smartphones. We investigate how the typing speed(character entry per minute) varies for different current layouts.We calculate the speed using javascript in the backend side of our website from the 50 users.

The result is illustrated in the figure below:

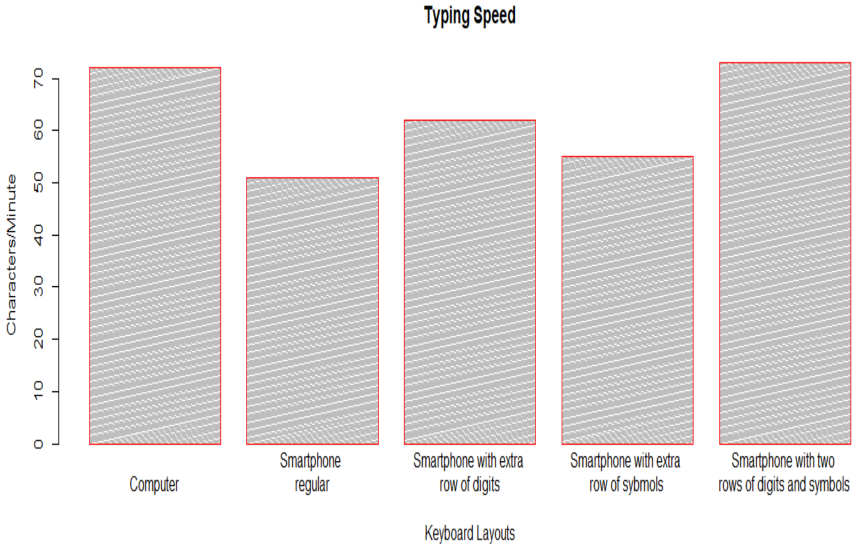


Figure 6: Typing Speed in different keyboard layouts.

From the above diagram, it is conspicuous that the typing speed of the computer layout is significantly faster than the input constraint device like smartphones. This supports the prior speculation that due to the limitation of the keyboard size in smartphones the entry of the characters are frustrating and time consuming. On the context of the smartphones, the diagram implies that adding an extra row of symbols or digits increases the typing speed of the textual passwords generated from the smartphones. The typing speed increases even more when two extra row of digits and symbols are added in the regular layout of the smartphones.This emphasizes the fact that extra row of symbols and digits reduce the time of changing the layer of keyboard for accessing digits and symbols which are generally not accessible from the first layer.

5.3 Error Rate Analysis

From prior calculation we get that the textual passwords generated from the smartphones can be more strong and usable while extra rows of symbols and digits are added. Since smartphones are input constraint devices due to the limitation of the sizes of the screen there is more concern when the keyboard size is incresed.For this reason we find a keyboard density range which will allow us to extend the keyboard size while keeping the usability concern intact.

To determine this range we made 11 android keyboard with an extra row of digits and symbols.The sizes of the layouts ranges from 20 dP(density pixel) to 70 dP. For increasing the dp the density of the keyboard decreases which implies the bigger keyboard layouts.For interval of 5 dp differences we calculate the error rate from 10 persons.We take data from 10 persons who uses smartphones and their screen size is approximately equal to that of samsung galaxy j7 prime. Each person registered in our perviously made website.For different layout size we noted the error occured in the back end of the website through javascript and php.The table below is the summary of the data collected from 10 person.

For example, for 20 dp(density pixel) the density is 2.32 which implies that there is 2.32 number of keys for 1sq.cm and the diagonal of the keyboard layout is 7.4 .we take input from 10 persons using this layout and find the mean error is 11.15%. Similarly the mean error is calculated for the other keyboard layouts.

Key Density Table			
Android Key size (DP)	Density (key/cm^2)	Keyboard Diagonal Length	Avg. error rate
20	2.32	7.4	11.15%
25	1.92	7.58	10%
30	1.59	7.82	9.3%
35	1.39	8.06	5.8%
40	1.21	8.38	4.6%
45	1.07	8.72	2%
50	0.97	9.02	0%
55	0.88	9.41	3%
60	0.80	9.83	13.83%
65	0.75	10.18	20%
70	0.69	10.63	30%

people generally use smartphones with one hand. The figure below gives the idea about how the smartphones are hold in hand. We measure the thumb size as depicted in the figure for 10 persons.

