A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication

Mohd Anwar and Ashiq Imran

Department of Computer Science

North Carolina A&T State University
manwar@ncat.edu, aimran@aggies.ncat.edu

Abstract

Mobile devices such as smartphones and tablets are widely used to perform security critical and privacy sensitive activities, such as mobile banking, mobile health care, mobile shopping, etc. Screen locks are used in mobile devices to protect sensitive information. Graphical password and alphanumeric password are two common types of screen locking schemes. The alphanumeric password scheme has shown some security and usability drawbacks. For example, a user may pick an easy to remember alphanumeric password that may also be easy to guess. On the contrary, if as user picks a password that is hard to guess it may also be hard to remember. Several alternative password mechanisms have been introduced. Graphical password is one of them, and it is based on pictures or patterns. However, graphical password is also vulnerable to certain types of attack. In this paper, we study an alphanumeric password method (i.e., PIN) and a graphical password method (i.e., pattern) in order to unravel security and usability issues related to mobile device authentication. The study uses observation and survey data to compare these two authentication methods on following criteria: creation time, memorability, and login time and login success rate. In addition, we also measure how the screen size of a mobile device affects usability and security aspects of screen locks by measuring differences on creation time, memorability, login time, login success rate for Android smartphone and tablet.

1. Introduction

Humans are often considered the weakest link for security in information and communication technology. Patrick, Long, and Flinn (2003) identify three security areas for which human factor issues are very important: authentication (passwords), security operations (intrusion detection) and developing secure systems (developing the security). If a user misplaces a mobile device in which a screen lock is not activated, then whoever finds it may have access to sensitive information. Therefore, an authentication mechanism is necessary to protect sensitive information on mobile devices. In order to build an efficient and feasible mobile authentication there is a need to strike a balance between usability and security.

Generally user authentication is based on three factors: what the user knows; what the user has; and what the user is. The authentication methods in our study are based on what the user knows (knowledge-factor). Based on knowledge-factor, different types of authentication methods have been proposed over the years. Alphanumeric passwords are the most common but they have some drawbacks. Previous studies have shown that users tend to choose short alphanumeric passwords that are easy to remember (Adams and Sasse 1999) but that password can be easily guessed. On the other hand, if an alphanumeric password is hard to guess, then it is often hard to remember (Suo, Zhu, and Owen 2005). Since users can remember a limited number of alphanumeric passwords, they often write down their passwords or use same password for multiple accounts (Kotadia 2005). Graphical password has been introduced as an alternative to alphanumeric password. The motivation behind graphical password is that users can remember pictures better than text. Human psychology supports such assumption (Shepard 1967). Because of this memorability advantage, there is significant interest in graphical password (Everitt et al. 2009).

At present, digit lock or PIN is considered the most popular password among mobile device authentication methods. Approximately 88% mobile users set the PIN in their devices (Jakobsson et al. 2009). This method is typically required to select four-digit personal identification number (PIN) that users memorize and enter using a virtual keypad to unlock a locked phone. The PIN for screen lock provides 10000 different combinations. This method belongs to alphanumeric password scheme. In recent times, a graphical password scheme named pattern lock is getting popularity amongst the Android OS users (Aviv et al. 2010). The Android pattern lock requires traversing an on-screen 3 × 3 grid of contact points. Android pattern lock provides 389112 distinct patterns for 9-point combination.

This paper explores user behavior regarding these two password schemes and discusses security threats for mobile devices. We have done a survey study to get some knowledge on user preference and feedback on both password schemes. We present a comparative study between graphical (Pattern) and alphanumeric password scheme in terms of usability and security. Lastly, we analyze data to determine the performance of pattern and PIN with respect to screen size.

This paper will provide an overview of various kinds of graphical password authentication systems and then do a comparison between graphical password and alphanumeric password. We study android pattern lock as a graphical password scheme and PIN as an alphanumeric password scheme for our experiment. The remainder of this paper is structured as follows: Section 2 presents related works of our approach. We describe our experiment in section 3. In section 4, we present results. We discuss result in section 5. Section 6 describes the limitation and future work. This paper is concluded in section 7.

2. Related Works

Mobile devices contain various type of sensitive personal information such as text messages, emails, notes, apps, app data, music, pictures, and so much more. Though it is really a great convenience to have all of these information in our mobile devices, it also allows security risk if all of the information is easily accessible. One way to avoid and prevent the security attacks is to set some sort of screen lock, which provides authentication on our mobile devices.

