Towards Secure User Interaction in WebXR

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

PURDUE UNIVERSITY · UCI University of California, Irvine · AUS American University of Sharjah

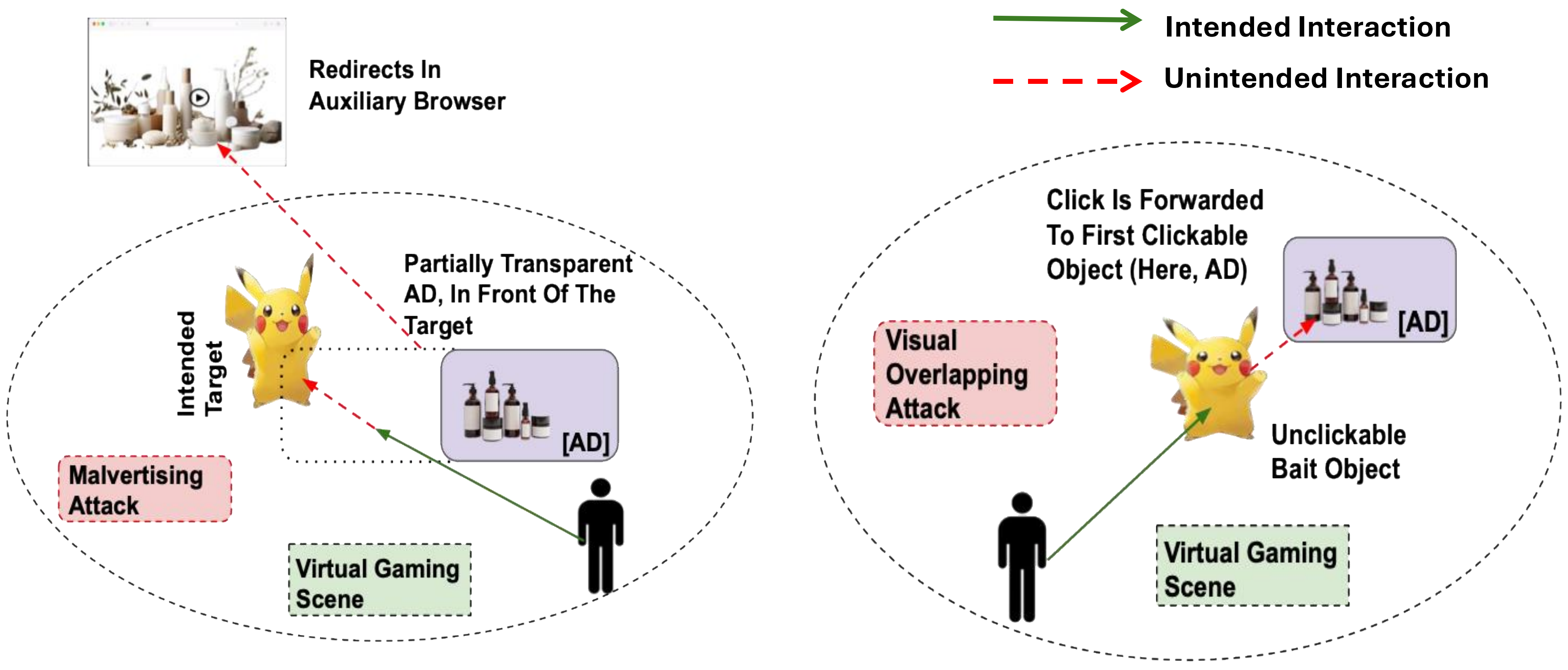
HumanSys 2025

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 [1,2,3].
- Our prior work [3] identifies four categories of UI attacks: (A) Click Manipulation, (B) Peripheral Exploitation, (C) Functionality Disruption, and (D) UI-based Privacy Leakage.
- To assess the impact of these attacks on users, we developed a **logging framework** that captures fine-grained 3D interaction data.

Attack Category	Description
🖱 Click Manipulation (**A**)	Generates revenue from unintentional ad clicks.
👁 Peripheral Exploitation (**B**)	Inflates ad impressions or clicks by exploiting blind spots.
🚫 Functionality Disruption (**C**)	Prevents users from performing intended actions.
🔍 UI-based Privacy Leakage (**D**)	Extracts sensitive user information.