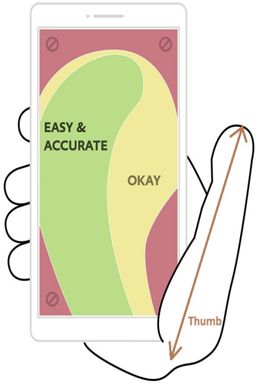


Figure 7: Human Thumb Size

Relation Table			
Person	Thumb(T) (cm)	Comfortable Max Diagonal distance(MAX) (cm)	Relation $(r = (MAX/T) * 100\%)$
1	12	9.2	76.6%
2	11	8.21	74.6%
3	10.5	8.5	80.9%
4	10	7.5	75%
5	12	9	75%
6	13	9.77	75.1%
7	10	7.4	74%
8	11	8.2	74.5%
9	10.5	7.8	74.2%
10	12	9.1	75.8%
			Avg. = 75.5%

From the users we get the maximum comfortable range of a person when typing in the smartphone keyboard layout.The relation between the thumb size and the maximum comfortable distance implies that the maximum comfortable distance is 75% or (3/4) of the thumb size.

For each person we measure the error rate of 11 android keyboard layouts of different key density.

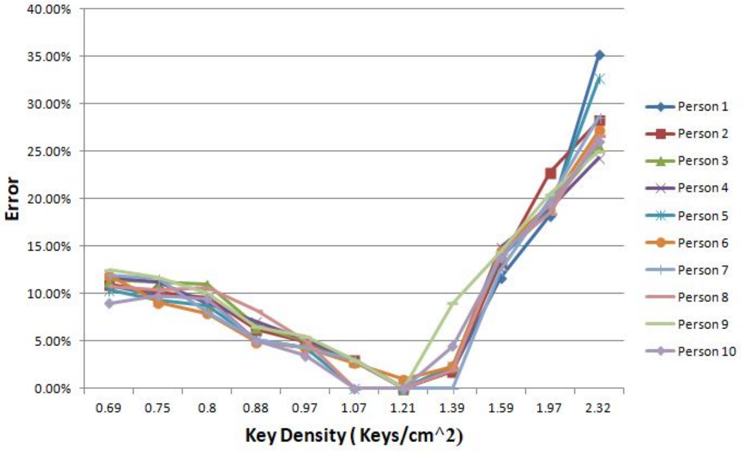


Figure 8: Dependency of error rate on key density.

The graph[Figure 4] is drawn which depicts the change of error rate due to the increase of the keyboard density.For 10 person 10 curves are drawn in the graph.From the graph it is speculated that the error rate decreases when the density is increasing. When the density is around .95 to 1.4 the error is tolerable (5%). This is because when the density is less the diagonal of the keyboard crosses the maximum comfortable range of the thumb for human. We take the average error of 10 persons on each keyboard with a fixed density.

