PhD Forum Abstract: Towards Secure and Immersive Mixed Reality

Yasra Chandio
University of Massachusetts, Amherst
ychandio@umass.edu

ABSTRACT

A key requirement for MR applications is to make a user feel fully **immersed** in her virtual and/or physical environment **safely**. The immersiveness relies on sensing of user activities and surrounding environment via commodity headsets. The key challenges for these devices are: (1) exploitation of security vulnerabilities that impact physical safety and (2) loss of cognitive safety due to system and development limitations. As a result, immersiveness can be easily disturbed by internal/external triggers, incurring a loss of user's *physical* and/or *cognitive* safety. I analyze vulnerabilities in MR that incur the loss of user's physical and/or cognitive safety.

CCS CONCEPTS

• **Human-centered computing → Mixed / augmented reality**;
• **General and reference → Measurement**.

KEYWORDS

mixed reality, security, safety, presence, dataset

ACM Reference Format:
Yasra Chandio. 2022. PhD Forum Abstract: Towards Secure and Immersive Mixed Reality. In *Proceedings of The 19th ACM Conference on Embedded Networked Sensor Systems (SenSys).* ACM, New York, NY, USA, 2 pages. https://doi.org/00.0000/0000000.0000000

1 INTRODUCTION

Mixed Reality (MR) has metamorphosed into an essential technology for critical applications such as surgery, therapy, etc. marking a significant evolution from its prior use mainly for leisure activities. Leading technology companies are presenting *metaverse* as the future of human interactions and experiences. These technological inventions are welcomed as they improve human lives, but there is a lingering concern that the change may happen too fast. Our recent history of adopting new computing technologies does not forecast an optimistic future. Technological developments have often focused on growth and enabling applications without due consideration of the effects on its users. For example, we are beginning to understand how social media platforms negatively affect their users, especially teenagers. Internet-of-Things (IoT) security and privacy is another example; we were too fast in connecting everything to the Internet without realizing the large attack surface we were enabling. I fear that, with the popularity and rapid adoption of *metaverse*, the effects of MR technologies — on their users will become an afterthought.

A fundamental requirement for MR applications is to make the user feel completely **immersed** in her virtual and/or physical environment **safely**. The immersiveness relies on multi-modal sensing of user activities and the surrounding environment via commodity sensing devices, such as Head-Mounted Devices (HMD), hand-held controllers, and similar devices. MR systems center on tracking humans and enhancing their experience by designing human-in-the-loop systems. The key challenges most human-in-the-loop systems face: (1) exploitation of security vulnerabilities that directly affect the physical safety of users and (2) loss of cognitive safety because of mismatched human visual and sensory information — caused by a variety of system and development limitations. As a result, immersiveness is a very delicate state and internal or external triggers can easily disturb that, leading to a loss *physical* and/or *cognitive* safety for the user. I seek to understand the fundamental problems in MR platforms and devices that might lead to loss of physical or cognitive safety for a user.

(1) **Physical safety:** What kind of attack surfaces are present in MR that an attacker can exploit to lower physical safety?
(2) **Cognitive safety:** How systemic and developmental limitations reduce cognitive safety of the MR users? How can we use systemic tools to quantify the loss of cognitive safety?

In my work, I answer these questions by (1) exploring MR-specific attack surfaces that a malicious entity can leverage to incur physical harm and (2) quantifying the loss of cognitive safety a user experiences when immersiveness is distributed.

2 CHALLENGES AND CONTRIBUTIONS

I next outline the research challenges and the contributions I have made towards ensuring physical and cognitive safety of MR users.

Exploring Security Vulnerabilities in MR. The extensive reliance of MR applications, such as tracking and navigation, on multi-modal sensing streams and spatiotemporal services opens the door for novel and stealthy attacks. Recent studies have demonstrated attacks on individual sensing modalities such as inertial sensor [5] and visual sensor [1]. My preliminary work shows that state-of-the-art sensor fusion techniques, such as SelectFusion, can mitigate such attacks [2]. In principle, when data from one sensor stream is degraded, other streams dominate the tracking algorithms for correct operation. My work focuses on a new attack surface that is resilient to sensor-fusion techniques as it concurrently manipulates multiple sensing streams across spatiotemporal axes. My work solves two key challenges to launching fast and stealthy attacks in MR: **1)** How and when to launch concurrent attacks such

SenSys, November 6-9, 2022, Boston, MA, USA

ACM ISBN 000-0-0000-0000-0/00/00…$15.00
https://doi.org/00.0000/0000000.0000000

that the malicious outcome is hidden both from the user and system checks? **2)** How can an adversary leverage contextual information in a scene to control the duration and impact of attack? Our proposed design uses a variety of frame manipulation techniques across spatialtemporal axes to craft stealthy attacks. The novelty of our attack surface lies in concurrently attacking sensor streams, only across spatiotemporal dimensions, at the right time and for the exact duration to remain stealthy and achieve the desired outcome. This work is under review at **IEEE AIxVR'24**.

