Shadowed Realities: An Investigation of UI Attacks in WebXR

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

Purdue University · American University of Sharjah · University of California, Irvine

Midwest Security Workshop

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

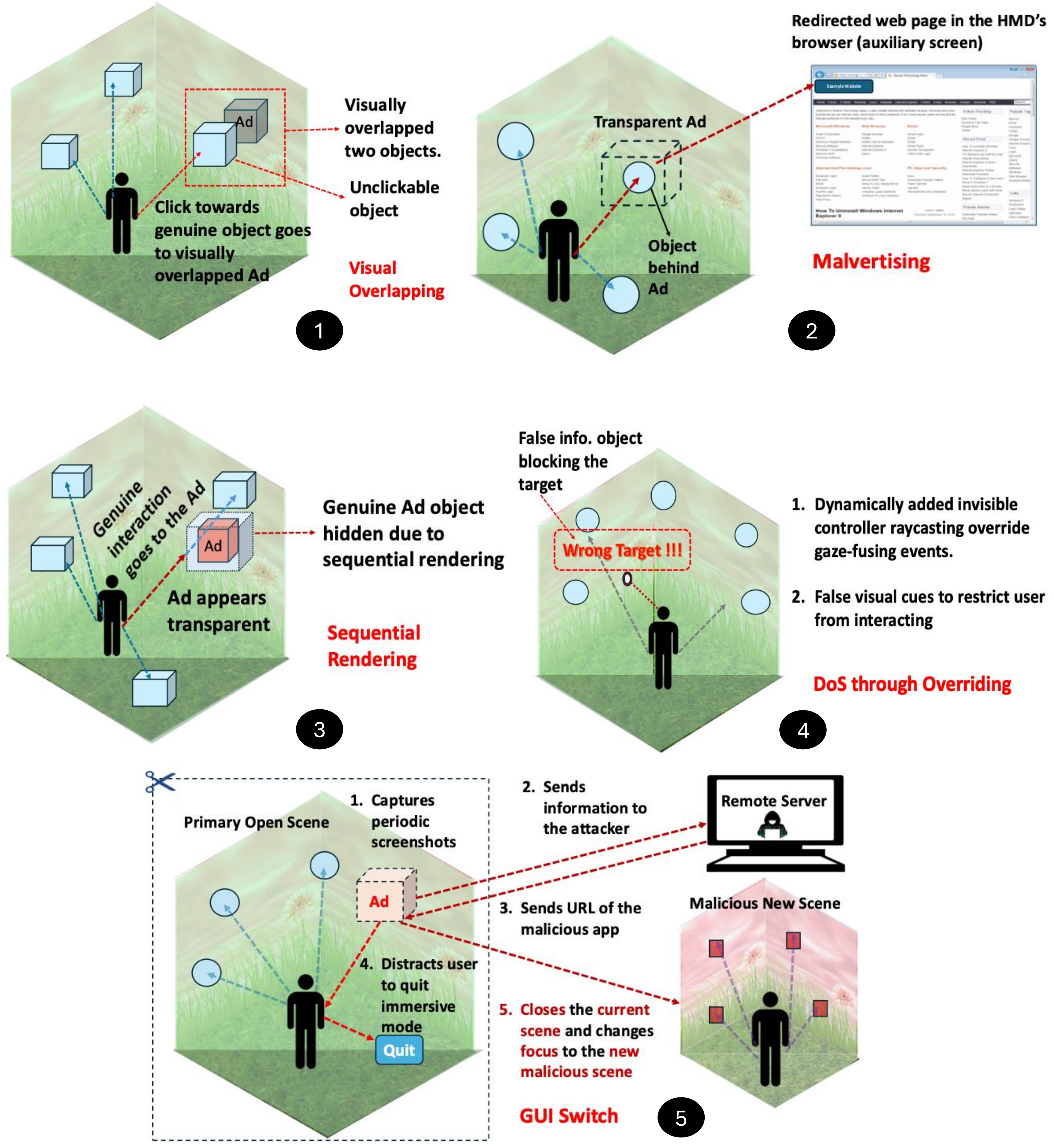
- We systematically investigate the UI properties enabling various UI-based attacks exploiting WebXR ad ecosystem and propose a taxonomy of such attacks.
- We also investigate the impact of these attacks on user perception and interaction behavior.

Security-Sensitive UI Properties

- We identify 14 security-sensitive UI properties.
- These properties can be beneficial –
  - Transparency - depth, motion, shadow, water effects.
  - Overlapping objects – complex scene architectures.
  - Synthetic input – dynamic object interactions.
  - Auxiliary screen – debugging.
  - Sequential rendering – performance optimization.
- However, these can be exploited to integrate dark patterns.

Proposed UI-Based Attacks

- Threat actors in WebXR ad ecosystem - developer, ad service provider, and advertiser.


