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

Sonia Chiasson
Carleton University
Ottawa, ON, Canada
chiasson@scs.carleton.ca

Heather Crawford
Florida Institute of Technology
Melbourne, FL, USA
heatherannecrawford@gmail.com

Serge Egelman
UC Berkeley
Berkeley, CA, USA
egelman@cs.berkeley.edu

Pourang Irani
University of Manitoba
Winnipeg, MB, Canada
irani@cs.umanitoba.ca

MobileHCI '13, Aug 27-30 2013, Munich, Germany
ACM 978-1-4503-2273-7/13/08.
http://dx.doi.org/10.1145/2493190.2499470

Abstract

The Second Usable Privacy and Security for Mobile Devices Workshop (U-PriSM 2) was held with MobileHCI'13. The U-PriSM 2 workshop was 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). Security often involves having non-security experts, or even novice users, regularly making important security 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. 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.

Author Keywords

Usable security, usable privacy, mobile devices, HCI

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous;K.6.5Computing MilieuxSecurity and Protection

Overview and Goals

The Second Workshop on the Usable Privacy and Security of Mobile Devices (U-PriSM 2) [1] was co-located with MobileHCI'13 in Munich, Germany. This followed the 2012 U-PriSM workshop co-located with the ACM Symposium on Usable Privacy and Security (SOUPS) in Washington, DC.

The U-PriSM 2 workshop 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). Participants had 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.

Themes

Computer security and privacy affect every aspect of computing and are of concern for all users. Security now involves having non-security experts, or even novice users, regularly making important security 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.

The popularity of smart phones 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, leaving security as a secondary concern. They 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 may not apply because of the adversarial nature of security and privacy: attackers will actively try to breach the system, will leverage interface cues available to legitimate users, and will deceive users by spoofing trusted indicators.

Topics for the U-PriSM 2 workshop included: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), new security or privacy functionality and design for mobile devices, user testing of mobile security or privacy features, lessons learned from deployment of mobile security or privacy features, comparisons of usable privacy or security features between mobile platforms.

Participation

Participants of the workshop submitted 2-4 page papers describing research results or work in progress, position papers, and practitioner/industry or experience reports focused on any workshop topic. Speculative or creative out-of-the-box ideas were welcome and encouraged. While completed work was not required, papers were required to

[1] http://people.scs.carleton.ca/~chiasson/uprism2

provide reasonable evidence to support their claims. Work in progress was encouraged to provide participants a chance to receive feedback and discuss ideas during the workshop.

Papers were selected by the organizing committee and were optionally be made available on the workshop website. Authors could choose to have only an abstract made publicly available on the web, especially for work-in-progress that will eventually be published elsewhere. As the workshop is intended for work-in-progress, papers were not included in the ACM DL and our intention was that these are NOT considered "published".

Organizers' Background

Sonia Chiasson is the Canada Research Chair in Human Oriented Computer Security and an Assistant Professor in the School of Computer Science at Carleton University. She participates in several national research networks in Canada. She is a Co-Principal Investigator in the NSERC ISSNet strategic network on computer security and leads its project on Human Behaviour and Computer Security. She is a Collaborative Network Investigator in the GRAND (Graphics, Animation, and New Media) Network of Centres of Excellence and is a Collaborating Researcher in the NSERC Surfnet (surface computing) strategic network. She has been on program committees and a reviewer for leading security, HCI, and usable security venues. She has organized workshops on the mobile security and privacy of mobile devices for ISSNet and for SOUPS, and has given tutorials on experimental design for usable security research. Her research group is currently conducting relevant research on user authentication for mobile devices and on alternative captchas for mobile devices.

Heather Crawford will be an Assistant Professor of Computer Sciences at Florida Institute of Technology, within the Harris Institute for Assured Information as of August 2013. Her PhD work focused on alternative authentication methods for mobile devices. Her expertise is in biometrics, transparent authentication and usable security. She has reviewed papers for leading security publications such as Computers & Security, Security & Privacy Magazine, and IEEE Transactions on Systems, Man and Cybernetics.

Serge Egleman is a researcher in Computer Science at the University of California, Berkeley. He received his PhD from Carnegie Mellon University and has also performed research at NIST, Microsoft Research, and Xerox PARC. He has served on numerous HCI, security, and usable security program committees and has organized workshops on usable security at CHI and at NIST. His current research focuses on usable privacy and security of mobile devices, particularly permission-granting interfaces for applications.

Pourang Irani is an Associate Professor in the Department of Computer Science at the University of Manitoba. He is a Collaborative Network Investigator in the GRAND (Graphics, Animation, and New Media) Network of Centres of Excellence and is a Collaborating Researcher in the NSERC Surfnet (surface computing) strategic network. He has been part of the MobileHCI organizing committee for the last two years. His research is in the areas of Human-Computer Interaction and Information Visualization. He has particular interest and expertise in mobile interfaces.