Position Paper: Measuring the Impact of Alphabet and Culture on Graphical Passwords

Adam J. Aviv
United States Naval Academy
aviv@usna.edu

Markus Dürmuth
Ruhr-University Bochum
markus.duermuth@rub.de

Payas Gupta
NYU, Abu Dhabi
payasgupta@nyu.edu

1. OUR POSITION

Android's graphical password scheme (sometimes referred to as the "password pattern") 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 [6, 7, 14].

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 password [3], 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 guessability strength of user-generated password patterns is on the order of a random 3-digit PIN [11, 2, 13] and provides weaker security than one might expect.

Much of the predictability of user generated graphical passwords comes from repetition of pattern features [2, 13]. For example, most passwords begin in the upper left and terminate in the lower right. Many patterns from users are duplicate of other's or are flip/rotation/reversal of other's. Leveraging these properties, it is straightforward to build advanced automated guessers based on these statistical properties that can accurately predict the kinds of graphical password patterns that people may choose.

Further, recent results suggest that demographics may play role in the predictability of graphical passwords [4]; for example, there may exist subtle differences in gender and handedness in selecting a pattern with respect to the spatial layout and the directionality. One underlying demographic factor that *has not* been considered but may also play an important role in graphical password selection is language proficiency and cultural background.

A graphical password system, being graphical, may be influenced by the writing style of the 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). A key open question that we wish to shine some light on is: *Does the cultural background and writing environment affect the kinds of graphical passwords that users select and use?*

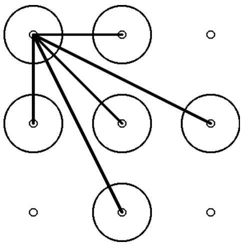

Figure 1: Points reachable from the top-left node.

In this position paper, we further motivate the need of such studies which we are in the pilot stage of developing and propose other important research questions that may impact graphical password selection based on culture or character-set of the language alphabet as well as cultural differences. Just as with text based passwords [9] definitive selection biases may be identifiable with these sub groups.

2. BACKGROUND AND RELATED WORK

Android's graphical password system (or "password pattern") was launched with the Android platform in 2008 and is based on prior systems such as Pass-Go scheme [12] and Draw-A-Secret (DAS) [8], one of the earliest graphical password schemes. The most common design of the password pattern requires users to select and recall a "pattern" drawn by contacting a set of contact points over a 3×3 grid[1]. The following rules apply to patterns:

(i) Patterns must contact at least four contact points,
(ii) Contact points may not repeat in a pattern,
(iii) All contact points along a path will be connected (unless it was selected before[2]).

Figure 1 demonstrates the points reachable from the top-left starting position as an example of pattern selection. In total, there are 389,112 possible patterns [3].

Due to its wide availability and usage, this scheme is probably the most studied graphical password scheme to date. The

[1] Larger grid sizes are allowed in some Android variants, such as CynogenMod.

[2] Some Android variants allow users to avoid uncontacted points along a path, such as Samsung implementations, but we do not consider those variants in our research.

password pattern has been studied both from an attack perspective [5, 3], usage prevalence [6, 7, 14], and password strength [13, 1, 11, 2, 10].

However, one commonality of prior analysis of Android's graphical password systems is that participant recruitment and collection methodologies occurred in Latin-alphabet and western cultural settings[3]. Recent work by Aviv et. al [4] shows that there exists demographic differences within a single-cultural group (namely, individuals residing within the USA) between right and left handed participants and between genders. Analysis of non-Latin-alphabet users and Eastern cultural individuals has not been explicitly tested for graphical passwords.

3. RESEARCH DIRECTIONS

Questions. Based on this motivation, we argue that the following research questions should be pursued by the community, and we are in the pilot stage of launching studies to answer these questions.

(i) *What is the impact of the writing system on graphical passwords?* It is known, at least for Latin-based alphabet languages, such as English and German, that users tend to select passwords that begin in the upper-left and end in the lower-right [2, 13]. It is an open question if such tendencies exist in different writing systems.

A corollary to this research question relates to caligraphic languages, like Chinese, which would require many more contact points than 3x3 to input symbols. *If provided with larger grid sizes, would users of these writing systems select passwords related to their language's symbols?*

(ii) *What is the cultural and language impact?* Preliminary evidence suggests that western cultural have similar distributions of pattern selections, however, is cultural differences enough to change the kinds of patterns people select? For example, if an attacker were to target a certain demographic (say Eastern cultural user) but only have another demographics sample data (say Western cultural), how would the attack perform?

(iii) *Does bilingual users affected differently than unilingual users in password choice?* For those users who speak multiple languages, or have learned a language later in life, does the patterns they selected affected by one language over the other?

(iv) *Is there culturally tuned ways to improve password choice?* Leverage cultural differences, we seek to know if there are ways to *nudge* individuals in different cultures towards stronger passwords.

Challenges. To investigate these research questions, and more, we need to address a larger challenge, namely conducting research in languages and locations that are beyond the typical reach of the authors. Anecdotally, in discussions with a foreign language faculty member, recruited to translate a previously implemented survey, she responded that she is ill suited for the role because of the technical nature of the material. Instead, it was recommended instead to recruits a bilingual student, more versed in the technical vernacular of the language, to perform the translation. Beyond translations, challenges exist in recruitment. Identifying fair comparisons sets across geographic domainsrequires careful thought. Finally, there are challenges regarding the density of smartphone usage and knowledge of patterns in these locations. It is not known, for example, if Android or the Android graphical password is common enough to accurately measure user choice or have users generate relevant patterns.

4. CONCLUSION

In this position paper, we argue that there are important research questions pertaining to the demographic differences of graphical password choice that is yet to be investigated, and we are in the process of developing studies to address this gap. We have outlined a number of possible directions and challenges associated with answering those questions, and we hope shed light on this interesting topic.

Acknowledgments This work was supported in part by ONR grants N0001416WX01494 and N0001416WX01664, and via the Science of Security Lablet from the NSA.

5. REFERENCES

[1] P. Andriotis, T. Tryfonas, and G. Oikonomou. Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In *Human Aspects of Information Security, Privacy, and Trust*, pages 115–126. Springer, 2014.

[2] A. J. Aviv, D. Budzitowski, and R. Kuber. Is bigger better? comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In *Proc. Annual Computer Security Applications Conference (ACSAC)*, 2015.

[3] 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.

[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] 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.

[7] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. ItâĂŹsa 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.

[8] 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.

[9] Z. Li, W. Han, and W. Xu. A large-scale empirical analysis of chinese web passwords. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 559–574, 2014.

[10] H. Siadati, P. Gupta, S. Smith, N. Memon, and M. Ahamad. Fortifying android patterns using persuasive security framework. In *The Ninth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM) 2015*, 2015.

[11] 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.

[12] 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.

[13] S. Uellenbeck, M. Dürmuth, 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.

[14] E. von Zezschwitz, P. Dunphy, and A. D. Luca. 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 (MobileHCI)*, 2013.

[3] Granted, Song et. al meter work [11] was conducted in Korea, the online data collection occurred in English.