Security, But at What Cost?

An Examination of Security Notifications within a Mobile Application

Gregory D. Moody[1] and Dezhi Wu[2]

[1] University of Nevada, Las Vegas, Nevada, USA
gregory.moody@unlv.edu
[2] Southern Utah University, Cedar City, Utah, USA
wu@suu.edu

Abstract. Research on the behavioral-based security of information systems within organizations and for personal use has been common over the last decade, however little is known regarding how individuals perceive the security of their mobile devices. This study seeks to explore how the security notifications within a mobile application environment alter adoption and security-related beliefs concerning their device. We propose a theoretical model based on the technology adoption and psychological theories, and propose an experiment to test the model. Contributions and implications of the work are then proposed.

Keywords: Mobile device, mobile security, human-computer interaction, mobile application, security notification.

1 Introduction

The adoption of mobile devices continues at an unprecedented rate throughout the world. Some countries even boast an average of more than one mobile device for the entire country. However, despite this widespread adoption of the mobile/smart phone across the world, it is not fraught with difficulties and shortcomings. Only recently has researched begun to focus on the security awareness of users in regards to their devices. Research has shown that users are unaware of the risks that these devices pose to their own personal information. Additionally, these devices provide a host of security-related issues at the organizational level (e.g., policy for device usage of BYOD, government and corporate espionage enabled through mobile connectivity, use of personal devices for organizational functions without adequate monitoring and oversight on such devices). Therefore, mobile devices have become a new target for security attacks, which pose serious threats to the security of such devices [5], to individual users [10], and to organizations when used and transported outside of their physical organizational boundaries [7].

With rapid adoption of mobile technologies, it has achieved pervasive adoption levels as users have mobile devices for both personal and work-related activities. At the

S. Yamamoto (Ed.): HIMI/HCII 2013, Part II, LNCS 8017, pp. 391–399, 2013.

individual user level, mobile user experiences are increasingly enriched by various mobile applications customized for different mobile devices. However, mobile applications can be a double-edged sword, which can cause serious security risks and threats to individual users. Research [10] points out that users are not fully aware of the potential damage to their personal assets and private information saved in their mobile devices as they may be conditioned to the process of installing malicious mobile application. It is unclear how much users are aware of their mobile security settings, and how they should take proper actions to effectively protect their assets saved in mobile devices, in that two extreme approaches exist in current user practices: one approach is that users blindly apply existing security solutions that normally applied to desktop platforms to all mobile devices, and the other approach is that users only consider new security techniques for mobile devices. The truth usually lies in-between with some level of justifications in different mobile environments [3], [6], [10], [13].

Many practitioners have started to pay attention to mobile security issues; while current research especially focused on users' mobile security behavior is scant. This paper focuses primarily on the security awareness of mobile users as an initial project to explore how to increase the security of mobile devices through the use of security notifications to increased perceived perceptions of privacy and security. Building on theoretical ideas from community health theories, we propose that individual users must be first made aware of such problems prior to introduction of any solution to this dilemma. Specifically we explore how the usability of the mobile phones interface to display security notifications regarding attempted behaviors on the phone will alter the users' perceptions of security, feelings of irritation, and intentions to continue to use the devices.

In the next section, we briefly introduce theoretical background for this research, and propose a research model to examine how different levels of disruptive security notifications pushed into a mobile smartphone affect user security perceptions of their mobile devices and their intentions to continuous use the mobile application. Then we propose a study design and discuss expected contributions to the field.

2 Theoretical Background

The number of security threats to mobile devices is rapidly increasing, and effectively managing security in mobile environments is a challenge due to (1) mobility and small size of mobile devices despite the constraints in both computational and power capabilities; (2) disadvantages of being incapable of taking advantage of a platform's hardware architecture on the mobile devices; (3) obscurity between platform and network; (4) mobile attacks; and (5) mobile device usability issues [10]. Today's mobile users are exposed to all sorts of complex security services and mechanisms, which can be confusing and ineffective to them to protect their mobile device security. Josang and Sanderud [8] suggest making the security services and mechanisms as transparent as possible to users to ease the process, but can be constrained by users' background and capabilities to handle their mobile devices. Furthermore, they

indicate that it is crucial to design mobile security interfaces in an intuitive and intelligent way. Further, users are often completely unaware of any security vulnerabilities in their devices, which is drastically different than their view of computers. While users have a general sense of the potential harms due malware, security vulnerabilities, etc., they have no such belief regarding the vulnerabilities of their mobile devices.

