IARIA

The IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications (IARIA Congress 2022)

July 24, 2022 to July 28, 2022 - Nice, Saint-Laurent-du-Var, France

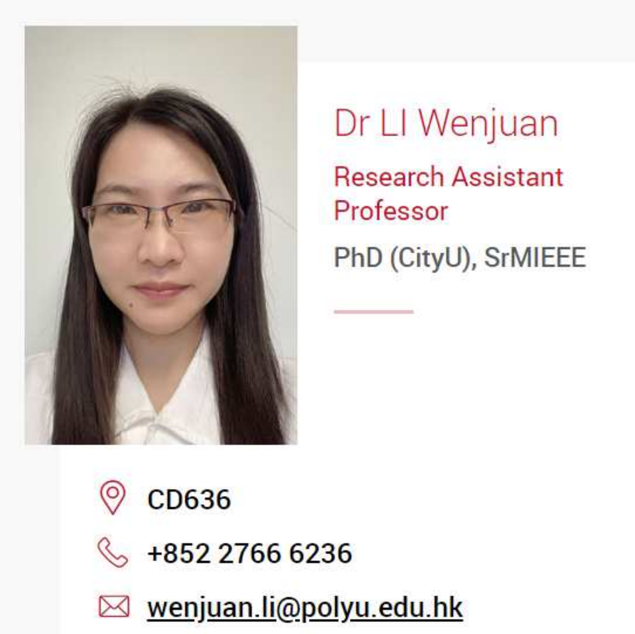
SwipeVLock: A Supervised Unlocking Mechanism Based on Swipe Behavior on Smartphones

Dr. Wenjuan Li (The Hong Kong Polytechnic University, Hong Kong SAR, China)