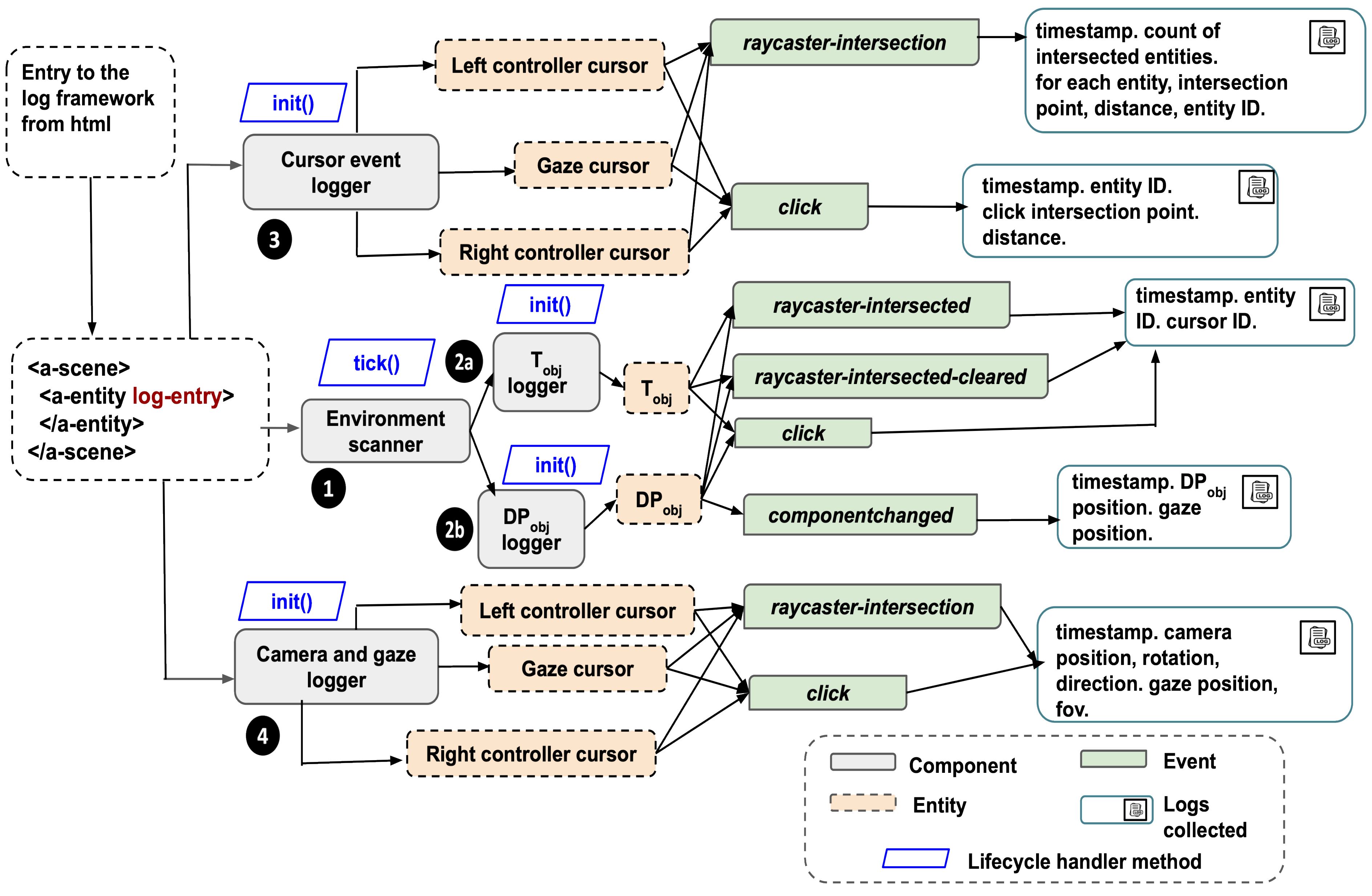
UI-Based Attack Examples


Intended Interaction
Unintended Interaction
Redirects In Auxiliary Browser
Partially Transparent AD, In Front Of The Target
Intended Target
[AD]
Malvertising Attack
Virtual Gaming Scene
Click Is Forwarded To First Clickable Object (Here, AD)
Visual Overlapping Attack
[AD]
Unclickable Bait Object
Virtual Gaming Scene

Methods Overview

- Integrated 14 UI-based attacks from four attack categories into four WebXR apps (gaming, shopping, reading, travel), implemented using A-Frame and Three.js.
- Labeled any objects related to the task as T_{obj} and others potentially linked to dark pattern (e.g., ads) as DP_{obj} .
- Designed a modular logging framework with a single-entry point and embedded it into each app.
- Conducted a between-subjects, in-lab study with 100 participants.

Design of Logging Framework



timestamp. count of intersected entities. for each entity, intersection point, distance, entity ID.

timestamp. entity ID. click intersection point. distance.

timestamp. entity ID. cursor ID.