In this research, we focus on mobile usability issues associated with mobile devices to examine users' awareness and ability to respond to various mobile security notifications. We begin by building on the Apple Usability Guidelines[1] and the technology adoption model to propose how the interface of a mobile device impacts users' intentions to continue to use the device. This underlying portion of our model provides a baseline to assess the general usability of a device, and ascertain how that impacts perceptions of security and intentions to use such a device in the future.

Next, we explore how security notifications pushed to the user due to application of device operations may interrupt the cognitive processing of the individual and cause a sense of irritation. This builds upon the work by McCoy et al. [9] by extending their web-based premises and manipulations to the mobile operating system context. We propose that more frequent or disruptive push notifications will cause the user to become irritated with the mobile device. By interrupting the operations of the phone or application and forcing the user to attend to such notifications, the sense of irritation will result in a general sense of dissatisfaction that will negatively impact the ability of a well perceived interface to positively impact intentions to use the device.

However, we propose that such disruptions also have a beneficial purpose. When users engage in a task, they become highly goal focused and are attempting to achieve such goals. By interrupting this process and providing some notification that these goals may conflict with security-related goals, we attempt to show that current goal-directed behaviors may in fact not be desired when considered by concurrent yet differing security-related goals. Thus, such notifications, although detrimental to the operations and usefulness of the phone, may improve perceptions of security for the phone.

Our proposed research model is summarized in Figure 1, which we now briefly propose.

The initial hypotheses are an extension of the Technology Adoption Model [4] to mobile devices, which has been previously validated [2]. As the users' main interactions with a mobile device are based on the graphical interface of the device, it becomes the predominant antecedent of the ease-of-use for the device. We thus replicate prior research and propose:

> *H1: The mobile device user interface will be positively related to the perceived usefulness and ease-of-use of the device.*
>
> *H2: The perceived usefulness / ease-of-use of the mobile device will be positively related to the intention to continue to use the device.*

[1] http://developer.apple.com/library/mac/#documentation/userexperience/conceptual/applehiguidelines/UEGuidelines/UEGuidelines.html

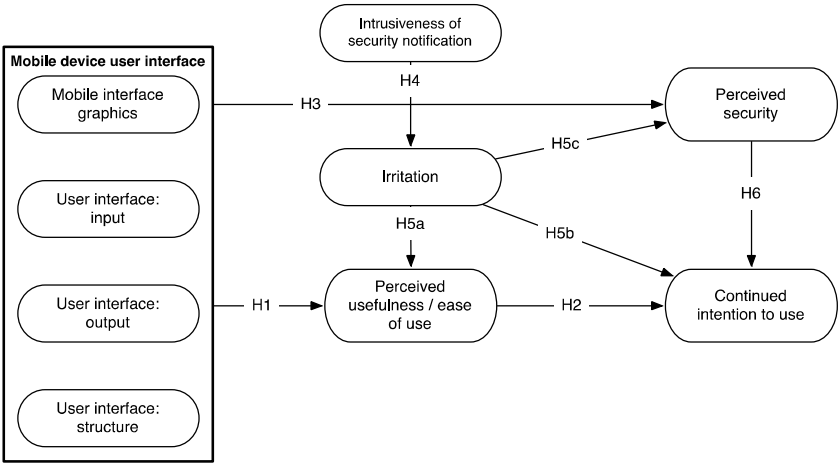

Fig. 1. Theoretical Model

Unlike computer operating systems and environments, mobile devices do not have built in security applications that provide dashboards regarding the relative security of the device. Rather, users are notified regarding any changes or requests by applications relative to private or secure information through the means of notifications. How these notifications are delivered to the user is determined by the interface of the mobile device. We thus posit that the awareness of the device's mobile security is primarily engendered through such notifications as afforded through the interface of the mobile device.

This is an extension from prior research on information system quality. Previous work has both proposed and found that systems that are perceived to be of higher interface design as perceived as being of higher quality [2]. We further extend this finding by proposing that higher quality systems, by being perceived in a more favorable view, are likewise perceived as more secure. This is in alignment with the cognitive psychological theory of attitude consistency, which emphasizes that individuals tend to align beliefs of the same attitude objects in order to avoid inconsistency [12]. Thus, users of the mobile device, believing it to be of superior quality will infer that its other attributes are also likely to be of equally high quality, even without any direct source of information to corroborate this belief [1].

