POSTER: Rethinking Fingerprint Identification on Smartphones

Seungyeon Kim
Yonsei University
Seoul, Korea
tribunus000@yonsei.ac.kr

Hoyeon Lee
Yonsei University
Seoul, Korea
yeoni_2@yonsei.ac.kr

Taekyoung Kwon*
Yonsei University
Seoul, Korea
taekyoung@yonsei.ac.kr

ABSTRACT

Modern smartphones popularly adopt a small touch sensor for fingerprint identification of a user, but it captures only a partial limited portion of a fingerprint. Recently we have studied a gap between actual risk and user perception of latent fingerprints remaining on a smartphone, and developed a fake fingerprint attack that exploits the latent fingerprints as actual risk. We successfully reconstructed a fake fingerprint image in good quality for small touch sensors. In this paper, we subsequently conduct post hoc experimental studies on the facts that we have missed or have since learned. First of all, we examine that the presented attack is not conceptual but realistic. We employ the reconstructed image and make its fake fingerprint, using a conductive printing or a silicon-like glue, to pass directly the touch sensor of real smartphones. Our target smartphones are Samsung Galaxy S6, S7 and iPhone 5s, 6, 7. Indeed we have succeeded in passing Galaxy S6, S7, and now work on the remaining smartphones. We also conduct an experimental study for one of our mitigation methods to see how it can reduce actual risk. Finally, we perform a user survey study to understand user perception on the fake fingerprint attacks and the mitigation methods.

KEYWORDS

smartphone; smudge; fingerprint spoofing; user perception

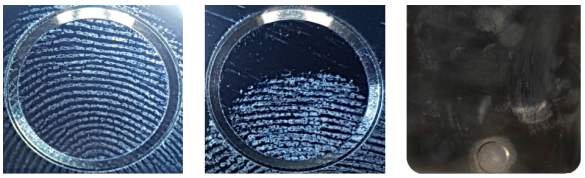
1 INTRODUCTION

Fingerprint identification is widely adopted in today's smartphones because of its convenience and believed-safety for device unlocking, and this trend is expected to continue in the future. One of the problems in fingerprint identification on smartphones is that the touch sensor used here is very small — it is capable of capturing only a partial limited portion of a fingerprint. Accordingly, various methods of manufacturing counterfeit fingerprints and passing the small touch sensors have been disclosed [2, 4, 7], but they commonly required a firm impression of a target user's fingerprint or its clear image in a good condition — unrealistic in a sense of attacks.

Lately, aiming at realistic attacks, we studied a fake fingerprint attack called SCRAP, which exploits only smudges and latent fingerprints remaining on a smartphone, i.e., without requiring the firm impression of a user, and successfully showed to reconstruct a fake fingerprint image in good quality for small touch sensors [5].

*Corresponding author.

CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA.
 ISBN 978-1-4503-4946-8/17/10.
DOI: https://doi.org/10.1145/3133956.3138832



(a) (b) (c)

Figure 1: Touch ID and smudges. (a) Full submission (passed with a partial portion of a fingerprint) (b) Half submission (surprisingly also passed with only a half of the partial portion) (c) Daily smudges remaining on a smartphone.

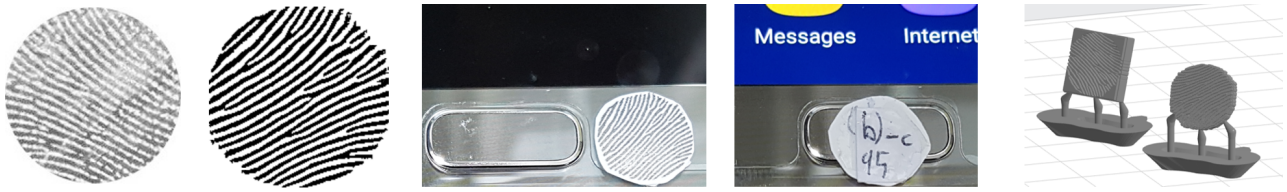
However, the question still remains: Is it possible for the SCRAP attack to pass small touch sensors of real smartphones?

