IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Special Issue.10, Nov 2018 E-ISSN: 2347-2693

A quantitative report on the present strategies of Graphical authentication

Norman Dias[1*], Reeja S R[2]

[1]Department of Computer Engineering, Dayananda Sager University, Banguluru, Karnataka, India
[2]Department of Computer Engineering, , Dayananda Sager University, Banguluru, Karnataka, India

[*]*Corresponding Author norman.dbce@gmail.com1, Tel.: +9850438230*

Available online at: www.ijcseonline.org

***Abstract*—** The foremost common authentication strategy is to use alphanumeric usernames and passwords. This strategy has been appeared to posses critical disadvantages. Clients prefer to choose passwords which are effectively speculated. At the same time, if the password is difficult to figure, then at that point its obviously difficult to keep in mind. To solve this issue a few analyst have created verification strategy's that utilizes images as passwords. This paper examines the qualities of the existing graphical passwords methodologies and we try to answer a question "whether a graphical password more secure to a text based password"?

Keywords- Authentication strategy, graphical passwords, secure passwords.

I. INTRODUCTION

Alphanumeric Passwords are widely used to authenticate a user on a network. Traditional password uses a sequence of alphanumeric characters to grant access to an authenticated user. However, the text-based passwords are prone to dictionary attack [1]. The dictionary attack is a method by which user's use different tools to break a password by automatically checking all the words that occur in either a dictionary or publicly available directories.

The alphanumeric password provides strong security, provided they are complicated enough to be guessed. Usually, a text-based password is a sequence of 8 characters or more which include upper and lower case character's, special symbols and digits [2]. Memorizing a random password which does not contain any meaningful information and is difficult and can be done only by repetitive learning which serves to be a very weak way of memorizing a password [3], and with n = number of password per user the rate of forgetting also increases that's the main reason why users tend to forget their complex password.

A survey conducted at the University of Malya, with 100 computer literates being faculties of Computer Science and Information Technology, keeping in mind to identify the vulnerability of textual passwords. The Table shows that 88% of users do not prefer using the combination of digits, symbols and letters as their passwords [4].

Table 1: Password Distribution [4]

Textual Passwords	Users(%)
Symbols & Letters	3%
Symbols & Numbers	5%
Symbols, Letters, Numbers	12%
Only Letters	25%
Only Digits	15%
Only Letters & Digits	40%

The following Figure1 depicts that more than half i.e. 55% of the users prefer to use the same password for all the services [4]

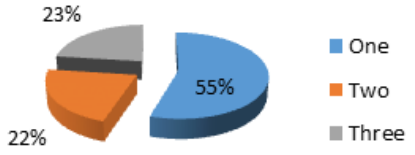


Figure 1: Different passwords frequently used

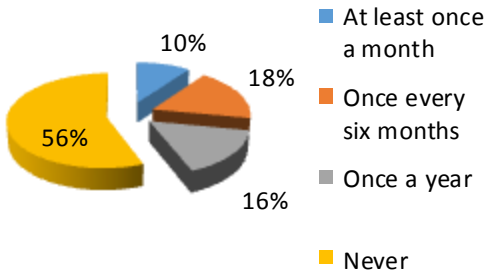


Figure 2: Depicts the frequency of changing the Textual Passwords [4]

These results clearly indicate that most of the users are totally unaware that their passwords are vulnerable to

© 2018, IJCSE All Rights Reserved

security threats especially in the case of users who use the same password for all the services or rarely change their password since it can be easily retrieved or hacked [5]. The guidelines for selection and maintaining a text password are already proposed by most of the researchers and can be obtained from [6].
Humans beings have a critical capacity to perceive and recall visual images this hypothesis is supported by psychological studies[7].

II. LITERATURE SURVEY

Cognometric Systems also known as recognition based system. This system is predicated on hash image technique, whereby a user should choose some number of pictures generated from a group of random images by the program, later so as to be echt the client is needed to spot identical pictures in sequence [8].

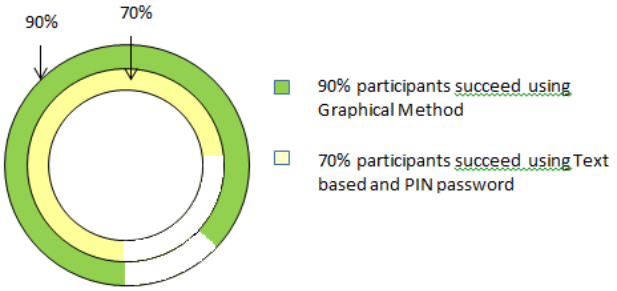


Figure 3: Success rate after using GP and Text, PIN Password

The average login time is longer than the standard approach. A downside is that the server must store an oversized quantity of images, which has to be transferred over the network, which will delay the authentication process. Another shortcoming of the framework is that the server stores the seeds of the portfolio pictures of every client in plain text. The way towards choosing picture from the database can be tedious for the client [8].
Similarly, the "Image Based Registration and authentication system", uses images as key to their accounts. The client usually supplies client ID and image as credential to the system, this technique uses Secure Hash Algorithm function SHA-1 where the output is 20 byte, thereby making the authentication process more secure [10].