> *H3: Devices that are perceived as having superior user interfaces will be positively related to higher perceptions of mobile device security.*

We propose that within application notifications are similar to pop-up and in-line ads present on the websites. We thus extend the work of McCoy et al. [9] that when such notifications are perceived to be more repetitive will have the potential of being perceived as being more intrusive. Constant repetition of the same information, or same type of notification is likely to disrupt the cognitive flow of information that an individual requires when focusing on a task. This disruption will likely be perceived as an

intrusive force, that disrupts the use of the current application. Following this, we pose that as the notification is perceived as being intrusive, it will lead to feelings of irritation by the user [9]. We thus extend this prior line of reasoning and research to the context of mobile security notifications and propose:

H4: The perceived intrusiveness of notifications will be positively related to the perceived irritation afforded by such notifications.

Building on psychological theories of attitude change, we pose that as negative emotions regarding the mobile device are increased, that intentions or perceptions regarding the device will also be negatively impacted [11]. Specifically, as the user becomes irritated with the security notifications, it is likely that these feelings will negatively impact the perceptions of the ease-of-use and usefulness of the device, which will negatively impact the intention of the user to continue to use the device. However, the engenderment of irritation will potentially positively impact perceptions of security. Irritation will likely raise the salience of cues regarding the security of the device, and provide the user with a sense of control over their data and their device, and thus increase the perceptions of security. We thus propose that feelings of irritation caused by the security notifications will produce the following outcomes:

H5a: Feelings of irritation caused by the security notifications will negatively impact the perceptions of usefulness and ease-of-use of the mobile device.

H5b: Feelings of irritation caused by the security notifications will negatively impact the intention to continue to use the mobile device.

H5c: Feelings of irritation caused by the security notifications will positively impact perceptions of security of the mobile device.

Finally, although practitioners have long proposed that security is at odds with the general day-to-day usage of an application, we formally test this assumption. Specifically, we pose that when users feel that a device is more secure they will have even more intentions to continue to use the device, as a potential negative future event (e.g., a data breach) would likely not occur. Thus, we propose:

H6: As the perceived security of the mobile device increases that the user will have greater intentions to continue to use the device.

3 Proposed Study Design

We intend to assess the accuracy of our theoretical model through the means of a 2 (high vs. low threatening conditions) x 3 (highly disruptive, moderately disruptive and no notifications treatment groups) randomized experiment with mobile phones. In the highly disruptive treatment condition, users would be exposed to push notifications during the process of the experiment that alerts them to security violations. The user

would be unable to perform any other task until they first read through the entire violation and then approve or disapprove of such an action. They would then be returned to the screen that they had been using.

In the moderate disruptive notification, the user would receive a push notification that is minimally inserted into their view, but does not obstruct or interfere with the tasks that the user is currently working on. Rather it would simply notify of the violation, and not require any interaction on the part of the user.

In the no disruption condition, we would allow the user to complete tasks as specified by the experiment, and they would never receive any notification of any security violation. This would serve as the control condition to ascertain how much variation in our model is simply caused by the notification process.

Currently, we have designed and implemented a mobile security notification system that can be run in various mobile phones. We plan to recruit users from several US university campuses in Spring 2013. The incentive will be extra points for participating in our study. We also designed two different scenarios for this experiment: one is a hedonic environment (i.e., a mobile game), and the other one is a non-hedonic environment (i.e., a Wikipedia article on "computers"). In both scenarios, users will be exposed to different levels of security notifications (see Figures A1 and A2). At the beginning, users will be instructed by researchers regarding the experiment, and then users will be randomly assigned to one of the ten treatment groups (2—high vs. low threat— x 2—highly vs. moderately disruptive— x 2—hedonic vs. utilitarian conditions, with one hedonic and one utilitarian control group). The whole experiment will take users about 15-20 minutes. After they complete the experiment using a mobile smartphone, they will be asked to fill out a questionnaire that assesses common demographic controls and items to assess the constructs of interest in this study. Screenshots for these treatment groups are shown in Appendix 1.

