POSTER: Breaking the Android Pattern Lock Screen with Neural Networks and Smudge Attacks

Panagiotis Andriotis*
University of Bristol, MVB,
Bristol, BS8 1UB, U.K.
p.andriotis@bristol.ac.uk

Theo Tryfonas
University of Bristol, QB,
Bristol, BS8 1TR, U.K.
theo.tryfonas@bristol.ac.uk

Zhaoqian Yu
University of Bristol, MVB,
Bristol, BS8 1UB, U.K.
zy13643.2013@my.bristol.ac.uk

ABSTRACT

The Android pattern lock screen is a popular mechanism offered for user authentication on smartphones and tablets. It is a graphical password scheme that provides usability and memorability. Despite the wide password space of the mechanism, there exist well-known techniques (such as smudge attacks) questioning its security strengths. With this study we aim to demonstrate that if we use previous knowledge, which describes the results of biased password input, in addition to a method that extracts traces of residues from a mobile device screen, we will be able to develop a lightweight automated tool capable to predict the user's chosen password.

Categories and Subject Descriptors

D.4.6 [**Software**]: Operating Systems—*Security and Protection*

General Terms

Security, Human Factors

Keywords

Graphical, password, heuristics, forensics, tool, smartphone, prediction

1. INTRODUCTION

The proliferation of mobile devices in modern societies and the increasing hardware capabilities have made smartphones and tablets affordable tools that support their users in various tasks. Most applications store data in the devices' internal memory in order to work properly. Thus, our smartphones and tablets contain a lot of personal information, which should be protected by adversaries.

*Corresponding Author

WiSec'14 Jul 23-25 2014, Oxford, United Kingdom.
ACM 978-1-4503-2972-9/14/07.

The Android Consortium introduced the pattern lock screen when they released the second version of their operating system and became very popular because of the usability it offers. However, studies have shown that the authentication scheme is vulnerable to smudge attacks [3] and shoulder surfing. We have also seen some early indications that the formation of a graphical password (such as the Android pattern lock) might be affected by heuristic rules originated from the human nature [2, 4]. The users' perception on the pattern lock screen security has been studied in a survey [1] that investigates the outcome of the introduction of a password meter on the authentication mechanism. The conclusion of this work is that a password meter could urge users to be more careful when they form their patterns and shield their systems with more complex passwords increasing the security of their Android mobile devices.

2. MOTIVATION

The current work aims to deliver an Android application, which will be used as a lightweight forensic tool able to predict the pattern that unlocks the mobile device. There are numerous ways to bypass the lock screen [5] but most of them need root privileges in order to work. Another drawback is that in most of the cases the mobile device must be restarted and this procedure could limit forensic examinations because the volatile memory loses all its data. Thus, our intentions are to present a framework that will use the oily residues left on the screen and also the heuristic rules that define the password construction. The combination of these resources will provide the capability to produce a list with the most possible patterns that unlock the device under examination.

In [3] the authors demonstrated the best conditions under which the retrieval of residues is possible. The study was replicated in [2] and additionally, the research included the examination of various features of patterns obtained by running a web survey. The analysis portrayed that there is an inclination the users to start their patterns from specific nodes. Also, the study revealed popular passwords, subpatterns (bigrams, trigrams) and ending points. We intend to feed all these information into a tool that will have the ability to capture a photo of the screen, extract residues (and directionality) and propose possible passwords to bypass the screen lock.

3. METHODOLOGY

We assume that we acquire an Android smartphone that runs the application we developed. The goal is to bypass

the pattern lock screen that protects a seized smartphone. The smudges that exist on the screen suggest that the user has cleaned it recently. We propose four distinct stages of activity in order to come up with the set of the patterns that match the criteria we stated at Section 2. These are described below.

3.1 Capture photo

The investigator captures a photo of the screen under examination, using properties described at [3].

3.2 Clear image from 'noise'

The application will perform various Image Processing steps on the acquired image to wipe the unwanted 'noise' and extract as many nodes as possible from the pattern that was used on the seized phone.

3.2.1 Decolourisation

Grayscaling is one of the most commonly used pre-processing techniques. It is the process of converting a colour image to a grayscale image, each pixel of which has the same value for all channels (i.e. RGB). It simplifies and reduces computational requirements, and is often used as a prerequisite for other processes such as thresholding.

3.2.2 Fingerprint detection

Being able to extract the contour of the trace-fingerprint is enough to perform node extraction, though a pattern lock can go in either direction; hence, we are also interested in directionality of the fingerprints.

3.2.3 Canny Edge detection

The aim of this stage is to extract the contour of the trace, which consists of edges, by the use of an edge detector. An edge can be defined as a discontinuity in pixel intensity within the given image.

3.2.4 Thresholding

Thresholding is a simple yet powerful image segmentation technique that converts a grayscale image to a binary image, so that objects can be separated from their background in an easier way.

3.3 Build a Neural Network

3.3.1 Node extraction

The processes discussed so far will provide a set of traces-nodes that will be put on a grid that is defined physically by the dimensions of the device.

3.3.2 Pattern Lock suggestion

This is the stage where the app has to figure out the probability of each pattern to occur and rank them in order to provide a sufficient password suggestion. For this task we will use Neural Networks (N.N.) and especially fuzzy N.N. The reason for using a fuzzy N.N. is that a fuzzy system has a set of IF-THEN rules incorporated into the system, which is expandable. In the context of this project, an example rule would be: "IF a pattern consists of knight moves, THEN the likelihood is 40%". With the addition of N.N., the fuzzy system is able to learn. Therefore, this approach would better suit here because we can use the results of previous studies [1, 2] to train our scheme and learn heuristic rules that define the formation of patterns.

3.4 Evaluate the proposed passwords

The final part involves the evaluation of the proposed scheme, which will be done on the actual seized device, by trying to break its pattern lock screen, using the proposed list from our system.

4. CONCLUSION

The current work aims to merge Image Processing methods and Machine Learning techniques to take advantage of possible security issues that biased input can cause to the Android's graphical user authentication scheme. The password space of the pattern lock screen shrinks dramatically if we take into account the fact that more than 50% of the passwords provided by users in previous studies [1, 2] started from the top left node. Such knowledge, in addition to the existence of nodes (monograms) retrieved from screens will provide a framework that will be able to propose lists of patterns that break the mobile devices' security scheme. The project extends the OpenCV functionality proposing improvements of existing algorithms (Otsu thresholding, Canny Edge Detector) and brings to the forensics community a lightweight, easy to use tool to bypass the Android pattern lock screen authentication.

5. ACKNOWLEDGMENTS

This work has been supported by the European Union's Prevention of and Fight against Crime Programme "Illegal Use of Internet" ISEC 2010 Action Grants, grant ref. HOME/2010/ISEC/AG/INT-002 and the Systems Centre of the University of Bristol.

6. REFERENCES

[1] P. Andriotis, T. Tryfonas, and G. Oikonomou. Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In *Lecture Notes in Computer Science*, volume 8533. Springer, 2014.

[2] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 1–6. ACM, 2013.

[3] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX conference on Offensive technologies*, pages 1–7. USENIX Association, 2010.

[4] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: the case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 161–172. ACM, 2013.

[5] xda developers. [android][guide]hacking and bypassing android password/pattern/face/pi. `http://forum.xda-developers.com/showthread.php?t=2620456`. Accessed May 05, 2014.