A Survey of Password Schemes in Different Contexts
Sean Caldwell¹, Ye Zhu¹ and Huirong Fu²

ABSTRACT

We conduct user surveys to investigate user preferences on password schemes for mobile devices. By preforming face-to-face interviews with several individuals and testing several hypotheses, we were able to provide insight on end users and their views on where password schemes should be used. The investigation also indicates that users value access speed and minimal gestures over security and memorability. Through the surveys, we also find out users are not caring about shoulder-surfing attacks although the shoulder-surfing resistance is one of the major research topics on security. The surveys also show strong interest from users to protect individual applications with password schemes.

INTRODUCTION

Mobile telephony plays a large part of today’s society and its security has been a growing concern ever since its introduction into the public over two decades ago. With the introduction of data into mobile telephony services, these mobile telephone shave grown increasingly complex to a point where many of us use these devices on a daily basis. Although we may use these devices everyday, these devices often contain data that we may want to protect, so we use one of the many varieties of password schemes available on these devices. It has long been recognized that no silver bullet exists to achieve both security and memorability [7]. Some of the most common and well known password schemes include PIN, alphanumeric, fingerprint and pattern unlock. However, there are several more password schemes that have been developed in labs that haven’t seen any practical use that strive to achieve this silver bullet. In this paper, we attempted to figure out where users would find password schemes useful on their cellular phones and in which context.

The original proposal for the graphical password is the US patent filed by Blonder [4] in 1996. It was inferred that a graphical approach provides better memorability because the human brain is relatively weak at remembering sequences of numbers or letters, but excellent at processing visual data [4],[5]. Since then, several password schemes have been created including Pass points, Google Pattern Unlock, and Draw-A-Secret [5]. However, although there are several schemes that have been published in research papers such as [2] and [3], very few of these schemes have made it to market for use, so this paper intends to clarify why this may be so, and provide insight on end user input on password schemes to drive future business and research in the right direction.

¹S. Caldwell, Y. Zhu, College of Electrical and Computer Engineering, Cleveland State University, 2020 Euclid Avenue, Cleveland, OH 44115-2214
²Huirong Fu, School of Engineering and Computer Science, Oakland University, 318 Meadow Brook Rd, Rochester, MI 48309-4478
Maintaining a current market view is an important part of both maintaining business and producing worthwhile research. By performing our interviews as we did, these researchers and business workers will have a reference to use when exploring the topic of password schemes. By providing path to market exploration results, this will not only provide these two groups valuable focus points, but it will also point future research in the right direction when taking research to market. According to our knowledge, no other survey papers of password schemes on the topic of path to market exist.

WHAT IS A PASSWORD SCHEME

A password scheme is a method used to create a multitude of non-similar passwords to be used to secure information on electronic devices. These password schemes are a method of security that has been around since before electronics. However, with information at our fingertips, it is now easier than ever to break into these passwords and password schemes, whether digital or analog.

This multitude of passwords, known as a password space, are generated using a set of rules that define what a password can or cannot be. For example, a typical alphanumeric password could have rules such that the scheme requires at least 8 alphanumeric characters with at least one number and one special character. Common password schemes that have large password spaces can include PIN, alphanumeric and pattern unlock, which all have the possibility of generating over 1050 different passwords [2]. However, because these password types are so common, with the right information, an attacker could easily brute-force a password and access the device or information easily, as the rules behind these common password schemes are simple and widely known. In addition, these passwords are also prone to shoulder surfing, in which an attacker could look over someone’s shoulder or use a video feed and watch them enter their password. By shoulder surfing, the attacker will have access to whatever password someone has entered onto their device. There have been attempts to combat shoulder surfing, however, many of these either require hardware, were not memorable, or did little to improve security[2].

To combat this approach, newer password schemes are not limited to just words and numbers, such as pattern unlock and biometric password schemes, which is the market’s current focus. Some of these new schemes use graphical approaches, like the Window’s 8 phone authentication scheme, which extends the Pass points scheme [3]. Some schemes already have applicable marketing potential, such as Google’s pattern unlock, while others, such as the traditional alphanumeric, since so commonly used, are free to use.

