Citation: Kaiming Cheng, Jeffery F Tian, Tadayoshi Kohno, and Franziska Roesner. 2023. Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality. USENIX Security 2023 (2023), 18.

Published paper: https://www.usenix.org/system/files/sec23summer_28-cheng-prepub.pdf

Abstract: Perceptual Manipulation Attacks (PMA) involve manipulating users' multi-sensory (e.g., visual, auditory, haptic) perceptions of the world through Mixed Reality (MR) content, in order to influence users' judgments and following actions. For example, a MR driving application that is expected to show safety-critical output might also (maliciously or unintentionally) overlay the wrong signal on a traffic sign, misleading the user into slamming on the brake. While current MR technology is sufficient to create such attacks, little research has been done to understand how users perceive, react to, and defend against such potential manipulations. To provide a foundation for understanding and addressing PMA in MR, we conducted an in-person study with 21 participants. We developed three PMA in which we focused on attacking three different perceptions: visual, auditory, and situational awareness. Our study first investigates how user reactions are affected by evaluating their performance on "microbenchmark" tasks under benchmark and different attack conditions. We observe both primary and secondary impacts from attacks, later impacting participants' performance even under non-attack conditions. We follow up with interviews, surfacing a range of user reactions and interpretations of PMA. Through qualitative data analysis of our observations and interviews, we identify various defensive strategies participants developed, and we observe how these strategies sometimes backfire. We derive recommendations for future investigation and defensive directions based on our findings.