In this paper, to explore the answers, we subsequently conduct post hoc experimental studies on the facts that we have missed or have since learned. As pictured in Figure 1, we found that only a half submission of a partial fingerprint successfully passed Touch ID as in Figure 1-(b), while latent fingerprints were easily detected from daily smudges as in Figure 1-(c). After reviewing the SCRAP attack, we proceed with real attack experiments against real smartphones, such as Galaxy (Samsung Galaxy) S6, S7 and iPhone 5s, 6, 7, and examine our mitigation methods as well experimentally. Finally, we perform a user survey study to understand user perception on the fake fingerprint attacks and the mitigation methods.

2 SCRAP ATTACK (ACSAC'17)

We briefly review our recent work [5] about the fake fingerprint attack that directly exploits latent fingerprints remaining on a smartphone. We call our attack SCRAP. The basic idea of SCRAP was to exploit fingerprint smudges left on a home button (as a key index of an authentic fingerprint) and more smudges [1] left on a touch screen (as a richer source of the authentic fingerprint) of a smartphone exposed to a daily use. There were several challenges to implement this idea. One was to examine the user's behavior whether the same finger is used for activities on both home button and touch screen. Another was to technically reconstruct an image of an authentic fingerprint in good quality, only from the messy smudges found as above. The other was to measure the quality of the reconstructed image for verification of the success in our attack.

To investigate user's touch behavior and perception gap, we conducted in-person surveys involving 82 participants. The survey results showed that the fingers most frequently used on the touch screen and the home button are the same, and the user's risk perception is very low. To reconstruct an authentic fingerprint image from messy smudges, we used domain knowledge of image processing and succeeded in reconstruction experiments that involve seven users in six conditions. The procedure of SCRAP includes (1) photographic smudge collection, (2) fingerprint smudge matching that



(a) (b) (c) (d) (e)

Figure 2: Attack experiments. (a) Fingerprint image produced by the SCRAP attack [5]. (b) Submission image: (a) was flipped and reversed, and then SourceAFIS was applied for enhancement. (c) Printed image of (b) with an AgIC conductive ink on the conductive paper (width 9.5mm). (d) Fake submission to Galaxy S7 with the printed image: The printed image was turned over and put on the touch sensor. As a result, the smartphone was successfully unlocked. (e) 3D modeling of the SCRAP images.

involves image preprocessing and SIFT-based matching, (3) image quality assessment that involves damage identification and correction decision, and (4) fingerprint image construction that involves image postprocessing for quality improvement. We measured the quality of the reconstructed image with regard to minutiae quality, match scores, and fingerprint image quality (NFIQ) under the domain of NIST Biometric Image Software (NBIS).

3 EXPERIMENTAL STUDY

We conduct the post hoc experimental study of the SCRAP attack using various materials and strategies on commodity smartphones. Our target devices include Galaxy S6, S7 and iPhone 5s, 6, 7 in our experiments. We asked a target user to enroll the fingerprint. To perform real attack experiments, we examined the well-known fingerprint spoofing techniques that actually required a firm impression of a fingerprint, and employed such experimental settings. They include forgery techniques using wood glue [6], conductive printing [2], and mold combining of hot glue and wood glue [7]. We apply the fingerprint image reconstructed by SCRAP to such settings. Figure 2 and Table 1, respectively, show the results in progress of our experiments. To form fake fingerprints, we use polyvinyl acetate emulsion and EPSON L361 printer (AgIC conductive ink and AgIC special paper) in each experiment scenario.

3.1 Conductive Printing

In 2016, Cao et al. [2] showed that a conductive printing is a potential forgery method for attacking smartphone touch sensors. They used AgIC conductive ink and AgIC special paper to print out a firm impression of a fingerprint, and used the print as a fake fingerprint for their attack. They claimed that this method is much faster and more consistent than conventional forgery methods using wood glue. They conducted experiments with Galaxy S6 and Huawei Honor 7 to prove the effectiveness of the proposed method. However, Cao et al. required that a firm impression of a fingerprint must be provided or scanned from the target user, for their attack.

In our experiment, we adopted the Cao et al.'s conductive printing method for the SCRAP image reconstructed by our attack. The forgery procedure is as follows. First of all, we follow the procedure of the SCRAP attack, as summarized in Section 2, and prepare a reconstructed SCRAP image, e.g., as shown in Figure 2-(a). For conductive printing, we flip horizontally the SCRAP image and reverse its black/white color, so as to directly submit the print-out to a touch sensor. Before printing, we reform the reverse image with SourceAFIS library [9] for improvement. Finally, we print out the image using AgIC conductive ink and AgIC special paper.

