International Journal of Advance in Computer Science & its application – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 7 : Issue 2 [ISSN : 2250-3765] - Publication Date: 25 June , 2018

Framework to suggest the most non predictable and secure user graphical password patterns in android phones.

[1. Dr. Syed Imran Ali, 2. Muhammed Zafar Iqbal, 3. Muhammed Khurram 4. Majed Said Al Busaidi]

Abstract— Graphical password scheme is perhaps the most widely used method to lock the mobile handsets but unfortunately they are easily guessable. In this paper, we have identified the security threat that the graphical password patterns in smart phones are predictable based on various important parameters like demographics, language proficiency, cultural backgrounds, etc. We further proposed a framework, which suggests you the most non-predictable and secure password pattern considering the demographics, language proficiency, and cultural backgrounds of the user.

Keywords— Security threats, Predictable passwords, Graphical password patterns, demographics, cultural background, language proficiency, secure passwords.

Introduction

The ever-increased use of smartphones in our daily lives and the amount of personal information being carried on these devices demands for stronger authentication measures than ever. Smartphones are used to perform sensitive personal and financial tasks including online banking, messaging.
Normally, there are following in built security measures available in smart phones like:
1. PIN (3/4/5 digit PINs)
2. Text based passwords
3. Graphical password patterns.
PIN based security is one of the traditional way of securing critical data and locking the phone [1]. However, a tremendous increase has been observed in graphical password scheme, due to its perceived user friendliness [2]. According to the latest study 40% of Android users prefer to use pattern based technique to unlock the phone instead of PIN based [3].

Graphical password scheme is perhaps the most widely used and most studied graphical password system to date. With its launch, Android's only authentication/unlock mechanism was the graphical password; however, other authentication systems are allowed today, such as PINs and text-based passwords. Despite the added authentication choices, the graphical password option remains a very popular choice among Android users [4, 5].
The graphical password system requires users to select and recall a "pattern" drawn over a 3x3 grid of contact points, connecting between 4 and 9 contact points, without repetition. There are 392,112 possible passwords [6] which provide more choices than a 4-digit PIN (10,000); however, like all password systems, users do not choose uniformly from the set of available passwords. Recent studies have shown that the guess ability strength of user-generated password patterns is about a random 3-digit PIN [7, 8] and provides weaker security than one might expect.

In theory, Password Pattern is more secure than a 5-digit PIN scheme but are known to be much skewed. They often include predictable shapes (e.g. and N), biases in selection of starting point, and predictable sequences of the points that make them easy to guess. In practice, this decreases the security of Password Pattern to that of a3-digit PIN scheme for at least half of the users.

Uellenbeck et al. [8] proved biased starting point (i.e. some points are usually chosen more than others) and n-grams (i.e. frequent subsequences of patterns) which can be easily predictable. According to these findings, it has been proved that 50% of the patterns with only 1000 guesses. On the other hand, we can state the effective android pattern password space is equivalent to just a 3 digit scheme for approximately 50% of Android users.

Much of the predictability of user generated graphical passwords depends on following parameters:
1. Repetition of pattern features: For example, most passwords begin in the upper left and terminate in the lower right.
2. Demographics: It may play role in the predictability of graphical passwords for example, there may exist subtle differences in gender and handedness (left hander or right hander) in selecting a pattern with respect to the spatial layout and the directionality.
3. Writing style of cultural background: For example, in some eastern settings, such as those that use Arabic language the script is written right-to-left as opposed to left-to-write in Latin.

BACKGROUND & RELATED WORK

The first ever graphical password "Draw a Secret" (DAS) was proposed by Jermyn et al. [10]. In DAS, user creates a password by drawing a pattern that connects cells of a grid on a screen.
Tao [11] introduced Pass-Go that uses intersections of the cell in a grid and improved its usability. Android Pattern is a type of Pass-Go system and is widely adopted by Android users. Several models and techniques have been proposed in literature to address this security issue but unfortunately fail to address the problem.

Dr. Syed Imran Ali
Nizwa College of Technology
Sultanate of Oman
Syed.imran@nct.edu.om

1. "Background Draw-a-Secret" (BDAS): By adding a background to the grid of the DAS scheme, increase in the length of patterns by using a usability test has been proved by the authors. [13] [14]. Gao et al. [15] and Zhao et al. [16] demonstrated that the probability of guessing which is based on the detectable hotspots in the background images in Windows 8 graphical password, which is almost similar to BDAS.

2. Rotation Draw-a-Secret" (R-DAS): In this scheme, degree of freedom as a rotation has been added to DAS [17]. This scheme may increase the theoretical password space as well as effective password space. Practically RDAS scheme is not appropriate in Android pattern because it is a single-stroke scheme. Usually Android patterns are used for frequent authentication and this rotation Draw a Secret probably effect on its usability on a layer scale.