Ad
Visually overlapped two objects.
Unclickable object
Click towards genuine object goes to visually overlapped Ad
Visual Overlapping
1
Transparent Ad
Object behind Ad
Redirected web page in the HMD's browser (auxiliary screen)
Malvertising
2
Genuine interaction goes to the Ad
Ad
Genuine Ad object hidden due to sequential rendering
Ad appears transparent
Sequential Rendering
3
False info. object blocking the target
Wrong Target !!!
1. Dynamically added invisible controller raycasting override gaze-fusing events.
2. False visual cues to restrict user from interacting
DoS through Overriding
4
Primary Open Scene
1. Captures periodic screenshots
Ad
2. Sends information to the attacker
Remote Server
3. Sends URL of the malicious app
Malicious New Scene
4. Distracts user to quit immersive mode
Quit
5. Closes the current scene and changes focus to the new malicious scene
GUI Switch
5

Taxonomy

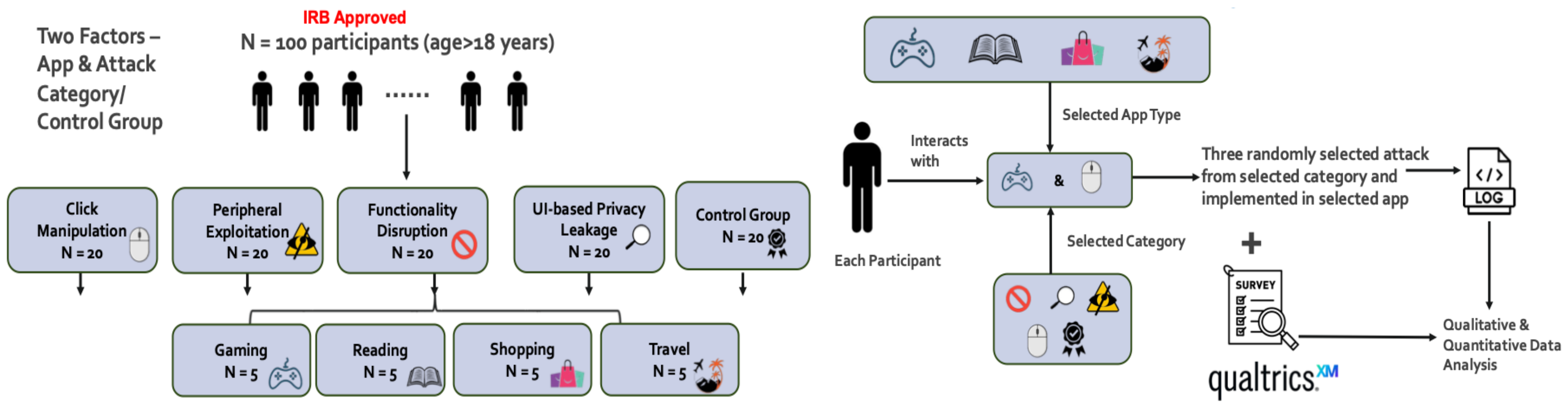
Click Manipulation: Generates revenue from unintentional ad clicks

Peripheral Exploitation: Inflates ad impressions or clicks by exploiting blind spots

Functionality Disruption: Prevents users from performing intended actions

UI-based Privacy Leakage: Extracts sensitive user information

User Study Design


Two Factors – App & Attack Category/ Control Group
IRB Approved
N = 100 participants (age>18 years)
Click Manipulation N = 20
Peripheral Exploitation N = 20
Functionality Disruption N = 20
UI-based Privacy Leakage N = 20
Control Group N = 20
Gaming N = 5
Reading N = 5
Shopping N = 5
Travel N = 5
Each Participant
Interacts with
Selected App Type
&
Selected Category
Three randomly selected attack from selected category and implemented in selected app
LOG
SURVEY
qualtrics XM
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