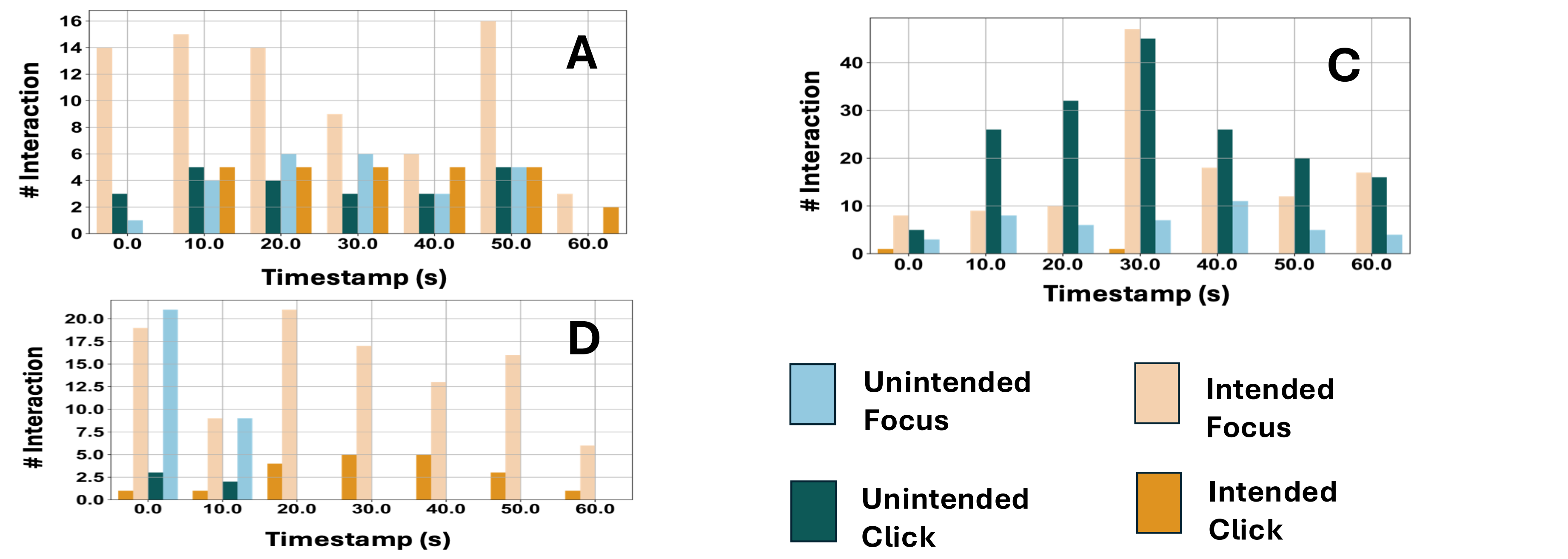
timestamp. DP_{obj} position. gaze position.

timestamp. camera position, rotation, direction. gaze position, fov.

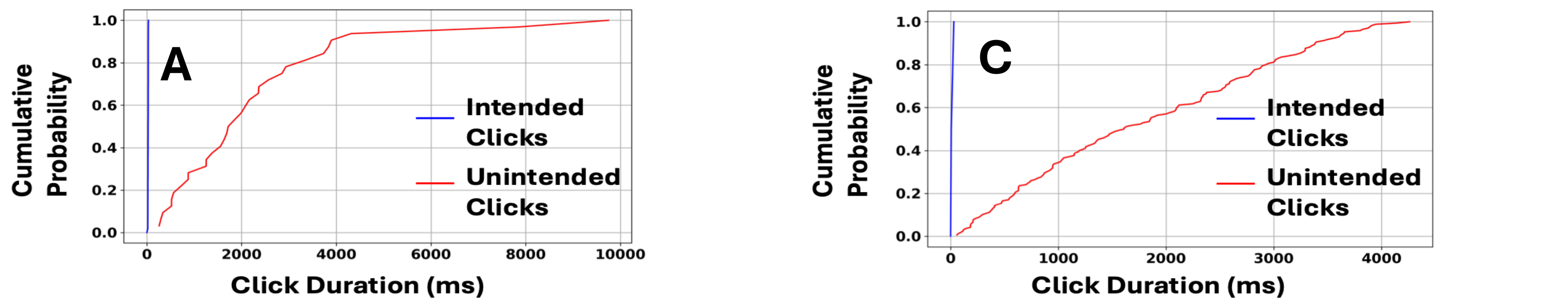
#	Logger Component	Purpose
1	Environment Scanner	Detects new entities and attaches T_{obj} and DP_{obj} logger components.
2	T_{obj} and DP_{obj} Logger	Logs focus initiation, removal, and click events on T_{obj} and DP_{obj}. Also detects intentional/unintentional actions and tracks DP_{obj} movements.
3	Cursor Event Logger	Captures simultaneous interactions with multiple objects via a single cursor.
4	Camera and Gaze Logger	Estimates user position and attention.

