Editorial

Alexander De Luca and Emanuel von Zezschwitz*

Usable privacy and security

DOI 10.1515/itit-2016-0034

Privacy and security research have been important topics for the longest time but are gaining even more importance in our networked world. New trends and technologies such as the internet of things further strengthen the need for good security and privacy supporting research and technologies. Unfortunately, respective tools were traditionally created by security experts for experts and were hard or impossible to use without a degree in IT security. What is end-to-end encryption worth if only a fraction of users has the technological capabilities of actually using it in their everyday lives? What is password protection worth if password choice is predictable and users tend to reuse the same password for multiple services?

In the last two decades, this situation has significantly changed to the better with the advent of the research field of usable privacy and security. The main goal of this field is to help users to maintain their privacy and security. Researchers focus on identifying threats and solving them by designing and creating technologies in a way that makes them actually usable by anyone, no matter the background knowledge that person has. For this purpose, new technologies are designed and evaluated from a human-centered perspective.

The focus of this special issue is to outline current threats to privacy and security that users face and how privacy and security can be achieved by taking the users into the loop when designing such systems. The articles we picked highlight some of the main challenges that privacy and security face these days and illustrate user-centered approaches to understand and solve these issues. The first part of this special issue deals with important privacy questions like online privacy, privacy policies and social cybersecurity. The second part focuses on usable security-enhancing technologies and presents insights from the domain of usable authentication.

In today's connected world, data collection takes place on a daily basis. For instance, in order to register for an online service, we usually provide personal identifiable information (PII) such as our names, email addresses or telephone numbers. In this light, Martin Ortlieb and Ryan Garner present the results of a large scale user study on online privacy in the UK. They investigate the sensitivity of personal data items in three different online contexts: online retail, social networking and information search. The results reveal that passively collected data is in general more sensitive than concrete data provided by the users and that while some data is acceptable to collect in certain contexts, it is a no-go in others, especially when its immediate use is not clear to the users.

Consequently, the work by Florian Schaub et al. sheds light on how to help users in better and more easily understanding such data collection practices. The Authors present an approach to use crowdsourcing to analyze privacy policies to provide more transparency about a service's data collection practices. Privacy policies are typically long and complex documents which are hard to understand for the average user. The presented approach illustrates how crowdsourcing can help users to make sense of privacy policies that are usually ignored by them. The authors discuss best practices, lessons learned and research challenges of using crowdsourcing to generate more effective notice formats.

An important, and often neglected, part of data collection is possible (social) consequences that come with sharing specific information with a service or the public (e.g. posts on a social networking platform). In the last article on privacy, Sauvik Das claims that users' low security sensitivity can partially be explained by the fact that security and privacy behaviors can have myriad of social consequences. For example, some users might fear to be perceived as paranoid or as someone with something to hide when using advanced security mechanisms.

The paper investigates social triggers for behavior change and describes recent work that establishes a theoretical foundation for a new genre of usable security research: social cybersecurity.

The second part of this journal is dedicated to usable security-enhancing technologies. In the first article, Daniel Buschek talks about how implicit information (e.g.

***Corresponding author: Emanuel von Zezschwitz,** Universität München, LFE Medieninformatik, Amalienstr. 17, 80333 München, Germany, e-mail: emanuel.von.zezschwitz@ifi.lmu.de
Alexander De Luca: Universität München, LFE Medieninformatik, Amalienstr. 17, 80333 München, Germany

from smartphone sensors) and biometrics can be used beyond user identification and verification. The paper highlights connections between different application areas of implicit information and discusses that results from usable privacy and security research can inform other disciplines. The paper enfolds a new design space and sheds light on the interconnections to UI personalization and digital self presentation.

One potential source for implicit information are wearable devices. Andrea Bianchi and Ian Oakley close this special issue with a discussion of trends and opportunities of this device class which has become widely spread in the last years. The authors claim that novel form factors and sensor-rich technologies pose new security challenges. They review wearable authentication schemes according to the traditional classification of authentication via tokens, passwords or biometrics and provide insights on whether and how such technologies have the potential to support users with their everyday authentication tasks. Finally, the paper summarizes challenges of maintaining privacy and security in wearable contexts and identifies four key themes that will drive future research.

We hope the readers will enjoy these articles and that they will walk away from this lecture with new insights on the importance of usable privacy and security.

Bionotes

Dr. Alexander De Luca
Universität München,
LFE Medieninformatik,
Amalienstr. 17, 80333 München, Germany
alexander.de.luca@ifi.lmu.de

Alexander De Luca has been active in the field of usable security and privacy for over a decade now. During this time, he has been working for different research institutes, including the media informatics group at Ludwig Maximilians-Universität München, Fraunhofer FIT Bonn and DFKI Saarbrücken (the German research center for artificial intelligence). He is very active in the research field and is a volunteer for many program committees of highly ranked conferences such as CHI and CCS.

Emanuel von Zezschwitz
Universität München,
LFE Medieninformatik,
Amalienstr. 17, 80333 München, Germany
emanuel.von.zezschwitz@ifi.lmu.de

Emanuel von Zezschwitz graduated in media informatics at the Ludwig Maximilian University of Munich in 2010 (German Diplom). Since 2011, he is a research assistant in the Group for Media Informatics at the Ludwig Maximilian University of Munich. He is particularly interested in usable privacy and security concepts for mobile devices. His work got published at leading venues like CHI, SOUPS and IUI. In addition, he is part of several program committees of HCI-related and security-related scientific conferences.