Baseline Measurements of Shoulder Surfing Analysis and Comparability for Smartphone Unlock Authentication

John T. Davin
United States Naval Academy
Annapolis, MD 21402, USA
m171368@usna.edu

Adam J. Aviv
United States Naval Academy
Annapolis, MD 21402, USA
aviv@usna.edu

Flynn Wolf
University of Maryland, Baltimore
County
Baltimore, MD 21250, USA
flynn.wolf@umbc.edu

Ravi Kuber
University of Maryland, Baltimore
County
Baltimore, MD 21250, USA
rkuber@umbc.edu

CHI'17 Extended Abstracts, May 06-11, 2017, Denver, CO, USA
ACM 978-1-4503-4656-6/17/05.
http://dx.doi.org/10.1145/3027063.3053221

Abstract

In this paper, we describe a novel approach to measure the susceptibility of smartphone unlock authentication to shoulder surfing attacks. In our methodology, participants play the role of attackers, viewing video-recorded footage of PIN and graphical password pattern authentication input with various camera angles, hand positions, phone sizes, and authentication length and strength. Based on the data collected and recording methodology developed, we aim to provide insight into the factors of mobile unlock authentication which best and least resist shoulder surfing attacks and examine scenarios where weaknesses may occur. The goal is to identify more effective guidance for mobile device users to avoid observational attacks. We also aim to advance the methodologies used to measure the shoulder surfing attack surfaces where baselines of comparisons to preexisting systems (e.g., PINs and patterns) are not standardized. Utilizing the methodology and recordings, other researchers may build upon this approach to analyze future systems and replicate our results.

Author Keywords

Shoulder surfing; mobile security; password security; usable security; graphical passwords; PIN passwords; mobile authentication.

ACM Classification Keywords

H.5.m. [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; K.6.5. [Management of Computing and Information Systems]: Security and Protection

Introduction

Personal and sensitive data is often stored on mobile devices, making these technologies an attractive target for attackers. This has resulted in a heightened focus on the vulnerabilities of mobile unlock authentication, and the susceptibility of these authentication methods to shoulder surfing attacks, or when an attacker directly observes a user authenticating entry in order to acquire a password or other sensitive information from the mobile device [8, 14]. One of the most cited dangers for smartphone unlocking mechanisms are shoulder surfing attacks [10].

Many users utilize biometric authentication as a supplement to the dominant PIN and graphical (stroke-based) pattern password entry mechanisms. However, one study showed that nearly 70% of respondents reported that they utilize either a PIN or Android graphical pattern as their mobile authentication mechanism [6]. While biometrics and other forms of authentication are present, these mechanisms still require a pattern or PIN to utilize the device. Thus, PIN and pattern mechanisms still exist even in the realm of biometrics and, given the opportunity, an attacker will attack the PIN or pattern- not the biometric authentication. Biometrics are also unlikely to ever stand alone as an authentication mechanism due to the concerns of reliability, privacy, security, and ease of use of other technologies [14].

There is much related work that both proposes and studies shoulder surfing resistant authentication mechanisms [6, 7, 10, 5, 9]. We believe our research will further this prior work in providing avenues for new methodologies to test resilience to shoulder surfing attacks compared to conventional PINs or patterns, as a baseline measure. Similar work has utilized cameras to recreate the pattern authentication based on oily residues, or smudges, left on the screen after the user successfully authenticated [3]. Closer to the work we are performing, von Zezschwitz et al. measured the susceptibility of Android's graphical passwords to observation attacks by utilizing simulated observations focusing only on a single dimension, the visibility of the line [13]. These authentications were simulated and single dimensional, while we include multiple dimensions that compare different authentication types and multiple camera angles. Other areas examined include device size, hand position, length of authentication sequence, among others.

Obtaining a user's PIN or pattern may not be very difficult and may not limit an attacker solely to the data stored on the mobile device [5]. In one study, half of the users admitted to choosing PINs based off PINs that they used elsewhere (e.g. bank PINs or physical locks) [6], meaning that a third party may be able to enter multiple systems without the user's knowledge. With regard to difficulty and password strength, graphical passwords suggest trends with respect to easily guessed and non-complex passwords [1, 12]. These studies confirm the need for multidimensional research in the realm of PIN and pattern vulnerability analysis as users suffering from shoulder surfing attacks are exposing themselves to greater risk than the content of their mobile device.

