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

1. 360 Degrees of Security: Can VR Increase the Sustainability of ISA Trainings?

The first paper by Fertig, Henkelmann and Schütz is about Information Security Awareness (ISA), and how to enhance knowledge about it – by applying VR training situation. In order to compare the effectiveness, the state of the art regarding knowledge transfer has been used to create a computer-based video-training and a VR training, which allowed the user to grasp the situation without disturbances from the real world.

Although they were able to show an increase in knowledge about ISA via VR, they were not able to show it to be more effective than a traditional video-training.

2. Phishing, Data-Disclosure and The Cognitive Reflection Test

Within the second paper by Tjostheim, the author is focused on matters of phishing. Since there might be enough data ‘out-there’ to leverage a successful phishing attack, one beneficial security aspect might be to identify the willingness to disclose personal information online. Therefore, the results of three large-scale studies from Norway are reported, in which the cognitive reflection test and the willingness to share personal data was the subject matter.

3. Automated Measuring of Information Security Related Habits

The third paper by Fertig, Schütz & Weber is focused on the analysis of a user study regarding the measurement of habits as an influencing factor within the domain of Information Security Awareness.

URI: https://hdl.handle.net/10125/80265
978-0-9981331-5-7