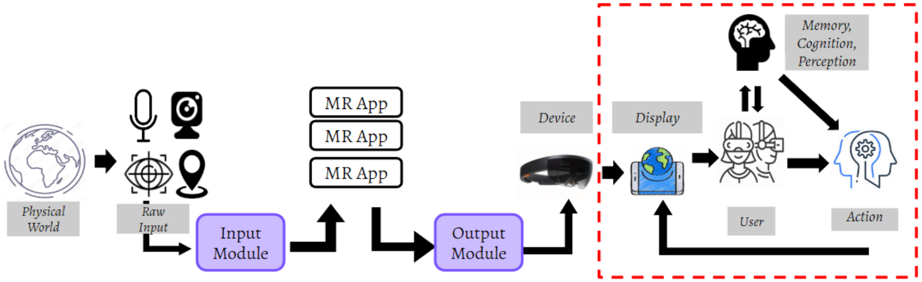
Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality

PAUL G. ALLEN SCHOOL W

SECURITY & PRIVACY RESEARCH LAB UNIVERSITY of WASHINGTON

Motivation

Mixed Reality (MR) output may **negatively** impact users' perception and subsequent behavior.
This paper investigates how users **perceive, react to,** and **defend against** such manipulations.



Human Brain as the Attack Surface

Research Questions:

RQ1: What physical or behavioral reactions and responses do users have when experiencing perceptual manipulation attacks (PMA) in Mixed Reality?

RQ2: What are user-reported reflections, reactions, and defensive strategies to PMA in MR during or shortly after they occur?

Methodology

Generate Perceptual Manipulation Attack (PMA) targeting visual, auditory, and spatial awareness perception.

Mount PMA when user is reacting to real-world stimuli.

In lab study of 21 participants with quantitative & qualitative methods

Results

Behavioral Reactions

- Participants were **susceptible** to manipulative MR content
- Reduced reaction time in **non-attack** setting
- Manipulative MR content **prevented** participants from reacting to real-world instructions

User-reported Reflections

- **Attack impact:** e.g., inability to distinguish between virtual and real
- **Defensive technique:** e.g., learning from past attacks
- **Attack attribution:** e.g., thought the attack outputs were supposed to help them

Takeaway

Users can be manipulated by perceptual manipulation attacks (PMA) in MR.

While participants develop a variety of hypothesis to explain PMA, such expectations can be leveraged by real attackers.

Participants adaptive strategies backfired when attack changed.

Kaiming Cheng kaimingc@cs.washington.edu
Jeffery F. Tian jefftian@cs.washington.edu
Tadayoshi Kohno yoshi@cs.washington.edu
Franziska Roesner franzi@cs.washington.edu

32ND USENIX SECURITY SYMPOSIUM
AUGUST 9–11, 2023
ANAHEIM, CA, USA
www.usenix.org/sec23