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

Sonia Chiasson, School of Computer Science, Carleton University, Ottawa, Ontario, Canada
Heather Crawford, Department of Computer Science, Florida Institute of Technology, Melbourne, FL, USA
Serge Egelman, University of California, Berkeley, CA, USA
Pourang Irani, Department of Computer Science, University of Manitoba, Winnipeg, 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: Human-Computer Interaction, Mobile Devices, Security, Usable Privacy, Usable 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 mo-
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.

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
Related Content

An Examination of Organization-Information System Fit from Perspectives of Technical Fit and User Fit

Conclusion
[www.igi-global.com/chapter/conclusion/63862?camid=4v1a](www.igi-global.com/chapter/conclusion/63862?camid=4v1a)
Human Factors in the "System Selection" Stage of Library Automation
www.igi-global.com/chapter/human-factors-system-selection-stage/24736?camid=4v1a

Private Power and New Media: The Case of the Corporate Suppression of WikiLeaks and its Implications for the Exercise of Fundamental Rights on the Internet
www.igi-global.com/chapter/private-power-new-media/64940?camid=4v1a