Photographic authentication is a strategy for logging into untrusted open Internet access terminals. It requires a client to recognize their very own photos from a set of randomized pictures. By changing the particular pictures that appear on each login attempt. This technique is resilient to replay attacks, which is a weakness with the traditional password based mechanism on systems for which every action could be deceitfully observed. A prototype implementation and relating client test demonstrate that not only the participants to a great degree proficient at rapidly, precisely and enjoyably perceive their own photos, however assailants are not in a position to figure out which photos are right, notwithstanding even when given examples of client photos.[9]

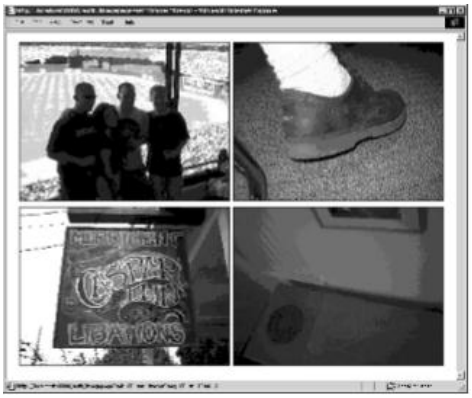


Figure 4: Photographic authentication web-browser interface

The triangle scheme Figure 4 arbitrarily scrambles an arrangement of N objects on the screen. Practically the the value of N ranges from a lower bound of hundred to an upper bound of thousand objects. The objects ought to be sufficiently diverse with the goal that the client can recognize them. There is a subset of K objects (i.e. k=10) prior picked and retained by the client. At login, the framework will arbitrarily pick an arrangement of N Objects. This framework first randomly chooses a patch that spreads a large portion of the screen, and arbitrarily puts the K picked objects in that patch. To login the client must find 3 of the pass objects and click inside the undetectable triangle made by those three objects. This means that the client must click inside the convex hull of the pass objects that are displayed[11].

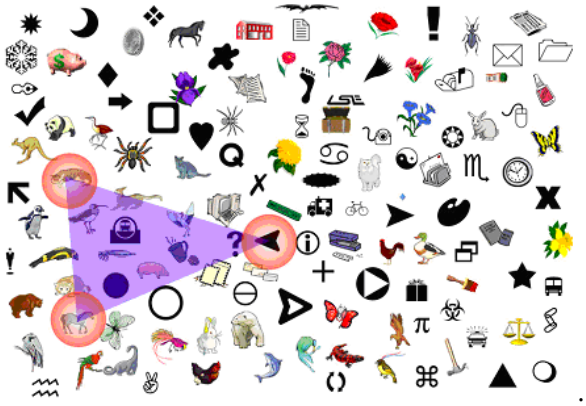


Figure 5: The Triangle Scheme

The number of possible passwords is the binomial coefficient. When N=1000 and K=10, the number of possible password is approx. $2.6*10^{23}$, which is more than alphanumeric password of length 15 ($36^{15}= 2.2*10^{23}$)

© 2018, IJCSE All Rights Reserved

The Background Pass go can be considered as an associate improvement over Pass-Go, because it keeps majority of the advantages of Pass-Go and gives higher security level and higher easy use level as compared to the Pass-Go theme.

In Pass Go theme , the delicate territories are measured with a sweep of 0.4*d (d=sideways length of cell), as compared to BPG (Figure 8)the area is set to 0.30*d range. Hence, the radius cannot be kept to large keeping in mind the end goal to lessen the achievement rate of figure assaults by just clicking at the focused areas without having prior knowledge of the genuine passwords, while in the meantime if the radius is too small then it will cause a sufficient measure of passwords input problems to the clients. In View of heuristic testing 0.30*d range proved to be satisfactory from clients viewpoint and the security result was also higher as compared to the Pass-Go [12]. Figure 5 & 6 represents the successful Access rate with indicator & without indicator respectively.

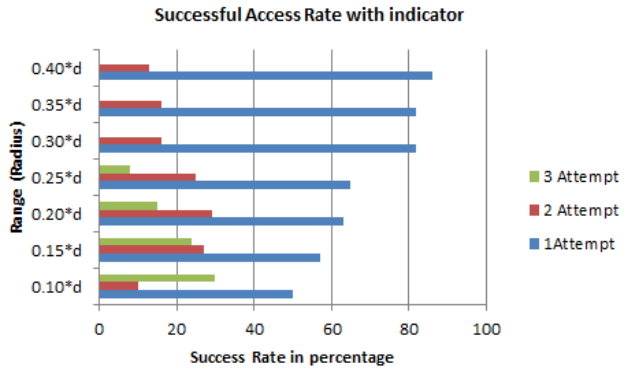


Figure 6: Successful Access Rate with Indicator

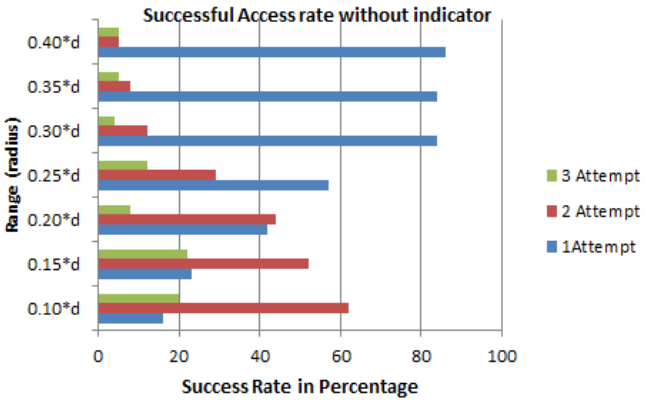


Figure 7: Successful Access Rate without Indicator

BPG utilizes a similar access function as I Pass go. The clients can draw a shape uninhibitedly relying upon their particular inclinations. The working of indicators is similar as in Pass go. On selection of one intersection a dot indicator will appear, whereas on a continuous selection of two or more intersections a line indicator will appear. The thickness and design of indicators can be upgraded according to the inclination of clients. BPG uses steady pointers to recognize the passwords since this approach has the capacity to quicken the procedure of retention by using invariable indicators. The password is then encoded as a succession of intersections, drawn by a 2 dimensional coordinate pairs

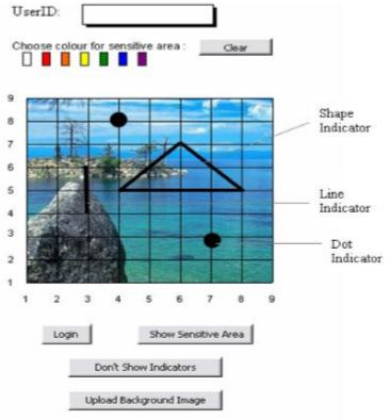


Figure 8: Background Pass-Go Scheme

The Password space of BPG as compared to déjà vu is quite higher since it is capable of enabling users to select different indicator type [12].