The Hong Kong Polytechnic University
香港理工大學

Opening Minds • Shaping the Future
啟迪思維・成就未來

About



Dr LI Wenjuan

Research Assistant Professor

PhD (CityU), SrMIEEE

📍 CD636

☎ +852 2766 6236

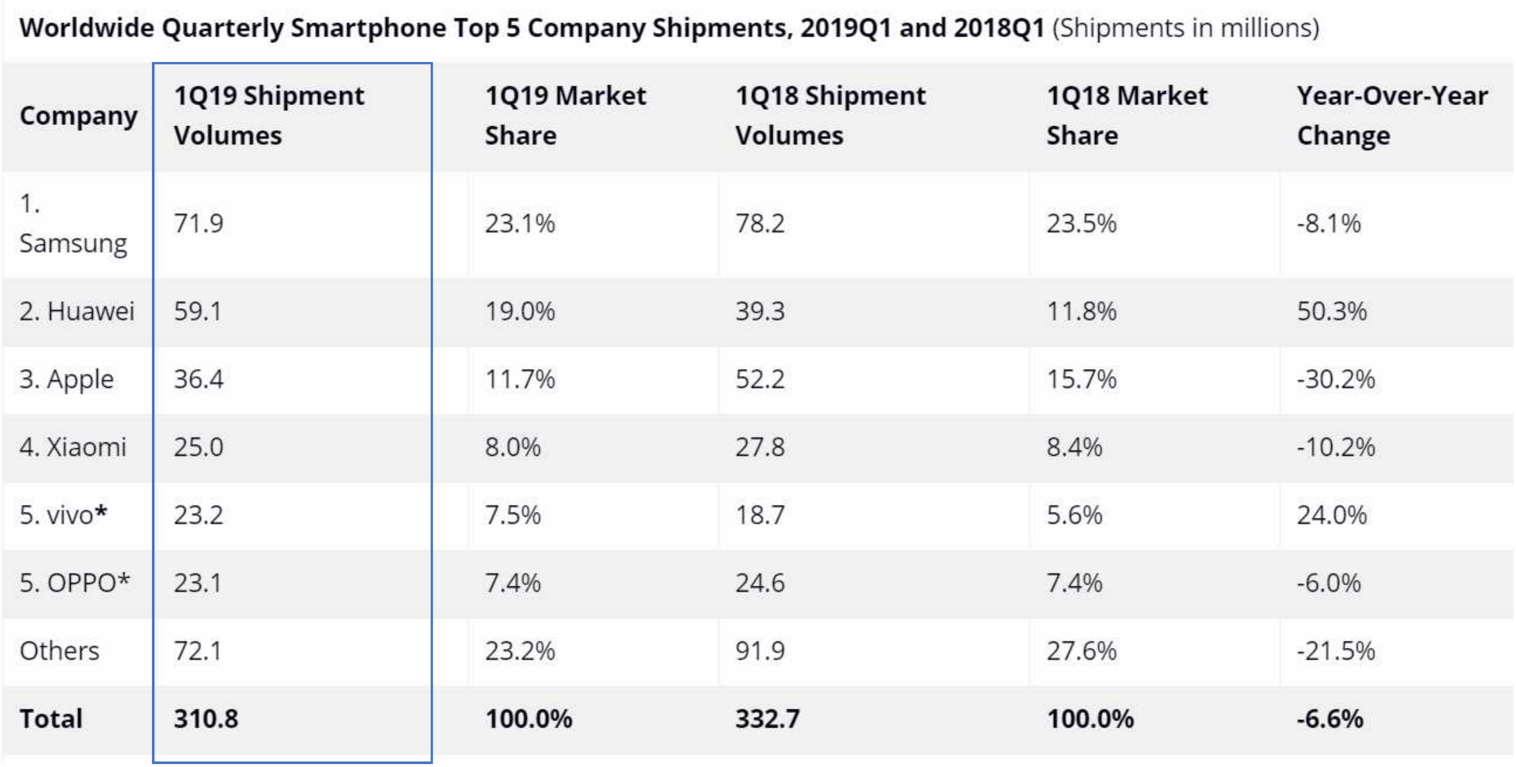
✉ wenjuan.li@polyu.edu.hk

My research interests include blockchain and cyber security, including intrusion detection, spam detection, trust management, biometric authentication, IoT security, and E-commerce security.

Outline

- Background and Motivations
- Our Approach - SwipeVLock
- User Study and Results
- Discussion
- Conclusion

Smartphone Shipments -- IDC



Worldwide Quarterly Smartphone Top 5 Company Shipments, 2019Q1 and 2018Q1 (Shipments in millions)

Company	1Q19 Shipment Volumes	1Q19 Market Share	1Q18 Shipment Volumes	1Q18 Market Share	Year-Over-Year Change
1. Samsung	71.9	23.1%	78.2	23.5%	-8.1%
2. Huawei	59.1	19.0%	39.3	11.8%	50.3%
3. Apple	36.4	11.7%	52.2	15.7%	-30.2%
4. Xiaomi	25.0	8.0%	27.8	8.4%	-10.2%
5. vivo*	23.2	7.5%	18.7	5.6%	24.0%
5. OPPO*	23.1	7.4%	24.6	7.4%	-6.0%
Others	72.1	23.2%	91.9	27.6%	-21.5%
Total	**310.8**	**100.0%**	**332.7**	**100.0%**	**-6.6%**

Sources: https://www.idc.com/getdoc.jsp?containerId=prUS45042319

Popularity of Smartphones

- Due to the capabilities and convenience, smartphones have been widely adopted by individuals.

- These devices have become a personal assistant, i.e., working as a social connection and work facilitator. A survey showed that nearly 40 percent of respondents play with their phones for three hours or more each day*.

- As modern smartphones can work like a mini-computer, users are willing to store personal data and complete sensitive tasks on the phones, such as personal photos, credit card information, transactions, etc.
  - **62 percent** of phone users in Denmark were using their phone for viewing bank account and online payment (Source: Global Mobile Consumer Survey 2017)
  - During the 2018 holiday season in the US, users purchased almost **40%** of all e-commerce products via a smartphone (Source: OuterBoxDesign)
  - **Up to 85%** of travellers use mobile devices to book travel activities (Source: Adweek)

*https://www.abc.net.au/news/science/2017-10-13/smartphone-survey-results-show-fascinating-differences-in-usage/9042184

Our Motivation – User Authentication

- Smartphones are becoming a more private device, cyber-criminals are always trying to exploit the stored data on smartphone.
- **User authentication mechanisms** become very important to protect phones from unauthorized access.