Evaluation

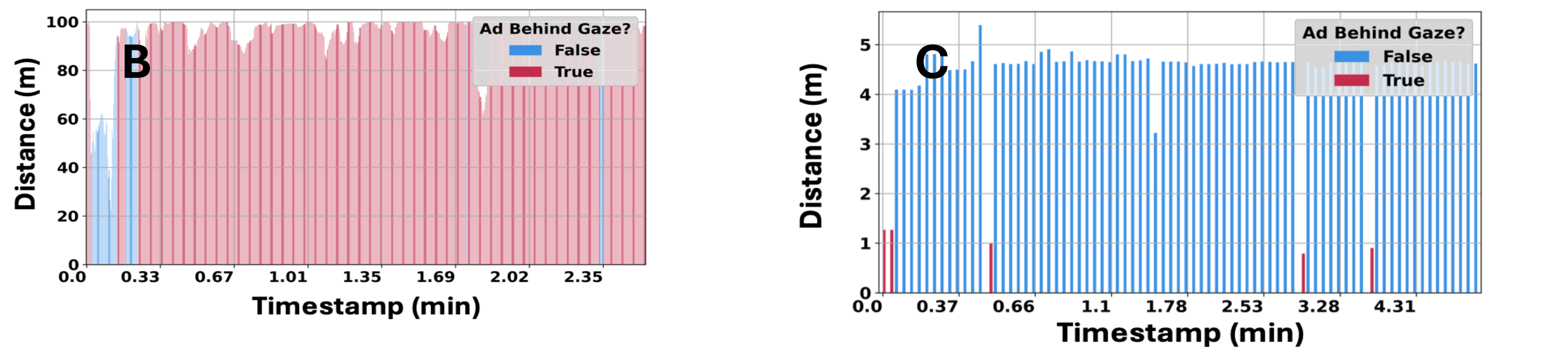
Interaction Trends Across Attack Categories



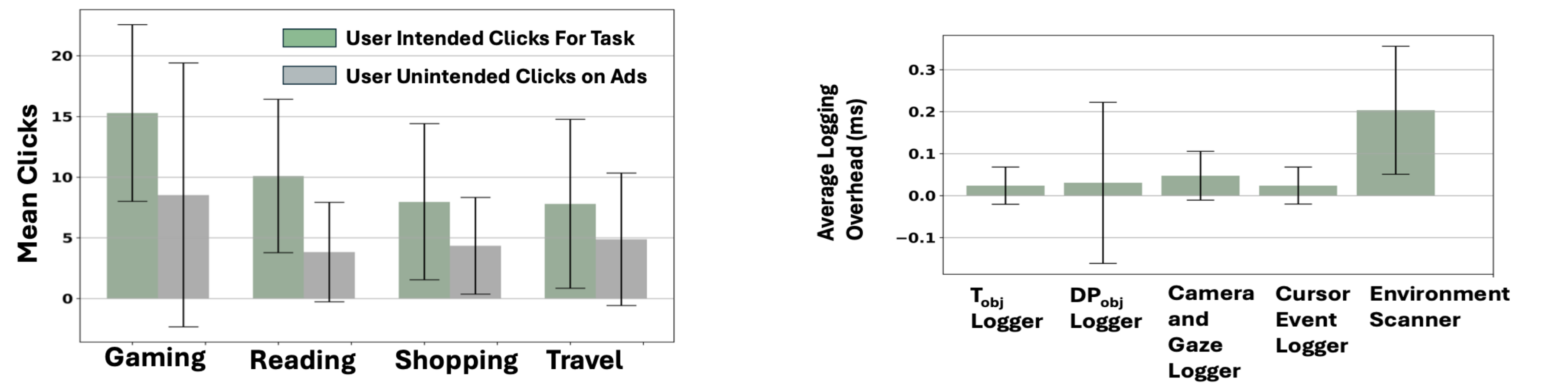
Click Uncertainty



Change in Position of Targets



Aggregated User Clicks and System Performance Overhead



Takeaways & Future Directions

- Developers can analyze user attention and interactions to optimize content placement and detect unintended interactions with third-party elements (e.g., ads).
- Development frameworks and platforms can identify malicious activities and warn users of UI manipulation threats.
- Future work will include detecting multiple attacks simultaneously and applying machine learning based techniques to preserve user autonomy in immersive environments.

Acknowledgements

This work was partially supported by NSF grants CNS-2144645 and IIS-2229876. The findings and recommendations in this work are those of the authors and do not necessarily represent the views of the NSF.

References

[1] Hyunjoo Lee, Jiyeon Lee, Daejun Kim, Suman Jana, Insik Shin, and Sooel Son. 2021. AdCube: WebVR Ad Fraud and Practical Confinement of Third-Party Ads. In USENIX Security.

[2] Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner. 2024. When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. In USENIX Security.

[3] Chandrika Mukherjee, Reham Mohamed, Arjun Arunasalam, Habiba Farrukh, and Z. Berkay Celik. 2025. Shadowed Realities: An Investigation of UI Attacks in WebXR. In USENIX Security.