Pass logix inc organization built up another graphical confirmation plot called Passlogix v-go shown in figure 8 . At enrollment stage the password is made by a sequential circumstance with rehashing a group of activities . In this technique the client is requested to tap on different things on the picture in the right grouping with a specific goal to be confirmed, one disadvantage is that this procedure gives just restricted password key space[20] .

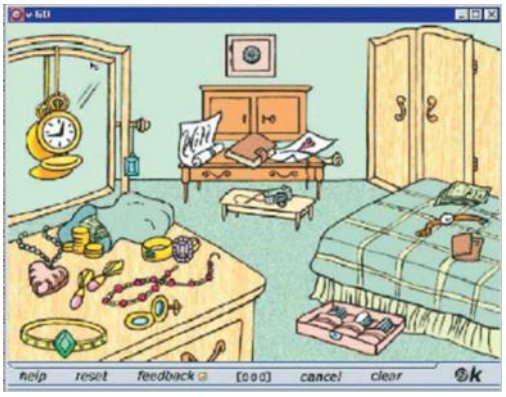


Figure 9: Passlogix Authentication

Passface (Figure 9) was a authentication technique that was developed by Real User Corporation. The essential plan is

© 2018, IJCSE All Rights Reserved

that , the user was asked to settle on 4 pictures of human faces among a decoy of faces, the user sees a grid of 9 faces, consisting of 1 face antecedently chosen by user, the user recognizes and clicks anyplace on the noted face. This method is recurrent for four rounds. This procedure is recurrent for many rounds. The user is echt if properly identifies the 4 faces. The technique is predicated on the idea that people will recall or memorize human faces very easily than different random images

Figure 10: Passfaces Authentication

Comparative studies by Sasse et al. [21] showed that passfaces had solely a 3rd of the login failure rate of text based passwords. Their study put together showed that the Passface login methodology took longer than text based passwords thus was used less frequently by users

Monrose et al.[22] examined the graphical passwords and located clear patterns among these passwords for e.g. most users preferred to settle on faces of individuals from identical race, which makes the system predictable to some extent, this downside could also be relieved by randomly assignment of faces to users, however following this procedure , therefore would make it laborious for users to recollect their password.

W.Jansen et al.[23-26] designed a graphical password mechanism for portable gadgets. Amid the enrolment stage , a client chooses a topic , which consist of thumbnail photographs and at that point registers a series of pictures as a password. In the verification stage , the client must provide the registered images within the redress grouping. One downside of this methodology is that, the number of thumbnail images is restricted to 30, therefore it has a very small password space. Each thumbnail picture is allotted a numerical value, and the arrangement of choice produces a numerical password. The outcome appeared that the length of image sequence was by and smaller than the textual of textual password

Voice based PIN and touch based PIN authentication techniques compared to the in built authentication techniques of the Google glass (Figure 10,11). The set of available gestures which is an in built authentication mechanism is prone to shoulder surfing. The gesture set is a combination of swipe or tap using one or two fingers, the sequence of finger movements is visible to others, Some gestures are very tedious and complicated to be performed.

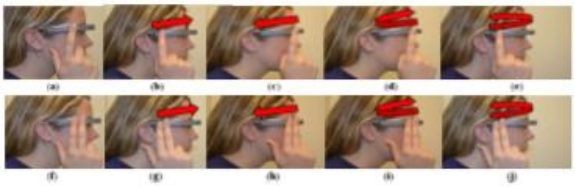


Figure 11: built in gesture set a)tap b)forward swipe c) back swipe d) forward hook swipe f e) back hook swipe f)two finger tap g)forward swipe two finger h)back swipe two finger i) swipe forward two finger hook j) swipe back two finger hook

Voice based mechanism (Figure 13) used voice to unlock the Google glass, the PIN spoken aloud is audible to all and the secret value can be compromised. The Google glass displays a numeric touchpad grid with each cell having two different numbers , the white digits represent the real PIN digits as available on a standard keypad and the second digit available next to it in red is mapped cipher digit that the client will utter in order to enter the corresponding real PIN digit. A reverse mapping of the cipher digits corresponding to real PIN Numbers.

In Touch based PIN authentication (Figure 12) the client navigates to each of the cells using swipes and on a tap select a digit, forward and backward swipe movements are allowed , the client is verified when the entered PIN matches the saved PIN. For every instance the assignment of digits is different, therefore the gesture sequence varies each time for the same PIN.