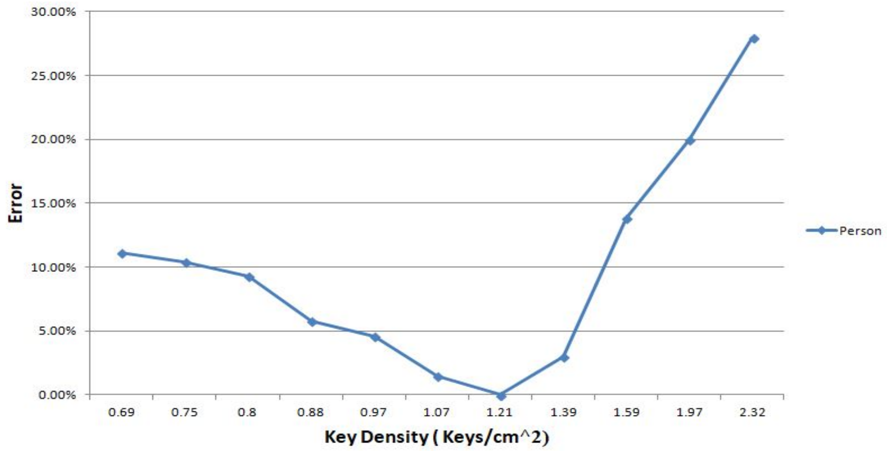


Figure 9: Dependency of error rate on key density.

This gives the graph [Figure 5] which implies that for increasing the size of the keyboard layout the maximum comfortable range of density should be .95 to 1.4. For this reason the addition of extra rows will not effect the usability concern since the error rate is tolerable in this density range.
We analyzed previously extra addition of rows of symbols and digits will increase the strength of the textual passwords generated from the smartphone layouts. The usability of the layout is maintained if the layout is changed according to the density range got from the above calculation.

5.4 Key stroke Analysis

Due to the limitation of the smartphone keyboard size the time of stroking a key varies in different layouts of smartphones. We investigate this effect on 10 person on the our previously made droid keyboards.

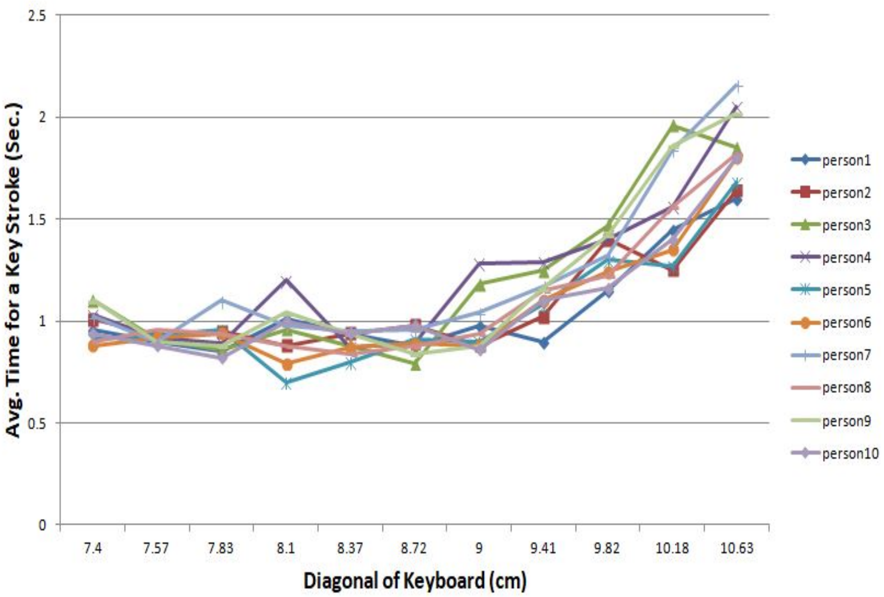


Figure 10: Dependency of key stroke time on diagonal length of keyboard.

In graph [Figure 6],for diagonal of the keyboard layouts from 7.4 to 9 we see that the average time for keystroke remains unchanged. This implies that the previously calculated comfortable thumb range is the threshold for the keyboard diagonals. When the diagonal of the keyboard increases from 9 the average time of keystroke increases due to the limitation of the human thumb size.

Now, we take the average keystroke time of each layouts from 20 dp to 70 dp for 10 persons. This gives the graph [Figure 7] which shows that the comfortable range for the keyboard diagonal is upto 9cm approximately.This gives the size of the keyboard at which we can add any extra row.

