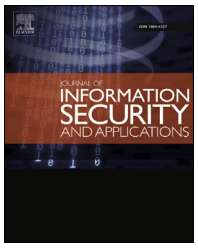
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



Dissecting pattern unlock: The effect of pattern strength meter on pattern selection

Chen Sun, Yang Wang, Jun Zheng *

Department of Computer Science and Engineering, New Mexico Institute of Mining and Technology, Socorro, NM, 87801, USA

ARTICLE INFO

Article history:
Available online 9 November 2014

Keywords:
Pattern unlock
Pattern strength meter
Mobile security
User study
Android

ABSTRACT

Pattern unlock is one of the entry protection mechanisms in Android system for unlocking the screen. By connecting 4–9 dots in a 3 × 3 grid, the user can set up an unlock pattern which is equivalent to a password or a PIN. As an alternative to the traditional password/PIN, the visual pattern has gained its popularity because of the potential advantages in memorability and convenience of input. However, the limited pattern space and existing attacks such as shoulder surfing, or smudge attack make this mechanism weak in security. In this paper, we analyzed the characteristics of all valid patterns and proposed a way to quantitatively evaluate their strengths. We then designed two types of pattern strength meters as visual indicators of pattern strength. We conducted a user study that involved 81 participants. The results of the user study showed that the presence of visual indicator of pattern strength did encourage users to create visually complex patterns, thus increasing the security of pattern unlock.

1. Introduction

The use of powerful mobile devices such as smartphones and tablets has seen tremendous growth in recent years. Google's Android is one of the most popular mobile platforms that powers hundreds of millions of mobile devices in more than 190 countries around the world (Android). These mobile devices are nearly as powerful as desktop PCs. Users can do many things on their devices including social networking, online shopping and mobile banking. Thus, tons of personal data can be accessed in these devices. Meanwhile, mobile devices can easily be lost or stolen due to their small size, so it poses a need to protect the sensitive data from unauthorized accesses.

Automatic screen lock is the most commonly used strategy in mobile devices to prevent unauthorized access. Android provides several screen lock options including slide, password, PIN (Personal Identification Number), pattern, and the latterly introduced face unlock (Android 4.0; Set Screenlock).

Among these screen lock options, slide unlock provides no protection on entry authorization. It is only used for preventing accidental touches that may trigger certain functions of the system. Password and PIN are very similar as they are also used in other contexts. The user needs to enter a predefined password or PIN to unlock the device. A password can be a combination of numbers, letters, and special symbols, while a PIN consists of only numbers. As required by Android, a password or a PIN should be no less than 4 characters (Set Screenlock). Pattern unlock is a relatively new gesture-based entry protection mechanism introduced by Google in 2008 (Android's Unlock Pattern). To unlock the device with pattern unlock, instead of typing a password/PIN into a text box, the

* *Corresponding author*. Tel.: +1 575 835 6182; fax: +1 575 835 5587.
E-mail address: zheng@nmt.edu (J. Zheng).
http://dx.doi.org/10.1016/j.jisa.2014.10.009
2214-2126/

user is asked to draw a user-defined path by connecting dots in a 3 × 3 grid. Such a path is called an unlock pattern such as the one shown in Fig. 1. The slide, password, PIN, pattern unlock options are available on all Android versions while the last option, face unlock, was introduced in Android 4.0. Using this option for screen unlocking, the system verifies the user by starting the front camera of the device to do a face recognition of the user. This sounds like a very interesting and convenient solution for entry authorization. However, according to some reviews, the face recognition may not work very well when the user angles his/her head slightly away from the camera, or when used in a low-light environment. Moreover, the face recognition can be even fooled by presenting a picture of the authorized user (Android 4.0).