Several types of authentication methods are proposed over the years. Alphanumeric password scheme is one of the most common methods for mobile authentication. However, it has some security and usability drawbacks such as: a difficult password is hard to remember, and a short password is easy to guess. Some researchers have developed graphical passwords as an alternative way or an extension to text password to address the drawbacks of guessing attacks and making it easy to remember. But graphical password may also be vulnerable for certain attacks (Lashkari et al. 2009). A comprehensive research study is needed to find out which mobile authentication method serves the purposes better in terms of usability and security.

Graphical password schemes can be categorized into three groups: recognition based, recall based, and cued recall based (Chiang and Chiasson 2013). In a recognition-based scheme, a set of images is given and the user needs to identify correct images that the user had already set in order to authenticate (e.g., Use Your Illusion (UYI)). In UYI scheme, the login screen displays 9 images randomly positioned in a 3 × 3 grid (Schaub et al. 2013). The user needs to recognize and select a right image amongst trap images. Both of the papers provide creation time, login time, and login success rate as the measurement criteria for usability. Chiang and Chiasson (2013) also described the password length and password strength as security criteria.

Recall schemes require recreating drawings without a hint (e.g., Android Pattern Lock). Chiasson et al. (2009) propose a recall based graphical password called the pass-point in which, users must select the same click-points in the same order to login. After comparing the pass-points with the alphanumeric password, they find that participants using pass-points have success rates approximately 99%, whereas participants have approximately 88% success rates for alphanumeric password.

Tao and Adams (2008) introduce a recall based password scheme called the pass-go. A user can either draw dots on intersection points or connect intersection points with strokes. Points and lines have to be drawn in the correct order for successful authentication. PassGo is a grid-based scheme, which is an improvement of Draw A Secret (DAS) (Jermyn et al. 1999).

Chiasson et al. (2008) introduce a cued recall based password where a sequence of points needs to be selected on a cue like an image. Another new technique, persuasive cued click points (PCCP), is proposed by Chiasson et al. (2012). They describe that graphical password is effective in terms of memorability and provide benefits over alphanumeric passwords because images can be used as cues for different passwords. They also point out graphical passwords are easy to learn but typically require longer login time.

An extensive research has been done in the quest for replacing passwords for web authentication (Bonneau et al. 2012). This paper offers some benchmark for comparative evaluation of authentication schemes. They enlist 11 types of alternative password methods, such as biometrics recognition, graphical password (PCCP), etc. that can be used to replace alphanumeric password. They categorize usability benefits of an ideal authentication scheme into 8 properties: memorywise-effortless, scalable-for-users, easy-to-learn, efficient-to-use, infrequent-errors, etc. Furthermore, an ideal authentication scheme should have following security benefits: resilient to physical observation, resilient to guessing, resilient to theft as the measurement to compare each password scheme with alphanumeric password.

Biddle, Chiasson, and Oorschot (2012) describe each category and compare 9 different graphical password methods. They compare required login time and login success rate in terms of usability. They also classified two types of security attacks, i.e., guessing attacks and capture attacks. They list shoulder surfing attacks as a category of capture attacks.

A comparative study is needed to determine advantages and disadvantages between graphical and alphanumeric password schemes on mobile devices. In our study, we compare Android pattern lock (graphical) and PIN (alphanumeric) to find out usability issues such as creation time, memorability, and duration of login and success rate of login. We explore whether screen size of the mobile devices has any impact on each usability criterion. In addition, we try to figure out which of usability and security matters most to the users. We also studied user perception about three methods of attack for pattern and PIN screen locks.

3. Experiments

Our experiment focuses on determining usability and security issues of pattern and PIN screen locks. In our study, usability is measured by password creation time, memorability, login time, and login success rate. We also determine whether the size of the mobile device has impact on the measurements. For security issues, we collect user perception data on three methods of attacks: guessing attacks, smudge attacks, and shoulder surfing attacks. In our study, we used Android OS smartphone (HTC Smartphone Model ADR6330VW) and tablet (Samsung Galaxy Tab 2 -10.1 GT- P5113), which provide PIN and pattern screen locks.