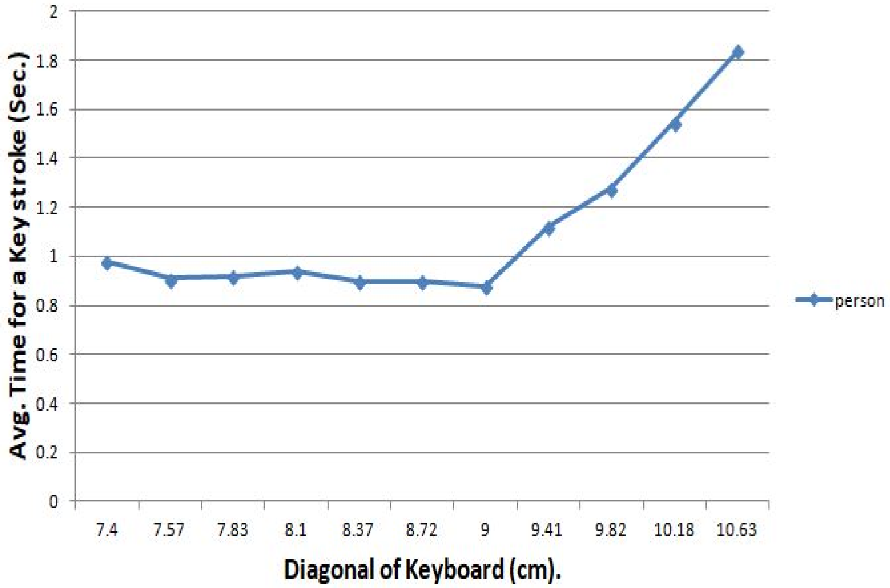


Figure 11: Dependency of key stroke time on diagonal length of keyboard.

From these measurement we get that the extra addition of symbols and digits will not reduce the usability of the keyboard until the key density and the diagonal range is between the calculated results.

5.5 Summary

The design and experiments of entropy of different keyboard layout demonstrate that Smartphone Layout With Extra Two Rows of Symbols and Digits make the users tempted to create more secure password. At usability section, the bar diagram has demonstrate that it also increases typing speed. So, it would be best for the users to add extra two rows of symbols and digits to smartphone regular layout. But there remain a question of error rate and key stroke rate.

At error rate analysis part we have found that error rate depends on key density of key board layout. Error rate remain tolerable within range $[0.9 - 1.4] key/cm^2$. While developing a layout, the density should not be more than $1.4 key/cm^2$. But the lower limit of density can be changed geographically. You can make keyboard as large as possible but the diagonal distance of layout should not exceed comfort length (3/4 of thumb) of human being. As Human height change with geographic location. So, lower limit of density can be changes with global location.

Finally, it is clear that two rows of symbols and digit can be added between that density range for most of the smartphone.

6 Discussion

Before highlighting the implication of the result it is important to denote the limitations of our study.

6.1 Limitation

First, we agree with the fact that it is difficult to demonstrate ecological validity in password study where the sample persons know that their data will be used for experimental purpose, rather than for accounts they value in real life for regular use over a long period of time. However, in the context of this work, We make a utility website which will diminish the possibility of invalid data entry. But even then we take the data after the approval of the account holder. We note, however, that our participants were not required to return on a second day to re-enter their passwords, and as such, some of them might have constructed less memorable random passwords.

We also agree that the sample size of our study is not very large (n=50) and the study is comprised of students and service holders who may vary significantly from other populations in their password behavior, and in particular their password sharing behavior. However, compared to the sample sizes of prior works , our sample size can be considered reasonable.

For the usability analysis like key stroke and error rate we have used fixed sized smartphones which is not in general for all the smartphones. This gives the scope of further work on this generalization for smartphones of any sizes.

6.2 Implication

In our work we find the effect of input constraint devices like smartphones on textual password formation. From the response of the data collected from random users we get that the strength of the textual passwords increases when an extra row of symbols or digits is added. This implies the necessity of the change of the entry methods for security concern.

We also conducted a data analysis after adding prototype layout for smartphones which comprises of both symbols and digits rows. This supports the fact that the textual passwords when generated from the smartphones get stronger due to the change of the layout. But extra addition of rows increases the density of the keyboard layout which has usability issue.

