Poster: Cellphones and Punishment: Encouraging Secure Mobile Behavior Through Morality

[Poster Abstract]

Dirk Van Bruggen
Department of Computer Science and Engineering
University of Notre Dame
Notre Dame, Indiana
dvanbrug@nd.edu

Shu Liu
Department of Computer Science and Engineering
University of Notre Dame
Notre Dame, Indiana
sliu6@nd.edu

Aaron Striegel
Department of Computer Science and Engineering
University of Notre Dame
Notre Dame, Indiana
striegel@nd.edu

Chuck Crowell
Department of Psychology
University of Notre Dame
Notre Dame, Indiana
ccrowell@nd.edu

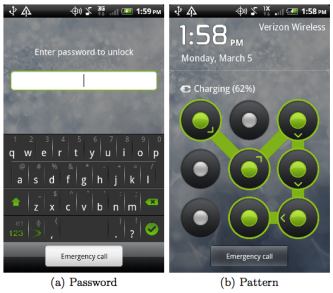
John D'Arcy
Department of Business
University of Notre Dame
Notre Dame, Indiana
jdarcy@nd.edu

1. INTRODUCTION

Cellular mobile devices have become an increasingly large part of society, permeating almost every aspect of life. Over the last decade, the number of mobile subscribers in the United States has more than doubled with 2011 seeing the number of cellphones surpass the number of people in the United States [1]. In addition to a growth in subscribers, usage of mobile devices has exploded with monthly text messages seeing more than a 700-fold increase over the past decade. Not all of the cellular devices are simply phones anymore either, with smartphones making up a significant portion of the market. These smartphones allow users to run a wide variety of software on their phones, ranging from document editors to games. Unfortunately, with the expanding availability and usage of mobile devices comes an increased security threat.

Smartphones are no longer being used only for personal life with corporations becoming more permissive of allowing employees to use their personal mobile devices within the corporate environment [4]. The more relaxed position on personal devices may be related to the significant cost savings when employers no longer need to purchase and pay a monthly fee for a mobile device for each employee. This situation leads to an interesting dilemma where employers no longer own the mobile devices but employees are placing company data on the devices. The corporations will still need to push out security policies regarding devices on the network but without ownership corporations are left trying to influence secure behavior among users.

In this study we ask can a user's security behavior be modified without express enforcement of policies, and if so, which methods are the most effective ways to cause the change? Towards evaluating secure mobile device behavior, we conducted a study on 166 college freshman smartphone users with regards to measuring the usage of secure practices on their smartphones without prior influence. Furthermore, we explored the ability to drive change in the users' behavior, in this case influencing users to lock the screens of their mobile devices, through a series of targeted interventions.



(a) Password (b) Pattern

Figure 1: Android Screen Locks

The contributions of this paper are

- *We conducted the first study to evaluate influencing change with regards to smartphone screen locking.*
- *Initial baseline data shows that greater than 60% of users secure their devices without prior interventions.*
- *Of the users who were targeted to influence change, 31% changed their behavior by the end of the study.*

These findings show that while a significant portion of users are securing their devices without prior intervention, those who do not secure their devices are not easily influenced to change. Thus, if a corporation wants to keep their network secure, the majority of their effort must be placed on enforcement methods for personal devices with a less significant effort placed into training and awareness materials.

Symposium On Usable Privacy and Security (SOUPS) 2012, July 11-13, 2012, Washington, DC, USA.

Screen Lock Type	Before	After
Text Based	13%	20%
Pattern Based	50%	47%
No Screen Lock	37%	33%

Table 1: Screen Lock Usage

2. APPROACH

In order to study user behavior related to smartphone security, we worked with the ongoing NetSense study at the University of Notre Dame[3]. The study provided Android Nexus S smartphones to 200 incoming college freshman students and also covered the monthly access costs for each device. Each phone contained a software application which collected a wide variety of usage and mobility data about the smartphones as well as the user's behaviors.