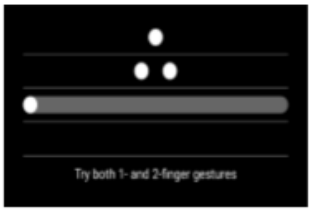


Figure 12: Built in mechanism: the first three entered gesture are tap, two finger tap and swipe back

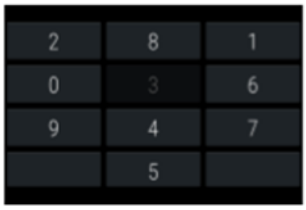


Figure 13 Touch based Mechanism: keypad assigned randomly, every instance different layout is displayed

© 2018, IJCSE All Rights Reserved

Figure 14: Voice based Mechanism keypad assigned randomly, every instance different layout is displayed

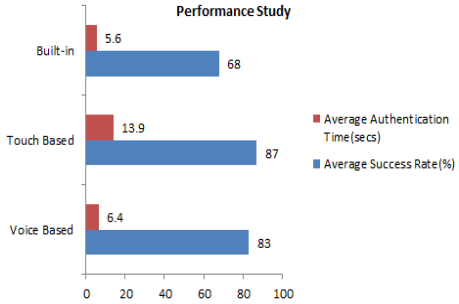


Figure15: success rate Voice based and Touch based & Built-In

The above figure 14, indicates that the success rate with built in features is the lowest when compared with the other two methods i.e. Voice based and Touch based.

Cheng Sun et.al [14] performed analysis on pattern strength meter using pattern selection.

On a 3*3 grid based dots login system. Google has defined rules & a proper unlock pattern must follow the rules.

R1: Minimum number of Dots to be connected in a pattern in at least 4

R2: At the max 9 dots are connected

R3: the unconnected dots are connected on the path of creating a pattern

R4:to connect an unconnected dot a pattern can pass through a previously connected dot. The physical strength of the pattern strength were defined as follows:

Size: Pattern size is defined as the number of dots the pattern connects. The proper Pattern must be an integer$\{x \mid X \in Z$ and $4 \leq x \leq 9\}$.

Length: Physical length is the summation of all the lengths of all its segments

Overlaps: pattern line segment covered by other segment is counted as an overlap. The below presented table gives the statistics of the sizes of valid pattern

Table 2: Size statics of all valid Patterns[14]

Number of dots	Number of valid Shapes
4	1624
5	7152
6	26,016
7	72,912
8	140,704
9	140,704
Total	389,112

Cheng Sun et.al proposed strength score of a pattern.

$PS_P = S_p * \log_2(L_p + I_p + O_p)$

PS_p Strength score of Pattern P.

S_p Size of Physical strength

L_p physical length

I_p no. of intersections

O_p Overlaps of p

It was observed that connecting more dots could would aid in increasing the visual complexity, resulting in a higher strength score, cheng Sun et al. came up two types of pattern strength meter

1. A 5 segment colour changing bar as show in in fig 15
2. A gradient colour ratio bar with percentage strength score fig16

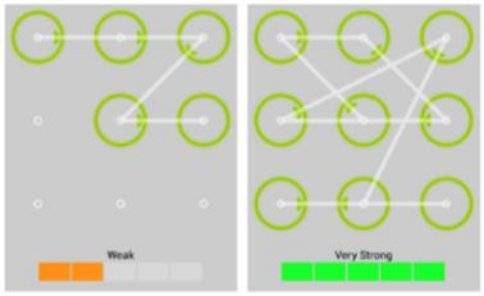


Figure 16: Pattern strength meter with colour changing bar[14]

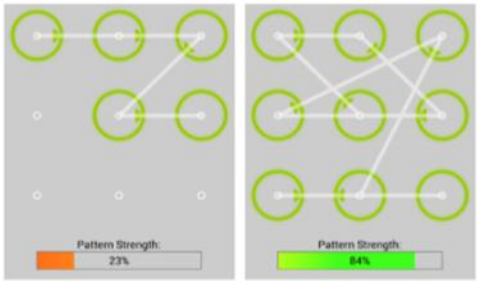


Figure 17: Pattern strength meter with percentage strength score [14]

The presence of visual indicators with pattern strength helped in creating strong patterns as shown in fig 13 and 14, which helped in enhancing the security of pattern unlock. But in comparison with PIN/Password the overall security of pattern unlock is still weak , as a result of limited pattern space

© 2018, IJCSE All Rights Reserved

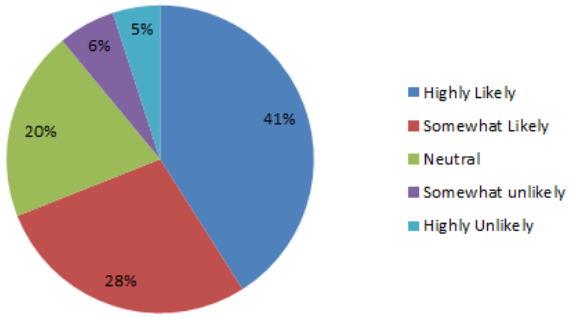


Figure 18: Feedback [14]

A feedback collected from the participant indicated that in total 69% of all participants preferred the new mechanism of pattern strength meters, as shown in fig 17 (69%= 41%+28%=Highly Likely + Somewhat Likely) . It was also concluded that memorability becomes a main issue when complex patterns are used, which includes longer lengths, more intersections and overlaps but not with all users. It was empirically concluded that a few participants utilize designs which resemble alphabets, or digits to encourage memorability. For instance alphabets like C,L,N,Z and digits like 2,7,9 can be effortlessly reproduced in a 3*3 grid. Such shapes will experience ill effects of shoulder surfing assault due to generally poor visual complexity. The table 3 below shows strengths of sample letters and number patterns along with their strength score.

Adam J Aviv et. al performed 4 experiments on smudge attack on smartphone touch screen, the experiment was performed on two variants of phone HTC G1 and HTC Nexus1, under different lighting and camera condition as shown in figure 18.