Textual Password

- Shoulder surfing
- Recording attack
- JFC Charging attack

Graphical Password

- Shoulder surfing
- Recording attack
- JFC Charging attack

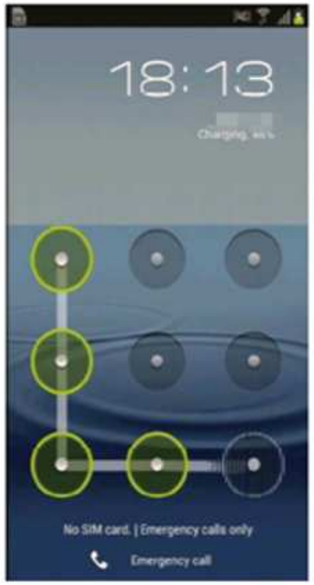
- Users have difficulty remembering their textual information for a long time due to the long-term memory (LTM) limitation.
- They are likely to choose and use weak textual passwords
- One-time verification

Biometric authentication

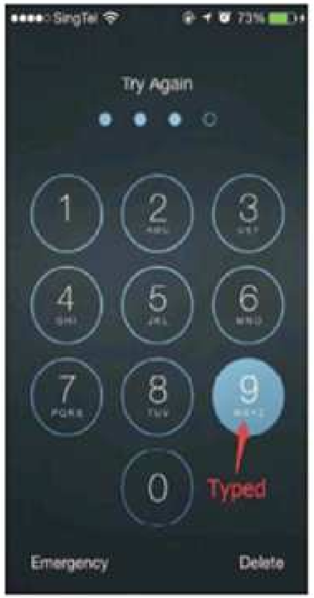
Physiological

Behavioral

Our Motivation – Phone Unlocking Mechanism



- Brute force attack
- ‘hot spot’ attack
- One-time verification



- Long-term memory (LTM) limitation.
- Easy to crack
- One-time verification

Android unlock patterns may be vulnerable to many attacks in real-world usage, as users can only choose a pattern with 4 dots at least and 9 dots at most. This makes Brute-force attack feasible because the total number of possible patterns is only 389,112.
Also, it suffers **recording attacks** and **charging attacks.**

Our Motivation - Biometric Authentication

Biometric authentication

Physiological

uses measurements from the human body

1. One-time verification
2. Additional hardware

Behavioral

use measurements from human actions

Continuous verification

No need for Additional hardware

1. False rate
2. Not Commercialized

State-of-the-Art

- There are many touch behavioral authentication schemes available in the literature, but how to design a behavioral authentication scheme for a long-term period still remains a challenge.

- Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunary, B., Jiang, Y., Nguyen, N.: Continuous mobile authentication using touchscreen gestures. In: Proc. of the 2012 IEEE Conference on Technologies for Homeland Security (HST), pp. 451- 456 (2012)
- Meng, Y., Wong, D.S., Schlegel, R, Kwok, L.-F.: Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. In: Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT), pp. 331-350, Springer, Heidelberg (2012)
- **Frank, M., Biedert, R., Ma, E.,Martinovic, I.,Song, D.: Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. IEEE Transactions on Information Forensics and Security 8(1), pp. 136-148 (2013)**

Algorithm Improvement

Refine Touch Actions (Swipe, Zoom)

Hybrid Scheme

Outline

- Background and Motivations
- Our Approach – **SwipeVLock**
- User Study and Results
- Discussion
- Conclusion

Our Contributions

- We design **SwipeVLock**, a phone unlocking scheme 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 additional hardware on smartphones. We also test several typical supervised learning algorithms for authentication.
- In the user study, **we involve a total of 30 common phone users to evaluate the performance of SwipeVLock**. Based on the collected data and users' feedback, it is found that our scheme can provide good usability in practice. **SwipeVLock can be considered as one alternative to complement existing solutions.**

Design of SwipeVLock (1)

- An ideal touch behavioral authentication scheme has to continuously monitor the behaviors and make an alert (or lock the phone) when any anomalies are detected. The high-level architecture of touch gesture-based authentication system is presented in Fig. 1.