EXPERIMENTAL DESIGN

The purpose of this paper is to evaluate what people value in password schemes such as PIN, alphanumeric, fingerprint, pattern unlock, and MAPS [2], and provide results and insight to these evaluations.
Interview Structure

Unlike a normal interview, our interviews were meant to gain insight on password schemes. Certain questions were asked that targeted how end users most commonly use password schemes and where they wanted to see it most. Some of the questions where generic, asking about how end users use their phone. Other questions where scale based, where 1 indicated “don’t care”, 2 indicated “nice to have”, and 3 indicated “must have”. Some of the questions included:

- Do you lock your phone?
  - Why/Why not?
  - What was the reason behind selecting that?
- Are you comfortable unlocking your phone in a crowded space?
  - Why?
- Are you comfortable entering your passwords in a crowded space?
  - Why?
- Are you comfortable unlocking your phone around people you’re close to?
  - Why?
- Are you comfortable entering your passwords around people you’re close to?
  - Why?

These questions were designed around asking important questions about password schemes in order to value the importance of different contexts such as usability as explored in [9], [10], [11], [12], shoulder surfing as explored in [8], and other topics covered in [2].

Choice of Subjects

Subjects for these interviews were chosen at random who were free to talk wherever we happened to interview them. Subjects had to be smartphone users with some technical knowledge of their smartphone. Most subjects indicated they either had a Samsung smartphone or an Apple iPhone. The locations in which these smartphone users were interviewed included Cleveland State University, Los Angeles International Airport, and various locations around Cleveland and Los Angeles. This mix ensured that interviews were not biased and that we would get an accurate view on the market. All subjects were above the age of 18, however the subject’s age range varied easily from 20 to 70 years old. Actual ages of the participants were rarely gathered unless freely given. All subjects were exposed to the same question set, however, questions that were asked may have gone deeper into detail or may have gotten skipped depending on the subject’s response.

Practical Details

By conducting the interview and asking these questions in-person, we are able to gather more data and better judge a person’s reaction because of facial expressions. When interviewing any given subject, we limited ourselves to 10 minutes to conduct the interview. This was to ensure that we did not annoy the interviewee, ensuring quality data. A web-based survey was not performed as these would not be as accurate and useful as in-person interviews, as highly recommended by [1].
Each interview was started off by introducing ourselves as researchers from Cleveland State University. Once we got introductions out of the way, we started asking questions in a way that would help the interviewee get into the mindset of being comfortable talking about password protection on their phones. Questions started off simple as to which phone they used and what password scheme(s) they use to lock their phone, and ended with questions that answered where passwords were wanted. The order of questions was very similar to the order of the questions provided in section 3.1.

DATA ANALYSIS

Although we explored more hypothesis beyond this paper, this paper focuses on the hypothesis tested with end users, which we classify into seven separate hypothesis, each of which were used as potential value proposition points while in the cohort. As the data is straightforward, it can be taken verbatim and does not require any additional analysis. To accompany each hypothesis, however, significant points brought up by the end users have been mentioned that correlate to and confirm a discard or accept decision. A discard decision was made if “don’t care” reached forty-five percent or above and “must have” was below thirty-five percent; an accept decision was made if “must have” interest was above thirty-five percent when combined with “nice to have” ending up with at least eighty percent interest. Finally, two other interesting statistics were gathered from various bank and cellular service associates that were observed and repeatedly confirmed.

Distribution of Data

![Distribution of interest for Hypothesis 1.](image)

HYPOTHESIS 1:
The first hypothesis was as follows: “End users do not feel comfortable to unlock smartphones in crowded spaces.” 50 percent of end users indicated that they did not care, 17 percent indicated that it was nice to have, 22 percent indicated that it was a must have, and 11 percent did not answer. End users, regardless of whether those around them are close or not, did not care about unlocking their phone around other people. Most will either tend to not unlock their phone to prevent people from seeing
sensitive information or are completely willing to unlock their phone in public simply because they have nothing to hide. Carrier stores such as Cricket, T-Mobile and Verizon confirmed this disinterest. This find may be important to papers such as [8].