3.1 Recruitment

The study protocol, consent form, and recruitment flyer were approved by the Institutional Review Board (IRB) of the University. Our study involved human subjects performing different screen lock tasks and participating in a survey. The recruitment flyer was disseminated through email and posted on social media sites. The flyer has two parts. In the first part, the details of the project and tasks are stated. In the second part, the eligibility of the participants was described. An inclusion criterion was set that a participant should have experience of using smartphones or tablets. The consent form is a formal description of the survey. The type of the task and duration of the survey were mentioned. A participant must be 17 years old to participate in the survey. We designed the online survey using Qualtrics toolkit. We launched and distributed the link to survey site in different social media website such as Facebook. Online survey provides us the opportunity to gather participants in a short time. We recruited 33 participants in the online survey. Among the participants, 25 of them are male and 8 of them are female. Majority of participants (61%) belongs to 22-26 age group and most of them are graduate students.

3.2 Task

The purpose of user tasks is to find out the creation time and login time of pattern lock and PIN for Android smartphone and tablet. In addition, we want to know whether device size has any effect on these two criteria. The subjects performed these tasks in the campus of North Carolina A&T State University. The recruited subjects were volunteers from our university. We provided each subject with a smartphone and a tablet. We measured the creation and login time using a stopwatch. For measuring creation time of pattern password, we asked them to create the pattern lock in the smartphone and tablet. We asked whether the subject created the same pattern password in both the devices or not. We asked them to login in the same order that they created the pattern. In the same manner, we measured the creation time of and login time with PIN for both devices. We ask whether they create same PIN in both devices or not. We ran these experiments with 33 participants. In addition, we calculated the average length of both the screen locks and user behavior of creating same screen lock for both the smartphone and the tablet.

3.3 Survey

We deployed an online survey using Qualtrics toolkit. After designing and adding survey questions, we launched the survey and distributed the survey link in different social media websites such as Facebook. The online survey gave us the opportunity to gather more participants in a short time. It also provides more flexibility to collect and analyze data. Total number of questions in our survey is 29. The survey was anonymous. The participants' information is kept confidential. The survey had some demographic questions. For example, *in which age group do you belong?* Some questions were on users' security behavior. For example, *how often do you change your password on a mobile device?* The survey includes multiple 5-point likert scale items. For example, small screen devices (Smartphones) are more suitable for screen lock than big screen devices (Tablets). Some ranking type questions were in the survey. For example, rank different methods of attack (Guessing attacks, Smudge attacks, Shoulder surfing attacks etc.) for mobile devices? The survey also asks whether the subject will prefer a difficult screen lock to an easy screen lock.

4. Results

We analyzed data collected from user tasks and survey responses to identify usability issues and user preferences when using graphical passwords on mobile devices. We determined how screen size affects login performance by comparing differences between Android smartphone and tablet on creation time, login time, and login success rate for each scheme. For the creation time and login time, we used t-tests to determine whether there are significant differences for different devices. All the t-tests are performed at 95% confidence interval (i.e., the α-value is set at 0.05).

Creation Time

The password creation time is measured as the time between first touch on mobile devices to touch the submit button. An unpaired t-test showed some significant difference between pattern password and PIN when we used tablet ($p = 0.04$). We compared pattern creation time and PIN creation time for both tablet and phone. We get significant result for only pattern creation time ($p = 0.0007$). We calculated unpaired t-test of PIN creation time for both tablet and phone. The result is not significant. Figure 1 shows the box-and-whisker plot for the creation time of both PIN and pattern on mobile devices. The pattern on the tablet takes the highest time among other comparison.

Login Time

The login time is measured as the time for successful login into the mobile device. We run our task to compare both pattern and PIN in mobile device of different size. We run unpaired t-test for four cases. We calculate t-test of login time of pattern and PIN for separately and together with tablet and phone. When measuring login time, we treated user reset as fail attempts. We get no significant result for login time between pattern and PIN schemes. Figure 2 shows the box-and-whisker plots for login time of both PIN and pattern on different size mobile devices (phone and tablet). The pattern takes slightly less time to log in on phone, and PIN takes slightly less time on tablet.

Login Success Rate

Table 1 shows the login success rate of both PIN and screen lock. From 31 participants 29 participants can enter successfully correct PIN 18 times out of 20. On the contrary, 23 participants think that they can enter 18 times out of 20 successful patterns.

Table 1 Login success rate

Type of screen lock	Login Success rate
PIN	88%
Pattern	83%

Memorability

Most of the participants provide memorize screen lock for login into mobile devices. From our survey, approximately 81% participants memorize their screen lock. Some participants (12%) write down their screen lock in a piece of paper. According to the participants, about 39% of them never forget their PIN whereas 56% of the participants never forget their pattern. In our study, 80% participants create same PIN and pattern passwords for both mobile devices.

