Squeezing Your Privacy Away: Privacy Analysis of Squeeze Authentication

Alexandru Bara
abara@uwaterloo.ca
University of Waterloo
Waterloo, Ontario, Canada

ABSTRACT

There are many different types of authentication and each has a degree of privacy and safety. Squeeze authentication is a new way of authentication that works by squeezing a smartphone in a user pre-defined pattern that is based on pressure, duration and number of fingers[5]. The authors claim that squeeze authentication has a strong privacy guarantees and is hard to shoulder-surf. It This paper aims to re-evaluate the privacy provided by squeeze authentication by doing 3 user studies. In the first user study, I show that using a simple squeeze password is easy to break with a shoulder-surfing attack. In the second user study, I show that more complex squeeze passwords are also vulnerable to shoulder-surfing attacks as long as the attacker has access to a video of the victim inputting their password. In the last user study, I show that there is a strong correlation between dominant hand of the user and the hand used for squeeze authentication as well as show a small correlation between the sex of the user and the pressure used for squeeze authentication.

CCS CONCEPTS

• **Security and privacy** → *private authentication.*

KEYWORDS

Authentication, Privacy

ACM Reference Format:
Alexandru Bara. 2023. Squeezing Your Privacy Away: Privacy Analysis of Squeeze Authentication . In *Proceedings of Project Report (Adv. Tpcs 23')*. ACM, New York, NY, USA, 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

As we move to a digital world, more user data can be found online. Each user has data that is specific to them and some users do not like when companies use their data without their consent. One way to protect a user's data is to use an authentication scheme. A piece of data would be securely stored and can only be accessed by a user that is authenticated. It is crucial to have a strong authentication scheme that is hard to break to keep private data away from malicious users.

There are multiple authentication techniques and each has its pros and cons. Knowledge-based authentication relies on a code that a user needs to memorize. Examples of knowledge-based authentication are passwords, pins, and patterns. This type of authentication are widely used in industry and does not expose any private information about the user. That means there is no user-specific attribute that is used for authentication. Knowledge-based authentication can also be changed by the user whenever they want. However, knowledge-based authenticators are susceptible to shoulder surfing attacks since the code that a user inputs can be reproduce by anyone if they know the code.

There is another type of authenticator that is called biometric authenticator and they rely on the unique biological traits of users. Some examples of biometric authenticators include face, fingerprint and iris. Unlike knowledge-based authentication, a malicious attacker cannot do a shoulder-surfing attack on biometric authenticators as they are unique to the user and cannot be reproduced by attackers. However, having a unique password that cannot be changed has privacy concerns. The password is part of who the user is and if an attacker gets access to that information, the attacker can learn unmodifiable information about the user like their face, iris print or fingerprint.

Yi et al. [5] introduce squeez'in, a squeeze authentication scheme that claims to provide the privacy properties of knowledge-based authentication and protect from shoulder surfing like the biometric authenticators. A squeeze password consists of several squeezes of the user's device in a pattern chosen by the user. The user can always change the password by inputting a new squeeze sequence. The authors claim that squeeze authentication doesn't have any privacy concerns and the squeeze password cannot be shoulder surfed.

However, the claims made by Yi et al. [5] have not been properly evaluated. This paper aims to revisit the security of squeeze authentication by executing a shoulder attack on the system and showcasing what privacy leaks are possible with this authenticator. The three research questions that I am trying to answer are the following.

RQ1: Are simple squeeze passwords easy to break with a shoulder surfing attack? To test this claim, I did a study where a simple squeeze password was chosen and inputted in the presence of an attacker. The attacker only saw the password once and had to guess the parameters the password was using.

RQ2: Can attackers break a complex squeeze password from any angle given a video of the user inputting their password? To test this claim, I did a study where I took a video from four angles of a user inputting their complicated password. Four attackers were chosen and each one was given a video of one angle and they had to guess the parameters of the password.

Adv. Tpcs 23', December 2023, Waterloo, ON, Canada

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/XXXXXXX.XXXXXXX

RQ3: What private user information is being exposed by a squeeze authenticator and how can an attacker use this information? This claim was tested by doing a user study and trying to find correlations between users and the parameters of their squeeze password.

My contributions are as follows.

- I evaluate the efficacy of shoulder surfing attacks on squeeze authenticators.
- I evaluate the claims that a squeeze authenticator does not divulge any private data by trying to correlate touch intensity with the sex of the user and to correlate the number of fingers on each side of the device with the user's dominant hand.
- I provide actionable steps forward to make the squeeze authenticator safer and more private.

2 BACKGROUND

Authentication is a way to protect a user's private data which makes it a pivotal part of security. There is constant research towards creating new authenticators and research towards breaking current authenticators. This paper will focus on a new type of authentication called squeeze authentication and the security and privacy it provides.

2.1 Squeeze Authentication

Squeeze authentication is a new form of authentication introduced by Yi et al. [5] with their system called squeez'in. It works on a smartphone and the first step is a registration phase where the user squeezes the phone with what their definition of low and high pressure. The squeeze must be done on the screen of the phone and once squeez'in has a user profile of the squeeze pressure (unique to each user), it will ask a user to register their squeeze password. The squeeze password has four parameters which are the code length, touch pressure, number of fingers, and touch duration. The code length is the number of squeezes and it is between four and seven. The touch pressure can have two values of low intensity, and high intensity. The number of fingers is between two and four. The touch duration also has two values: short and long. The touch pressure, number of fingers and touch duration are attributes that are specific to each squeeze.

2.2 Shoulder Surfing Attacks

Shoulder surfing attacks have been around for a long time and new authentication schemes need to consider it in their design. There is a lot of research on breaking authentication schemes with shoulder surfing attacks. Khan et al. [2] evaluate shoulder surfing attacks on touch-sensitive pins which are PINS that take into consideration the PIN and the touch intensity when a user presses each number. Khan et al. showcased that touch-sensitive PINS are still prone to shoulder surfing since an attacker can guess the touch intensity by looking at the target's hand movement and gestures. Von Zezschwitz et al. [4] demonstrate the importance of pattern length, number of intersections and number of overlaps when evaluating shoulder surfing attacks on PIN authentication. A low pattern length is more susceptible to shoulder surfing attacks.

2.3 Threat Model

There are two types of attackers that will be considered. The first attacker is a knowledgeable and spontaneous attacker. This attacker knows how squeeze authentication works as well as the parameters it uses. However, the attacker does not plan an attack in advance which means he does not have any other tools to help him. So he can do a shoulder surfing attack but he cannot record the victim input their squeeze password. This is the attacker that will be used for study 1. The second attacker is a knowledgeable and planned. He knows how squeeze authentication works as well as the parameters it tracks. The attacker can also record a victim while they are inputting their squeeze password. This is the attacker that is used for study 2.

3 STUDY 1: BREAKING SQUEEZE AUTHENTICATION

In this section, I evaluate the ease of breaking into a smartphone that is protected with squeeze authentication.

3.1 Experiment Design

The first step in trying to break into squeeze authentication is to get the running implementation of a squeeze authenticator. I have contacted the authors of squeez'in [5] to get access to their squeeze authenticator but I got no response from them. I then tried to create my own squeeze authenticator but I ran into a major step back. For this experiment, I have used a Google Pixel 3a and I have coded a way to track when a user presses on the screen, how many fingers the user is using and the time-pressed. However, I ran into an issue when trying to get this information towards the edge of the device. Android devices have accidental touch rejection which is useful in most cases but a detriment when it comes to squeezing authentication. Smartphones have a capacitive image which captures all inputs on the screen [1]. Android however does not expose this raw information to the user. The Android kernel gets rid of accidental inputs and exposes only what it considers to be valid. Touches around the edge of the device are considered by the kernel to be accidental and it does not provide this information at the application layer. To get past this hurdle, I would have to override the kernel which I have decided to pursue in the full paper.

For this study, I have decided to take the approach of simulating a squeeze password and having a random participant try to guess the password attributes that I have used for the simulation. Squeez'in [5] shows a sample of registration for their authenticator so I have decided to use those attributes for my study. The first attribute was the code length which was of size four. The number of fingers used was consistent for the code length and it was three. The first and last squeezes had high touch pressure with high duration. The second and third squeezes had low touch pressure and low duration.

3.2 Procedure

I chose a participant for this study to try and guess the password chosen in the previous section. This participant is not aware of squeeze authentication and is not an expert in the domain of computer science. I went into an isolated room with the participant. I explained to the participant how squeeze authentication works and the 4 parameters that are being tracked as well as the possible

Squeeze nb.	Parameters	Password	Guessed
1^{st}	duration	Long	Long
	nb. of fingers	3	3
	pressure	High	High
2^{nd}	duration	Short	Short
	nb. of fingers	3	3
	pressure	Low	Low
3^{rd}	duration	Short	Short
	nb. of fingers	3	3
	pressure	Low	Low
4^{th}	duration	Long	Long
	nb. of fingers	3	3
	pressure	High	High

Table 1: Shoulder surfing attack on squeeze authentication

values for these parameters. I then held the smartphone in my right hand and told the participant to overlook my shoulder when I input my squeeze password. I proceeded to input the chosen squeeze password once and then put the phone away. The participant was asked the following questions. What do you think the length of the password is? Based on that answer, for each of the squeeze, the participant was asked what they think the duration, number of fingers and pressure used is. The actual parameters used and the parameters the participant guessed can be found in table 1. The participant was then asked about their experience trying to decode the password.

3.3 Discussion

From the results in table 1, we can see that the participant was able to guess all parameters. The participant only knew what parameters were being tracked in squeeze authentication and got one opportunity to look at the password. The participant also had no experience with squeeze authentication or breaking passwords. These results showcase the vulnerability of squeeze authentication. A malicious actor that is armed with the knowledge of squeeze authentication parameters and can see a user input their password will be able to crack the user's password. **These results show that the answer for RQ1 is yes, an attacker can use shoulder-surfing attacks on simple squeeze passwords.**

The participant was asked about their experience with guessing the squeeze password, here is what they said. The password was easy to guess based on the hand movement. It was easy to tell if a user was squeezing the phone with high pressure or with low pressure. The duration of the squeeze was harder to guess but they felt a harder squeeze was correlated with a longer squeeze duration.

4 STUDY 2: BREAKING SQUEEZE AUTHENTICATION FROM ALL ANGLES

In this section, I evaluate the feasibility of breaking into a smartphone by looking at a user input their password from any angle.

4.1 Experiment Design

In the previous section, the participant was looking over the shoulder of the user when they were inputting their password. For this experiment, I want to see if an attack can be extended to all angles an attacker can view the victim input their password. A more complex password will be used to determine if that affects the ability of an attacker to guess the password. The target of this attack will be asked to input the following squeeze password. The password will consist of seven squeezes and the parameter of each squeeze can be found in table 2.

For this experiment, a video is taken from four angles. The first angle is from behind the shoulder of the target and it is meant to simulate a shoulder surfing attack. The second angle is from the left of the target and the attacker will be able to see the fingers on the side of the device. The third angle is from the right of the target and is meant to have an obstructed view of the phone. The fourth angle will be from the front of the victim and the attacker will only see the back of the hand.

4.2 Procedure

A random participant was chosen to be the target of the attack. I explained to the participant the main concepts of squeeze authentication and asked them to get comfortable with squeezing patterns on the smartphone. I then explained the different parameters that are being tracked and the different options for each parameter. I proceeded to tell the participant the password they had to input for this test. The participant was given 5 minutes to familiarize themselves with the password and input it. Once the participant was comfortable, videos were taken of them inputting the password from the four angles previously mentioned.

Four random participants were chosen to be attackers for this experiment. The participants were explained how squeeze authentication works The parameters that squeeze authentication tracks were explained as well as the potential value for each parameter. Each participant was then interviewed separately where they were shown only one of the angles of the target inputting their squeeze password. They had to look at the video as guess what the parameters were used for the password. The participants also recorded how many times they replayed the video in order to make their guess. The results can be found in table 2.

4.3 Discussion

This section will analyse the results found in table 2 as well as the experience of the participants in the study.

Experience of the victim: The participant that learn the squeeze password and input it had this to say about their experience. The password that was provided was very hard to learn and they found it was annoying to learn. There is too much variation and they felt like their hand would cramp from constantly switching the number of fingers. The password was also long to input which made it unusable and they would not use a complicated squeeze password if they had the choice. The learning rate for the complicated password was also low and it took the participant upwards of 10 minutes before they got comfortable inputting the password. There were also concerns about breaking the phone from squeezing it too hard which led to discomfort while using it.

Squeeze nb.	Parameters	Password	Guessed back angle	Guessed Left angle	Guessed Right angle	Guessed Front angle
1^{st}	duration	Long	Long	Long	Long	Long
	nb. of fingers	2	2	2	2	2
	pressure	Low	Low	High	High	Low
2^{nd}	duration	Short	Short	Short	Short	Short
	nb. of fingers	3	3	3	3	3
	pressure	High	High	High	High	High
3^{rd}	duration	Short	Short	Short	Short	Short
	nb. of fingers	4	4	4	3	4
	pressure	Low	Low	Low	Low	Low
4^{th}	duration	Short	Short	Short	Short	Short
	nb. of fingers	4	4	4	3	4
	pressure	High	High	High	Low	High
5^{th}	duration	Long	Long	Long	Long	Long
	nb. of fingers	2	2	2	4	3
	pressure	High	High	High	High	High
6^{th}	duration	Long	Long	Long	Short	Long
	nb. of fingers	3	3	3	4	3
	pressure	High	High	High	High	High
7^{th}	duration	Short	Short	Short	Short	Short
	nb. of fingers	2	2	2	4	3
	pressure	High	High	Low	Low	High

Table 2: Breaking squeeze authentication from four angles

Front angle attack: The participant who was given the front angle of the squeeze password was able to guess it in four tries. The participant was able to guess all parameters except the number of fingers in the fifth squeeze. This means that 21/22 parameters were guessed for a 95% accuracy. The participant said that the parameters were easy to guess when they had the ability to rewatch the videos. The number of fingers was hard to guess because of the angle of the video. The back of the hand was blocking most of the view and the participant had to rely on the number of fingers not touching the device to guess the number of fingers used for squeezing. The pressure was easy to guess by looking at the hand movement, and how much the hand shook during the squeeze and the finger movement. The participant also noted that more pressure levels would have made it harder for them to guess the password.

Back angle attack: The participant who was given the front angle of the squeeze password was able to guess it in four tries. All of the 22 parameters were successfully guessed. The participant said that the number of fingers was the easiest to guess as they had a clear view of the fingers and which ones were being utilised. The duration was also easy to guess and there was a substantial difference between a long and short duration. The pressure was the hardest to guess and the participant had to rely on the movement of the hand and the phone. The participant also noted that more of the screen was covered by the fingers when there was a hard press. With video access, the task of guessing a password became almost trivial but without video they would not have been able to do so.

Left angle attack: The participant who was guessing from the left angle looked at the video ten times. They said it was difficult to analyse all at once and had to get familiar with the concept first. They also took many tries to verify the guessed password and make sure the parameters matched. The participant was able to guess 20/22 parameters for a 91% accuracy. The first squeeze pressure and the seventh squeeze pressure were the wrong parameters. The participant did not that guessing the pressure was very difficult from the angle and had to rely on hand phone movement. The number of fingers was easy to guess as they had a clear view of which fingers were moving and participating in the squeezing. The duration also did not pose any issue as it was easy to tell when a squeeze started and when it ended.

Right angle attack: The participant who had the right angle looked at the video six times. They struggled to guess the password and ended up only guessing 13/22 for a 59% accuracy. The participant said that only seeing the forearm and back of the hand was a big nuisance to their ability to guess. The fingers were obstructed so the participant looked at which fingers they could see. Those fingers were not touching the phone so they deduced they were not part of the squeezing. The pressure was also hard to tell as they would not see the phone move or the fingers squeeze. They had to rely on the hand movement only from a bad angle. The duration was the easiest to guess since they could look at the hand movement and determine when a squeeze started and when it ended.

The results from table 2 can help us answer **RQ2**. The answer is a partial yes. With a video of the password, the attacker can watch the video multiple times, slow down the video and analyse it. However, not every angle can be used to guess the password. Some angles are more revealing than others. More specifically, a video taken from the side of the victim where only the back of the forearm can be seen will pose an issue to an attacker. The back, front and the other side angles can all be used to guess the password with high accuracy. **The answer to RQ2 is that squeeze authentication is not secure against shoulder surfing and it also fails to provide security against other angles of attack.**

5 STUDY 3: PRIVACY CONCERNS FOR SQUEEZE AUTHENTICATION

In this section, I will evaluate privacy concerns for squeeze authentication by finding correlations between users and their squeezing patterns. This study will focus on the correlation between sex and pressure, and the correlation between finger location and the dominant hand.

5.1 Experiment Design

The first correlation that will be analysed will be for the sex of the user and the pressure they use when squeezing their phone. The hypothesis is that a male user will apply a higher level of pressure when squeezing. To test the hypothesis, I made an application that tracks the pressure a user exceeds on the screen as well as the time the fingers are touching the screen. There are three light presses and three hard presses that are being tracked.

The second correlation that is analysed is the finger location on the smartphone and the dominant hand of the user. The hypothesis is that users hold their phones with their dominant hand and use squeeze authentication with their dominant hand. To test the hypothesis, I made a survey that asked the participants about their dominant hand, what hand they held on their phone and if they were using squeeze authentication which hand they would use.

5.2 Procedure

I recruited 12 participants from the university campus (4 females and 8 males). For each of the participants, I explained to them how squeeze authentication works. The experiment was run on a Google Pixel 3a. I then gave them the Pixel 3a which had the application to track pressure and time. I told them to familiarize themselves with the device for 2 minutes and to play around with touch pressure. The participants were told that there were two levels of pressure (high and low). The pressure intensity is user-specific and it is up to the users to define what they want light and hard pressure to be. This information has been relayed to the participants. Whenever the participants felt comfortable with the smartphone and touch pressure, they were asked to do three light touches followed by three hard touches. The touch pressure and time of press was then graphed and the results can be found in figure 2. An average for the light and hard pressure was taken based on the sex of the users and the results can be found in figure 1.

Once the participants finished with the touch pressure test, they were asked questions to test the second correlation that is between the finger location. The participants filled in a survey with the following questions: What is your dominant hand? What hand do you hold your smartphone in? Assuming you use squeeze authentication, which hand would you do the squeezing pattern in? The three possible answers for each one of these questions are left hand, right hand or both hands.

Figure 1: Average touch pressure based on sex

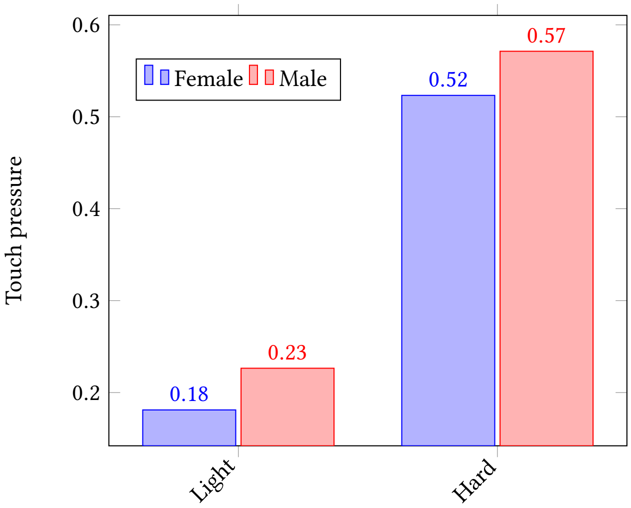
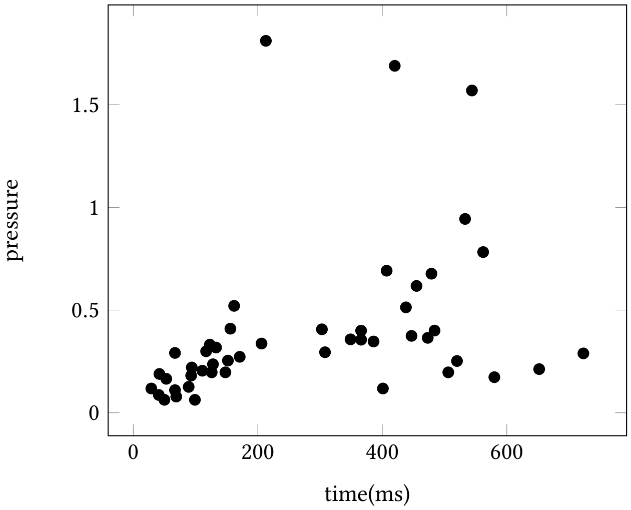


Figure 2: Touch pressure based on time



5.3 Discussion

The results from figure 1 shows us that there is a difference between the average touch pressure of males and females. On average, females have less touch pressure for light presses and for hard presses. However, there was a higher variance between the participants so I cannot say that there is a strong correlation between the sex of the user and the touch pressure. This is also a pilot study and 12 participants is not enough to draw a strong conclusion and a bigger study is needed to prove this hypothesis.

In figure 2, there is an interesting correlation that appeared. The touch pressure is heavily correlated with the duration of the press. When participants were asked for a light pressure, they always had a shorter duration then when they were asked for a hard pressure. This shows a subconscious tendency for users to relate pressure with duration. So the parameters for squeeze authentication for duration and pressure are actually correlated and cannot be considered independent. This further weakens the security of squeeze authentication.

The last part of this study was to look at the dominant hand of the user in relationship with the hand users use squeeze authentication. All the participants said that they would use squeeze authentication with their dominant hand. This is also the same hand they hold their smartphone in. This means there is a strong correlation between the dominant hand of the user and the hand they use for squeeze authentication.

To answer RQ3, we can say that there is a weak correlation between pressure and sex, and a strong correlation between dominant hand and hand for squeeze authentication. This means that there still are some privacy concerns when using squeeze authentication and the next section will explain why that is dangerous.

5.4 Case Study

This section will discuss how malicious actors can use squeeze authenticators to gain private information about their users. A malicious actor can have a website that allows for squeeze authentication to be used for a user to log in. The website can claim that squeeze authentication is private and does not expose any private information about the users. A user who wants to remain private and does everything in their power to not share information about their identity might see these claims on the website and decide to use squeeze authentication for the website. The user will register a squeeze password and think that their private information is safe. However, as shown in the section above, squeeze authentication parameters reveal information. The website operators can guess the dominant hand of the user and the sex of the user based on the squeeze password they registered with the website. Equipped with that information, the malicious operator can sell that information to other websites or show targeted ads to the users against their will.

6 SQUEEZE AUTHENTICATION IMPROVEMENTS

This section will talk about the improvements that can be made regarding squeeze authentication to increase its security and privacy. There are three key points that I believe will help make squeeze authentication viable in the future and these are constant pressure, multiple pressure options and using actual squeezing.

Constant pressure: Squeeze authentication currently works by having the user define what a light and hard squeeze means to them. However, I have shown that this poses a privacy risk as a malicious actor can infer the sex of the user. To prevent that from happening, there should be clear pressure thresholds that are constant between users. This would force everyone to use the same amount of pressure for a light and hard squeeze. To make the system more usable and for users to know what pressure they are using, there could be a feedback system that would vibrate the phone gently to inform the user when they switch pressure levels.

Multiple pressure options: From case study 2, the attackers had an easy time guessing the pressure level a victim was using based on the hand and finger movement. All of the participants said that more pressure levels would make it a lot harder for them to guess which pressure was being used. From a user point of view, having more pressure levels would make it harder to know which pressure level you are in. For that reason, a feedback system would work very well in conjunction with multiple pressure levels. The feedback would help the user understand what level they are in and the multiple pressure levels would prevent malicious actors from guessing the password.

Using actual squeezing: One of the biggest issues with the current squeeze authentication is the reliance on squeezing the screen. The users have to squeeze the screen of the device and make a conscious effort to wrap their fingers around the device to squeeze it. The participant who was inputting the password in Study 2 said that it was very uncomfortable trying to squeeze the screen. An easy way to solve this issue is to squeeze the actual device instead of forcing the squeeze to be done on the screen. Some pixel devices have active edge [3] which tracks the squeeze pressure on the side of the device. A new and improved squeeze authenticator can use actual smartphone squeezing by utilising existing modules in smartphones like Active Edge.

7 FUTURE WORK

I have been working on implementing the squeeze authenticator from scratch. The biggest challenge is to get the raw capacitive data since it requires changing the kernel. I am currently working on this. Once that is done, the squeeze authenticator is easy to implement. All of the studies will be repeated in a formal manner and more participants will be used to have stronger results.

8 CONCLUSION

This paper evaluates the security and privacy of current squeeze authentication with three user studies and recommends a path forward to make squeeze authentication more secure and usable. The first study shows that a simple squeeze password can be easily guessed by an attacker equipped with a basic understanding of the parameters used in squeeze authentication. The second studied proved that even a complicated squeeze password can be guessed by attackers if they have a video of the user inputting the password with a clear view of their hands and fingers. The third study showed that there is in fact some correlations between pressure and sex as well as dominant hand and hand used for squeeze authentication which leads to privacy leaks. Based on these results and the participants feedback three recommendations were made for the next generation of squeeze authenticators. Constant pressure threshold with feedback, more pressure options and phone squeezing instead of screen squeezing is needed to make squeeze authentication more private, secure and usable.

9 CODE

The videos of the participants inputting the squeeze password as well as the code used for the studies can be found here: https://github.com/Squeezing-your-privacy-away/Breaking-Squeeze-Auth.

REFERENCES

[1] [n. d.] Accessing raw capacitive images on commodity smartphones | huy viet le. Accessing Raw Capacitive Images on Commodity Smartphones | Huy Viet Le. Retrieved Feb. 22, 2024 from http://huyle.de/blog/capacitive-images/.

[2] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Evaluating attack and defense strategies for smartphone PIN shoulder surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). Association for Computing Machinery, New York, NY, USA, (Apr. 19, 2018), 1–10. isbn: 978-1-4503-5620-6. doi: 10.1145/3173574.3173738.

[3] Philip Quinn, Seungyon Claire Lee, Melissa Barnhart, and Shumin Zhai. 2019. Active edge: designing squeeze gestures for the google pixel 2. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19). Association for Computing Machinery, New York, NY, USA, (May 2, 2019), 1–13. isbn: 978-1-4503-5970-2. doi: 10.1145/3290605.3300504.

[4] 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). Association for Computing Machinery, New York, NY, USA, (Apr. 18, 2015), 2339–2342. isbn: 978-1-4503-3145-6. doi: 10.1145/2702123.2702202.

[5] Xin Yi, Shuning Zhang, Ziqi Pan, Louisa Shi, Fengyan Han, Yan Kong, Hewu Li, and Yuanchun Shi. 2023. Squeez'in: private authentication on smartphones based on squeezing gestures. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (CHI '23). Association for Computing Machinery, New York, NY, USA, (Apr. 19, 2023), 1–15. isbn: 978-1-4503-9421-5. doi: 10.1145/3544548.3581419.