

Midwest Security Workshop (MSW 10)

September 20th, 2025
Indiana University

Best Poster Award Selected by Faculties

- **Shadowed Realities: An Investigation of UI Attacks in WebXR**
 - Chandrika Mukherjee, Reham Mohamed Aburas, Arjun Arunasalam, Habiba Farrukh, and Z. Berkay Celik

Shadowed Realities: An Investigation of UI Attacks in WebXR

Chandrika Mukherjee, Reham Mohamed Aburas, Arjun Arunasalam, Habiba Farrukh, and Z. Berkay Celik

Midwest Security Workshop
PURDUE UNIVERSITY **AUS American University of Sharjah** **UCI University of California, Irvine**

Background & Motivation

- **WebXR** enables immersive AR/VR experiences through browsers on head-mounted displays (HMDs).
- **Security-sensitive UI properties** (e.g., transparency, synthetic input) can be exploited for UI-based attacks [1,2].
- Unlike the standard web, **WebXR lacks <iframe>** like element that separates execution of different origins.
- Third-party entities, such as advertisements, **share the same 3D scene** as other objects within the publisher's WebXR site.
- These UI properties can be exploited to integrate **dark patterns**, undermining user autonomy.

Research Overview

- We systematically investigate the UI properties enabling various UI-based attacks exploiting WebXR ad ecosystem and propose a taxonomy of such attacks.
- We also investigate the impact of these attacks on user perception and interaction behavior.

User Study Design

Two Factors – App & Attack Category/ Control Group

IRB Approved
N = 100 participants (ages ≥ 18 years)

Click Manipulation N=20
Peripheral Exploitation N=20
Functionality Disruption N=20
UI-based Privacy Leakage N=20
Control Group N=20

Each Participant

Interacts with Selected App Type

Three randomly selected attack from selected category and implemented in selected app

Qualtrics

Qualitative & Quantitative Data Analysis

User Study Framework


Log Framework: Captures user intended and unintended interactions with objects part of main scene and others such as advertisement

Interaction Metrics: Obtains meaningful quantitative insights from collected logs

Applications: 4 apps x 14 attacks and 4 control group apps incorporating the logging framework

Best Poster Award Selected by Students

- **AutoSpec: A Multi-Agent Framework for Formal Specification of Robotic Vehicle Control Software**
 - Chaoqi Zhang, Hyungsub Kim

**AutoSpec: A Multi-Agent Framework for Formal Specification of Robotic Vehicle Control Software**
Chaoqi Zhang, Hyungsub Kim
Indiana University Bloomington

Motivation

Background: Metric temporal logic (MTL) is a formal specification language used to verify behaviors of robotic vehicle control software, such as ArduPilot and PX4.

Problems:

- Manually writing MTL formulas is time-consuming and error-prone, making it difficult to scale—for example, two experts spent an entire day to create 56 formulas.
- A single large language model (LLM) performs poorly at automatically generating MTL, achieving only 18% accuracy.

Key Idea: Multi-Agent LLM Framework

We introduce **AutoSpec**, a modular multi-agent framework that automatically generates MTL formulas from natural language documentation by decomposing the task into *logic extraction*, *context identification*, and *synthesis*.

Let's thank our hard working student volunteers!

Abhishek Bisht
Chaoqi Zhang
Soyeon Lee

Cloris Shan
Linyun Du

MSW 2026...

University of Wisconsin—Madison!

Early October 2026



Rahul Chatterjee
(Wisconsin)



Kassem Fawaz
(Wisconsin)

Thank you all for attending!

MSW 10
September 20th, 2025
Indiana University