This method of shoulder surfing vulnerability analysis provides a baseline for researchers to utilize. Whether to confirm prior work in the realm of shoulder surfing analysis or to test and compare new mobile authentication systems, this multifaceted approach has the potential to create a standard capable of being replicated.

Name	Phone Type	Dimensions
Red	Nexus 5x	5.427" x 2.723"
Black	OnePlus One	6.02" x 2.99"

Table 1: Phones used in experiments, and their short hands, *Red* or *Black*

Name	Hand Position
Thumb	One handed
Index Finger	Two handed

Table 2: Phone holding configurations used

Authentication	Description
PIN	Numeric PIN entry
Pattern	Android pattern with visible lines
No Lines	Android pattern *without* visible lines

Table 3: Authentication methods being studied

Camera Angle	Description
Near Left	Over target's left shoulder at a height of 5'
Near Right	Over target's rigth shoulder at a height of 5'
Far Left	Over target's left shoulder at a height of 6'
Far Right	Over target's right shoulder at a height of 6'
Top	Over target's head at a height of 6'

Table 4: Camera Locations

Methodology

A within subjects study was designed where participants would be exposed to video footage of researchers entering authentication sequences on a mobile device. Participants would be asked to view the footage and recreate entry, to determine the susceptibility of the authentication sequence to observational attacks.

We recorded over 600 videos simulating shoulder surfing in a controlled lab space with the aim to better understand the vulnerabilities of conventional mobile unlocking mechanisms and to study the impact both the user and the environment has upon the attack. These videos, which take into account hand position, phone size, authentication type, and differing camera angles, have been compiled into a web-based survey that will collect data (e.g. success rates, respondent's biographical information) about the susceptibility to shoulder surfing. We expect to recruit over 1000 responses online via Amazon Mechanical Turk and roughly 100 in person respondents. The in-person surveys will provide a control to compare against the online responses and ensure these respondents are providing true responses in an uncontrolled setting.

Research Objectives

In examining the videos of simulated shoulder surfing attacks and the data collected from the survey, we hope to solidify our understanding of the vulnerabilities features of PINs and patterns have to observation attacks. These conclusions will not only help identify what type of PINs and patterns are more susceptible to shoulder surfing attacks but also identify environmental factors, user actions, and password features (e.g. length, left-vs-right shifting, etc.) that directly increase or reduce the likelihood of a successful attack. These recordings are also unique in that they will provide a public corpus of shoulder surfing attacks.

Treatments	Views	Attempts
A	One	One
B	One	Two
C	Two	One
D	Two (different angles)	One
E	Two (different angles)	Two

Table 5: Five different treatments for each authentication

4-Length PINs	Properties	6-Length PINs	Properties
1328	Up Shift	153525	Up Shift
1955	Neutral	159428	Neutral Cross
5962	Right Shift	366792	Right Shift
6702	Down Shift	441791	Left Shift
7272	Knight	458090	Down Shift Cross

4-Length Patterns	Properties	6-Length Patterns	Properties
0145	Up Shift	014673	Neutral Cross
1346	Left Shift	136785	Down Shift
3157	Neutral	642580	Left Cross
4572	Right Knight/Cross	743521	Up Shift Non-Adjacent
6745	Down Shift	841257	Right Shift

Table 6: Ten PIN and Pattern passwords being studied and the properties each one highlights

Recordings

The videos are designed to simulate shoulder surfing settings under varied attack conditions. Camera angles have been selected to mimic the locations where observational attacks may take place from. Tables 1, 2, and 3 show the independent variables randomly assigned to participants. These are kept throughout the survey. Tables 4-6 show dependent variables that change with each authentication attempt in the survey. Selection of these variables are discussed in later subsections. Every respondent will attack all 10 passwords of either PIN or Pattern while given a random treatment at load time for each attack - shown in Table 5.

