Hacking Mobile Phones Using 2D Printed Fingerprints

Kai Cao and Anil K. Jain
Department of Computer Science and Engineering
Michigan State University
East Lansing, Michigan 48824
Biometrics.cse.msu.edu
February 19, 2016

Fingerprint is the most popular biometric trait due to the perceived uniqueness and persistence of friction ridge pattern on human fingers [1]. Following the introduction of iPhone 5S with Touch ID fingerprint sensor in September 2013, most of the mobile phones, such as iPhone 5s/6/6+, Samsung Galaxy S5/S6, HTC One Max, Huawei Honor 7, Meizu MX4 Pro and others, now come with embedded fingerprint sensors for phone unlock. It has been forecasted that 50% of smartphones sold by 2019 will have an embedded fingerprint sensor [2]. With the introduction of Apple Pay, Samsung Pay and Android Pay, fingerprint recognition on mobile devices is leveraged for more than just for device unlock; it can also be sued for secure mobile payment and other transactions.

Despite growing usage and claimed security of fingerprint recognition for mobile unlock and payment, spoofing attacks on the embedded fingerprint systems have not been investigated in detail. Spoofing refers to the process where the fingerprint image is acquired from a fake finger (or gummy finger) rather than a live finger. Just a few days after iPhone 5S was released, Germany's Chaos Computer Club[1] hacked the capacitive sensor built in the phone by lifting a fingerprint of the genuine user off a glass surface and then making a spoof fingerprint[2]. A similar spoofing technique was also used to successfully attack Samsung Galaxy S6[3]. The main steps of this attack are summarized as follows:

1) Photograph the fingerprint of the genuine user;
2) Print the fingerprint on a transparent sheet with a thick toner setting;
3) Create a "spoof fingerprint" (we referred to it as a 2.5D fingerprint) using latex milk or white wood glue.

There are two limitations of above method of hacking mobile fingerprint reader: (i) the spoof is fabricated manually, where the hacker experience may affect the quality of spoof fingerprint and the accuracy of spoof attack, and (ii) it takes significant amount of time to create a spoof; for example, wood glue takes around 20~30 minutes to get dry. This report presents a simple yet effective method for spoofing the fingerprint sensor embedded in a mobile phone using a 2D fingerprint image printed on a special paper. The spoof fingerprint is generated automatically. The main steps of our process are summarized as follows.

1) Install three AgIC[4] silver conductive ink cartridges (Figure 1 (a)) as well as a normal black ink cartridge in a color inkjet printers (Brother MFC-J5910DW printer was used by us); better conductivity can be achieved if a brand new (unused) printer is used;
2) Scan the target fingerprint image (of the authorized user) at 300 dpi or higher resolution;

[1] https://www.ccc.de/en/
[2] http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked
[3] http://www.cnet.com/news/samsung-galaxy-5-fingerprint-scanner-thwarted-by-hack/
[4] https://agic.cc/en

3) Mirror (reverse the image in the horizontal direction) and print the original or binarized fingerprint image on the glossy side of an AgIC special paper (Figure 1 (b)).

Once the printed 2D fingerprints are ready (Figure 2), we can then use them for spoofing mobile phones. In our spoofing experiment, we selected Samsung Galaxy S6 and Huawei Hornor 7 phones as examples. We enrolled the left index finger of one of the authors and used the printed 2D fingerprint of this left index finger to unlock the fingerprint recognition systems in these phones. Figures 3 and 4 show that the proposed spoof can successfully unlock Samsung Galaxy S6 and Huawei Honor 7, respectively. The videos illustrating the spoofing process for Samsung Galaxy S6 and Huawei Honor 7 are available here[5]. We tried several fingers of different subjects and all of them can successfully hack these two phones. But, Huawei Honor 7 is slightly more difficult to hack (more attempts may be required) than Samsung Galaxy S6.

(a) (b) (c)

Figure 1. Spoof creation. (a) Three AgIC silver conductive ink cartridges, (b) Brother MFC-J5910DW printer, and (c) AgIC special paper.

(a) (b) (c)

Figure 2. Examples of spoof. (a) Finger used for enrollment, (b) and (c) 2D printed fingerprint images for hacking Samsung S6 and Huawei Hornor 7, respectively. Note that (c) was cropped from (b) to have the same size as the

[5] https://youtu.be/fZJI_BrMZXU

fingerprint sensor of Huawei Hornor 7. AgIC silver ink marker was used to mark the periphery of the images to increase the conductivity.

Figure 3. Unlocking Samsung Galaxy S6 using a printed 2D fingerprint image in Figure 2 (b).

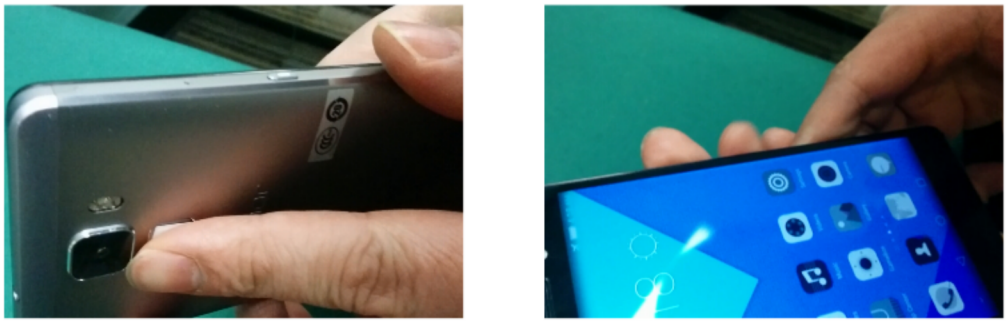

Figure 4. Unlocking Huawei Honor 7 using a printed 2D fingerprint image in Figure 2 (c).

In summary, we have proposed a simple, fast and effective method to generate 2D fingerprint spoofs that can successfully hack built-in fingerprint authentication in mobile phones. Furthermore, hackers can easily generate a large number of spoofs using fingerprint reconstruction [3] or synthesis [4] techniques which is easier than 2.5D fingerprint spoofs. This experiment further confirms the urgent need for anti-spoofing techniques for fingerprint recognition systems [5], especially for mobile devices which are being increasingly used for unlocking the phone and for payment. It should be noted that not all the mobile phones can be hacked using proposed method. As the phone manufactures develop better anti-spoofing techniques, the proposed method may not work for the new models of mobile phones. However, it is only a matter of time before hackers develop improved hacking strategies not just for fingerprints, but other biometric traits as well that are being adopted for mobile phones (e.g., face, iris and voice).

References

[1] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Second Edition, Springer, 2009

[2] http://www.marketresearch.com/Research-Capsule-v4026/Fingerprint-Sensors-Smart-Mobile-Devices-8918844/

[3] K. Cao and A. K. Jain, Learning Fingerprint Reconstruction: From Minutiae to Image, *IEEE Trans. Inf. Forens. & Security*, 10(1): 104-117, 2015.

[4] Q. Zhao, A. K. Jain, N. G. Paulter and M. Taylor, Fingerprint Image Synthesis based on Statistical Feature Models, *IEEE Conf. Biometrics, Technology* & Systems (BTAS), Washington, D.C., 2012

[5] E. Marasco and A. Ross, "A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems," *ACM Computing Surveys*, Vol. 47, No. 2, Article 28, January 2015.