Thinking like a Fraudster: Cognitive Walkthrough in Malicious Settings

Andreas Gutmann[1,2] and Steven J. Murdoch[1,2]

[1] OneSpan Innovation Centre, Cambridge, UK
[2] University College London, London, UK
andreas.gutmann@onespan.com, s.murdoch@ucl.ac.uk

Abstract. Usability evaluations are commonly used as part of a Privacy and Security by Design approach. The main purpose is to identify residual or new privacy and security risks, but the findings can also improve the overall usability of those technologies. A common assumption during such evaluations is about the presence of malicious actors in the environment of the technology. An evaluation in a malicious setting requires a fundamentally different approach than in a benign: The former attempts generalisation over all adversary strategies, while the latter assumes a fixed environment.

In recent work [1], we adapted the well-known Cognitive Walkthrough (CW) usability inspection method to support malicious settings. The CW is a usability inspection method with a history of more than 20 years in the HCI community and a staple for many practitioners. It can be applied during any phase of the product design and development process with less time and resource requirements than an empirical user study. But the requirement to fix the environment of a CW can be at odds with attempts to generalise over all adversary strategies.

Our extension to the CW method allows the evaluator to model malicious actors during their walkthroughs while keeping the UI, its user, the user's goal, and the context-of-use fixed. Furthermore, using this method we avoided deceiving participants about the specific purpose and objective of our study, which would have been required in an empirical user study.

In this talk, we present the Cognitive Walkthrough in Malicious Settings methodology and recommend to consider it as an alternative method to empirical user studies, where feasible.

Keywords: Cognitive Walkthrough · Usable Privacy and Security · Privacy and Security by Design · Heuristic Evaluation.

References

1. Gutmann, A., Murdoch, S.J.: Taken out of context: Security risks with security code autofill in ios & macos. Who Are You?! Adventures in Authentication Workshop (WAY) (2019)