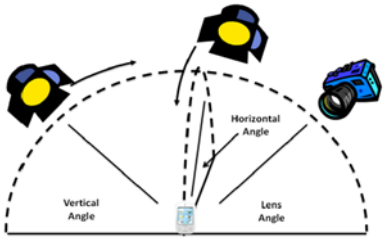


Figure 19: Principle photographic Setup[15]

For the principle photographic setup (Figure 18) a single light source in vertical or horizontal orientation. A vertical angle increments in plane with the camera ,while a horizontal angle increments in perpendicular plane to the camera were setup, and all angles were calculated in reference to smartphone. In total 188 setups were created.

The goal of the first examination was to determine the conditions by which an assailant can track the patterns under perfect settings. Four different models of phones were used to extract the patterns.

- Phone 1: HTC G1 phone, shape entry was through normal touches
- Phone 2: HTC G1, shape entry was through light entries
- Phone 3: HTC G1,shape entry was done after a phone call after the phone came in contact with face
- Phone 4: HTC Nexus phone, shape entry was carried out with normal touches.

Shapes that were entered via phone 3 , in 68% of the setups complete patterns was recovered, in comparison to the other phones , phone 3 was dirty since it came in contact with the facial skin. Fig 19 shows a pattern entry with phone C.

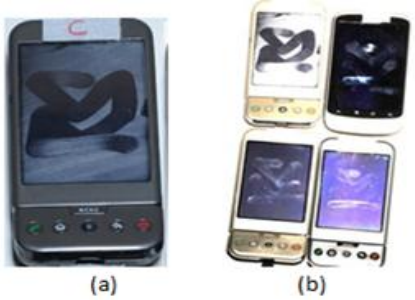


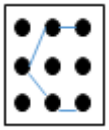
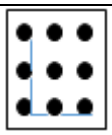
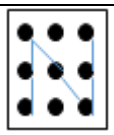
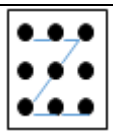
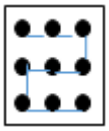
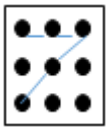
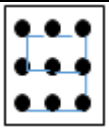
Figure 20: (a))Phone C from experiment (b) All phones from exp 1

Table 3: The average rating with application usage of patterns entered over and under the application

App Noise	G1		Nexus 1	
	over	under	over	under
dots	4	4	2.7	3.7
streaks	3	2	3	3
dots & streaks	3	1.6	3	3
face	4	2.3	4	2

In the second experiment , a telephone application was used and If the user had to dial a phone number then a series of presses or smudge dots on the screen would be required , in case of a contact list to be checked then because of scrolling up & down smudge streaking or right and left based on the orientation of the phone would be generated. The consideration was that the pattern had to be entered prior to using the application and post application. Result is shown in table 4

© 2018, IJCSE All Rights Reserved

Table 4: common patter on screen lock		
Letter /Number	Pattern	Strength Score
C		24%
L		14%
N		41%
Z		41%
2		30%
7		14%
9		36%

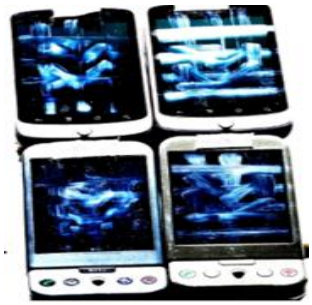


Figure 21: patterns recovered with noise –expt-2

In experiment 3 the impacts of smudge distortion caused by accidental contact with or wiping with apparel were recorded, a simple contact with apparel does not remove smudges and in all the scenarios the smudge was perfectly retrievable

Sebastian et al. conducted a survey to quantify the graphical password with respect to android unlock patterns. The survey shows the preference i.e. the strong bias on the selection of the initial point which is usually at the corners as shown in figure21

Figure 22: Android unlock pattern, Bias of initial point

The figure 21 shows a total of around 75% for selection around all the 4 corners . The centre , right, lower and upper comprises only 14% of selection chances as the starting point. But the chances of selection the upper left corner is 38% .The researchers conducted an analysis on 3-grams v/s 2-grams patterns.

Figure22 (a) & (b) shows the 3-grams the most frequent to less frequent patterns.[16]

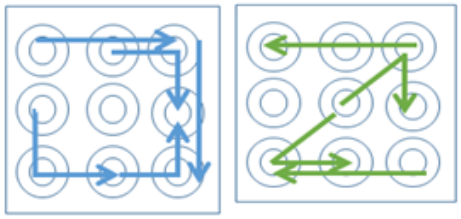


Figure 23: (a) (b)

Modification was done to the original Android lock screen-four different versions Leftout Small, Leftout Large, Circle and Random. As show in Fig 23 for the left out Small pattern the upper left point was omitted as it was having the highest bias , the intention was to spread the bias from the upper left corner to the remaining points, as a result the first point was distributed more uniformly. Figure23 b shows the most frequent 3-grams patterns and it had the lowest number of possible patterns[16]

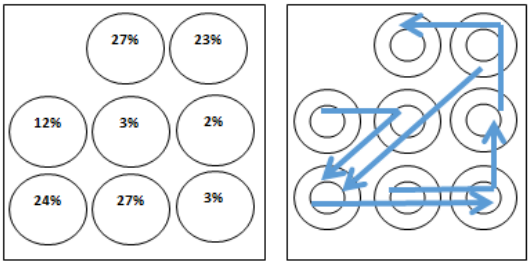


Figure 24: (a) (b)

Similarly for the leftout Large, which has a 3*4 grid ,the first point remains almost similar to the original Android

© 2018, IJCSE All Rights Reserved

lock fig 24 (a) shows the bias among the various selection points and b shows the frequent 3-grams patterns.[16]