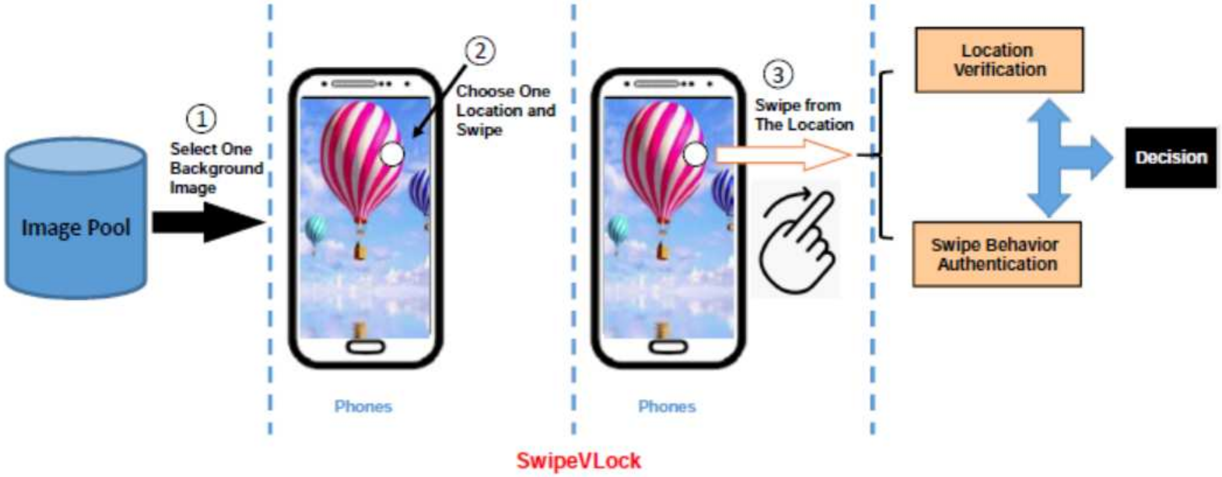


Image Pool
① Select One Background Image
② Choose One Location and Swipe
③ Swipe from The Location
Phones
Phones
Location Verification
Swipe Behavior Authentication
Decision
SwipeVLock

Figure 1. SwipeVLock: 1) Step1: select one background image from a pool; 2) Step2: choose one location on the background image; and 3) Step3: swipe from the selected location to unlock the phone.

Design of SwipeVLock (2)

- **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.

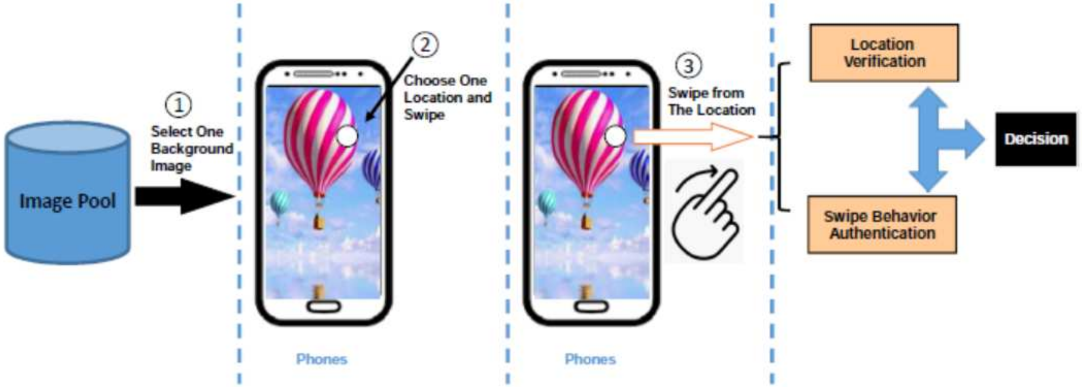


Image Pool
①
Select One Background Image
②
Choose One Location and Swipe
③
Swipe from The Location
Location Verification
Swipe Behavior Authentication
Decision
Phones
Phones

SwipeVLock

SwipeVLock Framework (1)

- Figure 2 depicts how to realize 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 swipe behavior, and compares it with the current swipe features. A decision will be output in the end.