HYPOTHESIS 2:
The second hypothesis was as follows: “End users do not feel comfortable to unlock smartphones while under video surveillance.” 50 percent of end users indicated that they did not care, 17 percent indicated that it was nice to have, 22 percent indicated that it was a must have, and 11 percent did not answer. End users, regardless of whether those around them are close or not, did not care about unlocking their phone while under video surveillance. Those who do lock their phone, but have nothing to hide see no point in hiding password entry from an attacker because they believe that the likelihood of their phone getting stolen is slim. They also believe that those behind the surveillance cameras are trustworthy.

HYPOTHESIS 3:
The third hypothesis was as follows: “End users do not feel comfortable to unlock near those they are close to such as family and friends.” 48 percent of end users indicated that they did not care, 33 percent indicated that it was nice to have, and 19 percent indicated that it was a must have. There was someone who expressed interest in hiding their password from those they are close to, so it was a hypothesis we tested
and invalidated during week 2 of the survey, thus the small number of samples. The assumption was that this would apply to female smartphone users, however this was quickly invalidated after several female smartphone users were interviewed for this purpose. Male smartphone users were also asked this question, however most of them, like the females, did not express interest in this value proposition, so it was quickly dropped and not tested further.

HYPOTHESIS 4:
The fourth hypothesis was as follows: “End users want to protect personalized information on apps such as news readers and shopping apps.” 50 percent of end users indicated that they did not care, 44 percent indicated that it was nice to have, and 11 percent indicated that it was a must have. It was expressed that most end users don’t care if others find out their shopping and reading interests. This may also explain why social media platforms such as Facebook and Twitter are so widely successful. As this hypothesis was clearly of no interest, it was discarded after the first week of the survey, which follows the ideas of the business model canvas as explained by [1].

![Figure 4. Distribution of interest for Hypothesis 4.](image)

![Figure 5. Distribution of interest for Hypothesis 5.](image)

HYPOTHESIS 5:
The fifth hypothesis was as follows: “End users want new or better password options for online services and apps.” 14 percent of end users indicated that they did not care, 57 percent indicated that it was nice to have, and 28 percent indicated that it was a
must have. End users expressed some interest to keep their online data that is already secure, more secure, however this interest was not high enough to be of any value to a business. However, this was one of the two deciding factors in switching our focus to app developers during the survey.

HYPOTHESIS 6:
The sixth hypothesis was as follows: “End users want new or better password options for online services and apps.” 11 percent of end users indicated that they did not care, 50 percent indicated that it was nice to have, and 39 percent indicated that it was a must have. End users expressed high interest in protecting the apps they use, especially those related with work and finances. This was the second of the two deciding factors in switching our focus to app developers during the survey.

HYPOTHESIS 7:
The seventh and final hypothesis was as follows: “End users want a more memorable way to authenticate themselves.” 25 percent of end users indicated that they did not care, 50 percent indicated that it was nice to have, and 25 percent indicated that it was a must have. Although there was an interest, password memorability is something that won’t likely be profitable as interest is not high enough. Although not collected as value points, some interviews with app developers later confirmed that memorability
is something that is “nice to have” but wouldn’t be profitable and recommended focusing on a scheme’s unlock speed instead. This find may be important to papers such as [13], [14] and [15].

Other Statistics

While interviewing carrier retail associates, we stumbled across interesting data points that may be useful in other contexts. It was found that depending on the company and size of the company, a tech representative of that company may have to help one out of every 20 customers deal with a forgotten password. This value is suited towards larger companies such as T-Mobile and Verizon, however this value can still be applied with smaller companies as a smaller value. It was also expressed by carriers that activations and new customers, especially through apple and Samsung products, are a carriers biggest source of revenue. Because of this, buying password schemes would likely not be of much interest to carriers, but may be of interest to cell phone manufacturers, which would help increase revenue of both manufacturers and carriers if the scheme was something that end users liked.

CONCLUSION

Unlike [6], a who used a psychology technique typically employed by researchers in the privacy sector, we decided to employ the techniques commonly used with the business model canvas as described in [1]. By doing so, we were able to gather valuable information that helped us find out where mobile device end users value security the most. By providing no financial incentives and being straightforward with our purpose, we were able to get a clear understanding of where password schemes have value in the market and were end users want to see these schemes the most.