Although pattern unlock is a ready-to-use entry protection mechanism available on all Android devices, it is relatively new compared to the traditional password/PIN. Due to the lack of basic knowledge of pattern unlock, users may choose some weak patterns that cannot provide enough protection against attacks like brute force attack (Botelho et al., 2012), shoulder surfing attack (Tari et al., 2006), and smudge attack (Aviv et al., 2010). In this paper, we examine the basic features of unlock patterns and let users be aware of their security strengths. The contributions of this paper are as follows:

- We studied the characteristics of all patterns allowed by Android, and proposed a way to quantitatively evaluate the complexity of a given pattern.
- We designed two types of pattern strength meters as the visual indicators of pattern strengths.
- We performed a user study involving 81 participants to investigate users' choices of unlock patterns and factors that influence their decisions.
- Based on the results from the user study, we showed that pattern strength meters were effective in encouraging users to create strong patterns.

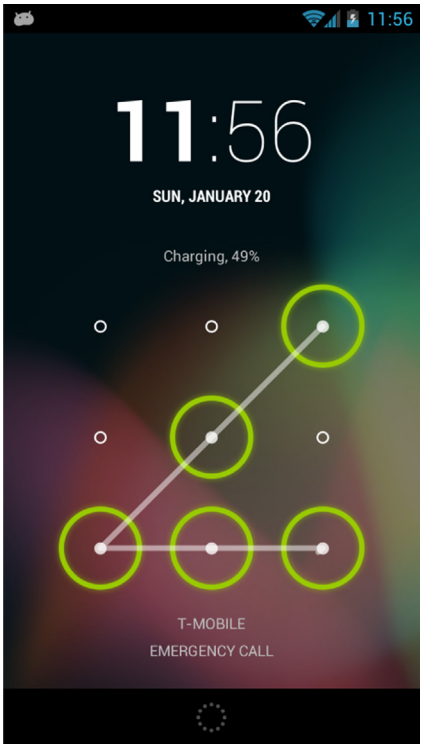


Fig. 1 – An example of unlock pattern.

2. Related work

2.1. Graphical password

Although Android's pattern unlock is relatively new, it can be viewed as a form of graphical password. The idea of the graphical password was originally introduced by Blonder in 1996: given a predetermined image, the user needs to select one or more predetermined positions in a specific order for authentication.

One of the most representative graphical password schemes is Draw A Secret (DAS) proposed by Jermyn et al. in 1999. The DAS scheme was proposed to be used as an encryption tool on Personal Digital Assistant (PDA) devices. In this scheme, the user draws one or more strokes on a $N \times N$ grid. The drawing is then mapped to a sequence of coordinate pairs served as a password.

Dunphy and Yan (2007) introduced background images to the original DAS scheme. In the BDAS (Background Draw a Secret), a user chooses a background image overlaid by the grid and then draws the strokes as in DAS. Their user study showed that users tended to draw more complex strokes when aided by background images.

Proposed by Tao and Adams (2008), Pass-Go is another successor of DAS. In this scheme, users select intersections instead of cells on a 2D grid as a way to input a password. The use of intersections instead of cells overcomes the major drawback of DAS: drawing diagonal lines is difficult. To add error tolerance to enable users to select intersections on a grid, Tao and Adams introduced sensitive areas as round circles with a radius of one-fourth of the side length of a grid cell. In this sense, Android's pattern unlock has a very similar design to Pass-Go.

Orozco et al. (2006) proposed a security enhancement to graphical password by incorporating the checking of haptic parameters such as velocity and pressure. Such a scheme is more resistive to shoulder surfing attacks than other traditional graphical password schemes.

YAGP (Yet Another Graphical Password), proposed by Gao et al. (2008) is another graphical password scheme that tries to distinguish different drawing styles due to user personality. Instead of using the physical haptic features, YAGP compares the stroke trends between two drawings.

2.2. Android's pattern unlock

For Android's pattern unlock, in 2010, Aviv et al. (2010) studied the feasibility of guessing a user's pattern from the oily residues, or smudges, left on the touch screen. In their work, the size of the pattern space, i.e. the total number of valid patterns, was calculated using a brute force method without any further study of the complexity of the patterns.