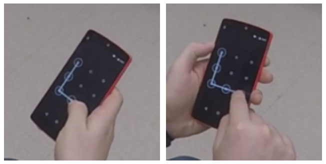


Figure 1: (*left*) Thumb hand position vs. (*right*) Index Finger hand position

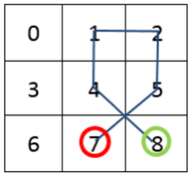


Figure 2: Converting graphical password to a numerical representation

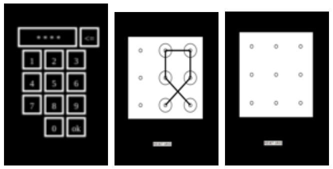


Figure 3: (*left*) PIN, (*center*) pattern, and (*right*) pattern with no-lines authentication entries

Hand Position

Referenced in Table 2, hand position is an important factor included in our survey. Based on the reviewing the videos, we hypothesize that videos with a user authenticating with one hand, using their thumb only, will be more difficult to shoulder surf than a user utilizing two hands, one hand to hold the phone and the index finger of the other to authenticate. We came to this projected conclusion based on the partial screen obstruction the one handed user has to shoulder surfers attacking from a side angle. Figure 1 demonstrates the subtle differences based on hand position.

Phone Size

Similar to the way a user authenticates, the choices users make in regard to phone size may also have an impact on a shoulder surfer's ability to successfully attack an authentication. We hope to answer whether larger screens significantly increase the vulnerability of a given authentication mechanism. Referenced in Table 1, the larger phone, the black OnePlus One (6.02 x 2.99 in), is comparable in size to more popular phones like the iPhone 6s Plus. The smaller phone, the red Nexus 5x (5.427 x 2.723 in), is comparable in size to the iPhone 6s.

Password Selection

There are ten PIN passwords and ten pattern passwords, described in Table 6, that are the subject of the study. These passwords were selected from real world data. The passwords each contain distinct properties that have been modeled in both the PINs and the patterns and form a representative, albeit a small, sample of real world passwords. The properties that these passwords encompass are described in Table 6 to the right of each password. As we are concerned with observational attacks, these properties are visual in nature, e.g, left shifted, right shifted, containing non-adjacency contact points, crosses, and repetitions. These features have also been identified and studied in prior work [1, 2]. An example of a PIN that features repetition in our data set is the PIN 7272. An example of a pattern that features a cross is pattern 841257. Patterns can be represented with numbers when the dots are replaced with numbers. Figure 2 demonstrates how to draw pattern 841257 given in the form of numbers, starting with the green 8 and ending with the red 7. These properties will help answer the research question whether or not certain PINs or patterns are more vulnerable to shoulder surfing solely on their placement and order on the screen. Figure 3 shows the different authentication screens the respondent could see in a video.

Angles

The camera setup is an integral part of design. It is important to ensure angles on the left and right accurately mirror each other in distance to the screen and orientation. Figure 4 on the following page shows the setup. The two lower GoPros are 5' high and 2.5' apart, angled inward at 45 degrees. The actor sits in the center of that, holding the phone 3' high. The two outer second tier of cameras stands directly 1' above the lower ones. The fifth camera, directly overhead, is at the same height as the two higher ones centered between them. Over 600 videos were recorded at this site, over a three day period. As displayed in Table 4, the videos were recorded from five angles: far left, far right, near left, near right, and top. Previous work has only touched on three of these angles and allowed the participants to choose the password [11]. Of the numerous research questions we hope to answer, these angles will answer the environmental question whether or not there is an optimal angle for shoulder surfing. Screen shots of these angles are shown in Figure 5.

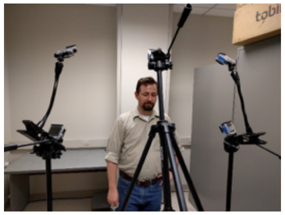


Figure 4: GoPro Camera Array: lower cameras are *near*, higher cameras are *far*, and the middle camera is *top*

