Using Facial Behavior Biometric Modalities for Smartphone Authentication

Guixin Ye[†], Zhanyong Tang[*,†], Dingyi Fang[†], Xiaojiang Chen[†], Kwang In Kim[‡], Ben Taylor[§], and Zheng Wang[*,§]
[†]School of Information Science and Technology, Northwest University, China
Email: gxye@stumail.nwu.edu.cn, {zytang, dyf, xjchen}@nwu.edu.cn
[‡]Department of Computer Science, University of Bath, UK
Email: k.kim@bath.ac.uk
[§]School of Computing and Communications, Lancaster University, UK
Email: {b.d.taylor, z.wang}@lancaster.ac.uk

***Abstract*—Pattern lock is widely used as a mechanism for authentication and authorization on Android devices. This paper presents a novel video-based attack to reconstruct Android lock patterns from video footage filmed using a mobile phone camera. Unlike prior attacks on pattern lock, our approach does not require the video to capture any content displayed on the screen. Instead, we employ a computer vision algorithm to track the fingertip movements to infer the pattern. Using the geometry information extracted from the tracked fingertip motions, our approach is able to accurately identify a small number of (often one) candidate patterns to be tested by an adversary. We thoroughly evaluated our approach using 120 unique patterns collected from 215 independent users, by applying it to reconstruct patterns from video footage filmed using smartphone cameras. Experimental results show that our approach can break over 95% of the patterns in five attempts before the device is automatically locked by the Android operating system. We discovered that, in contrast to many people's belief, complex patterns do not offer stronger protection under our attacking scenarios. This is demonstrated by the fact that we are able to break all but one complex patterns as opposed to 60% of the simple patterns in the first attempt. Since our threat model is common in day-to-day life, this paper calls for the community to revisit the risks of using Android pattern lock to protect sensitive information.**

I. Introduction

1. Smartphone is easily lost or stolen by an attacker as its small size. This may result in privacy leakage and finance lost. It is reported by lookout.com that nearly $2.5 billion worth of devices were lost or stolen in 2011[1].

2. Human face plays an important role in our social interaction. As compared with other biometric modalities such as fingerprint and iris, face recognition has distinct advantages because of its non-contact process. Face images could be captured from a distance without touching person being identified and identification does not require interaction with person. In addition, face recognition serves crime deterrent purpose because face images that have been recorded and archived could later help identify a person.

3. Human identification system based on biometrics other than the face have already led to commercial products with very high identification rates: the iris [2] and fingerprints [3] can be cited as example. However, these systems are not always appreciated by users, as they require some close interaction with the machine often perceived as invasive. Moreover, they require the user to stop at the device and be cooperative, which is acceptable for access control to restricted areas, but not for other applications like surveillance. Face recognition may overcome some of these limitations.

4. Challenges in face recognition arise because the face is not a rigid object and images can be taken from many different viewpoints of the face.

5. Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, thses methods examine an individual's physiological and/or behavioral characteristics in order yo determine and/or ascertain his identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged.

Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioral traits (such as gait, signature and keystroke dynamics). Face recognition appears to offer several advantages over other biometric methods as follows:

1) Almost all these technologies require some voluntary action by the user, i.e., the user needs to place his hand on a hand-rest for fingerprinting or hand geometry detection and has to stand in a fixed position in front of a camera for iris or retina identification. However, face recognition can be done passively without any explicit

*Corresponding authors: Zhanyong Tang and Zheng Wang

NDSS '17, 26 February -1 March 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2017.23xxx

action or participation on the part of the user since face images can be acquired from a distance by a camera. This is particulary beneficial for security and surveillance purposes.

2) Data acquisition in general is fraught with problems for other biometrics: techniques that rely on hands and fingers can be rendered useless if the epidermis tissue is damaged in some way (i.e., bruise or cracked). Iris and retina identification require expensive equipment and are much too sensitive to any body motion. Voice recognition is susceptible to background noises in public places and auditory fluctuations on a phone line or tape recording. Signatures can be modified or forged. However, facial images can be easily obtained with a couple of inexpensive fixed cameras.
3) Good face recognition algorithms and appropriate preprocessing of the images can compensate for noise and slight variations in orientation, scale and illumination.
4) Technologies that require multiple individuals to use the same equipment to capture their biological characteristics potentially expose the user to the transmission of germs and impurities from other users. However, face recognition is totally non-intrusive and does not carry any such health risks.

ACKNOWLEDGEMENTS

We would like to thank all participants who help for completing the experiments. Thank all volunteers for their time and insights as well as the anonymous reviewer for their critical and constructive comments. This work was supported by NSFC (Grant No. 61672427) and the UK Engineering and Physical Sciences Research Council (Grants No. EP/M01567X/1(SANDeRs) and EP/M015793/1(DIVIDEND)).

REFERENCES

[1] "Lookout inc." https://www.lookout.com/resources/reports/mobilelostand-found/billion-dollar-phone-bill, 2012.
[2] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE transactions on pattern analysis and machine intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.
[3] R. R. Rogers, "Biometric identification systems: The science of transaction facilitation," in *SPIE's 1994 International Symposium on Optics, Imaging, and Instrumentation*. International Society for Optics and Photonics, 1994, pp. 194–199.