3. Layering: An extension of DAS called touch screen multi layered drawing (TMD) proposed by Chiang et al. [18] where he introduced "wrap cells", this extension allow users to continuously draw their passwords across multiple layers. This technique may improves the theoretical password space however according to the study, which proves, that biases of starting point and shape of the patterns remains pertinent.

4. Black listing: This technique forbids frequently-chosen patterns, this scheme allows only shifts the distribution to a new set of frequent-chosen pattern, and therefore the drawback is it does not hinder a resourceful attacker.

5. Random Assignment: This scheme is designed as it choses random pattern for the users, the drawback in this system is it comes with a significant cost on usability and memorability.

6. Rearrangement: In this scheme, the user has to removed frequently chosen starting points and then it supposed to be rearranged all the points. The issue in this this technique is that itself does not expand the effective password-space.

7. User Education: Awareness should be created among the users to differentiate between strong and weak passwords so that they may prefer the latter over the former.

PROPOSED METHODOLOGY

In this paper, we have proposed a methodology where system will conduct a questionnaire with some set of questions related to the details of user like name, left hander or right hander, cultural background etc. Then the system will analyze the user details and suggest him the most possible unpredictable and secure password.

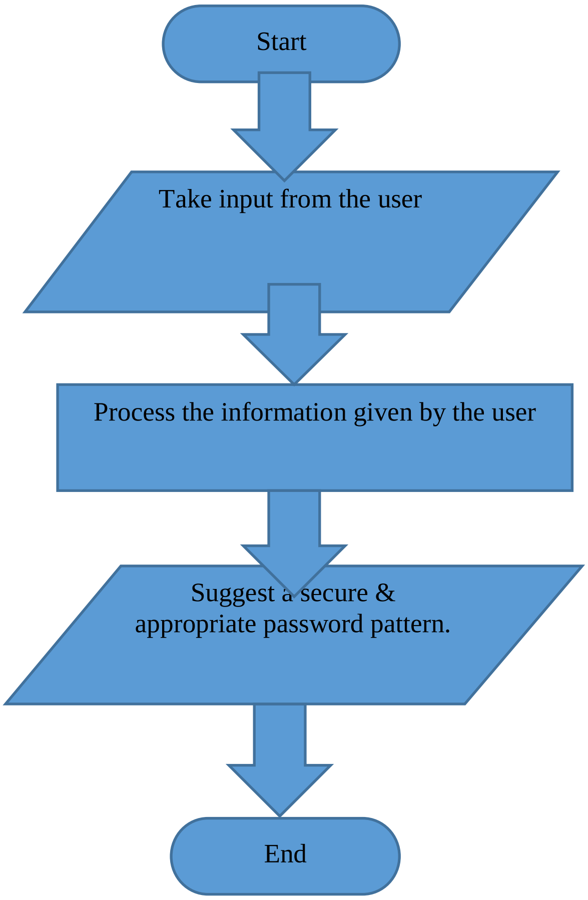
Start
Take input from the user
Process the information given by the user
Suggest a secure &
appropriate password pattern.
End

Fig 1. Flowchart of the proposed system

The user would be asked to enter his basic details like Name, Cultural background (Mother language) hand writing style (left hander or right hander).
After getting the details system will analyze the entered information and would try to suggest a password that is not predictable based on these details.
For example, a user enters following information:
Name: Naveed
Handwriting style: Right hander
Mother language: Arabic

Based on the given information, the following patterns are not secure at all as they are predictable.

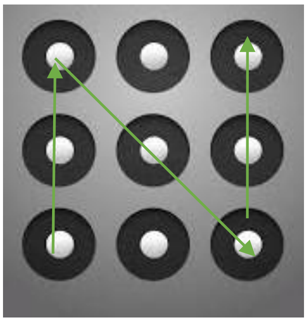

Fig.2.1

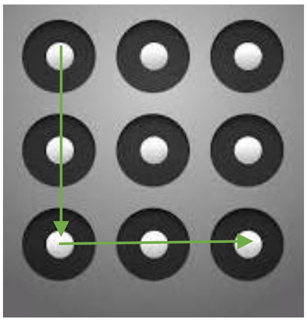

Fig.2.2

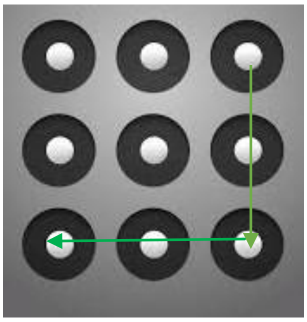

Fig.2.3

Since the name of the user is starts from alphabet 'N', the pattern should not be like Fig 2.1., his handwriting style is left hander so the patterns like that of Fig.2.2 (starting from left and ending towards right) are not advisable and his mother language is Arabic so the patterns like that of Fig.2.3 (starting from right and ending towards left) are not suggested.

