Multi-Touch Passwords for Mobile Device Access

Ian Oakley
Madeira-ITI
Funchal, Portugal
ian@uma.pt

Andrea Bianchi
KAIST
Daejeon, Korea
andrea@kaist.ac.kr

ABSTRACT
This paper explores how possible richer input graphical passwords based on multi-touch input could improve traditional graphical passwords, like the Pattern Lock for mobile devices. The results indicate user perceptions and usability issues relating to this new design and highlight mechanisms by which it can be improved.

Author Keywords
Multi-touch, Password, Authentication, Security.

ACM Classification Keywords
H.5.m Information interfaces and presentation: Misc.

General Terms
Human Factors, Security

INTRODUCTION

Smart-phones are powerful personal devices that manage and store sensitive, private information. However, more than 50% of users do not secure them with a password [1], typically due to factors such as impatience with authentication processes. To address this issue, Google introduced the *Pattern Lock* authentication scheme for Android devices. Inspired by the rapid and effective Draw-a-secret system[4], Pattern Lock requires users to enter strokes connecting a specific pattern of on-screen dots rather than a traditional PIN.

Two key problems with this method are that it is highly susceptible to observation [3] and also decreases the input space of possible passwords (*password entropy*) by enforcing connections only between adjacent points and by disallowing repeated selections. Additionally, attackers can infer passwords from the oily residues left by fingers stroking on the phone screen (a smudge attack [2]). Partially, addressing these limitations, researchers have explored variations that allow repeated item selections [5].

This paper explores how users' behavior and perceptions of security change given the chance to construct graphical passwords that allow more sophisticated patterns including sequential combinations of taps and strokes, multi-touch input and off target interaction. The objective of these manipulations is to increase password entropy and the difficulty of observation and smudge attacks. The remainder of this paper describes MT-Lock, a prototype system implementing these features and an explorative study of how users create and input passwords with it.

UbiComp '12, Sep 5-Sep 8, 2012, Pittsburgh, USA.

INTERFACE AND IMPLEMENTATION

MT-Lock is based on the Google Android Pattern Lock authentication system. It features 9 circular targets arranged in a three by three grid occupying the center of a mobile device screen. When a target is tapped, it is highlighted with a green ring. If the tap is extended to a stroke, the highlight remains on the target and a grey beam illustrates the stroke path. Multiple targets can be connected by a single stroke, but targets cannot be revisited. MT-Lock implements novel functionalities extending the Android Pattern system: strokes can start and end off-target and multiple taps and strokes can take place simultaneously. The MT-Lock interface and features are illustrated in Figure 1.

MT-Lock was built for an Android Nexus S smartphone (4 inch touch screen, 800x480 resolution) using Processing 1.5. The application ran full screen and targets were 120 pixels (roughly 1.2 cm) in diameter; their visual representations were half this size. This size facilitated targeting by avoiding fat-finger problems; in fact, the targets large size, and smaller visual size, made them easy to select. Inter-target spacing was 30 pixels. The maximum number of simultaneous touches supported was five.

USER STUDY

Participants, Procedures and Measures

An exploratory study was conducted in order to to explore how participants perceived, understood and used the novel features of MT-Lock. The experiment involved users completing a brief demographics questionnaire, reading a set of instructions introducing the MT-Lock interface, testing MT-Lock out (5 minutes max) and finally defining an MT-Lock password of their choice. They were then asked to enter their chosen password 6 times, initially storing it then making 5 repetitions. During this time, all raw touch events (presses, motions, releases) and widget and application level events (buttons presses, strokes over) were recorded. The study closed with a semi-structured interview gathering opinions

about perception of mobile security, phone security, MT-Lock and users rationale for their password choice.

10 participants (8 male, mean age 34) completed the user study. All owned a mobile device and reported familiarity with these technologies (3.7 on a scale from one to five). Three reported using a numerical PIN lock on their phone.

Results

Participants selected a wide range of passwords. On average, each password contained 2.9 screen interactions: 1.5 taps (SD 1.27) and 1.4 strokes (SD 0.84). Six participants combined taps and strokes, while three used only strokes and one only taps. Most screen interactions were singular and sequential. Two participants selected multi-touch passwords, one performing two simultaneous taps, the other two simultaneous stokes. Three users terminated one or more gestures off-target (over empty space). These involved small displacements from the final target, simply stroking beyond it at the end of the gesture. Strokes covered a mean of 3.9 targets (SD 1.59). No user started gestures in empty space.