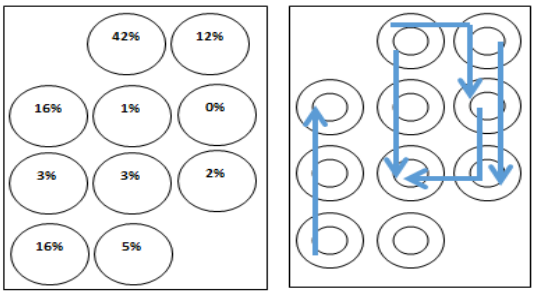
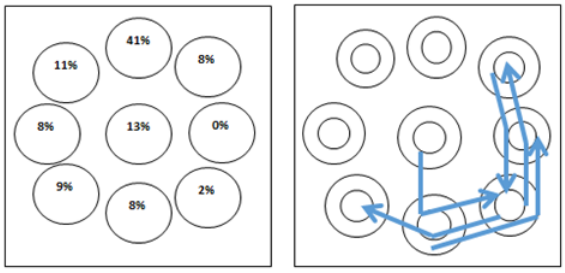


Figure 25: (a) (b)

The circle pattern performed the best among all the four experiments, even tough there were chances that the user may choose circular patterns , they were aware of the security problems, most of the user's preferred using geometrical structures like square or a triangle in the circle, but the starting point still has a higher preference of 41%, as shown in figure 25 (a), figure 25(b) shows the 3-gram pattern



,Figure 26: (a) (b)

The last experiment was performed on a Random pattern wherein the points were loosely spaced ,this pattern did not support any symmetrical patterns, since there were no more than two points in the same line, and no upper left corner point was provided , but in spite of this random pattern , its performance was poor, since the users tried to fit certain obvious pattern like the alphabet a. The figure 26 (a) below shows that the first point still has a higher preference, and figure 26 (b) shows the most frequent 3-gram patterns

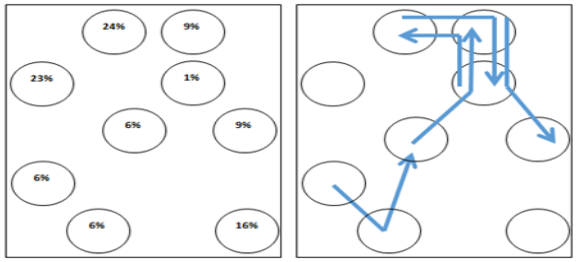


Figure 27: (a) (b)

Patric et al worked on the password meters and tried to prove the impact of password meter in the selection of a strong password.

As show in figure 27 there are different types of password meters that can affect in the selection criteria of a strong password , they used password scoring algorithm that would assign or negate certain points if a certain criteria was met in the selection of a password, the score obtained by a certain password would then be displayed to the user in a graphical view(meter view) , which would indicate if the password chosen was weak, moderate or strong. The control conditions were without a meter and a baseline meter. In the no meter condition the user had just to create a password, whereas in the Baseline meter (figure 27) the fitting in the criteria would fill the meter bar, the colour would change from red to yellow/orange to green as the value increases , a suggestion depending on the strength of the password was provided [17-18].

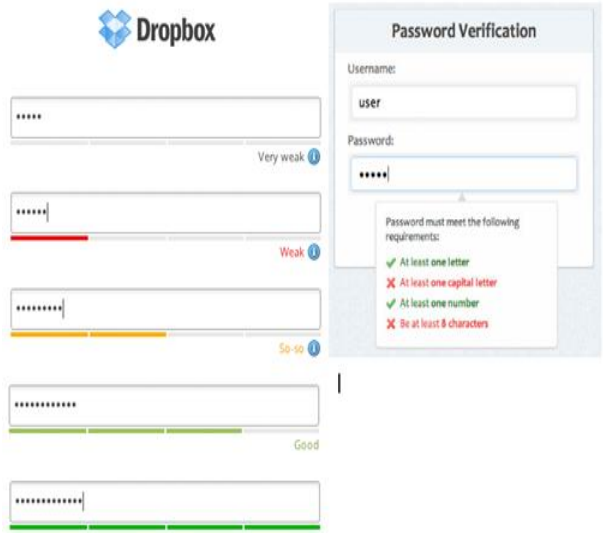


Figure 28: sample visual meter

The metrics for the result were based on Composition, Guess ability, Creation Process, memorability and Sentiment. It was observed that Meters lead to longer password as compared to without meters, the next metric was Guess

ability, with the help of a cracking algorithm & a Guess calculator tried to guess the password, assuming a weak adversary that would make 50 million guesses, A medium adversary that would make 50 billion guesses, and a strong adversary that would make five trillion guesses, the observation was that with No Meter 35% of the passwords would be cracked with a Medium adversary, the Baseline meter performed a little better and was more resistant to password cracking as compared to No meter. The best among all were the Half –score[17,18] and the One-third –score, observation was that[resistance to guess a password could be increased by providing stringent meters and visual bars. The next metric was the creation of password , In particular it was

© 2018, IJCSE All Rights Reserved

observed that Half-score, One-third score and Bold text only half score required more time in creating password with this types of stringent meters, when the participants were made aware of the working of the meters, it lead to change their mind during the password creation. Also with respect to memorability the users were able to memorize their password even after two or more number of days, there was no huge differences across the conditions for any of these metrics. The metric sentiment resulted in proving that stringent , meters were a bit more annoying , therefore the important features was scoring stringency, & having a visual component, as compared to the less other features such as colour, segmentation , size & Bunynness

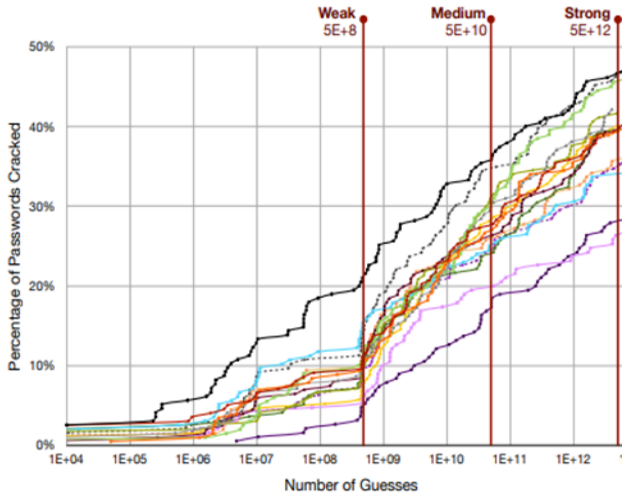


Figure 29: % of password cracked in each condition

The graph above figure 28 show the % of password cracked in each condition no meter was 46.7%, text only was 46.2%, green was 45.5%,tiny was 42.1%,huge was 4.6%,bunny was 40.1%, baseline meter was 39.4%,Three segment was 39.4%, no suggestions was 39.3%,nudge-comp8 was 39.2%,bold text-only half was 35.6%, text-only half was 34.7%,nudge-16 was33.7%,one-third score was 27.9% and half score was 26.3% the best among the all[17,18]. Felecia Alfieri et al. performed a similar study on the password meters and came up with a solution where[19] the earlier password meters stated if the password was weak, average or strong but would never give any suggestions as to how the password could be made strong. In this study along with the password meters that displayed the strength of the password a text feedback was also displayed , this feedback gave appropriate feedback to avoid dictionary attacks , keyboard patterns, moving away of digits from the end of the password , moving away uppercase letters from the beginning of the password, and include symbols and digits .

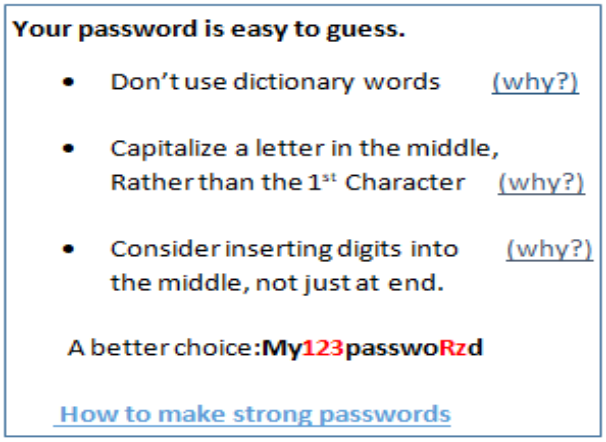


Figure 30

It also provided improvements for the password to make it strong as shown in fig 29 above, this feedback was designed using a combination of neural networks and Twenty one combination of heuristics, it was very evident that the strength meter of 1class8 was difficult to guess it performed independently well without the colour meter. It was also observed a significant security effect was lesser for 3class12 password

III. CONCLUSION

As the research demonstrates that the passwords graphical as well as text based have their weakness and strengths , the text based passwords is one of the most easiest way to authenticate a user but on a very large extent users bypass the security features and develop a weak password which can be easily cracked, as an advancement to alphanumeric passwords the baseline meter to some extent helped the users to revive their password to make it stronger but then memorability becomes a major issue of concern, the graphical passwords such as the in the Android pattern lock , the first point on the lock remains to be the preferred choice , even though different patterns of android locks were tried and most of the patterns could be easily guessed, researchers were also successful in performing a smudge attack under various lighting conditions and camera angles. The login for the built in Google glass was prone to shoulder surfing, the touch based mechanism for Google glass had a higher success rate as compared to the voice based. The graphical passwords provided a higher password space but still has its own weakness , it could suffer from a shoulder surfing attack, if the password is randomly chosen the memorability becomes an issue. To conclude a good password strategy has to be developed such that it offers better usability, better security, also a visual feedback to the user while choosing a password stating the strength of the password and prevent attackers from building a dictionary attack.

© 2018, IJCSE All Rights Reserved

REFERENCES

[1] Fledmeier, D' and Karn, P., UNIX password security ten years later .In proceedings of the 19th International Conference on Advances in Cryptology (CRYPTO '89). Lecture Notes in Computer Science, Vol 435, Springer , Verlag

[2] Sobrado , L, Briget,J.C.,Graphical Password , The Rutgers Scholar, An electronic bulletin of Undergraduate Research, Vol 4. 2007

[3] Adams, A., Sasse, M.A.and Lunt, P., Making Passwords Secure and Usable, in H.Thimbleby, leby, B. O'connailal and P. Thomas(Eds), HCI'97-people and computers XII, Springer-Verlag, Bristol ,pp.1-20,1997

[4] L.Y.Por, X.T.Lim,M.T.Su,F.Kianoush. The Design and Implementation of Background Pass-Go Scheme Towars Security Threat, WSEAS Transactions on INFORMATION SCIENCE & APPLICATION ISSN:1790-0832,Issue 6,Volume 5 June 2008.