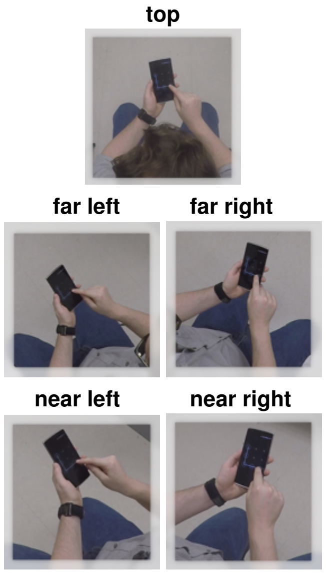


Figure 5: Camera Views

Realism and Limitations

In accounting for and analyzing all the variables described above, there were some limitations and unintended variables that we did not account for. Examples include the environmental and situational considerations which have been used to evaluate mobile interfaces [4]. Glare was not addressed because it makes the simulations more realistic given that shoulder surfers cannot control glare on the victim's screen. We also did not include text-based passwords because of their limited use for mobile authentication in the wild and difficulty selecting similar strength passwords compared to PIN and pattern.

Website and Database

The survey is all tied together within a website and back-end database. When a respondent accesses the main page, they are prompted for an authentication code to continue on to the IRB consent, training, and then the survey. For in-person survey administering, the authentication codes will be assigned randomly as the volunteers enter the lab room for the survey. For online respondents, authentication codes will be generated when the volunteer accepts the terms via Amazon Mechanical Turk.

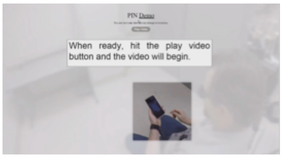
Upon entering the authentication code, the respondent has to read and consent to the USNA IRB statement. This statement makes the respondent aware of their rights as an individual taking the survey and ensures that their data and any identifiable information about them is safeguarded and not made public.

Survey – Initialization

Initializing the survey and ensuring the respondent is following instructions is an important aspect to maintaining accurate data collection. Once the respondent starts the survey, they are randomly assigned three variables that remain constant for the entire survey – Phone (Table 1), Handedness (Table 2), and Authentication Type (Table 3). In order to ensure the respondent is following the instruction disallowing the use of mobile devices or tablets to take the survey, the survey at this stage tests for those conditions and does not allow them to proceed if they are not abiding. Similarly, we request that the respondent maximize their screen. To make sure this is taking place, we record the resolution of their screen. If the resolution is too small, we will omit the data from the set. We also ask the respondent to report their sex, age, eye sight, and skill level with modern smart phone technologies. The eye sight question has four options: normal, corrected with glasses/contacts, deficient and not corrected, and not sure. The skill level question gives the options: none, below average, average, above average, and professional. This information not only helps us in screening accurate data but also may provide insight into the characteristics of users, which appear more susceptible to observational attacks.

Survey – Training

After accepting the terms and conditions of the IRB consent page and entering the biographical information, the respondent goes through a video step-by-step tutorial. This tutorial video can be replayed as many times as the respondent needs. Figure 6 shows a part of the tutorial video. Following the tutorial video, the respondent is given an interactive tutorial in which they shoulder surf a simple authentication (e.g. 1234 for a PIN) and they are sent to a recreation page in which they are expected to enter the password, the same task they perform ten times throughout the survey. Figure 7 shows the recreation page for a respondent tasked with PINs. All respondents with the same authentication type receive the same training, thus creating a baseline.



When ready, hit the play video button and the video will begin.

Figure 6: Tutorial page

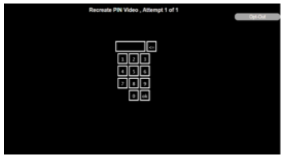
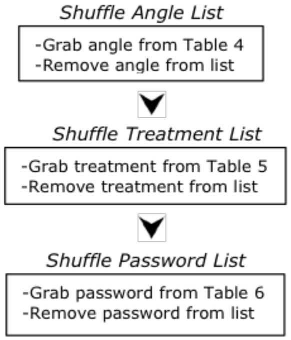


