Reading Response 3: Risk Representation in Usable Privacy and Security Research

CSEC 759 - Mehul Sen

"A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research" by Distler et al. [1] is a systematic literature review of usable privacy and security (UPS) research papers between 2014 and 2018 attempting to identify the most common methods employed by researchers within the UPS community, how risk was represented in these papers and how deception was used within their study protocols. Their research included reviewing 284 papers across top publications and exploring the trends found within them. They primarily focused on how the papers represented and measured risk and the approaches used by researchers to represent the participants' risk level.

They categorized risk representation by the researchers into four categories: naturally occurring, simulated, mentioned, and no induced risk. Each category has advantages and disadvantages, with certain types being more effective in particular research than others. The first type is the naturally occurring risk category, which refers to the risk arising naturally from participants' daily lives. This category provides the most accurate data for researchers, as it is how participants behave and react to risks in their daily lives. However, it is also the most time-consuming, as researchers have to observe the participants for an extended period, hoping that a risky event will occur naturally. Moreover, if self-reported, the study's accuracy relies entirely on the participants. Additionally, researchers have no control over the study variables or risk conditions, which may expose participants to significant harm from risks. Therefore, this type of risk representation should be performed where the risk to participants is minimal, and the study takes a long time. For example, Huh et al. conducted a study to observe the effectiveness of a password reset email to LinkedIn users, which did not pose a significant risk to the users should they have not changed their passwords while providing sufficient time to submit their responses to an online survey. [2]

The second type is simulated risks, represented through prototypes, assigned tasks, or deception and observing participants' behavior. This category allows researchers to simulate a rare, risky event while completely controlling the risk conditions or study variables. Additionally, this ensures that the participants are protected if appropriately conducted. However, the downside of this category is that it depends entirely on how capable the participant is to put themselves in the presented simulation and react as they would in the real world. Thus, it only sometimes provides the most accurate results due to the risk of priming the participants for the study. Therefore, researchers should perform this type of risk representation when considering otherwise harmful risks that can be simulated in a safe scenario while requiring participants to react relatively realistically. This type of risk representation is observed in Ur et al.'s study, which required participants to create a password for an account they should consider critical. This scenario simulated an otherwise harmful aspect, such as a password to a primary account, allowing the researchers to observe how the participants realistically reacted. [3]

The third type is mentioned risk, which involves presenting participants with a questionnaire asking them to put themselves in hypothetical scenarios without using simulations through prototypes and assigned tasks. This type of risk representation requires the least effort, allowing it to be performed on a much larger population of participants. However, it relies on the participants' imagination more than simulated risks, lacking engaging scenarios. This could remove necessary context from the participants' responses, thus providing relatively inaccurate results. Therefore, researchers should perform this type of risk representation when requiring a consensus about a subject. For example, Sen et al.'s study required participants to encode clauses of a privacy policy in legalese terms, using twelve participants recruited via a company mailing list who were primarily privacy champions. [4]

Lastly, Distler et al. also categorize a no-induced risk representation category where researchers do not create perceptions or representations of risk for the participants. This type of risk representation allows participants to focus solely on the usability aspect of their products without any confounding risk effects, thus avoiding any bias about security/privacy. However, it completely disregards any perceptions or behaviors related to risks, which, if included, might have the participants behaving differently than they do within this category. Therefore, researchers should perform this type of risk representation when the risk does not need to be represented or is not the primary focus of the research paper, letting the participants focus more on the usability of a product than any associated risks. For example, Crawford and Ahmadzadeh's study had participants type phone sentences to understand participant movement's effect on keystroke dynamics, with the focus of the paper not being on the risk associated with keystroke dynamics as an authentication method but solely on the technical aspects of the keystroke dynamics. [5]

References

[1]: "A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privact and Security Research" Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig, *ACM Transactions on Computer-Human Interaction*, Dec. 2021.

[2]: "I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails" Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, Konstantin Beznosov, *Conference of Human Factors in Computing Systems*, May 2017.

[3]: ""I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab" Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor, *Symposium on Usable Privacy and Security*, July 2015.

[4]: "Bootstrapping privacy compliance in big data systems" Shayak Sen, Saikat Guha, Anupam Datta, Sriram K. Rajamani, Janice Tsai and Jeannette M. Wing, *IEEE Symposium on Security and Privacy*, May 2014.

[5]: "Authentication on the Go: Assessing the Effect of Movement on Mobile Device Keystroke Dynamics" Heather Crawford and Ebad Ahmadzadeh, *Symposium on Usable Privacy and Security*, July 2017.