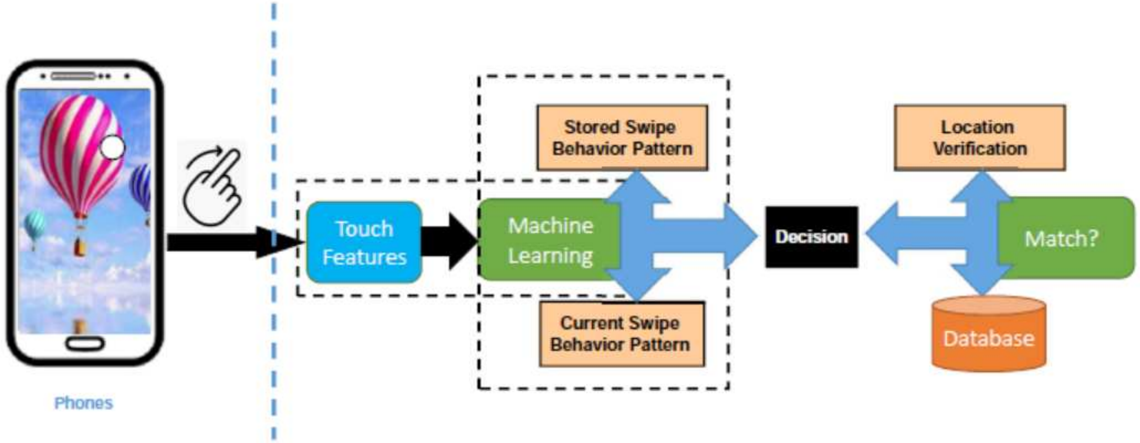


Fig. 2. Detailed authentication processes for SwipeVlock.

SwipeVLock Framework (2)

- 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 to a 21x21 pixel box around the selected location.**
- **This selection is based on the previous work like GeoPass.**

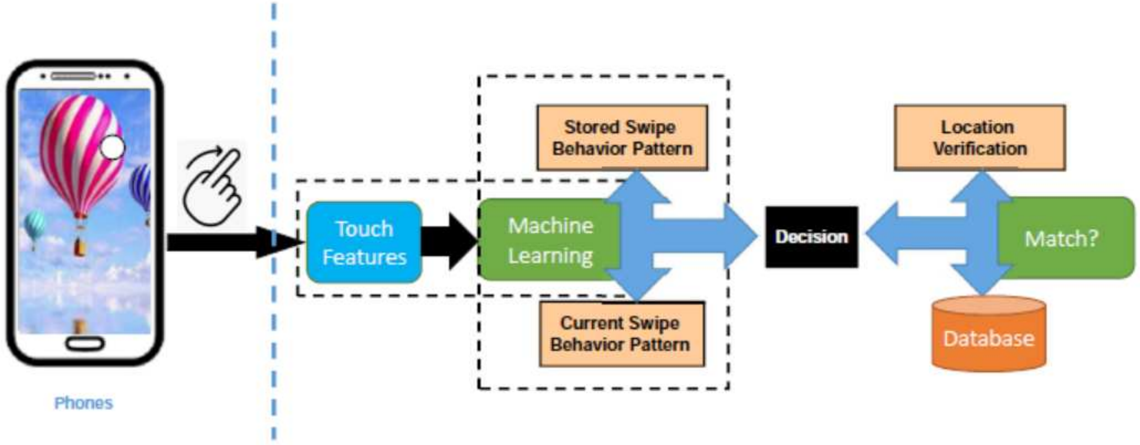


Fig. 2. Detailed authentication processes for SwipeVlock.

Swipe Features

- 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 identify 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 [24], 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).

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

Outline

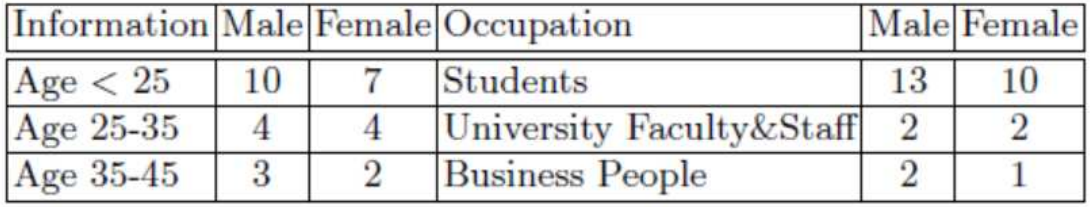
- Background and Motivations
- Our Approach - SocialAuth
- User Study and Results
- Discussion
- Conclusion

User Study – Methodology - 1

- To investigate the performance of our scheme, we perform a user study with 30 participants who are regular Android phone users.
- In particular, we have 17 males and 13 females who aged from 18 to 45. Most of them are students in addition to business people, university staff and faculty members. A $20 gift voucher was provided to each participant.

- Table 1 details the background information of participants.

Table 1. Participants information in the user study.



Information	Male	Female	Occupation	Male	Female
Age < 25	10	7	Students	13	10
Age 25-35	4	4	University Faculty&Staff	2	2
Age 35-45	3	2	Business People	2	1

User Study – Methodology - 2

- As mentioned in Figure 2, SwipeVLock uses supervised learning algorithms to help verify users. In this work, we consider the following classifiers as a study: **Decision tree (J48), Naive Bayes, SVM and Back Propagation Neural Network (BPNN)**. These are the typical and popular classifiers in the literature.