One of the many things we wanted to test during the survey was to verify if users actually valued certain points brought up in [2] such as view on shoulder surfing. After several interviews and different approaches to the question, it was quickly ruled out that shoulder surfing resistance, was of no concern or value to mobile device end users. These results suggest that although shoulder surfing may occur, most users are not concerned with its occurrence since shoulder surfing’s usefulness is viewed as highly unlikely in the eyes of most users. It was also found that if a user is aware of shoulder surfing, most combat it simply by not using their device, often because of necessity of knowledge of the information on the device.

It was also made clear through several interviews that although full of shortcomings, people prefer traditional password schemes and fingerprint schemes. This shows that mobile end users value access speed and minimal gestures over security and memorability. This will be a valuable point to focus on in future research in an effort to find a way to easily and memorably secure our mobile devices and the data behind them.

Finally, from all of these interviews, mobile end users need a better way to protect their apps. Although many were not specific as to exactly which apps, mobile end users expressed clear interest in adding or bettering passwords schemes to apps that were online or were used for financial purposes.
REFERENCES

1. S. Blank and B. Dorf. 2012. “The Startup Owner’s Manual Vol. 1: The Step-by-Step Guide for Building a Great Company”, K and S Ranch Publishing.
2. J. Gurary, Y. Zhu, Ye, G. Corser, J. Oluoch, N. Alnahash, and H. Fu. 2015. “MAPS: A Multi-Dimensional Password Scheme for Mobile Authentication” 409-412.
3. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon. July 2005. “Passpoints: Design and Longitudinal Evaluation of a Graphical Password System”, Int. Journal of Human-Computer Studies. 63(1-2): 102–127.
4. G. Blonder. “Graphical Password”, (Sep 1996), Patent 5,559,961.
5. I. Jermyn, A.. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin. 1991. “The Design and Analysis of Graphical Passwords.” Proceedings of the 8th Conference on USENIX Security Symposium, Volume 8. SSYM’99, Berkeley, CA, USA, USENIX Association. 1–1.
6. G. Danezis, S Lewis and R. Anderson. 2005. “How Much is Location Privacy Worth?”, In Proceedings of the Workshop on the Economics of Information Security Series, WEIS.
7. C. Herley, P. Van Oorschot. Jan 2012. “A Research Agenda Acknowledging the Persistence of Passwords”, Security Privacy, IEEE 10(1):28–36.
8. N.H. Zakaria, D. Griffiths, S. Brostoff, J. Yan. 2011. “Shoulder Surfing Defense for Recall-Based Graphical Passwords”, Proceedings of the Seventh Symposium on Usable Privacy and Security. SOUPS ’11, New York, NY, USA, ACM, 6:1–6:12.
9. A. Eljetlawi, N. Ithnin. Nov 2008. “Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods”, Third International Conference on Convergence and Hybrid Information Technology, Volume 2. 1137–1143.
10. M. Hafiz, A. Abdullah, N. Ithnin, H. Mamm. May 2008. “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”, Second Asia International Conference on Modeling Simulation, 396–403.
11. E. Stobert, R. Biddle. 2013. “Memory Retrieval and Graphical Passwords”, Proceedings of the Ninth Symposium on Usable Privacy and Security. SOUPS ’13, New York, NY, USA, ACM 15:1–15:14.
12. R. Biddle, S. Chiasson, P. Van Oorschot. Sep 2012. “Graphical Passwords: Learning From the First Twelve Years”, ACM Comput. Surv. 44(4):19:1–19:41.
13. J.G. Raaijmakers, R.M. Shiffrin. 1992. “Models for Recall and Recognition”, Annual Review of Psychology 43: 205–234.
14. A.L. Titcomb, V.F. Reyna, F. Dempster, C. Brainerd. 1995. “Memory Interference and Misinformation Effects”. Interference and Inhibition in Cognition263–294.
15. M. Defetyer, R. Russo, P. McPartlin. 2009. “The Picture Superiority Effect in Recognition Memory: A Developmental Study using the Response Signal Procedure”, Cognitive Development 24(1): 265–273.