Reflections on U-PriSM 2: The Second Workshop on Usable Privacy and Security for Mobile Devices

*** Sonia Chiasson**
Carleton University, Canada

Heather Crawford
Florida Institute of Technology, USA

Serge Egelman
University of California, Berkeley, USA

Pourang Irani
University of Manitoba, Canada

ABSTRACT

The Second Usable Privacy and Security for Mobile Devices Workshop (U-PriSM 2) was co-located with MobileHCI'13 in Munich, Germany. The U-PriSM 2 was an opportunity for researchers and practitioners to discuss research challenges and experiences around the usable privacy and security of mobile devices (smartphones and tablets). Security and privacy often involve having non-security experts, or even novice users, regularly making important decisions while their main focus is on other primary tasks. This is especially true for mobile devices where users can quickly and easily install apps, where user interfaces are minimal due to space constraints, and where users are often distracted by their environment. Likewise, mobile devices present unique privacy and security risks because they allow third-party applications access to personal information and sensor data. The amount and sensitivity of such personally identifying information is likely to increase as device functionality increases. The convergence of these factors means that improvements to security and privacy provisions on mobile devices are becoming increasingly important. Workshop participants had a chance to explore mobile device usage and the unique usable security and privacy challenges that arise, discuss proposed systems and ideas that address these needs, and work towards the development of design principles to inform future development in the area.

Keywords: Mobile devices, usable privacy, usable security, human-computer interaction, security

INTRODUCTION

The Second Workshop on the Usable Privacy and Security of Mobile Devices (U-PriSM 2) was held with MobileHCI'13 in Munich, Germany. This followed the 2012 U-PriSM workshop co-located with the Symposium on Usable Privacy and Security (SOUPS) in Washington, DC. U-PriSM 2 provided an opportunity for researchers and practitioners to discuss research challenges and experiences around the usable privacy and security of mobile devices (smart phones and tablets). The full-day workshop offered participants a chance to explore mobile device usage and the unique usable security challenges that arise, discuss proposed systems and ideas that address these needs, and work towards the development of design principles to inform future development in the area. Given that these issues are most relevant to those involved in the design of mobile devices, co-locating with MobileHCI was a clear advantage.

Participants to the one-day workshop included established academics, industry practitioners, and students. The schedule allowed ample opportunity for interaction, discussion, and exchange of ideas amongst workshop participants. Approximately half of participants had also attended the previous year’s workshop.

Authors’ copy. This article appears in S. Chiasson, H. Crawford, S. Egelman, P. Irani (2014). Reflections on U-PriSM 2: The Second Workshop on Usable Privacy and Security for Mobile Devices. Special Issue of the International Journal of Mobile Human-Computer Interaction (IJMHCI), v2(2).

OVERVIEW AND GOALS

Themes

Computer security and privacy affect every aspect of computing, and are of concern for all users. The mobile device environment is no exception. With the ever-increasing functionality of modern smartphones comes the ability to store personally identifying, private information. While security provisions on traditional desktop and laptop computers have benefitted from increased research in usable security and privacy, parallel research for the unique mobile device environment is still in its infancy. This environment is characterized by the ability of users to install apps quickly and easily, a bursty use pattern in which the device is used frequently for short periods of time, and minimal user interfaces. This unique environment means that traditional security and privacy provisions such as passwords and PINs are a poor choice.

The popularity of smartphones has created an urgent need for usable security research targeted at understanding the distinct security threats arising from ubiquitous and mobile usage. Security and privacy are challenging design spaces because of several unique characteristics. For example, users typically focus on primary tasks while leaving security and privacy as secondary concerns or ignoring them altogether. Users may concentrate on some aspects of strong security (e.g., choosing a secure password) but undermine their efforts by neglecting other aspects (e.g., entering their password on their mobile device without considering that shoulder surfing is possible), and they may act insecurely without realizing that this can have later ramifications (e.g., installing apps from unknown sources). Accepted human-computer interaction (HCI) design principles do not necessarily apply because of the adversarial nature of security and privacy: attackers actively try to breach the system, leverage interface cues available to legitimate users, and deceive users by spoofing trusted indicators. The very mobility of the devices also have privacy and security ramifications that go beyond accepted HCI design principles. When a device may be easily lost, stolen or forgotten, efforts must be made to allow for privacy and security methods that protect the device and its data in this situation.

The topics within scope for the U-PriSM 2 workshop included the following: user authentication on mobile devices, permission management for applications, secure mobile payment, security indicators and features for mobile web browsing, do-not-track on mobile devices, protecting location privacy of mobile users, physical security of mobile devices (against loss or theft), and comparisons of usable privacy or security features between mobile platforms.

Submissions

Participants of the workshop submitted 2-4 page position papers or descriptions of work in progress. Speculative or creative out-of-the-box ideas were welcome and encouraged. While completed work was not required, papers were required to provide reasonable evidence to support their claims. Work in progress was especially encouraged to provide participants a chance to receive feedback and discuss ideas during the workshop, with the expectation that the idea would be refined and then submitted to a venue with published proceedings at a later time. This early feedback from the community provides valuable insight that will strengthen the eventual publication.

Papers were selected by the organizing committee and were optionally made available on the workshop website. Authors could choose to have only an abstract made publicly available on the web, and this was especially important for work that will eventually be published elsewhere. Papers were not included in the ACM Digital Library (DL) and our intention was that accepted submissions would **not** be considered “published.”

Workshop format

The schedule for the one-day workshop included multiple sessions, each addressing a particular workshop theme. Each session combined two papers on related topics that were presented back-to-back without questions, followed by a combined panel discussion in which the two authors fielded questions from both the audience and each other.