Participants were rapid, accurate and showed few difficulties in remembering their passwords. Mean entry time for the selected passwords was 1.8 seconds; the error rate, calculated by comparing each users created password to the five they subsequently entered, was 8% (4 incorrect entries out of 50). Of these errors, each of which was made by a different participant, three were due to failures to correctly interact with the targets (e.g. unintentionally slipping fingers off a target) while only one was due to entry of incorrect information.

The data from the semi-structure interviews indicated participants were relaxed about phone security; seven used no phone lock system. However, most indicated concern about observation attack, but also suggested that locks are unnecessary - physical possession was deemed sufficient to guarantee security. When asked to rationalize their MT-Lock password choice, eight cited ease of remembering the password as the driving factor; shapes or letters were used to achieve this. Most users were negative about the idea of a multitouch password, citing concerns about input practicalities (e.g. that it requires both hands) and the feasibility of remembering and reliably replicating multitouch inputs. Conversely, most users reported that multi-touch input would provide security benefits, but that the additional input complexity out-weighed the potential benefits.

DISCUSSION, FUTURE WORK AND CONCLUSIONS

The empirical data showed that password entry was rapid and accurate and, from the ten users studied, many choose to utilize the novel functionalities provided. Six chose to combine taps with strokes, while two more used passwords composed of multiple strokes. Three also used strokes that ended off-target and two used simultaneous, multi-touch input of either taps or strokes. This argues for the inclusion of more complex stroke based passwords on mobiles. In contrast, it is interesting to note that most users (70%) were unconcerned by mobile security issues and felt that possession was the only necessary precaution to ensure security.

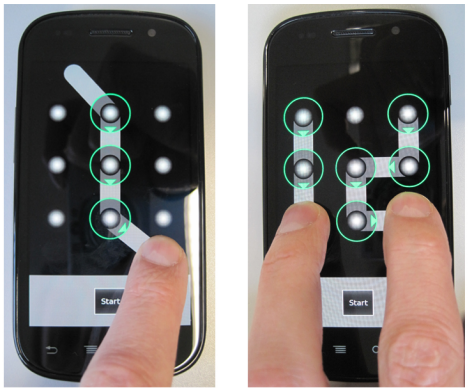

Figure 1. An example of off-target gesture (left) and multi-touch input pattern (right) used as elements of a password with MT-Lock.

Participants were generally positive about many aspects of MT-Lock (the use of multiple sequential inputs and the ability to mix of taps and strokes were thought to improve security). However, they were concerned about the feasibility and memorability of multitouch input. This suggests that if multitouch input is to be included in a security system, incorporating visualizations or feedback that effectively convey system state to users will be a requirement.

In sum, this paper proposed potentially overlapping sequences of taps and strokes as a password entry modality on mobile devices, described a system that realizes this functionality and conducted an exploratory user study to explore its viability. The empirical data are broadly positive and interviews revealed a range of attitudes to the novel forms of input enabled, highlighting the challenge of creating password entry techniques that are quick and easy enough for users to accept them into frequent tasks such as unlocking a mobile device. Future work will develop the MT-Lock system based on this feedback, formally establish its strength (e.g. higher password entropy and better security against observation attacks) and conduct formal empirical user studies.

REFERENCES

1. Symantec news release, accessed 8 jan 2012. *http://www.symantec.com/about/news/release/article.jsp?prid=20110208_01*.

2. A. Aviv, K. Gibson, E. Mossop, and M. Blaze. Smudge attacks on smartphone touch screens. In *Proceedings of USENIX*, 2010.

3. S. Gold. Android insecurity. *Network Security*, (10):5–7, 2011.

4. I. Jermyn, A. Mayer, F. Monrose, and M. Reiter. The design and analysis of graphical passwords. In *Proceedings of USENIX*, 1999.

5. K. Shin, J. Park, and J. Lee. Design and Implementation of Improved Authentication System for Android Smartphone Users. *Proceedings of AINA*, 2012.