- To avoid any bias during classifier implementation, we adopted WEKA platform, which is an open-source machine learning collection in Java. We used the default settings for all classifiers in the 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 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. Then we randomly divided participants into two groups. In particular, Group-A was asked to perform the experiment in our lab, while the participants in Group-B could set their SwipeVLock in the lab and keep using the phone outside. Below are the detailed study steps.

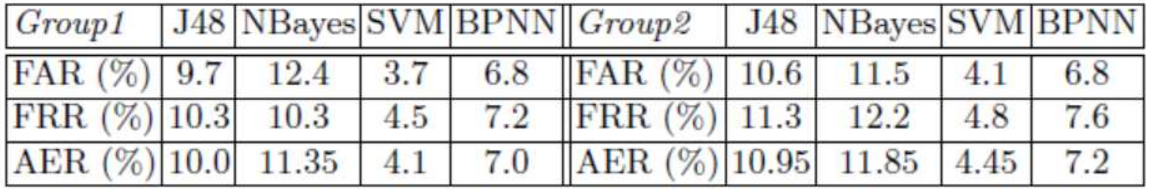
- Participants from both groups should follow the same steps shown as below:
  - Step 1. Creation phase: participants should create a password according to SwipeVLock' steps.
  - Step 2. Confirmation phase: participants should confirm the password by verifying both the image location and swipe behavior for 10 times (used for classifier selection). Participants could modified their credentials if they fail or want to change it.
  - Step 3. Distributed memory: participants were provided one paper-based finding tasks to distract them for 15 minutes.
  - Step 4. Login phase: participants should swipe to unlock the phone for 10 trials. The system recorded all the data for analysis.
  - Step 5. Feedback form: participants should complete a feedback form regarding password creation, confirmation and login.
  - Step 6. Retention. After three days, participants were asked to return and unlock the phone for 10 times in our lab.
  - Step 7. Participants have to finish another feedback from regarding our scheme usage.

Study Result (1)

- In the confirmation phase, we could collect 150 trials in the login phase for each Group1 and Group2. We used 60% of them as training data and the rest as testing data (with a cross-validation mode).

- The performance of different classifiers is depicted in Table 2.
- It is found that SVM could achieve a smaller error rate than other classifiers, i.e., it could reach an AER of 4.1% and 4.45% in Group1 and Group2, respectively. In contrast, BPNN could reach an AER of around 7%, while J48 & NBayes may cause an AER over 10%.

Table 2. The performance of different classifiers under different groups.

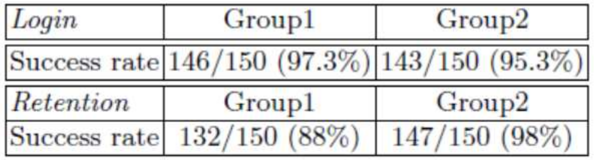


Group1	J48	NBayes	SVM	BPNN	*Group2*	J48	NBayes	SVM	BPNN
FAR (%)	9.7	12.4	3.7	6.8	FAR (%)	10.6	11.5	4.1	6.8
FRR (%)	10.3	10.3	4.5	7.2	FRR (%)	11.3	12.2	4.8	7.6
AER (%)	10.0	11.35	4.1	7.0	AER (%)	10.95	11.85	4.45	7.2

Study Result (2)

- In this case, we used SVM as the classifier in SwipeVLock. Table 3 shows the successful unlock trials for login phase and retention phase in Group1 and Group2.
  - Login phase. It is observed that participants in both groups could perform well with a success rate of 97.3% (Group1) and 95.3% (Group2), respectively. The errors were mainly caused by behavioral deviation, i.e., some participants may perform a swipe too fast.
  - Retention phase. After three days, it is found that participants in Group2 performed much better than those in Group1. This is because participants in Group2 could keep the phone and practice the unlocking behavior. Some participants reported that they might unlock the phone 16 times a day, making their swipe behavior more stable.

Table 3. Success rate in the login and retention phase for Group1 and Group2.