We find which is the limit of the density of the keyboard for smartphones which is requied to be maintained for the sake of usability. Analyzing on 11 different sized layout we get a range of density within which extra row addition does not have any usability concern.

7 Conclusion

In this work we find a device new technique for stronger yet memorable textual password for smartphone. We investigate on the different existing smartphone keyboard layouts. The strength variation on different layouts imples the need of further work since there is security concern. A new prototype which generate stronger textual password is found from the analysis. But the usability concern is the impediment in this context. Smartphones are input constraint devices which makes the usability maintenance important. We find the limitation of changing the size of the keyboard layouts by laboratory experimentation. This implies the range of density of keyboard layouts at which extra row addition is possible keeping the usability unharmed

8 References

1.Usability and Security of Text Passwords on Mobile Devices.
William Melicher, Darya Kurilova,∗ Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle L. Mazurek†

2.Passwords and Interfaces: Towards Creating Stronger Passwords by Using Mobile Phone Handsets.
S M Taiabul Haque Matthew Wright Shannon Scielzo* eresh03@gmail.com, mwright@cse.uta.edu, scielzo@uta.edu

3.A. Forget. A world with many authentication schemes. PhD thesis, Carleton University, 2012.(uta 38)

4.J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In CHI Extended Abstracts, 2002.(uta 45)

5.J. Thorpe, B. MacRae, and A. Salehi-Abari. Usability and security evaluation of geopass: A geographic location-password scheme. In SOUPS, 2013.(uta 115)

6.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 IEEE S P, 2012.hoq 11

7.C. Herley, P. C. Oorschot, and A. S. Patrick. Passwords: If we're so smart, why are we still using them? In FC, 2009. hoq 55

8.S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In SOUPS, 2005.hoq 120

9.Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring Password Guessability for an Entire University. In Proc. ACM Conference on Computer and Communication Security.chi 39

10.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 Proc. Symposium on Usable Privacy and Security.chi 45

11.Blase Ur, Patrick Gage Kelly, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In Proc. USENIX Security Symposium.chi 48

12.Adrienne Porter Felt and David Wagner. 2011. Phishing on Mobile Devices. In Proc. Web 2.0 Security Privacy. chi 18

13.Markus Jakobsson and Ruj Akavipat. 2012. Rethinking Passwords to Adapt to Constrained Keyboards. In Proc. Mobile Security Technologies chi 29

14.Tara Matthews, Jeffrey Pierce, and John Tang. 2009. No Smart Phone is an Island: The Impact of Places, Situations, and Other Devices on Smart Phone Use. In IBM Research Report. chi 37

15.Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In Proc. International Conference on Mobile and Ubiquitous Multimedia. Article 13 chi 42

16.M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In HotSec, 2009.hoq 60

17.Kristen K. Greene, Joshua Franklin, and John Kelsey. 2015. Tap On, Tap Off: Onscreen Keyboards and Mobile Password Entry. chi 24

18.Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-Based Authentication on Mobile Devices. In Proc. International Conference on Human-Computer Interaction with Mobile Devices and Services. 10. chi 51

19.KoreLogic. 2010-. ”Crack Me If You Can” - DEFCON 2014.chi 35

20.Dan Goodin. 2012a. 8 million leaked passwords connected to LinkedIn, dating website. (Jun 2012) chi 21

21.Steve Kovach. 2014. We Still Don’t Have Assurance From Apple That iCloud Is Safe. (September 2014).chi 36

22.Megan Geuss. 2015. Mozilla: data stolen from hacked bug database was used to attack Firefox. (Sep 2015). chi 20

23.Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performance. In Proc. NordiCHI’14: 12th Annual Nordic Conference on Human-Computer Interaction. 10. chi 50

24.Patti Bao, Jeffrey Pierce, Stephen Whittaker, and Shumin Zhai. 2011. Smart Phone Use by Non-Mobile Business Users. In Proc. International Conference on Human Computer Interaction with Mobile Devices and Services chi 2.