Security and Privacy Aspects of Human-Computer-Interactions

Nicholas H. Müller
University of Applied Sciences
Würzburg-Schweinfurt
nicholas.mueller@fhws.de

Kristin Weber
University of Applied Sciences
Würzburg-Schweinfurt
kristin.weber@fhws.de

Paul Rosenthal
University of Rostock
research@paul-rosenthal.de

Special-Track Introduction

With increasing digitization, the security and privacy aspects of information are a non-negotiable factor in information system design and operation. Especially the human factor of information systems is a pivotal role in information security and increasingly relevant in establishing user-privacy concepts. More often than not, their knowledge about security aspects and ways of user-manipulation tactics are the last line of defense against cyber-attacks. However, studies show users are also seen as the weakest link in information security. Therefore, they are also the primary target of attackers.

In addition to the traditional forms of user-computer-interactions in the form of mouse-keyboard-input-devices, new ways of system-interactions, e.g., physiological data from fitness-trackers, eye-tracking devices or even pupillary responses indicating cognitive-load-levels, are increasingly feasible as everyday HCI-components. With the interest in data privacy increasing, are users aware how valuable those personal input data is and how do they value data privacy measures?

Therefore, we have identified two main aspects relevant to researchers within the domain of Software Technology:

1) how to securely deal with input data (also focusing on privacy aspects)
2) how this data can be utilized in order to increase secure behavior or to raise awareness among users (help the users to make better security-related decisions)

In this minitrack we sought papers that explore concepts, prototypes and evaluations of how users interact with information systems and what implications these interactions have for information security and privacy. Further, we welcomed new and innovative ways of human-computer-interaction and security-related concepts currently examined in the field.

This year four papers will be discussed within this minitrack which cover the above-mentioned facets of security aspects.

1. Why Phishing Works on Smartphones: A Preliminary Study

The first paper by Loxdal, Andersson, Hacks and Lagerström is about the possibilities to acquire sensitive information from a target by posing as trustworthy. Building upon data from another study in 2006, they checked for changes in user behavior in another study in 2015. With phishing being one of the largest security threats, the topic is nowadays as relevant as it was previously. The usual tactic is to pretend to be a familiar website but redirecting to another location. This can be identified as a scam by looking at the URL. Therefore, the authors cloned certain sites and invited their subjects to use their own smartphones to access those sites and asked about user behavior during their encounters with the sites.

2. A Shoulder-Surfing Resistant Scheme Embedded in Traditional Passwords

Our second paper presentation by Lai & Arko is focused on matters of password security. Since typing passwords is vulnerable to simply watching someone entering it, they propose a security feature to prevent this type of attack. When the password field is in focus, a pattern appears and tells the user how to enter the password. Following this hint, some characters are skipped while typing. Since the characters to be skipped are selected at random, any observer would not be able to decipher the whole password even if a recording of the keyboard would be used. They evaluated their pattern-system in a usability study and showed similar levels of accuracy while only marginal longer time to authenticate.

URI: https://hdl.handle.net/10125/71480
978-0-9981331-4-0

3. Understanding Security Behavior of Real Users: Analysis of a Phishing Study

The third paper by Kang, Shonman, Subramanya, Zhang, Li and Dahbura is focused on the analysis of a user study regarding the sorting of phishing emails. They assigned participants to multitasking and/or incentive conditions. Their results indicate that multitasking and incentives create complex dynamics while demographic traits and cybersecurity training can be informative predictors of user security behavior.

4. Immersive Storytelling for Information Security Awareness Training in Virtual Reality

Our fourth paper presentation by Ulsamer, Schütz, Fertig & Keller is about their research regarding Virtual Reality and storytelling. Since the need for information security awareness (ISA) is constantly increasing, the need for successful trainings increases as well and they have to be performed regularly. According to their research, storytelling in VR might be a solution to learning fatigue. Because education via VR has led to a sustainable learning effect in other fields and therefore, they evaluated the use of immersive VR storytelling for ISA trainings, too. They evaluated their approach by having two groups: one with traditional e-learning and one using the immersive VR training. The results showed that the VR group achieved higher scores than the e-learning. And furthermore, the retention in the VR group might indicate a sustained learning effect from the VR training.