Investigating the Correlation Between Presence and Reaction Time in MR. Prior work on quantifying *presence* in MR environments leverages subjective questionnaires that provide post-experience, self-reported, and often inconsistent measure. To find a non-intrusive, objective, and unbiased measure of *presence*, this segment of my work investigates a fundamental question in mixed reality: Would an individual experiencing more *presence*[1] show better performance, e.g., faster *reaction time*[2]? If the answer is yes, we could use a systemic metric such as *reaction time* to quantify *presence*. Prior work has investigated and established a relationship between *presence* and different aspects of human performance [3, 4]. We conduct a 40-participant user study to specifically understand the relationship between *presence* and *reaction time*. We change the *presence* of users, wearing HoloLens 2, by manipulating *place illusion*, changing the appearance of objects, and *plausibility illusion*, altering the behaviour of objects, when interacting with an MR environment. We systemically measure the *reaction time* of users in response to a visual stimulus. Our post-experience questionnaires show a significant change in the presence between experiments. We also observe a change in user *reaction time* as the sense of *presence* changes, demonstrating a correlation between *presence* and *reaction time*. This work is accepted to appear in **IEEE TVCG'23**.

HoloSet - A Dataset for Visual-Inertial Pose Estimation in MR. There is a lack of datasets for visual-inertial odometry applications in MR. To the best of my knowledge, there is no dataset available that is captured from an MR headset with a human as a carrier. To bridge this gap, I present a novel pose estimation dataset — called `HoloSet` — collected using Microsoft Hololens 2, which is a state-of-the-art HMD for MR. Potential applications for `HoloSet` include visual-inertial odometry, simultaneous localization and mapping (SLAM), and additional applications in MR that leverage visual-inertial data.

`HoloSet` captures both macro and micro movements. For macro movements, the dataset consists of more than 66,000 samples of visual, inertial, and depth camera data in a variety of environments (indoor, outdoor) and scene setups (trails, suburbs, downtown) under multiple user action scenarios (walk, jog). For micro movements, the dataset consists of more than 12,000 samples of additional articulated hand depth camera images while a user plays games that exercise fine motor skills and hand-eye coordination. We present basic visualizations and high-level statistics of the data and outline the potential research use cases for `HoloSet`. This work is published at **ACM DATA'22** workshop (to appear).

[1] *presence* is the feeling of being physically and spatially located in an environment.
[2] time taken between when humans perceive something and when they respond to it.

3 FUTURE WORK

While my prior work on exploring security vulnerabilities in MR demonstrated the efficacy of our attack surface, the research thread remains tantalizingly open. I plan to devise new attack mechanisms that leverage signal processing techniques for frame manipulations. I will explore machine learning techniques for finding the right time to attack, and context-aware optimization techniques for maximizing the attack impact and to keep it stealthy. I will also extend this work to explore applications that require micro movements of arms, hands, and fingers, such as surgery and electronics assembly. I also plan to explore additional attack surfaces, such as attacking spatial mapping and eye-gesture tracking. Broadly speaking, I will explore additional security aspects of MR such as ways to steal keys for authentication in keyboard logging as all of these security aspects relate to physical and cognitive safety of MR users.

In investigating the relationship between *presence* and *reaction time*, we used simple one-object scenarios, a design choice to minimize the effect of variables other than presence on the reaction time. Therefore, the setup may not be sensitive to the broader effects of varying the feelings of presence on reaction time in a multi-object virtual scene. Future work should investigate how presence relates to reaction time with different degrees of scene complexity, cognitive load, and dynamic physical environment. Similarly, we investigated the effects of varying the feelings of presence with only periodic tasks and active interaction (tap). It is worth investigating how the presence and reaction time can be affected in other types of non-periodic tasks and passive interaction (eye gaze).

4 CONCLUSION

As Mixed Reality (MR) finds its applications in critical domains such as surgery and therapy, it is important to ensure the physical and cognitive safety of its users. My work has made key strides in this domain by exploring the attack surfaces that could be exploited to incur physical harm and building tools that allow real-time and objective measurement of user's cognitive safety. In the future, I will investigate these research threads further to design mitigation techniques for the attack surface and develop systemic tools for quantifying user's cognitive safety in MR environments.

5 BIOGRAPHY

Yasra Chandio is a third-year Ph.D. student at the University of Massachusetts Amherst. She is advised by Prof. Fatima Anwar. She is a CRA-E graduate fellow[3], Grace Hopper scholar, and Google CSRMP scholar. She plans to submit her dissertation in 2025.

REFERENCES

[1] P. Casey, I. Baggili, and A. Yarramreddy. 2019. Immersive Virtual Reality Attacks and the Human Joystick. *IEEE TDSC*.
[2] Changhao Chen, Stefano Rosa, Yishu Miao, Chris Xiaoxuan Lu, Wei Wu, Andrew Markham, and Niki Trigoni. 2019. Selective Sensor Fusion for Neural Visual-inertial Odometry. In *IEEE/CVF CVPR*.
[3] Arthur Maneuvrier, Leslie Marion Decker, Hadrien Ceyte, Philippe Fleury, and Patrice Renaud. 2020. Presence Promotes Performance on a Virtual Spatial Cognition Task: Impact of Human Factors on Virtual Reality Assessment. In *Frontiers in Virtual Reality*. Frontiers Media SA.
[4] Eric B. Nash, Gregory W. Edwards, Jennifer A. Thompson, and Woodrow Barfield. 2000. A Review of Presence and Performance in Virtual Environments. *International Journal of Human–Computer Interaction*.
[5] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. In *EuroS&P*.

[3] https://cra.org/cra-selects-new-graduate-fellow-yasra-chandio/