Figures 2-(a) to (c) show a forgery example of the SCRAP image. We then turn over the printed image and put it on the touch sensor of Galaxy S6 and S7, as shown in Figure 2-(d). We successfully unlocked the target smartphones with the conductive print-out of the SCRAP image. Figure 3-(a) shows that three participants unlocked Galaxy S7 using the print-out of the SCRAP attack without difficulties, i.e., in one or two attempts.

We additionally conducted a half submission experiment, as we described in Figure 1, for the same target devices with participant P1. We asked P1 to submit only a half of the print-out for unlocking, and as shown in Figure 3-(b), P1 unlocked Galaxy S7 in two or four attempts. Since Galaxy S6 and S7 allow up to 14 times in the first hour (37 times in the first 24 hours) along the failed attempts, our attack is definitely actual risk to Samsung Galaxy series.

Unfortunately, we found that the conductive printing methods failed against iPhone series even with a firm impression. Thus, we move on to the wood glue method for iPhones.

Table 1: Summary of attack experiments.

Material	Source	Success
Conductive printing	Firm impression	Galaxy S6, S7
	SCRAP image	Galaxy S6, S7
Silicon-like glue	Firm impression	iPhone 5s, 6, 7 Galaxy S6, S7
	SCRAP image	in progress

3.2 Wood Glue and 3D Printing

Wood glue is a widely-used forgery material for fingerprint spoofing attacks. We also verified that wood glue can be used with a firm impression of a fingerprint to bypass Touch ID of iPhones, as summarized in Table 1. We asked a participant to firmly press a candle-based mold, so that the fingerprint is taken in good quality, and put wood glue onto the mold. We then obtained the forged fingerprint in silicon-like form, and successfully passed the touch sensors of both iPhone 5s, 6, 7 and Galaxy S6, S7 by exploiting it. Thus, to adopt the SCRAP image in this attack setting, we need to build a mold based on the SCRAP image. For the purpose, we are working on 3D modeling and printing of a fake 3D fingerprint and we will use the 3D printout to make a candle-based mold. Figure

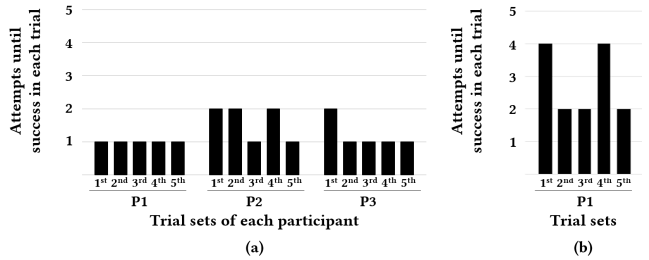


Figure 3: Attack experiment results: Conductive printing of the SCRAP image was exploited against Galaxy S7. (a) Unconstrained full submission of the conductive printing was asked to three participants. (b) Half submission was asked to P1.

2-(e) shows a modeling example of the SCRAP image. Finally, we plan to put wood glue onto the mold again.

4 MITIGATION

To mitigate the forgery problems we raised above, a touch sensor must be able to obtain a larger area of user's fingerprint. Interestingly, Apple, Samsung, and many other manufacturers have a plan to introduce the under-screen touch sensor, which enables a larger sensor under the touch screen. For instance, Apple recently patented under-screen fingerprint recognition systems that use acoustic imaging [3] or conductive scanning [8], expected to be an alternative to the futuristic Face ID of iPhone X.

With this trend, we proposed a mitigation method assuming the under-screen touch sensor as shown in Figure 4, and its appearance is a slight modification of the slide bar which was used in the previous iPhone models [5]. We may expect many users are already familiar with such an interface. The user is asked to unlock iPhone by sliding the circle to left or right. When a user touches the circle, the under-screen touch sensor will read the fingerprint. The swiping action required to slide the bar will then remove the fingerprint smudge on the touch sensor as shown in Figure 4-(d). We also proposed to read the remaining smudges, as shown in Figure 5-(c) and (f), to distinguish a real fingerprint from a fake fingerprint.