The Android operating system provides two types of screen locks for users to choose from. The first method, which can be seen in Figure 1a, allows users to enter a password similar to that used on a standard computer. A related method presents the user with a numeric keypad, resulting in a PIN similar to those used at ATMs. Standard, textual passwords can be difficult to use given the small screen and lack of physical keyboards on mobile devices. The second method, seen in Figure 1b, allows users to create patterns instead of text based passwords. Android provides an interface which consists of a 3x3 grid of dots which the user must connect together in some pattern. To unlock the phone, a user is presented with the grid and is asked to re-enter the pattern before access is granted. The pattern based methods are easier to input on the small screens of mobile devices and may be easier to remember.

Utilizing the data collection system developed as part of the NetSense study, an initial 2 week sample of data was collected. This sample was taken to assess the baseline usage of screen locking among the study population before any interventions were performed. From the initial data, two groups were identified that could be used for targeted interventions trying to influence more secure behavior. The first group consisted of participants who did not use any type of screen lock and could benefit from upgrading to either type of screen lock. The second group was made up of participants with a pattern based screen lock which previous research has shown is not as secure as text based methods [2]. The inclusion of the second group also allowed for a larger sample size on which to test targeted intervention messages.

In order to evaluate the best method to persuade users to enhance secure behavior, 3 message types were devised to send to each group. These types were based on deterrence, morality and incentives. The group of participants using no screen locks and the group using pattern based screen locks were both divided into 4 subgroups, one for each type of intervention message and a control group using random sampling. This resulted in a total of 99 participants that would receive an intervention message and 30 who would act as a control group. The messages were then sent to the participants via text message to the target phones. These messages were then followed by reminder messages, at 1 week intervals for 4 weeks, to anyone who did not modify their behavior.

The incentive messages were based on being entered in a drawing for taking action. Unlike the externally motivated incentive method, the morality based messages focused on the possible consequences to others due to not following organizational practices. Finally, the deterrent based intervention messages focused on the possible consequences to self for not following organizational practices.

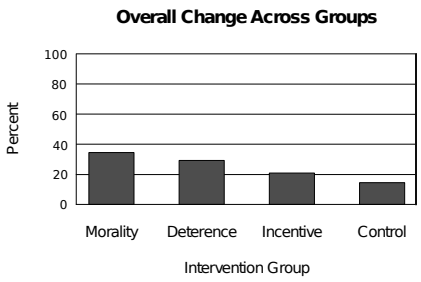


Figure 2: Overall Change

3. RESULTS

Surprisingly, 63% of participants were using some type of screen lock to protect their device as outlined in Table 1. While pattern based locks were in the majority with 50% of the population using them, text based locks accounted for only 13% of the study's population. Given the large percentage of users employing some type of screen lock it is evident that most users understand the importance of smartphone locking mechanisms. The higher rate of usage among pattern based methods suggest that the traditional keyboard entry methods are not as easy to use as the pattern based methods which have been built around the functionality inherent in smartphones.

After the targeted interventions, 31% of targeted participants changed their screen locking behavior in the manner that was suggested in the intervention messages. While usage of both patterns and no screen lock decreased, the drop in patterns is attributed to the users who upgraded to text based locks. Figure 2 shows the percent of each intervention group that changed their behavior over the course of the study. While morality had the highest conversion rate, none of the groups were able to get more than 40% of the users to change their behavior. This suggests that for users who do not initially use secure behavior, influencing them to change through intervention messages is not an effective course of action.

4. REFERENCES

[1] U.S. Wireless Quick Facts. http://www.ctia.org/advocacy/research/index.cfm/aid/10323, 2012.

[2] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith. Smudge attacks on smartphone touch screens. In *USENIX 4th Workshop on Offensive Technologies*, 2010.

[3] S. Liu and A. Striegel. Accurate extraction of face-to-face proximity using smartphones and bluetooth. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pages 1 –5, 31 2011-aug. 4 2011.

[4] Research In Motion. Smart Policies for Personal-Liable Smartphones. 2010.