4 Expected Study Contributions

This study would have several important contributions for research and practice. First, by examining how the user perceives highly and moderately disruptive notifications, we would be able to offer practical guidelines for practice as to how to notify users about security violations. Given the predominance of these two types of notifications, this has strong practically implications regarding whether security-related notifications should be reported with one or both types of notifications. Further, given potential future results of this study, we could explore whether the type of notification interacts with the degree of threat being broadcast via the notification. It is possible that the level of threat may fit with a specific type of notification. For example, highly threatening notifications may produce better outcomes if it is notified with a highly disruptive means, while low threatening notifications should be broadcast with moderate disruptions. We would explore this potential fit condition.

Thus work would also validate our theory in that the disruptive effect of notifications serves to increase perceptions of security by the user, this is a novel notion. Currently, with the scant amount of mobile security research that has been published,

no research to date has reported any antecedents that increase the perceptions of security afforded by a mobile device. This would be the first such study to begin this important process by showing a process whereby security notifications are able to improve the perceived security of the device, while likewise decreasing the perceived usability and ease-of-use of the device.

Another important contribution that this work would provide is the inherent trade-off between the usability of an application and its perceived security. This is a topic that is commonly discussed within practitioners of security, but has yet to be validated in any meaningful or empirical way. This would provide the first real empirical validation of this assumption. By showing whether this assumption is valid or not, this research could initiate the first steps towards identifying antecedents that may potentially increase the perceived security of a device while likewise increasing the perceived usefulness and ease-of-use of the device.

5 Conclusion

Mobile devices are becoming a way of life around the globe. While the development of more applications, and the adoption by more users increases the incentives for users to also adopt, there is little research exploring how users can be made aware of the potential security issues and problems inherent in such devices. Whereas most users are aware of virus, malware and other such dangerous software on their personal computers and laptops, very few are aware of similar threats on their mobile devices.

This is an initial study that proposes an adoption-based theoretical model to explore how the interface notifications impact the perceptions of security, and the intention to continue to use the device. We propose a laboratory experiment, using mobile device users on their own devices, in which they are exposed to differing levels of security-related notifications and varying levels of security-related threats. We propose to analyze the results of such a study and explore potential fit conditions between the type of notification and the type of threat being communicated. Further, we would test the theoretical veracity of our model.

We propose several important contributions for research in practice, with the most important being a call to focus on mobile-based security research. This area of security in regards to information technology is lacking, which is an appalling condition given the lack of awareness that exists in the general populace. We also note that this would be the first study to explore how the interface of the mobile device is able to impact perceptions of security, and likewise how the perceptions of security on the device impact the user's intention to continue to use the device.

References

1. Alba, J.W., Hutchinson, J.W.: Dimensions of Consumer Expertise. Journal of Consumer Research 19(4), 411–454 (1987)
2. Cyr, D., Head, M., Ivanov, A.: Design Aesthetics Leading to m-Loyalty in Mobile Commerce. Information & Management 43(8), 950–963 (2006)

3. Dagon, D., Martin, T., Starner, T.: Mobile Phones as Computing Devices: The Viruses are Coming. IEEE Pervasive Computing 3(4), 11–15 (2004)
4. Davis, F.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly 13(3), 319–340 (1989)
5. Distefano, A., Grillo, A., Lentini, A., Italiano, G.F.: SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle. In: CSIIRW 2010 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, vol. 27, pp. 1–4 (2010)
6. Furnell, S.: Handheld Hazards: The Rise of Malware on Mobile Devices. Computer Fraud & Security 10(5), 4–8 (2005)
7. Halpert, B.: Mobile Device Security. In: Proceedings of InfoSecCD Conference, Kennesaw, GA (2004)
8. Josang, A., Sanderud, G.: Security in Mobile Communications: Challenges and Opportunities. In: Proceedings of the First Australian Information Security Workshop (AISW 2003), vol. 21, pp. 43–48. CRPIT, Adelaide (2003)
9. McCoy, S., Everard, A., Polak, P., Galletta, D.F.: An Experimental Study of Antecedents and Consequences of Online Ad Intrusiveness. International Journal of Human-Computer Interaction 24(7), 672–699 (2008)
10. Oberheide, J., Jahanian, F.: When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments. In: Proceedings of the Eleventh International Workshop on Mobile Computing Systems and Applications, Annapolis, MD, USA, February 22 (2010)
11. Petty, R.E., Wegener, D.T.: Attitude Change: Multiple Roles for Persuasion Variables. In: Gilbert, D.T., Fiske, E., Lindzey, G. (eds.) The Handbook of Social Psychology, vol. 1, pp. 323–390. McGraw-Hill, New York (1998)
12. Thompson, M.M., Zanna, M.P.: The Conflicted Individual: Personality-Based and Domain-Specific Antecedents of Ambivalent Social Attitudes. Journal of Personality 63(2), 259–288 (1995)
13. Xie, L., Zhang, X., Chaugule, A., Jaeger, T., Zhu, S.: Designing System-level Defenses against Cellphone Malware. In: Proceedings ofthe 28th IEEE International Symposium on Reliable Distributed Systems, pp. 83–90 (2009)

Appendix

Screenshots from the experimental website.