Screen Size Impact

In the survey, we asked the participants a 5-point likert scale question about screen size impacts on both PIN and pattern screen locks. Figure 3 shows the result of that question. For PIN, participants do not agree with: the screen size can have an effect on usability. Most of the participants agree that PIN is easier to use on phone than tablet (SD =1.3). On the contrary, most of the participants (SD = 1.02) support that pattern is easier to use on tablet than on phone.

Observation of attacks

We observe users and noted relevant behaviors and feedback. Most of the users create same PIN and same pattern for both tablet and phone. About 20% of them create different PIN and pattern password for different mobile devices. The majority of the participants (75%) choose to create difficult pattern points (e.g., 1->4->5->8->9) instead of easy pattern points (e.g., 1->2->3->6). For PIN, 87% of participants choose a difficult PIN (e.g., 1928). According to participants shoulder surfing attacks has 43% chance to be a threat for PIN. On the other hand, smudge attacks has 50% chance for pattern.

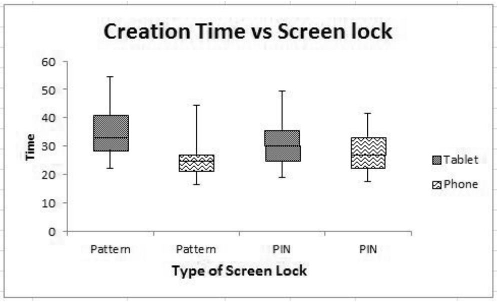

Figure 1: Comparison of creation time of pattern and PIN.

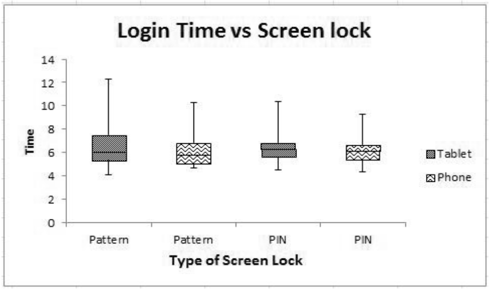

Figure 2: Comparison of login time of pattern and PIN.

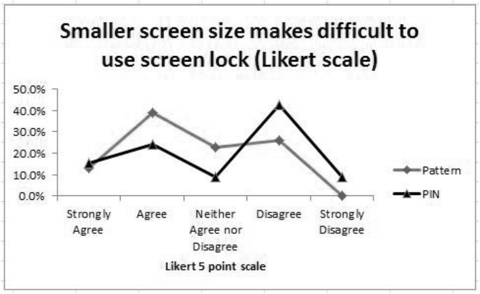

Figure 3: Smaller size factor of pattern and PIN.

5. Discussions

We measured creation time and login time for PIN and pattern password in two different sizes of mobile devices to find out whether the size of the device has any effect. Our observations are drawn from user tasks and survey results.

Observation 1: The creation time of both PIN and pattern-based screen locks in mobile phone is less than that in tablet.

Observation 2: The creation time of pattern password is quicker than the creation time of PIN in Android mobile phone.

Observation 3: People who used same pattern/PIN for different devices take slightly less time to log in than people who use different pattern/PIN.

Observation 4: Login time is dependent on the length of pattern password. Longer (7-8) pattern takes more time than shorter pattern. Since PIN has fixed length of 4 digits, the login time is consistent.

Among the study participants, 87% want to have a difficult PIN, and 75% want to have strong pattern password. Therefore, the majority of the participants preferred security to usability.

One indicator of the security strength of a password scheme is the total number of possible passwords, also known as possible *password space*. A brute-force attack against a specific password would involve exhaustively searching the password space. The possible password space for PIN is 10000 (a PIN is 4-digit long, which results in total 10^4 possible PINs), whereas a 9-point pattern has 389112 distinct patterns (Kaseorg 2013).

6. Limitations and Future Work

Our paper studied alphanumeric and graphical password schemes by comparing two screen lock methods in Android devices: PIN and pattern password. Screen lock protects Android phones and tablets from unauthorized access. Our study explored usability and security issues with two screen lock methods: PIN (alphanumeric password) and pattern (graphical password).