The probable password for this type of user is patterns may be those that:
a.) Does not starts from left and ends towards right (as user is right hander),
b.) Does not starts from right and ends towards left (as user is Arabic)
c.) Should not be similar to alphabet N (as user name stars from N)

The secure password for such user may be any password, which avoids above mentioned 3 cases. The non-predictable pattern for such user may be as shown in fig.3

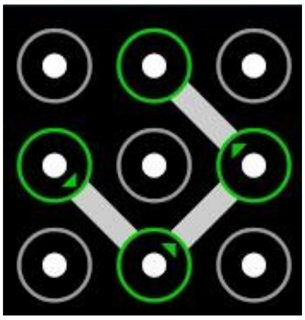

Fig.3 Suggested secured pattern lock

CONCLUSION

In this paper, we proposed a framework to suggest the most non predictable and secure user graphical password patterns in android phones. The system will conduct a questionnaire with some set of questions related to the details of user like name, left hander or right hander, cultural background etc. Then the system will analyze the user details and suggest him the most possible unpredictable and secure password. For the proposed idea, authors are developing an android App which would be uploaded soon on Play store

References

[1] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 750–761.

[2] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM, 2013, p. 10.

[3] D. C. Van Bruggen, "Studying the impact of security awareness efforts on user behavior." Ph.D. Thesis, University of Notre Dame, 2014.

[4] A. J. Aviv, J. Maguire, and J. L. Prak. Analyzing the impact of collection methods and demographics for android's pattern unlock. In Proc. Workshop on Usable Security (USEC). Internet Society, 2016.

[5] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith. Practicality of accelerometer side channels on smartphones. In Proc. Annual Computer Security Applications Conference (ACSAC), 2012.

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In Proc. Workshop on Offensive Technology (WOOT), 2010.

[7] Y. Song, G. Cho, S. Oh, H. Kim, and J. H. Huh. On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In Proc. Annual ACM Conference on Human Factors in Computing Systems (CHI), 2015.

[8] S. Uellenbeck, M. D¨urmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In Proc. ACM Conference on Computer & Communications Security (CCS), pages 161–172. ACM, 2013.

[9] H. Tao and C. Adams. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security, 7(2):273–292, 2008.

[10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The Design and Analysis of Graphical Passwords. In USENIX Security Symposium, 1999.

[11] M. Harbach, A. De Luca, and S. Egelman. The anatomy of smartphone unlocking: A field study of android lock screens. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI '16, pages 4806–4817, New York, NY, USA, 2016. ACM.

[12] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. Itaˆ˘ A´Zsa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In Symposium On Usable Privacy and Security (SOUPS 2014), pages 213–230, 2014.

[13] P. Dunphy and J. Yan, "Do background images improve draw a secret graphical passwords?" in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 36–47.

[14] Z.Zhao,G.-J.Ahn,J.-J.Seo,andH.Hu,"Onthesecurityofpicturegesture authentication," in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 383–398.

[15] H. Gao, W. Jia, N. Liu, and K. Li, "The hot-spots problem in windows 8 graphical password scheme," in Cyberspace Safety and Security. Springer, 2013, pp. 349–362.

[16] Z. Zhao, G.-J. Ahn, J.-J. Seo, and H. Hu, "On the security of picture gesture authentication." in USENIX Security, 2013, pp. 383–398.

[17] S. Chakrabarti, G. V. Landon, and M. Singhal, "Graphical passwords: drawing a secret with rotation as a new degree of freedom," in Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks. ACTA Press, 2007, pp. 561–173.

[18] H.-Y. Chiang and S. Chiasson, "Improving user authentication on mobile devices: A touchscreen graphical password," in Proceedings of the 15th international conference on Human-computer interaction with mobile devices

About Author (s):

Dr. Syed Imran Ali
Lecturer
Engineering Department
Nizwa College of Technology
Sultanate of Oman
syed.imran@nct.edu.om

Mr. Muhammad Zafar Iqbal Khan
Lecturer
Engineering Department
Nizwa College of Technology
Sultanate of Oman
Zafar.iqbal@nct.edu.om

Mr. Muhammad Khurram
Lecturer, Engineering Department, Nizwa College of Technology,
Sultanate of Oman
muhammad.khurram@nct.edu.om

Majed Said Al Busaidi
Undergraduate Student,
Electronics and Communication Engineering,
Nizwa College of Technology
Sultanate of Oman