Log Framework

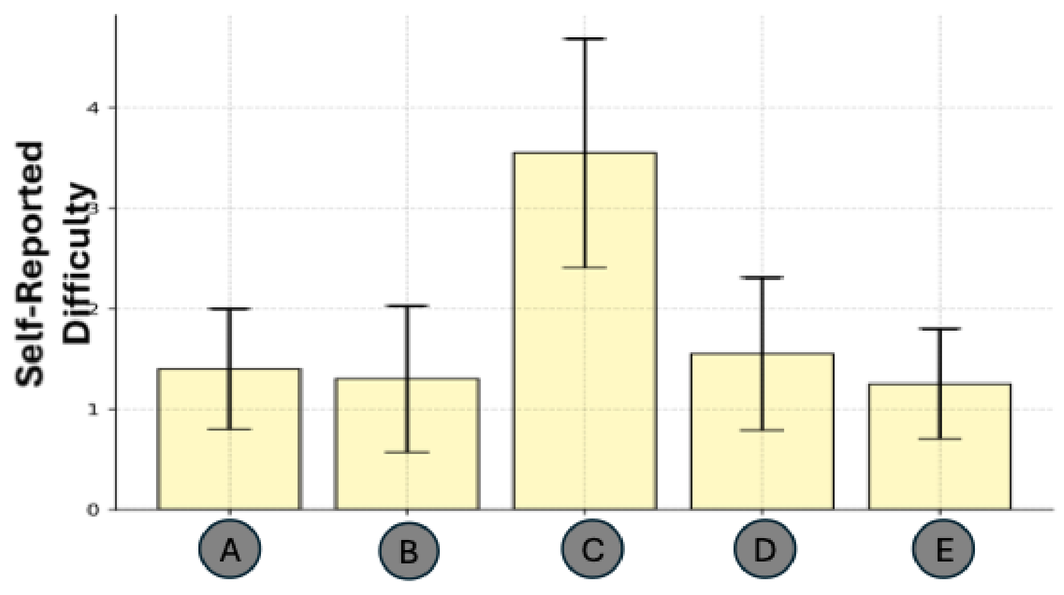
1. Continuous monitoring of objects
2. Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional
3. Captures simultaneous interactions by single cursor
4. Estimates user's position and attention

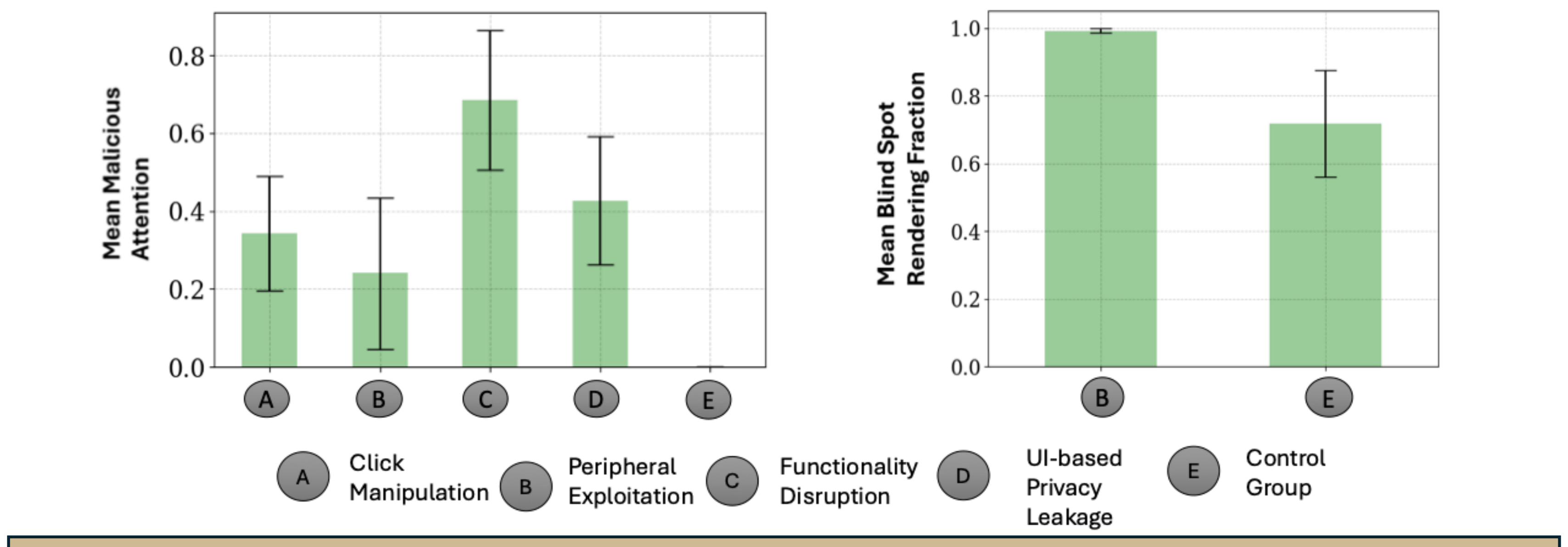
Interaction Metrics

- **Presence (P):** User's focus on task.
- **Safe Engagement (E_s):** Impact on user interaction with task under attack conditions.
- **Malicious Attention (MA):** Unintended clicks on advertisements.
- **Blind Spot Rendering Fraction (BSR_f):** Advertisements rendered outside the FoV.

User Study Results

- Most of the attack categories go unnoticed by users.
- Attacks are effective in achieving their objectives.
- Impact of the attacks generalizes to different apps.
- Attacks force users to shift their engagement with the given task.





Discussion

- The beneficial UI properties of WebXR can be exploited for malicious purposes, such as by leveraging the advertising ecosystem.
- Developers and platform owners can use the list of identified properties and attacks to secure user interactions in WebXR.
- Future work includes automatic detection of these UI-based attacks.

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 & Paper Link

Key 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.

34TH USENIX SECURITY SYMPOSIUM