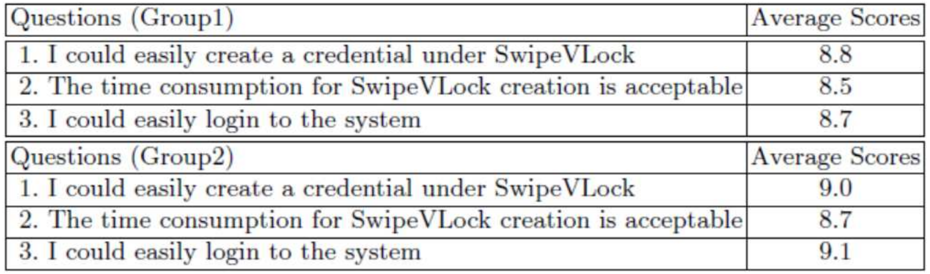
Login	Group1	Group2
Success rate	146/150 (97.3%)	143/150 (95.3%)
Retention	Group1	Group2
Success rate	132/150 (88%)	147/150 (98%)

*It is interesting to notice there are fewer errors caused by location selection, indicating that the error tolerance is suitable in practical usage. Further, our results validate that more practice can make the touch behavior more stable, which is in-line with the observations in previous work.

User Feedback

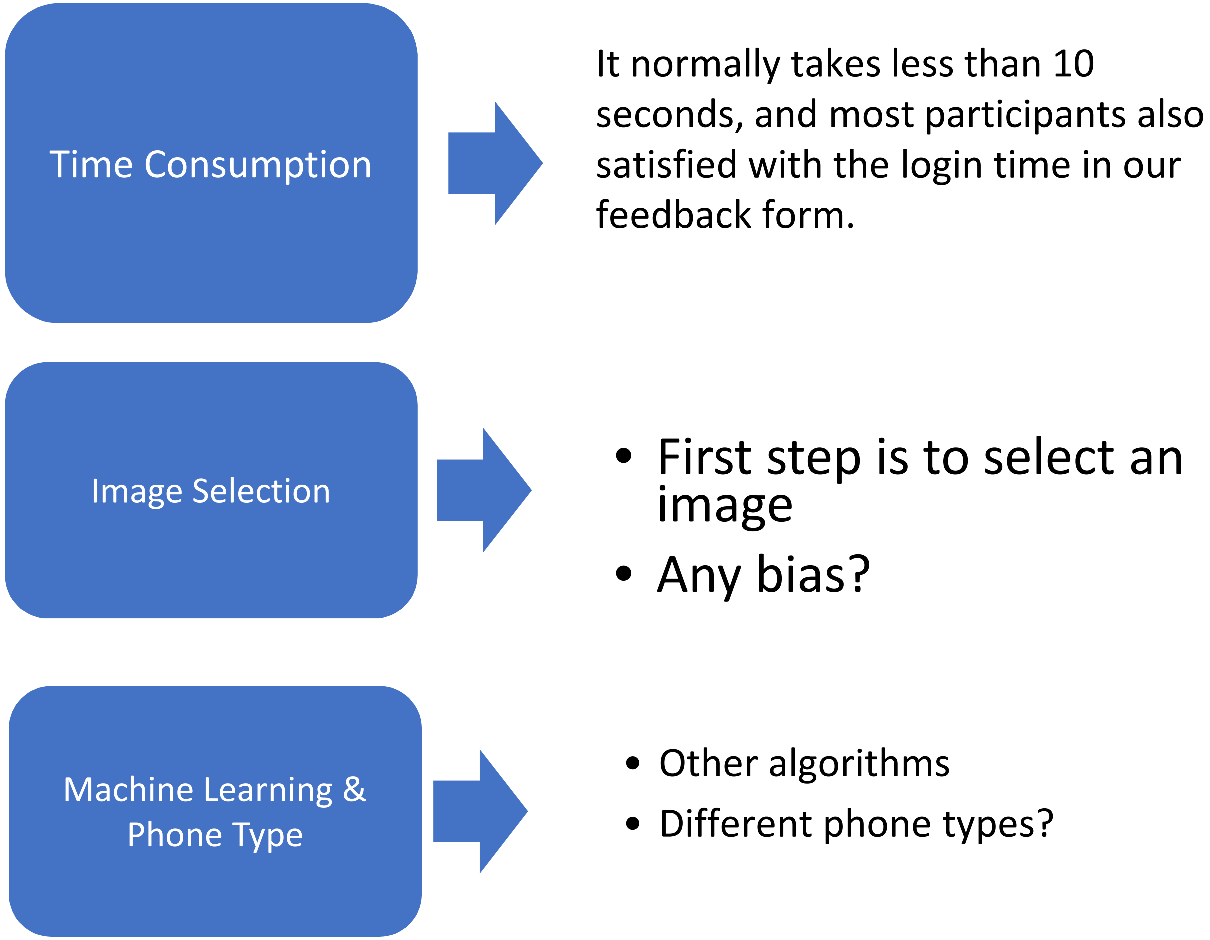
- During the study, we gave two feedback forms to each participant regarding the scheme usage. Ten-point Likert scales were used in each feedback question, where 1-score indicates strong disagreement and 10-score indicates strong agreement. Several key questions and scores are summarized in Table 4.
  - Group1. Most participants were satisfied with the usage of SwipeVLock, resulting in a score of over 8.5 on average for each question. We informally interviewed 10 of them, and they believed this is an easy-to-use unlock mechanism.
  - Group2. The participants in this Group2 provided a higher score than Group1, i.e., 9.1 vs. 8.7 for the third question. The reason may be due to that the participants in this group could keep the phone and try it for three days. We also informally interviewed 12 of them, and found that they had fun of using this mechanism. Most of them have an interest to use it in their own phones.