5 CONCLUSION

We performed post hoc experimental studies regarding the SCRAP attack [5], which has been introduced recently as a practical attack to circumvent fingerprint identification on smartphones, and the following mitigation method. We have validated prior fingerprint spoofing techniques to evaluate the practical effectiveness of the SCRAP attack. Based on the previous work, we attempted to construct a methodology for deceiving smartphone fingerprint biometrics by combining proven methods and new methods with SCRAP techniques. Our mitigation method assumed an adoption of under-screen touch sensors, of which the adaptation is expected in the near future [3, 8]. So, we also performed a small experiment to see its effect on a touch screen.

We plan to conduct a survey study to understand user perception of the fake fingerprint attacks and the mitigation methods. The procedure of this survey is as follows. First, we ask users if latent fingerprints remaining on a smartphone is perceived as actual risk.

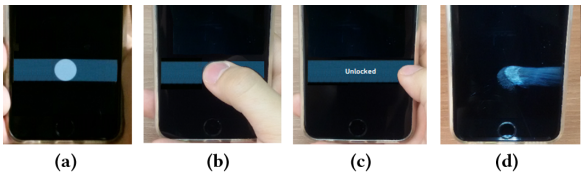


Figure 4: Mitigation concept assuming under-screen sensors. (a) Slide bar (b) Pressing (c) Sliding (d) Smudge.

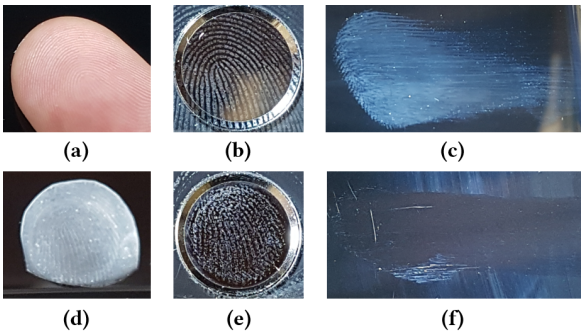


Figure 5: Comparison of actual and fake fingerprint smudges. (a) Actual finger (b) Smudge after Touch ID unlock action with actual finger. (c) Smudge after Slide Touch ID unlock action with actual finger. (d) Wood glue fake finger. (e) Smudge after Touch ID unlock action with fake finger. (f) Smudge after Slide Touch ID unlock action with fake finger.

We then show the SCRAP attack is possible and ask users again about possible changes in their perception. Finally, we introduce our mitigation method and let participants try our prototype, and ask them about acceptance of the mitigation method.

ACKNOWLEDGMENTS

This work was partly supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00380), and also by the MSIT under the ITRC (Information Technology Research Center) support program (IITP-2017-2016-0-00304) supervised by the IITP.

REFERENCES

[1] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In *Proceedings of WOOT '10*, Vol. 10. 1–7.
[2] Kai Cao and Anil K. Jain. 2016. *Hacking mobile phones using 2D printed fingerprints.* Technical Report. Department of Computer Science and Engineering, Michigan State University.
[3] Eric Decoux and Patrick Bovey. 2017. Marking comprising two patterns on a surface. (Aug. 2017). US Patent 9,747,473.
[4] JLaservideo. 2016. *How To Copy a Fingerprint Like a Spy - iPhone Touch ID Hack!!!* https://www.youtube.com/watch?v=bp-MrrAmprA.
[5] Hoyeon Lee, Seungyeon Kim, and Taekyoung Kwon. 2017. Here is your fingerprint! actual risk versus user perception of latent fingerprints and smudges remaining on smartphones. In *Proceedings of ACSAC '17.*
[6] Marc Rogers. 2014. *Hacking Apple TouchID on the iPhone 6.* https://www.youtube.com/watch?v=GPLiEC_tG1k.
[7] Oki Rosgani. 2013. *faking the Apple trackID fingerprint sensor.* https://www.youtube.com/watch?v=qjRD8_ZoGuE.
[8] Dale R Setlak. 2017. Electronic device including finger biometric sensor carried by a touch display and related methods. (Feb. 2017). US Patent 9,582,102.
[9] Robert Važan. 2017. *SourceAFIS.* https://sourceafis.angeloflogic.com/.