The purpose of the study on screen lock of mobile devices was to look into the usability and security issues through observing user behavior. Since user behavior has security implications on mobile devices, we examined user behavior for two different attacks on mobile devices: smudge attacks and shoulder surfing. Smudge attacks can be a threat for capacitive touch based smart phones and tablets. Our study focuses on comparison between two popular screen locks. Our study is limited to 33 participants and three usability criteria. We also limit our study to two attacks. In the future, we want to conduct a large-scale study with more usability criteria and attack schemes. Future studies will also be informed by lessons we have learned from the screen locking study.

7. Conclusions

In this paper, we compared the usability and security of pattern and PIN passwords for Android devices. We conducted a user survey on usability and security issues of pattern and PIN. We gathered data about creation time, login time, and login success rate of each of the methods in both tablet and phone. Our survey results show that 75% of participants prefer strong pattern screen locks, while 87% prefer strong PIN. We also collected user perception about secure screen locks and related attacks such as guessing attacks, smudge attacks and shoulder surfing attacks for each password scheme.

The pattern password for mobile devices is vulnerable to security attacks such as smudge attacks and shoulder surfing attacks. Further research is needed to address security issues with Android pattern locks. The users also need to create strong pattern passwords or PINs as well as make efforts to protect them.

References

Patrick, A.S., Long, A.C., Flinn, S. 2003. HCI and security systems. In *Proceedings of the CHI 2004*, 1056-1057, New York, NY: ACM Press.

Adams, A., and Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM* 42(12): 40-46.

Suo, X., Zhu, Y., and Owen, G.S. 2005. Graphical passwords: A survey. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, 463-472, Tucson, AZ: IEEE Press.

Kotadia, M. 2005. Microsoft: Write down your passwords. *ZDNet Australia, May*, 23.

Everitt, K.M., Bragin, T., Fogarty, J., and Kohno, T. 2009. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing System (CHI),* 889-898, Boston, MA: ACM Press.

Shepard, R.N. 1967. Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior* 6(1): 156-163.

Jakobsson, M., Shi, E., Golle, P., and Chow, R. 2009. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security, 9-9,* Montreal, Canada: USENIX Association.

Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., and Smith, J.M. 2010. Smudge attacks on smartphone touch screens. In *WOOT*, 10, 1-7, Berkeley, CA: USENIX Association.

Zakaria, N.H., Griffiths, D., Brostoff, S., & Yan, J. 2011. Shoulder surfing for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS),*1-12, Pittsburgh, PA: ACM Press.

Lashkari, A.H., Farmand, S., Zakaria, D., Bin, O., and Saleh, D. 2009. Shoulder surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security* 6(2): 145–154.

Chiang, H.-Y., and Chiasson, S. 2013. Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 251-260, Munich, Germany: ACM press.

Schaub, F., Walch, M., Könings, B., and Weber, M. 2013. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS),* 1-14, Newcastle, UK: ACM Press.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P.C., and Biddle, R. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM conference on Computer and communications security*, 500-511, Chicago, IL: ACM Press.

Tao, H., and Adams, C. 2008. Pass-go: A proposal to improve the usability of graphical passwords. *IJ Network Security* 7(2): 273-292.

Jermyn, I., Mayer, A.J., Monrose, F., Reiter, M.K., and Rubin, A.D. 1999. The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium*. 1-14, Washington D.C.: Usenix Security.

Chiasson, S., Forget, A., Biddle, R., and van Oorschot, P.C. 2008. Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction* Volume 1, 121-130, Liverpool, UK: ACM Press.

Chiasson, S., Stobert, E., Forget, A., Biddle, R., and Van Oorschot, P.C. 2012. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *Dependable and Secure Computing*, IEEE Transactions on 9(2): 222-235.

Bonneau, J., Herley, C., Van Oorschot, P.C., and Stajano, F. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceeding of Security and Privacy (SP)* IEEE Symposium on, 553-567, San Francisco, CA: IEEE Press.

Biddle, R., Chiasson, S., and Van Oorschot, P.C. 2012. Graphical passwords: Learning from the first twelve years. In *ACM Computing Surveys (CSUR)* 44(4): 1-41.

Kaseorg, A. 2013. How many combinations does Android 9 point unlock have?. In *Quora*. Retrieved February 25, 2015, from http://www.quora.com/How-many-combinations-does-Android-9-point-unlock-have.

Qualtrics: Online Survey Software & Insight Platform. 2014. Qualtrics [software]. Retrieved February 25, 2015, from http://www.qualtrics.com.

Passfaces Corp. 2009. The Science behind passfaces. White Paper http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf