Journal of Network and Computer Applications 165 (2020) 102687

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A swipe-based unlocking mechanism with supervised learning on smartphones: Design and evaluation☆

Wenjuan Li [a,b], Jiao Tan [c], Weizhi Meng [a,d,*], Yu Wang [a]

[a] *Institute of Artificial Intelligence and Blockchain, Guangzhou University, China*
[b] *Department of Computing, The Hong Kong Polytechnic University, Hong Kong Special Administrative Region*
[c] *KOTO Research Center, Macao, China*
[d] *Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark*

ARTICLE INFO

Keywords:
User authentication
Behavioral biometric
Swipe behavior
Smartphone security
Touch dynamics

ABSTRACT

With the rapid development of mobile devices, smartphones have become common in people's daily lives, i.e., retrieving community happenings and connecting with peers. Due to the convenience, users often store a large amount of private information on their phones (e.g., photos) and use the phone to process sensitive operations (e.g., financial transactions). Thus, there is a great need to protect the devices from unauthorized access in order to avoid privacy leakage and financial loss. Passwords are the most widely used authentication method, but attackers can take over the phone after it is unlocked. Instead, behavioral authentication can verify current users in a continuous way, which can complement the existing authentication mechanisms like passwords. With the increasing capability of smartphone sensors, users can perform various touch actions to interact with their devices. Motivated by this, in this work, we focus on swipe behavior and develop SwipeVlock, a supervised unlocking mechanism on smartphones, which can authenticate users based on their way of swiping the phone screen with a background image. In the evaluation, we measure several typical supervised learning algorithms and conduct two user studies with over 150 participants. As compared with similar schemes, it is found that participants could perform well with SwipeVLock, i.e., with a success rate of 98% during login and retention.

1. Introduction

With the rapid development of mobile technology, smartphones have become a necessity to assist peoples' daily lives. The IDC report presents that 79% of adults may have their smartphones with them 22 h a day, and during the first 15 min of waking up, four out of five phone users are likely to check their phones (An IDC Research Report). Due to the capability and convenience, many users would use their phones to store private information like photos and personal ID images. They may also use their phones to handle sensitive operations like bank transfer and payment (Yang et al., 2019). Smartphones are so important due to the connectivity they provided, whereas they have also become a major target by cyber-criminals (Nyang et al., 2018). If attackers obtain the phone and unlock it successfully, all stored information and data will be leaked. Hence there is a significant demand for deploying appropriate user authentication mechanisms to defend against unauthorized access.

Currently, textual passwords are still the most widely used authentication approach on smartphones, but its use may suffer from many security and usability limitations. For instance, iPhones use PIN code to authenticate users, but it cannot defend against many attacks, e.g., recording attacks where attackers can record the phone screen when inputting the code (Nyang et al., 2018). In addition, practical users often have multiple accounts and may choose easy-to-remember passwords due to both the multiple password inference (Meng et al., 2017d) and the limitation of long-term memory (Yan et al., 2004). As an example, the SplashData report indicates that the most frequently used password in 2018 is "123456" (SplashData et al., 2018). Many research studies on password analysis like (Bonneau, 2012; Weir et al., 2010) revealed that this situation may become even worse under existing state-of-the-art attacks and cracking tools.

☆ A preliminary version of this paper appears in Proc. of the 2nd International Conference on Machine Learning for Cyber Security (ML4CS 2019), pp. 140–153, 2019 (Li et al., 2019).

* Corresponding author. Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark.
E-mail address: weme@dtu.dk (W. Meng).

https://doi.org/10.1016/j.jnca.2020.102687
Received 31 December 2019; Received in revised form 19 March 2020; Accepted 29 April 2020
Available online 11 May 2020

To complement textual passwords, graphical passwords (GP) are designed in the literature to provide better usability, since many studies like (Nelson et al., 1976; Shepard, 1967) identified that users can remember images better than conventional passwords. For instance, Jermyn et al. (1999) developed a GP scheme called DAS (draw-a-secret), which requires users to draw their passwords on a 2D grid. Wiedenbeck et al. (2005) showed a GP system called *PassPoints*, which allows users to create secrets by clicking on some locations on an image. In current market, Android phones adopt a practical GP application called *Android unlock patterns*, which needs users to input correct patterns to unlock their phones in a grid size of 3 × 3 points (Churchill, 2013; De Luca et al., 2012). For authentication, users have to recall the same pattern registered during the enrollment.

However, Android unlock patterns may be vulnerable to many attacks in practice, as users can only choose a pattern with 4 dots at least and 9 dots at most. This makes a brute-force attack still feasible because the total number of possible patterns is only 389,112 (Aviv et al., 2010). In addition, it is vulnerable to recording attacks (Nyang et al., 2018) and charging attacks (Meng et al., 2017a, 2017b), i.e., the phone screen can be captured by attackers during phone charging. Further, Andriotis et al. (2013) conducted a pilot study and found that users have preferences on choosing the *start points* and *end points* when creating the pattern. Therefore, how to enhance the security of Android unlock mechanism remains a challenge.

Contributions. In the research community, many research studies like (De Luca et al., 2012; Meng et al., 2016; Zhao et al., 2014) have shown that combining behavioral features can help enhance the security of Android unlock patterns. For example, De Luca et al. (De Luca et al., 2012) designed a scheme that combines behavioral biometric with unlock patterns via dynamic time warping (DTW). Meng et al. (2016) also presented a scheme that verifies users based on their touch movement. Motivated by the previous work, we advocate the merit of enhancing authentication with behavioral biometric, and develop SwipeVLock, a swipe behavior-based unlock mechanism on smartphones. In our scheme, users can choose a background image and unlock the phone by swiping their finger with the selected location on the image. The contributions can be summarized as follows.

- We design SwipeVLock, an unlock mechanism on smartphones that verifies users based on how they swipe the touchscreen. For enrollment, users have to choose one background image and one location, and then register their swipe behavior. This mechanism is transparent without the need of additional hardware on smartphones.
- In the evaluation, we perform two major user studies to explore the performance of SwipeVLock. We first conduct a user study with 30 participants and use the data to test some typical supervised learning algorithms. We then involve 130 common phone users to evaluate SwipeVLock in the aspect of success rate as compared with a similar scheme proposed by De Luca et al. (De Luca et al., 2012). We further provide an outside-lab experiment to validate the results.

Overall, SwipeVLock can be considered as a combination of graphical passwords and behavioral authentication. Different from the previous version (Li et al., 2019), in this work, we perform a new user study with 30 participants to investigate the performance of different supervised learning algorithms on SwipeVLock. In the evaluation, we launch a new user study with a total of 130 participants to explore the usage of our scheme in the aspects of login and retention, as compared with a similar scheme developed by De Luca et al. (De Luca et al., 2012).

Road map. The remainder of this paper can be structured as follows. Section 2 introduces relevant graphical password schemes and touch behavioral authentication schemes. Section 3 describes our scheme of SwipeVLock in detail. In Section 4, we present main user studies with a total of 160 participants to evaluate the scheme performance. Section 5 discusses some open challenges and we conclude our work in Section 6.

2. Related work

In this section, we introduce related research studies regarding graphical passwords and touch behavioral authentication.

2.1. Authentication based on graphical passwords

Graphical passwords (GPs) have been studied over decades. A traditional GP scheme can be classified as three types (Chiasson et al., 2007; Meng et al., 2017e; Suo et al., 2005): recognition-based scheme, pure recall-based scheme and cued recall-based scheme.

- Recognition-based scheme. This kind of scheme (e.g., (Davis et al., 2004; Passfaces)) needs users to remember and recognize several images. Taking *PassFaces* (Passfaces) as a typical example, it requires users to figure out human faces for user authentication.
- Pure recall-based scheme. This type of scheme requires users to generate a pattern on an image. For example, Jermyn et al. (1999) introduces *DAS* (‘draw-a-secret’), in which users have to create their passwords on a grid. Android unlock pattern (AUP) mechanism belongs to this type, asking users to swipe their finger to input a correct pattern and unlock the device. It is indeed a modified version of Pass-Go (Tao and Adams, 2008), in order to fit a small touchscreen. AUP has some rules, i.e., it defines a valid pattern with 4 dots at least and 9 dots at most, within a grid of 3 × 3 points on smartphones.
- Cued recall-based scheme. Such schemes require users to create a pattern on an image or more images. Taking a typical system of *PassPoints* (Wiedenbeck et al., 2005) as an example, it needs users to remember five points on one image in an order. Then Chiasson et al. (2012) introduced Persuasive Cued Click-Points (PCCP), in which users have to select a point on a sequence of background images.

In recent years, GP schemes have received much attention. Lavanya et al. (2019) applied graphical passwords for building a secure group communication scheme between group members, where the group key is a graphical password. Meng (2015) introduced *RouteMap*, a map- and route-based graphical password scheme, allowing users to draw a route on a world map as their secrets. Then they applied this scheme for improving the security of FinTech applications (Meng et al., 2019).

To combine the merits from different schemes, more hybrid GP schemes are developed. For example, Gyorffy et al. (2011) used a graphical password to defeat Trojan and virus by constructing an image hash. Meng (2012) first combined all input types and proposed click-draw based graphical password scheme (CD-GPS), with two steps: image selection and secret drawing. Then they studied the effect of using multi-touch actions (Meng et al., 2013, 2017c), user guidelines (Meng and Li, 2012b) and proper tolerance (Meng and Li, 2012a) to enhance the performance of CD-GPS. Yu et al. (2017) presented EvoPass, an evolvable graphical password authentication system to defeat shoulder-surfing attacks. It can transform a set of user-selected pass images to pass sketches as user credentials.

With the aim of enhancing the password space, world map has been used as the background image, in which users can choose a location worldwide (Fox, 2010; Spitzer et al., 2010). Based on this idea, Sun et al. (2012) designed *PassMap* that requires users to choose two locations (in an ordered sequence) on a world map. Then Thorpe et al. (2013) introduced *GeoPass* that only requires users to select one location. The previous study showed that there is no significant difference between the selection of one or two locations (Meng et al., 2017e).

Similar to textual passwords, graphical passwords may also suffer the issue of multiple password interference. Meng et al. (2017d) investigated this issue with 60 participants between textual passwords and map-based passwords under six account scenarios. They found that participants in the map-based graphical password scheme could perform better than the textual password scheme in both short-term (1-h session) and long term (after two weeks) password memorability tests.

To construct a practical GP scheme, how to make a balance between security and usability is still a challenge. Some other typical GP studies could be referred but not limited to (Dirik et al., 2007; Dunphy and Yan, 2007; Lin et al., 2007).

2.2. Touch behavioral authentication

With the advent of touchscreen, touch dynamics has become popular on smartphones. Fen et al. (Feng et al., 2012) developed a finger gesture-based authentication system on touchscreen devices, reaching a false acceptance rate of 4.66% and false rejection rate of 0.13% by means of a random forest classifier. Meng et al. (2012) validated the feasibility of touch behavioral authentication on smartphones, where they designed a scheme with 21 touch-related features and achieved an average error rate of around 3% based on a combined classifier of PSO-RBFN. Then Frank et al. (2013) developed *Touchalytics*, a touch behavioral authentication scheme with 30 features extracted from up-down and left-right scrolling touch actions, which reached a median equal error rate of around 4% (one week after the enrollment phase).

Up to now, more touch behavioral authentication schemes have been proposed (Meng et al., 2015). Zheng et al. (2014) researched users' tapping behaviors on a passcode-enabled smartphone, and achieved an averaged equal error rate of nearly 3.65% by using a one-class algorithm. Smith-Creasey and Rajarajan (2016) achieved an equal error rate of 3.77% by means of a stacked classifier approach. Sharma and Enbody (2017) studied how users would interact with the application interface, and achieved a mean equal error rate of 7% for user authentication based on the SVM-based ensemble classifier. Shahzad et al. (2017) researched users' particular behavior and designed an authentication scheme based on how users input a gesture or a signature, such as velocity, device acceleration, and stroke time.

3. Our approach

This section first discusses the security issues of Android unlock mechanism and then describes our proposed SwipeVLock in detail, including the adopted authentication framework and features.

3.1. Unlock mechanism

Android unlock pattern is a special version of Pass-Go (Tao and Adams, 2008), in which a valid pattern should be created with 4 dots at least and 9 dots at most, within a grid of 3 × 3 points. This unlock mechanism has been widely implemented on Android phones, but would be still vulnerable to various attacks like recording attacks (Nyang et al., 2018) and charging attacks (Meng et al., 2017a, 2017b), which can record the screen when a user inputs the pattern. In addition, Aviv et al. (2010) indicated that as the password space of Android unlock pattern is around 389,112, brute force attacks could be feasible. They also presented an attack called smudge attacks, which can recover the pattern based on the residual oils on touch screens. Andriotis et al. (2013) observed the results from a pilot study and figured out that around 52.08% of the participants preferred to start their patterns from the top left node. This may greatly reduce the effective password space of unlock mechanisms.

Previous studies like (De Luca et al., 2012; Meng et al., 2016) have shown that the security of unlock mechanisms can be enhanced by integrating with touch behavioral authentication on touch screen devices. By adding another layer of authentication, it would become more difficult for attackers to compromise the authentication, i.e., attackers may need more time to get into the system. Further, to avoid the limitation of 3 × 3 grid, there is a need to design more flexible and usable schemes in practice.

3.2. Design of SwipeVLock

Motivated by the above observations, in this work, we thus propose SwipeVLock, a swipe-based unlocking mechanism aiming to complement existing unlock mechanisms on smartphones, by involving touch behavioral authentication. Different from the previous schemes like (De Luca et al., 2012; Meng et al., 2016), our scheme allows users to choose a background image and perform the authentication based on how users swipe their fingers. Fig. 1 shows the main idea of SwipeVLock including three major steps.

SwipeVLock enrollment. Users have to select one background image from an image pool, with different themes such as fruits, cartoon characters, sport, landscape, food, buildings, transportation, people, etc. Then, users can choose one location as the starting point and then swipe the screen from this selected location.

SwipeVLock verification. For authentication, users have to select the same background image from the pool, and swipe the screen from the same location on the image. The authentication process can be regarded to be successful, if and only if both image location and swipe behavior are verified by our scheme.

SwipeVLock implementation. Fig. 2 depicts how to implement SwipeVLock. In this work, our scheme employs a supervised learning-based framework to help model users' touch behavior. When users swipe the screen, SwipeVLock will extract the touch features from swipe behavior and train the classifier. The classifier mainly generates a normal profile based on the historical swipe behavior, and compares it with the current swipe features. A decision will be output in the end.

On the other hand, SwipeVLock can compare the image location with the stored location in the database. If there is a match, then it is considered to be successful. In particular, we set the error tolerance as a 21 × 21 pixel box around the selected location. Such setting is based on the previous work like (Meng et al., 2017e; Thorpe et al., 2013). For example, *GeoPass* (Thorpe et al., 2013) proved that an error tolerance of 21 × 21 pixel is usable in practice.

Swipe features. In this work, based on the previous studies (De Luca et al., 2012; Frank et al., 2013), we consider some common and typical touch features that can be used to model swipe behavior: the coordinates of location (XY), touch pressure, touch size, touch time, and touch speed.

- Coordinates of location. Our scheme records the location coordinates on the selected image. Intuitively, users may have their own selection preference, making the location different from others.
- Touch pressure. With the increasing capability of smartphones, current screen sensors are able to record the values of touch pressure, which can be used to model users' touch behavior.
- Touch duration. This feature can be computed by measuring the time difference between touch press-down and touch press-up. It is a common feature that can be used to distinguish different users, i.e., some users may press longer while some may press shorter.
- Touch speed. Intuitively, swipe behavior can be treated as a swift touch movement. Based on (Meng et al., 2016), suppose a swipe action starts from (x1, y1) and ends at (x2, y2), if we know relevant time of occurrence *T1* and *T2*, then we can calculate the touch speed according to Equation (1) as below.

$$Touch\ Speed = \frac{\sqrt{(x2-x1)^2+(y2-y1)^2}}{T2-T1} \quad (1)$$

4. Evaluation

In this section, we design two major user studies to investigate the performance of different supervised classifiers and the usability of SwipeVLock, respectively. We also provide one outside lab experiment to validate the results.

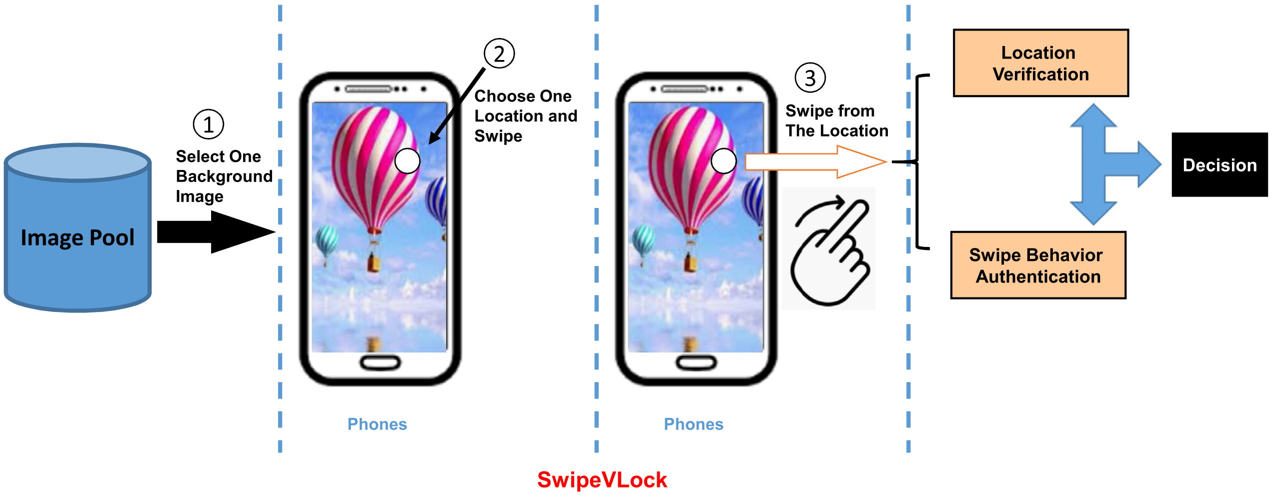

Fig. 1. SwipeVLock: 1) Step 1: select one background image from a pool; 2) Step 2: choose one location on the background image; and 3) Step 3: swipe from the selected location to unlock the phone.

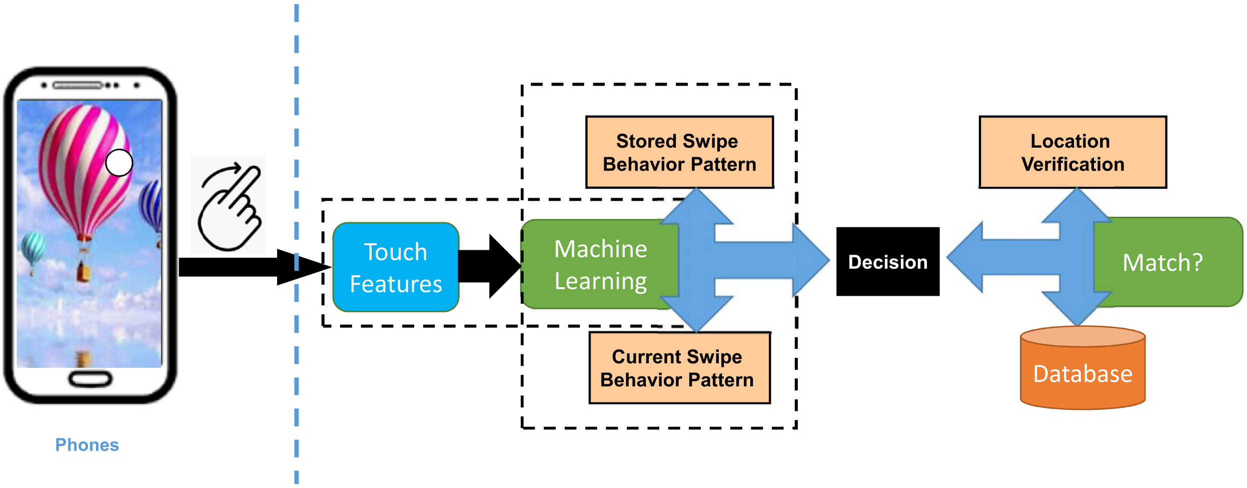

Fig. 2. Detailed authentication processes for SwipeVlock.

4.1. *User study on classifier performance*

To investigate the performance of typical supervised learning on SwipeVLock, we perform a user study with 30 participants who are regular Android phone users. This is a new user study that is different from the one in our previous work (Li et al., 2019). The detailed information of participants is shown in Table 1. In particular, we have 20 males and 10 females who aged from 16 to 50. Most of them are students in addition to business people, university staff and faculty members. The participants were recruited via online recruitment. A $20 gift voucher was provided to each participant.

Supervised authentication. As mentioned in Fig. 2, SwipeVLock can apply supervised learning algorithms to authenticate users. In this work, we consider the following typical and popular supervised classifiers: Decision tree (J48), Naive Bayes, SVM and Back Propagation Neural Network (BPNN).

- J48 is a decision tree classifier (Quinlan, 1996), which can label data based on the pre-trained tree-like structure.
- Naive Bayes is kind of supervised learning algorithms based on Bayes theorem that assumes conditional independence between every pair of features by given the value of class variable (Rennie et al., 2003).
- BPNN is a kind of neural network classifier (Rumelhart et al., 1986), which uses a differentiable transfer function at each network node and then applies error back-propagation process to modify the internal network weights after each training round.
- Support Vector Machine (SVM) (LIBSVM) is a linear model for both classification or regression challenges, by generating a line or a hyperplane that separates the data into classes.

To avoid any bias during classifier implementation, we adopted WEKA platform, which is an open-source machine learning collection in Java (Weka). We used the default settings for all classifiers in the user study. Below are two metrics used to evaluate the performance of our scheme.

- False Acceptance Rate (FAR): indicates the percent of how many intruders are classified as normal users.
- False Rejection Rate (FRR): indicates the percent of how many legitimate users are classified as intruders.

Study steps. In the study, we first introduced our objectives to all

Table 1
Participants information in the first user study.

Information	Male	Female	Occupation	Male	Female
Age <25	11	4	Students	14	6
Age 25-35	5	4	University Faculty&Staff	4	2
Age 35-45	4	2	Business People	2	2

participants and demonstrated what kind of data would be collected. Each participant could get one Android phone (Samsung Galaxy Note) and before the experiment, each of them has three trials to get familiar with the scheme. All participants were required to do the experiment in our lab. Below are the detailed study steps.

- Step 1. Creation phase: participants have to create their credentials according to SwipeVLock' steps.
- Step 2. Confirmation phase: participants should confirm the password by verifying both the image location and swipe behavior for 10 times (used for classifier evaluation). Participants can update their credentials if they fail or want to change it.
- Step 3. Distributed memory: participants were provided with one paper-based finding task to distract them for 15 min.
- Step 4. Login phase: participants should swipe to unlock the phone for 10 trials. The system recorded all the data for analysis.

Study results. In the confirmation phase, we could collect 300 trials from all participants in the login phase. We used 60% of them as training data and the rest as testing data (with a cross-validation mode).

Table 2 depicts a comparison regarding the classifier performance (e.g., average error rate - AER) between our study and the previous work (Li et al., 2019). The results verified that SVM could provide the best performance, i.e., it could reach an AER of 4.1% and 3.8% in Li et al. (2019) and this study, respectively. For other classifiers, BPNN could achieve an AER of 7% and 7.3%, while the AER was above 10% for J48 and Naive Bayes. Based on the results, we decided to use SVM in SwipeVLock for user authentication in the next study.

4.2. User study on SwipeVLock

To investigate the usage of SwipeVLock, we perform another user study as compared with the De Luca et al.'s scheme (named as DeLucaUnLock) (De Luca et al., 2012). The selection of this scheme is because our work has the same purpose. They added an implicit authentication layer to improve the security of unlock patterns. For authentication, their system checks both the pattern and how users input this shape. They considered touch data, such as pressure, coordinates, size, speed and time, and used dynamic time warping (DTW) to determine whether the user is legitimate.

In this study, we involved a total number of 120 participants who are regular Android phone users, including 72 males and 48 females. The participants were recruited via online recruitment and colleague recommendation. The detailed information of participants is shown in Table 3. A $20 gift voucher was provided to each participant. Similar to the first study, we first introduced our objectives to all participants and demonstrated what kind of data would be collected.

Each participant could get one Android phone (Samsung Galaxy Note) and before the experiment started, each of them has three trials to get familiar with the scheme. Then we randomly divided participants into two groups. The participants in Group-1 were asked to use our scheme, while the participants in Group-2 were required to use scheme of DeLucaUnLock. Below are the detailed study steps.

- *Group-1.* Participants in this group were required to complete the authentication under our scheme of SwipeVLock.
  - Step 1. *Creation phase:* participants should create their credentials based on the steps of SwipeVLock.
  - Step 2. *Confirmation phase:* participants should confirm the password by verifying both the image location and swipe behavior for 10 times. Participants could update their credentials if they fail or want to change it.
  - Step 3. *Distributed memory:* participants were provided with one paper-based finding task to distract them for 15 min.
  - Step 4. *Login phase:* participants should swipe their finger to unlock the phone for 10 trials. The system recorded all the data for analysis.
  - Step 5. *Feedback form:* participants should answer several questions in a *feedback form* regarding our scheme usage.
  - Step 6. *Retention:* after three days, participants were asked to return and unlock the phone for 10 times in our lab.
  - Step 7. *Retention feedback:* participants have to finish another *feedback from* regarding our scheme usage.
- *Group-2.* Participants in this group could complete the authentication under the DeLucaUnLock scheme.
  - Step 1. *Creation phase:* participants have to create their credentials according to DeLucaUnLock' steps.
  - Step 2. *Confirmation phase:* participants should confirm the password for 10 times. Participants could update their credentials if they fail or want to change it.
  - Step 3. *Distributed memory:* participants were provided with one paper-based finding task to distract them for 15 min.
  - Step 4. *Login phase:* participants should swipe their finger to unlock the phone for 10 trials. The system recorded all the data for analysis.
  - Step 5. *Feedback form:* participants should answer several questions via a *feedback form* regarding our scheme.
  - Step 6. *Retention:* after three days, participants were asked to return and unlock the phone for 10 times in our lab.
  - Step 7. *Retention feedback:* participants have to finish another *feedback from* regarding our scheme.

In the confirmation phase, we could collect 600 trials for each scheme. Table 4 presents the successful unlock trials for login phase and retention phase between two groups.

- Login phase. We found that participants in both groups could perform well with SwipeVLock and DeLucaUnLock scheme, i.e., achieving a success rate of 98.2% (Group1) and 98.3% (Group2), respectively. The errors were mainly caused by behavioral deviation for both schemes.
- Retention phase. After three days, it is found that participants in Group-1 performed a bit better than those in Group-2. The accuracy reduction is mainly caused by the behavior deviation.

Outside lab validation. To validate the performance, we further recruited a total of 10 new users and randomly divided them into two groups. They followed the same steps for password creation and authentication, but could do the experiment outside the lab. All phone settings remained the same. For the retention phase, they could keep the phone and after three days, participants were asked to return and unlock the phone for 10 times in our lab.

Table 4 (*Retention-new*) shows that a better success rate could be achieved for both schemes. This is because participants could keep the phone and practice the unlocking behavior more. The results validate that more practice can make the touch behavior more stable, which is

Table 2
The performance of different classifiers under different groups.

Preivous work (Li et al., 2019)	J48	NBayes	SVM	BPNN	*This work*	J48	NBayes	SVM	BPNN
FAR (%)	9.7	12.4	3.7	6.8	FAR (%)	9.1	10.4	3.5	7.2
FRR (%)	10.3	10.3	4.5	7.2	FRR (%)	10.3	11.2	4.1	7.4
AER (%)	10.0	11.35	4.1	7.0	AER (%)	9.7	10.8	3.8	7.3

Table 3
Participants information in the second user study.

Information	Male	Female	Occupation	Male	Female
Age <25	52	28	Students	48	32
Age 25-35	12	12	University Faculty&Staff	14	10
Age 35-45	8	8	Business People	10	6

Table 4
Success rate in the login and retention phase for Group1 and Group2.

Login	Group-1	Group-2
Success rate	589/600 (98.2%)	590/600 (98.3%)
Retention	Group-1	Group-2
Success rate	556/600 (92.6%)	546/600 (91.0%)
Retention-new	Group-1	Group-2
Success rate	588/600 (98.0%)	578/600 (96.3%)

in-line with the observations in Meng et al. (2016). Further, it is found that there are fewer errors caused by location selection, indicating that the error tolerance is suitable in practical usage.

User feedback. During the study, we gave two feedback forms to each participant regarding security and usability of two schemes. Ten-point Likert scales were used in each feedback question, where 1-score indicates strong disagreement and 10-score indicates strong agreement. Several key questions and relevant scores are summarized in Table 5.

- Group-1. It is found that most participants were satisfied with the usage of SwipeVLock, resulting in a score of over 8.6 on average for each question. Especially, they provided a score of 9.1 regarding the scheme security, which is much higher than that of DeLucaUnLock.
- Group-2. The participants in this Group2 provided a similar score as compared with Group-1. The main difference is that participants gave a lower score regarding the scheme security. Most participants believe some attacks like mimic attacks may be effective in cracking the authentication of DeLucaUnLock.

Overall, as compared with the scheme of DeLucaUnLock, our proposed SwipeVLock can provide similar usability while providing better security. This is because users can choose their own background image and set a unique location to swipe the screen. Based on the feedback, we believe that our scheme could become a promising alternative to complement existing unlock mechanisms on smartphones.

5. Discussion

In the user study, we obtain promising results on the usage of our scheme. However, our work is still at an early stage to explore the performance of SwipeVLock. Below are some challenges and limitations that can be considered in our future work.

- Time consumption. In this work, we did not investigate the time consumption, as it normally takes less than 10 s. Most participants also satisfied with the login time in our feedback forms. In our future work, we plan to perform a larger study to explore this issue.
- Image selection. The first step of SwipeVLock is to select one background image from a pool (i.e., with 10 images). Intuitively, users have their own preference and are likely to choose a different image. However, with more users, it is unclear whether there would be a bias. This is an interesting topic in our future work.
- Location selection. The second step of SwipeVLock is to choose a location for swiping on the selected image. Similar to the image selection, it is also an interesting topic to investigate whether there is a selection bias, and explore which part of image is most likely to be selected.
- Diverse participants. In this work, we involved a total of 160 participants in the study. In our future work, we plan to recruit some more participants with diverse background to validate our results. In addition, it is also an interesting topic to investigate the difference between right handed and left handed participants, and verify the observations.
- Advanced attacks. Our focus in this work is to investigate the performance of SwipeVLock, we did not consider some adversarial scenarios, where an attacker may get the phone and try to unlock it. This is an important topic in our future work, i.e., exploring the impact of recording attacks and mimic attacks.
- Multi-touch behavior. At this stage, our scheme only considers a swipe action with a single finger, as single-finger action is quite common on mobile devices. For instance, Lee et al. (2019) studied the effect of a natural thumb position when designing a tapping task on a smartphone. In future, it is an interesting topic to extend our scheme by enabling two fingers.
- Phone type. In this work, we mainly used one type of Android phone in the user study, while it could be an interesting topic to explore whether phone models may affect the scheme performance. This is also an open challenge for existing authentication schemes.
- Machine leaning technique. Supervised learning algorithms are widely adopted when designing a user authentication scheme (Meng et al., 2015). In this work, we consider some common and popular machine learning schemes to model users' behavior. Our future work plans to involve more diverse learning algorithms, e.g., ensemble learning algorithms, and to investigate the effect of feature distance approaches.
- Comparison with other schemes. Our study focuses on evaluating the performance of SwipeVLock and compares it with the scheme of DeLucaUnLock. In our future work, we plan to consider more graphical password schemes, behavioral schemes and hybrid schemes in a comparison. This is also an open challenge in this area, as there lacks a unified platform for performing such comparison.

Table 5
Major questions and average scores received from the user study.

Questions (Group1)	Average Scores
1. I could easily create a credential under SwipeVLock	9.0
2. The time consumption for SwipeVLock creation is acceptable	8.6
3. I could easily login to the system	8.8
4. I think the scheme is secure	9.1
Questions (Group2)	Average Scores
1. I could easily create a credential under DeLucaUnLock	9.1
2. The time consumption for DeLucaUnLock creation is acceptable	8.5
3. I could easily login to the system	8.7
4. I think the scheme is secure	8.3

6. Conclusion

With the popularity of smartphones, there is an increasing need to protect the devices from unauthorized access. Unlock mechanisms like Android unlock patterns are an important security tool to protect smartphones and authenticate users. In this work, we develop SwipeVLock, a swipe behavior-based unlock scheme on smartphones, which requires users to choose one background image and a location to perform a swipe action for authentication. A successful trial should have both correct location selection and swipe behavior verification. In the evaluation, we performed two user studies. In the first one, we involved 30 participants and investigated the performance of typical supervised learning classifiers. Then we performed another study with 120 participants to compare the performance between our scheme and a similar scheme of DeLucaUnLock. We also provide an outside lab experiment to validate our observations. Our evaluation demonstrates that participants could perform well with our scheme and most participants believe our scheme is more secure than DeLucaUnLock.

CRediT authorship contribution statement

Wenjuan Li: Conceptualization, Methodology, Writing - original draft. **Jiao Tan:** Data curation, Resources, Investigation. **Weizhi Meng:** Conceptualization, Writing - review & editing, Supervision. **Yu Wang:** Resources, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We would like to thank the participants for their hard work in the user study. This work was partially supported by National Natural Science Foundation of China (No. 61802077).

References

An IDC research report, sponsored by facebook. How smartphones and social keep us engaged. https://www.nu.nl/files/IDC-Facebook20Always20Connected20(1).pdf.

Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C., 2013. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proceedings of WiSec. ACM, pp. 1–6.

Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M., 2010. Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX Conference on Offensive Technologies. USENIX Association, pp. 1–7.

Bonneau, J., 2012. The science of guessing: analyzing an anonymized corpus of 70 Million passwords. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy, pp. 538–552.

Chiasson, S., Biddle, R., van Oorschot, P.C., 2007. A second look at the usability of click-based graphical passwords. In: Proceedings of the 3rd Symposium on Useable Privacy and Security (SOUPS). ACM, New York, pp. 1–12.

Chiasson, S., Stobert, E., Forget, A., Biddle, R., 2012. Persuasive cued click-points: design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Trans. Dependable Secure Comput. 9 (2), 222–235.

Churchill, Berkeley, 2013. Unlock Pattern Generator. Available at: https://www.berkeleychurchill.com/software/android-pwgen/pwgen.php.

Davis, D., Monrose, F., Reiter, M.K., 2004. On user choice in graphical password schemes. In: Proceedings of the 13th Conference on USENIX Security Symposium (SSYM). USENIX Association, Berkeley, pp. 151–164.

De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H., 2012. Touch me once and I know it's you!: implicit authentication based on touch screen patterns. In: Proceedings of CHI. ACM, pp. 987–996.

Dirik, A.E., Memon, N., Birget, J.C., 2007. Modeling user choice in the passpoints graphical password scheme. In: Proceedings of the 3rd Symposium on Useable Privacy and Security (SOUPS). ACM, New York, NY, USA, pp. 20–28 (2007).

Dunphy, P., Yan, J., 2007. Do background images improve draw a secret graphical passwords? In: Proceedings of the 14th ACM Conference on Computer and Communications Security. CCS), pp. 36–47.

Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunary, B., Jiang, Y., Nguyen, N., 2012. Continuous mobile authentication using touchscreen gestures. In: Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE, USA, pp. 451–456.

Fox, S., 2010. Future Online Password Could Be a Map. http://www.livescience.com/8622-future-online-password-map.html.

Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D., 2013. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. 8 (1), 136–148.

Gyorffy, J.C., Tappenden, A.F., Miller, J., 2011. Token-based graphical password authentication. Int. J. Inf. Secur. 10 (6), 321–336.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D., 1999. The design and analysis of graphical passwords. In: Proceedings of the 8th Conference on USENIX Security Symposium. USENIX Association, Berkeley, pp. 1–14.

LIBSVM A library for support vector machines. https://www.csie.ntu.edu.tw/cjlin/libsvm/.

Lavanya, S., Saravana Kumar, N.M., Vijayakumar, V., Thilagam, S., 2019. Secured key management scheme for multicast network using graphical password. MONET 24 (4), 1152–1159.

Lee, S.C., Cha, M.C., Ji, Y.Gu., 2019. Investigating smartphone touch area with one-handed interaction: effects of target distance and direction on touch behaviors. Int. J. Hum. Comput. Interact. 35 (16), 1532–1543.

Li, W., Tan, J., Meng, W., Wang, Y., Li, J., September 2019. SwipeVLock: a supervised unlocking mechanism based on swipe behavior on smartphones. In: The 2nd International Conference on Machine Learning for Cyber Security (ML4CS 2019), pp. 140–153.

Lin, D., Dunphy, P., Olivier, P., Yan, J., 2007. Graphical passwords & qualitative spatial relations. In: Proceedings of the 3rd Symposium on Useable Privacy and Security (SOUPS), pp. 161–162.

Meng, Y., 2012. Designing click-draw based graphical password scheme for better authentication. In: Proceedings of the 7th IEEE International Conference on Networking, Architecture, and Storage (NAS), pp. 39–48.

Meng, W., 2015. RouteMap: a route and map based graphical password scheme for better multiple password memory. In: Proceedings of the 9th International Conference on Network and System Security (NSS), pp. 147–161.

Meng, Y., Li, W., 2012a. Evaluating the effect of tolerance on click-draw based graphical password scheme. In: Proceedings of the 14th International Conference on Information and Communications Security (ICICS), Lecture Notes in Computer Science 7618. Springer, pp. 349–356.

Meng, Y., Li, W., 2012b. Evaluating the effect of user guidelines on creating click-draw based graphical passwords. In: Proceedings of the 2012 ACM Research in Applied Computation Symposium (RACS), pp. 322–327.

Meng, Y., Li, W., Kwok, L.-F., 2013. Enhancing click-draw based graphical passwords using multi-touch on mobile phones. In: Proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference (IFIP SEC), IFIP Advances in Information and Communication Technology, vol. 405, pp. 55–68.

Meng, W., Wong, D.S., Furnell, S., Zhou, J., 2015. Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutor. 17 (3), 1268–1293.

Meng, W., Li, W., Wong, D.S., Zhou, J., 2016. TMGuard: a touch movement-based security mechanism for screen unlock patterns on smartphones. In: Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS), pp. 629–647.

Meng, W., Lee, W.H., Liu, Z., Su, C., Li, Y., 2017a. Evaluating the impact of juice filming charging attack in practical environments. In: Proceedings of ICISC, pp. 327–338.

Meng, W., Fei, F., Li, W., Au, M.H., 2017b. Harvesting smartphone privacy through enhanced juice filming charging attacks. In: Proceedings of ISC, pp. 291–308.

Meng, W., Li, W., Kwok, L.-F., Choo, K.-K.R., 2017c. Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones. Comput. Secur. 65, 213–229.

Meng, W., Li, W., Lee, W., Jiang, L., Zhou, J., 2017d. A pilot study of multiple password interference between text and map-based passwords. In: Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS), pp. 145–162.

Meng, W., Lee, W., Au, M.H., Liu, Z., 2017e. Exploring effect of location number on map-based graphical password authentication. In: Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP), pp. 301–313.

Meng, W., Wong, D.S., Schlegel, R., Kwok, L.F., 2012. Touch gestures based biometric authentication scheme for touchscreen mobile phones. In: Proceedings of INSCRYPT 2012, Lecture Notes in Computer Science 7763. Springer, pp. 331–350.

Meng, W., Zhu, L., Li, W., Han, J., Li, Y., 2019. Enhancing the security of FinTech applications with map-based graphical password authentication. Future Generat. Comput. Syst. 101, 1018–1027.

Nelson, D.L., Reed, V.S., Walling, J.R., 1976. Pictorial superiority effect. J. Exp. Psychol. Hum. Learn. Mem. 2 (5), 523–528.

Nyang, D., Kim, H., Lee, W., Kang, S., Cho, G., Lee, M.K., Mohaisen, A., 2018. Two-Thumbs-Up: physical protection for PIN entry secure against recording attacks. Comput. Secur. 78, 1–15.

Passfaces, http://www.realuser.com/.

Quinlan, J.R., 1996. Improved use of continuous attributes in C4.5. J. Artif. Intell. Res. 4 (1), 77–90.

Rennie, J.D.M., Shih, L., Teevan, J., Karger, D.R., 2003. Tackling the poor assumptions of naive Bayes text classifiers. In: Proceedings of the 20th International Conference on Machine Learning, pp. 616–623.

Rumelhart, D., Hinton, G., Williams, R., 1986. Learning representations by back-propagating errors. Nature 323, 533–536.

Shahzad, M., Liu, A.X., Samuel, A., 2017. Behavior based human authentication on touch screen devices using gestures and signatures. IEEE Trans. Mobile Comput. 16 (10), 2726–2741.

Sharma, V., Enbody, R., 2017. User authentication and identification from user interface interactions on touch-enabled devices. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), pp. 1–11.

Shepard, R.N., 1967. Recognition memory for words, sentences, and pictures. J. Verb. Learn. Verb. Behav. 6 (1), 156–163.

Smith-Creasey, M., Rajarajan, M., 2016. A continuous user authentication scheme for mobile devices. In: Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), pp. 104–113.

Spitzer, J., Singh, C., Schweitzer, D., 2010. A security class project in graphical passwords. J. Comput. Sci. Colleges 26 (2), 7–13.

SplashData, Inc, The worst passwords of 2018. Available at: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/.

Sun, H., Chen, Y., Fang, C., Chang, S., 2012. PassMap: a map based graphical-password authentication system. In: Proceedings of AsiaCCS, pp. 99–100.

Suo, X., Zhu, Y., Owen, G.S., 2005. Graphical passwords: a survey. In: Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC). IEEE Computer Society, USA, pp. 463–472.

Tao, H., Adams, C., 2008. Pass-go: a proposal to improve the usability of graphical passwords. Int. J. Netw. Secur. 2 (7), 273–292.

Thorpe, J., MacRae, B., Salehi-Abari, A., 2013. Usability and security evaluation of GeoPass: a geographic location-password scheme. In: Proceedings of the 9th Symposium on Useable Privacy and Security (SOUPS), pp. 1–14.

Weir, M., Aggarwal, S., Collins, M., Stern, H., 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of CCS, pp. 162–175.

Weka: Machine learning software in Java. https://www.cs.waikato.ac.nz/ml/weka/.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N., 2005. Passpoints: design and longitudinal evaluation of A graphical password system. Int. J. Hum. Comput. Stud. 63 (12), 102–127.

Yan, J., Blackwell, A., Anderson, R., Grant, A., 2004. Password memorability and security: empirical results. IEEE Secur. Priv. 2, 25–31.

Yang, Y., Guo, b., Wang, Z., Li, M., Yu, Z., Zhou, X., 2019. BehaveSense: continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Netw. 84, 9–18.

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W.T., Song, L., 2017. EvoPass: evolvable graphical password against shoulder-surfing attacks. Comput. Secur. 70, 179–198.

Zhao, X., Feng, T., Shi, W., Kakadiaris, I.A., 2014. Mobile user authentication using statistical touch dynamics images. IEEE Trans. Inf. Forensics Secur. 9 (11), 1780–1789.

Zheng, N., Bai, K., Huang, H., Wang, H., 2014. You are how you touch: user verification on smartphones via tapping behaviors. In: Proceedings of the 2014 International Conference on Network Protocols (ICNP), pp. 221–232.

Wenjuan Li obtained the Ph.D degree from the Department of Computer Science, City University of Hong Kong (CityU) in 2019. She received both *Research Tuition Scholarships* and *Outstanding Academic Performance Award* during her doctorate studies. Before, she was a lecturer in the Department of Computer Science, Zhaoqing Foreign Language College, China, and a Research Assistant in the Department of Computer Science, CityU from 2013 to 2014. She was a Winner of Cyber Quiz and Computer Security Competition, Final Round of Kaspersky Lab "Cyber Security for the Next Generation" Conference in 2014. Her research interests include network management and security, intrusion detection, spam detection, trust management, blockchain security, and E-commerce security.

Jiao Tan received his master degree in computer science from the University of Hong Kong, China. He is currently a senior engineer at KOTO Research Center. His research focuses on cyber physical security and IoT security.

Weizhi Meng is currently an assistant professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He received his B.Eng. degree in Computer Science from the Nanjing University of Posts and Telecommunications, China and obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. He was known as Yuxin Meng and prior to joining DTU, he worked as a research scientist in Infocomm Security Department, Institute for Infocomm Research, Singapore, and as a senior research associate in CityU. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. He also received the Best Paper Award from ISPEC 2018 and the Best Student Paper Award from NSS 2016 and Inscrypt 2019. His primary research interests are cyber security and intelligent technology in security including intrusion detection, smartphone security, biometric authentication, HCI security, cloud security, trust management, malware detection, blockchain in security, cyber-physical system security and IoT security. He is a senior member of IEEE.

Yu Wang received his Ph.D. degree in computer science from Deakin University, Victoria, Australia. He is currently an associate professor with the School of Computer Science, Guangzhou University, China. His research interests include network traffic analysis, mobile networks, social networks, and cyber security.