The workshop began with a keynote presentation by Alexander De Luca of Ludwig-Maximilians-Universität München, who discussed the "smartphone authentication dilemma." Dr. De Luca has over a decade of experience in research for mobile devices and much of his research investigates the challenges involved in usable privacy and security for mobile devices. The primary message of his keynote presentation was that given the diverse user base and the increasing amount of sensitive information accessible from mobile devices, it is critically important that mobile device authentication be both usable and secure in different usage scenarios. He gave participants a preview of some of the novel authentication research being conducted in his lab. Dr. De Luca finished the keynote with a series of suggestions for designing authentication systems for smartphones based on his years of experience.

WORKSHOP DISCUSSION POINTS

The workshop generated lively discussion and debate on many of the workshop themes. We summarize the main topics in an effort to capture some of the ideas generated at the workshop.

Two workshop papers were on user authentication. One explored the need for multiple levels of authentication depending on the applications and data presently being accessed. Debate followed about whether implicit authentication could be used in some circumstances to reduce the number of authentication actions required of users and how configuration of such a system could be accomplished given that the set of applications installed on each phone and the preferences of users are both highly individualized. The second paper examined whether recent phone activity could form the basis for fallback authentication, for example, by having users identify the recipient of the most recent text message. The audience raised several interesting privacy implications associated with the approach and discussed whether these could be addressed with careful design and positioning of the fallback questions.

The second session focused on user understanding of security and privacy risks associated with mobile usage. One paper presented findings of a large survey assessing user perceptions and explored the economics of how much users would be willing to pay for a privacy-protecting mobile device. The audience debated whether users fully understood the associated privacy implications and whether there is industry incentive to provide such devices given that their economic model relies on sharing user data. The next paper presented a prototype system that assists users by providing risk assessments and recommendations on whether it is safe to connect to available networked devices. Discussion touched on issues of liability if the system says a connection is safe and there is a security breach, whether it is possible to provide the user with enough information to be valuable without overwhelming them with technical details, and methodology for the evaluation of such a system.

User behaviour and understanding was the theme of the third session. The first paper examined differences in the privacy and security behaviour and attitudes of Android and iOS users. Debate followed on how the marketplace and the app permission models influence these perceptions and whether users of different skill levels gravitated towards different operating systems. The second paper presented research on smartphone users' folk models of security. Folk models are popular understanding or beliefs that may not necessarily reflect reality, yet influence user behaviour. Conversation focused on whether folk models for mobile security and privacy differed from those on desktop computers, whether cultural influences impacted users' perspectives, and how these might be used in the design of security and privacy features.

The final paper session of the day explored app permissions. First, we heard about a proposed system for location sharing that takes into account whether the current location is a known public space.

For public spaces, exact location is revealed while only approximate location is disclosed for private spaces. Discussion ensued about whether it is reasonable to assume that users are always willing to share their presence in public spaces and whether the technology can accurately differentiate between public and private spaces (e.g., if a high-rise building has a shopping mall on the ground floor and residential apartments on upper floors). The second paper examined whether the inclusion of developer-specified strings in iOS 6 to explain the need for specific app permissions actually helps users make more informed decisions. The audience debated the usefulness of such strings and questioned whether this could be used by developers to trick users or to downplay potential security or privacy risks.

The day concluded with an open-mic session where attendees could bring up any further topics for discussion and debate. Very early research ideas were discussed as well as plans for future U-PriSM events.

FUTURE OF THE MOBILE DEVICE SECURITY RESEARCH FIELD

Mobile devices are ubiquitous. Accordingly, mobile device manufacturers and developers have taken advantage of their ubiquity to provide devices that are both more functional and able to store increasing types and amounts of information. Consumers have responded by using the available functionality to the fullest. This means that consumers are performing tasks such as purchasing goods, taking photos and sending email and text messages, all of which may contain potentially private information. Currently, smartphones generally use PINs as a form of security, both for authentication and for access control. While such secret knowledge-based techniques have their place, the current research into the field of mobile device security has produced viable alternatives such as graphical passwords and biometrics-based models. It remains to be seen how these alternative authentication methods will address the usable security needs of mobile device users.

The work presented at the U-PriSM 2 workshop represents the cutting edge of mobile device security work. Future research is often strongly guided by past research and limitations of current technologies. The field of mobile security will see improvements in authentication choices for mobile devices, determination of access control methods that go beyond point-of-entry security, a better match between app permission models and user requirements, privacy features that protect individuals while maintaining viable economic models, as well as strong considerations and research into the needs and wants of end-users. These topics will come together to provide a more seamless security environment – one that does not expect the user to “do security” each time they pick up their mobile device or prior to accomplishing their main tasks. Other work will forward our provision of privacy on these always-connected devices, which are increasingly able to store and manipulate potentially private information. Such privacy research will aim to put control of data in the hands of the user, or at the very least give the user choices as to how and when their information is used. Future U-PriSM workshops will provide a forum for discussion and debate of such research efforts and directions.

CONCLUSIONS

The future of mobile device security and privacy research closely follows the work presented at U-PriSM 2. Significant focus was placed on moving beyond point-of-entry security, understanding user needs and actions on mobile devices, as well as methods of further protecting user privacy when using mobile devices. Other future work related to giving users more input into the security decisions that they are required to make on a daily basis as they use, and expand their use, of their mobile device.

The value of workshops such as U-PriSM 2 should not be overlooked. Providing researchers with a venue where they can discuss work-in-progress allows them to elicit opinions and receive feedback on early work that will help mature it into research that provides a demonstrable impact. Based on participant feedback and the success of the first two U-PriSM workshops, we intend to provide future workshops along the same lines.