Table 4. Major questions and average scores received from the user study.



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

Discussion & Limitations - 1



Time Consumption

It normally takes less than 10 seconds, and most participants also satisfied with the login time in our feedback form.

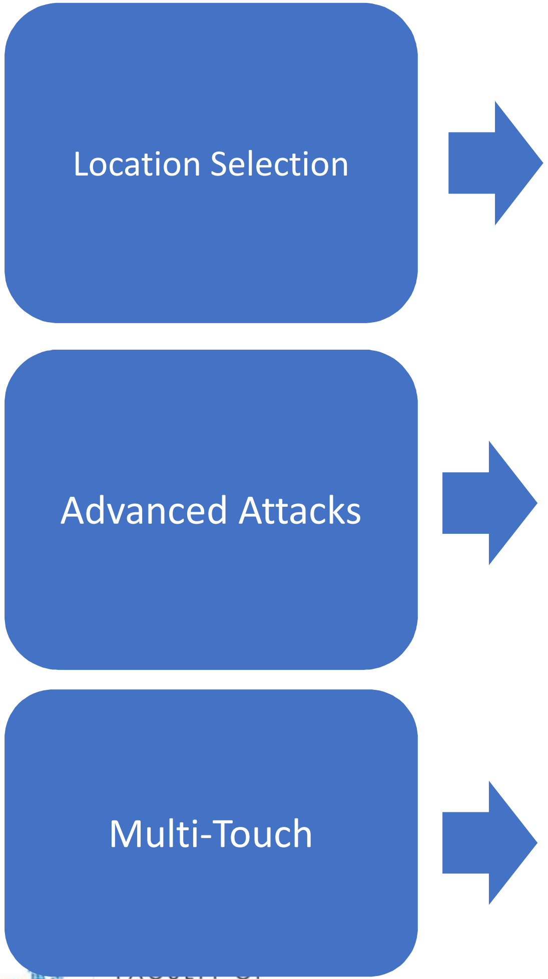
Image Selection

- First step is to select an image
- Any bias?

Machine Learning & Phone Type

- Other algorithms
- Different phone types?

Discussion & Limitations - 2



Location Selection

- The second step is to select a location
- Any bias?

Advanced Attacks

- Exploring the effect of recording attacks and mimic attack?

Multi-Touch

- How about two fingers?

Conclusion

- Unlock mechanisms like Android unlock patterns are an important security tool to protect smartphones from unauthorized access, but attackers can still compromise the phone via various attacks like shoulder surfing, recording attacks and charging attacks. As a result, there is an increasing need to enhance the security of unlock mechanisms.

- In this work, motivated by this issue, we develop SwipeVLock, a swipe behavior-based unlock scheme with a supervised framework on smartphones, which requires users to choose one background image and a location to perform a swipe action. A successful trial should have both successful location selection and swipe verification.

- In our user study, we involved a total of 30 participants and investigated their performance like success rate. Our results demonstrate that participants could reach a success rate of 98% in the best scenario. Most participants also provide positive feedback on the practical usage of SwipeVLock.

Q&A

If you have any question, you can contact via

wenjuan.li@polyu.edu.hk