[5] Wanli Ma,John Campbell,Dat Tran and Dale Kleeman, A conceptual Fran=me work for accessing Passwords Quality,IJCSNS, International Journal of Computer Science and Network Security, Vol. 7 No1 pp 179-185,2007

[6] Klein, D., Foiling the Cracker: a Survey of improvements to password security, Proceedings of the 2nd USENIX security workshop,http://www.citeseer.ist.psu.edu/112514.html,May 2008

[7] Paivio A., Rogers, T.B., and Symthe,P.C. 1968. Why are pictures easier to recall than words? Psychonomic Science,11:137-138,1968

[8] R.Dhamija and A.Perrig,"Déjà vu: A user Study using Images for authentication", in Proceedings of 9th USENIX Security Symposium,2000

[9] T. Pering, M. Sundar, J. Light, Roy W," Photographic Authentication through Untrusted Terminals", IEEE Pervasive Computing, January 2003,PP 30-36

[10] S.Akula & V. Devisetty, " Image Based Registration and Authentication System" in Proceedings of Midwest Instruction & Computing Symposium,2004

[11] S.Wiedenbeck, j. Waters,J.C. Birget, A.Brodskiy, N.Memon, "Design and Longitudinal evaluation of a graphical password system", International Journal of Human Computer Studies 63(2005) 102-127.

[12] L.Y. Por, X. T. Lim, M.T. Su, F. Kianoush,"The Design and Implementation of Background Pass-Go Scheme Towards security Threats" WSEAS Transactions on Information science and Applications, ISSN:1790-0832, Issue 6, Volume 5, June 2008

[13] Dhruv KumarYadav,Beatrice Ionascu, Sai Vamsi Krishna Ongole,Aditi Roy, Nasir Memon, "Design and Analysis of Shoulder Shurfing Resistant Pin Based Authentication Mechanisms on Google Glass", International conference on Financial cryptography and Data Security, pppp281-297,2015

[14] Chen Sun,Yang Wang, Jun Zheng "Dissecting pattern unlock:The effect of pattern strength meter on pattern selection" Journal of information security and applicaions Nov 2014, Elsevier,pp308-320

[15] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, Jonathan M Smith,"Smudge attacks on smartphone touch screens" WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies Article No.1-7 Washington DC, USENIX Association Berkley, CA

[16] Sebastian Uellenbeck, Markus Durmuth, Christopher Wolf and Thorsten Holz, CCS'13 Proceedings of the 2013 ACM SIGSAC conference of Computer & Communication security, Pages 161-172. Berlin Germany November 04-08,2013, ACM New york NY

[17] Blasé Ur, Patrick Gage Kelley,saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek,Timothy Passaro, Richard Shay,Timothy Vidas,Lujo Bauer, Nicholas Christin,Lorrie Faith Cranor,"How does your Password measure up?" The effet of strength meters on password creation", ACM,Proceeding Security'12 Proceedings of the 21st USENIX conference on Security Symposium, Bellevue ,WA, USENIX Association Berkeley, CA,USA.

[18] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, Cormac Herley, "Does my password go up to eleven? The impact of Password Meters on Password Selection" CHI'13 ,Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Pg 2379-2388, Paris, France –April 27- May 02-2013

[19] Blasé Ur, Felicia Alfieri, maung Aung,Lujo Bauer, Nicholas Christin, Jessica Colnago, Lorrie Faith Cranor, henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher, "Design and evaluation of Data-Driven Password Meter" CHI'17 ,Conference on Human Factors in Computing Systems, pg. 3775-3786,ACM ,ISBN:978-1-4503-4655-9

[20] L.D. Paulson "Taking a graphical Password to the approach", Computer(Volume 35,Issue 7,July 2002),IEEE Computer Society

[21] S. Brostoff and M. A.Sasse, "Are Passfaces maore usable than passwords", a field trial investigation in peiolple and computers XIV-Usability or Else:Proceedings of HCI, Sunderland, Uk: Springer-Verlag 2000

[22] D. Davis F. Monrose and M.K. Reiter,"On User choice in graphical Password Scheme" in proceedings of the 13th USENIX Security Symposium, San Diego, CA , 2004

[23] W.Jansen, S. gavrila, V Korolev, R Ayers and R Swanstorm, "Picture Password: A Visual Login technique for Mobile devices" National Institute of Standards and Technology Interagency Report NISTIR 7030,2003

[24] W. A. Jansen "Authenticating users on Handheld Devices" in proceedings of Canadian Information Technology Security Symposium,2003

[25] W.Jansen "Authenticating Mobile Device Users through image Selection" in Data Security,2004

Authors Profile

Mr Norman Dias pursued Bachelor of Computer Engineering from Goa University and Master of Computer Science in year 2013. He also pursued Diploma in Embedded Systen and Design at Centre of Development and Advanced Computing C-DAC, Kolkata. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Engineering, at Don Bosco College of Engineering, Goa University since 2014.. His main research work focuses on Security in textual and Graphical Passwords. He has 9 years of teaching experience.

Dr Reeja S R an Associate Professor in the Department of Computer Science and Engineering, earned her Ph.D in Computer Science & Engineering from Visvesvaraya Technological University (VTU), Govt. of Karnataka for her thesis Real Time Video Denoising. She has nearly 12 years of teaching experience in various engineering colleges and 5 years of research experience in the concerned field. She has worked in VSSC/ISRO as a Research Assistant in QRSG (Quality Assurance & Reliability Software & mission Group) for 1 year. She has published 8 international Journal, 1 national journal, 5 international conferences and 3 national conferences. She was also a Programme committee member for the first international conference on bioinformatics and bioscience (ICBB) held in Pune, first international conference on Computer science and information technology (CoSIT) held in Royal orchid centre Bangalore, the second international conference on Artificial intelligence and Application(ARIR) in Switzerland and the fourth international conference on Natural Language Processing (NLP) in Australia and Editorial Board member of an international journal Signal and image processing(SIPIJ).

© 2018, IJCSE All Rights Reserved