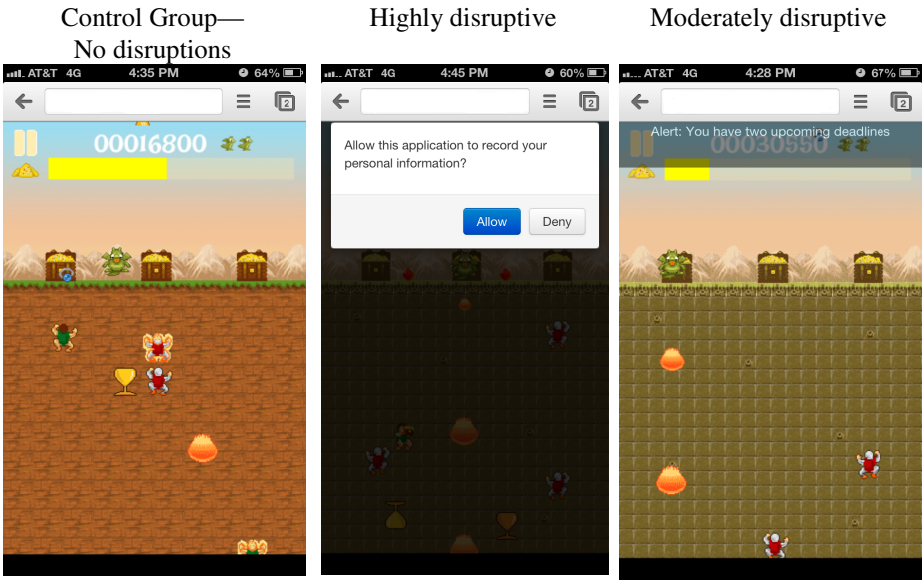

Fig. A1. Hedonic Scenario Mobile Smartphone Experiment Interfaces

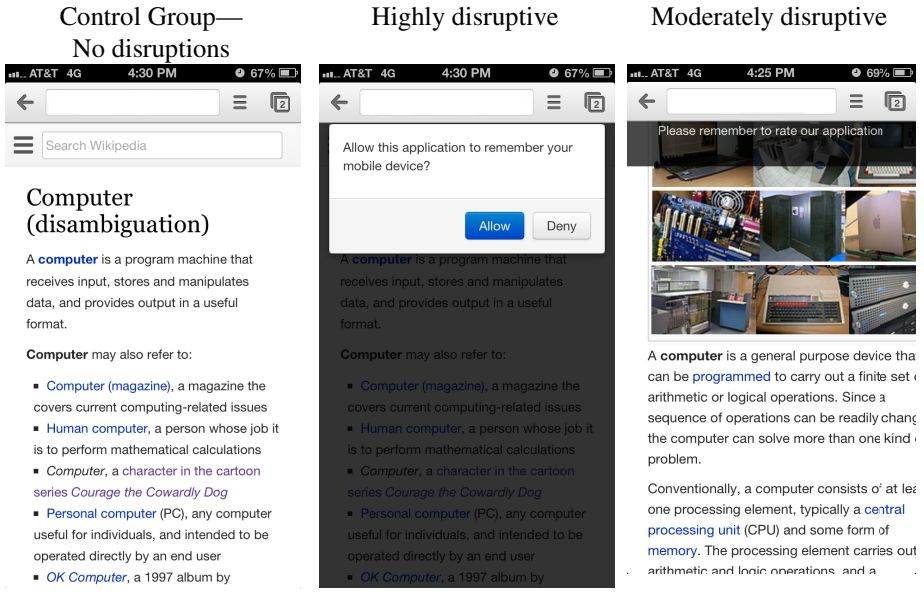

Fig. A2. Non-Hedonic Scenario Mobile Smartphone Experiment Interfaces