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 nonnegotiable 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 cyberattacks.

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? 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 data privacy. Further, we welcomed new and innovative ways of human-computer-interaction and security-related concepts currently examined in the field.

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

1. A Literature Review Regarding Aspects of Measuring Information Security Awareness

The first paper by Fertig & Schütz is about the available literature regarding the measurability of security awareness. To make employees aware of their important role for information security, companies typically carry out security awareness campaigns. The success and effectiveness of those campaigns have to be measured to justify the budget, for example. Therefore, they did a systematic literature review in order to learn how information security awareness (ISA) is measured in theory and practice. They covered published literature as well as unpublished information. The unpublished information was retrieved by interviewing experts of small and medium-sized enterprises. The results show that ISA is mostly measured via questionnaires. About 40 % of the questionnaires are based on the Knowledge-Attitude-Behavior-Model which is itself scientifically weak. According to studies, measuring knowledge is not sufficient and, instead, behavior has to be measured. Their results show that the answers of participants in questionnaires often differ from the truth due to wrong perception or social desirability bias. Therefore, behavior should be measured through behavior tests.

2. A User-Centric Semantic Model for Representing and Discovering Privacy Issues

Our second paper presentation by Lu & Li from the University of Kent is focused on matters of privacy. In today’s highly connected cyber-physical world, people are constantly disclosing personal and sensitive data to different organizations and other people through the use of online and physical services. Such data disclosure activities can lead to unexpected privacy issues.

URI: https://hdl.handle.net/10125/64539
978-0-9981331-3-3

However, there is a general lack of tools that help to improve users' awareness of such privacy issues and to make more informed decisions on their data disclosure activities in a wider context. To fill this gap, this paper presents a novel user-centric, data-flow graph based semantic model, which can show how a given user's personal and sensitive data are disclosed to different entities and how different types of privacy issues can emerge from such data disclosure activities. The model enables both manual and automatic analysis of privacy issues, therefore laying the theoretical foundation of building data-driven and user-centric software tools for people to better manage their data disclosure activities in the cyber-physical world.

3. Preparation of a Targeted Information Security Awareness Training

The third paper describes a procedure to enable the planning of targeted measures to increase the Information Security Awareness (ISA) of employees of an institution. The procedure is practically applied at a German university. With the help of a comprehensive analysis, which is based on findings of social psychology, necessary topics for ISA measures are identified. In addition, reasons are sought for why employees do not conduct information security. The procedure consists of a qualitative phase with interviews and a quantitative phase with a questionnaire. It turned out that the procedure provided many clues to the design of ISA measures. These include organizational and technical measures that can help employees to ensure information-safe behavior. In addition, it was found that there were deviations between the qualitative and quantitative phases and therefore, both phases are necessary. The paper critically discusses the procedure and also addresses the strengths and weaknesses of the analysis.