Figure 7: Recreation page


Shuffle Angle List

-Grab angle from Table 4
-Remove angle from list

Shuffle Treatment List

-Grab treatment from Table 5
-Remove treatment from list

Shuffle Password List

-Grab password from Table 6
-Remove password from list

Figure 8: Individual Shoulder Surfing Page Randomization Flow Chart

Survey – Randomization

Effectively randomizing the order and the type of videos is crucial to not avoid introducing bias or negatively impacting the data collection. Even with the best randomization functions, some videos would most likely be underrepresented in our data collection at the end trials. When the respondent finishes training and begins the survey of the ten authentications, the website knows the respondent's assigned phone (red Nexus 5x or black OnePlus One), finger (index or thumb), and authentication type (PIN, pattern with lines, pattern without lines). To ensure we collect all the data we need, we utilized a shuffle function on three lists to grab the password, angle, and treatment for each trial. Figure 8 shows a flow chart of how the randomization operates. Since the respondent shoulder surfs ten passwords, the list of treatments (five treatment options - shown above in Table 5) is doubled upon initialization to match the number of passwords being attacked. Since each participant will attack ten different passwords and there are only five treatments, this explains why each person taking the survey will encounter each treatment twice throughout the survey.

Preliminary/Prototype Results

We have run a prototype of the survey and have collected data from a group of 12 participants. While there is insufficient data to draw statistically significant conclusions, we found that a successful attack rate on the first attempt for PINs is 45.8%, followed by Pattern without lines at 87.5% and Pattern with lines at 95.8%. We hypothesize similar distributions will persist when the study is expanded to include both in-lab and online participants. Further work would need to be conducted to determine if camera angle or password shape will have an impact on attack rate.

Summary

This research aims to accurately measure the resilience conventional smartphone unlock authentications have to everyday shoulder surfing attacks. Through a survey that utilizes participants as attackers, we aim to identify weaknesses caused by the authentication, the environment, and the user in an effort to mitigate vulnerabilities. The intended contributions of this research include:

- Advance the methodology of shoulder surfing vulnerability analysis.
- Create a baseline for shoulder surfing analysis that is easily capable of recreation by other researchers.
- Test new authentication mechanisms by comparing results in similarly conducted studies against the conventional authentication mechanisms analyzed in this research.

The authentication videos will support other researchers when developing methodologies, providing a baseline comparison point for newly proposed systems that address shoulder surfing and other observation attacks.

While this document does not report extensive results, the survey has been prototyped and data collection is ongoing. We expect to present more results as part of the presentation at the conference.

References

[1] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC*

2015). ACM, New York, NY, USA, 301–310. DOI: http://dx.doi.org/10.1145/2818000.2818014

[2] Adam J. Aviv and Dane Fichter. 2014. Understanding Visual Perceptions of Usability and Security of Android's Graphical Password Pattern. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)*. ACM, New York, NY, USA, 286–295. DOI: http://dx.doi.org/10.1145/2664243.2664253

[3] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens.. In *Proceedings of the 2010 Workshop on Offensive Technology (WOOT'10)*. 1–7.

[4] Leon Barnard, Ji Soo Yi, Julie A Jacko, and Andrew Sears. 2005. An empirical comparison of use-in-motion evaluation scenarios for mobile computing devices. *International Journal of Human-Computer Studies* 62, 4 (2005), 487–520.

[5] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 987–996. DOI: http://dx.doi.org/10.1145/2207676.2208544

[6] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 750–761. DOI: http://dx.doi.org/10.1145/2660267.2660273

[7] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1107–1110. DOI: http://dx.doi.org/10.1145/1753326.1753491

[8] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. 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)*. ACM, New York, NY, USA, 4806–4817. DOI: http://dx.doi.org/10.1145/2858036.2858267

[9] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 13–19. DOI: http://dx.doi.org/10.1145/1280680.1280683

[10] Shushuang Man, Dawei Hong, and Manton M Matthews. 2003. A Shoulder-Surfing Resistant Graphical Password Scheme-WIW. (2003).

[11] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, New York, NY, USA, Article 13, 10 pages. DOI: http://dx.doi.org/10.1145/2406367.2406384

[12] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security (CCS '13)*. ACM, New York, NY, USA, 161–172. DOI: http://dx.doi.org/10.1145/2508859.2516700

[13] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2339–2342. DOI: http://dx.doi.org/10.1145/2702123.2702202

[14] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and Evaluation of a Shoulder-surfing Resistant Graphical Password Scheme. In *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '06)*. ACM, New York, NY, USA, 177–184. DOI: http://dx.doi.org/10.1145/1133265.1133303