Cracking Android Pattern Lock in Five Attempts

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

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].

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.

*Corresponding authors: Zhanyong Tang and Zheng Wang

NDSS '17, 26 February -1 March 2017, San Diego, CA, USA
Copyright 2017 Internet Society, ISBN 1-891562-41-X
http://dx.doi.org/10.14722/ndss.2017.23xxx