Shadowed Realities: An Investigation of UI Attacks in WebXR

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

USENIX Security Symposium 2025

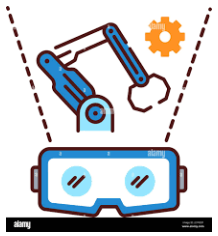
Extended Reality (XR)

XR encompasses immersive technologies enabling real-time interaction with both real and virtual content.

Education

Retail

Healthcare



Manufacturing

Entertainment

Extended Reality (XR)

Headsets from companies like Meta, Microsoft, and Apple rely on different development frameworks (Meta XR Core SDK, MRTK, ARKit).

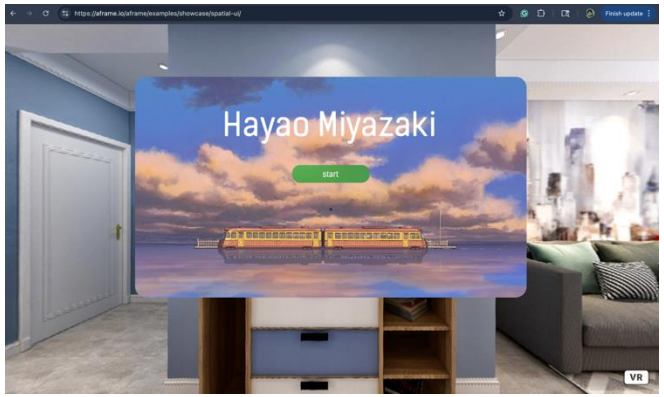
ARKit

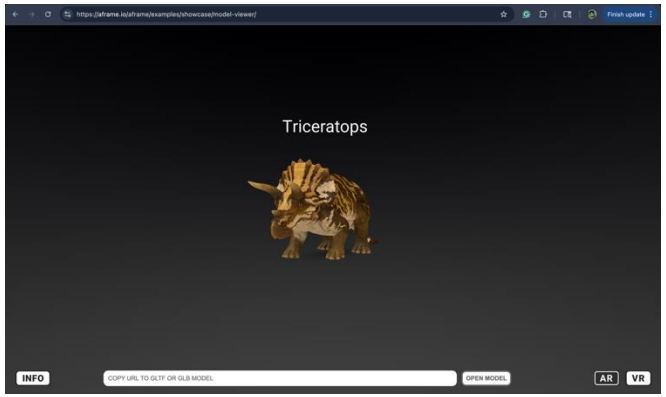
ARCore

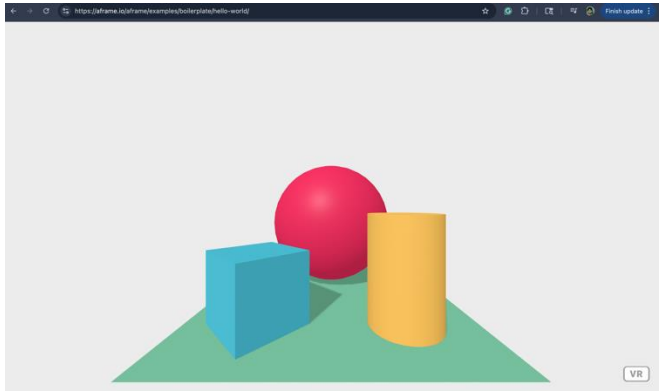
MRTK
MIXED REALITY TOOLKIT

Extended Reality (XR)

WebXR provides a unified way to create XR experiences across headsets / platforms.



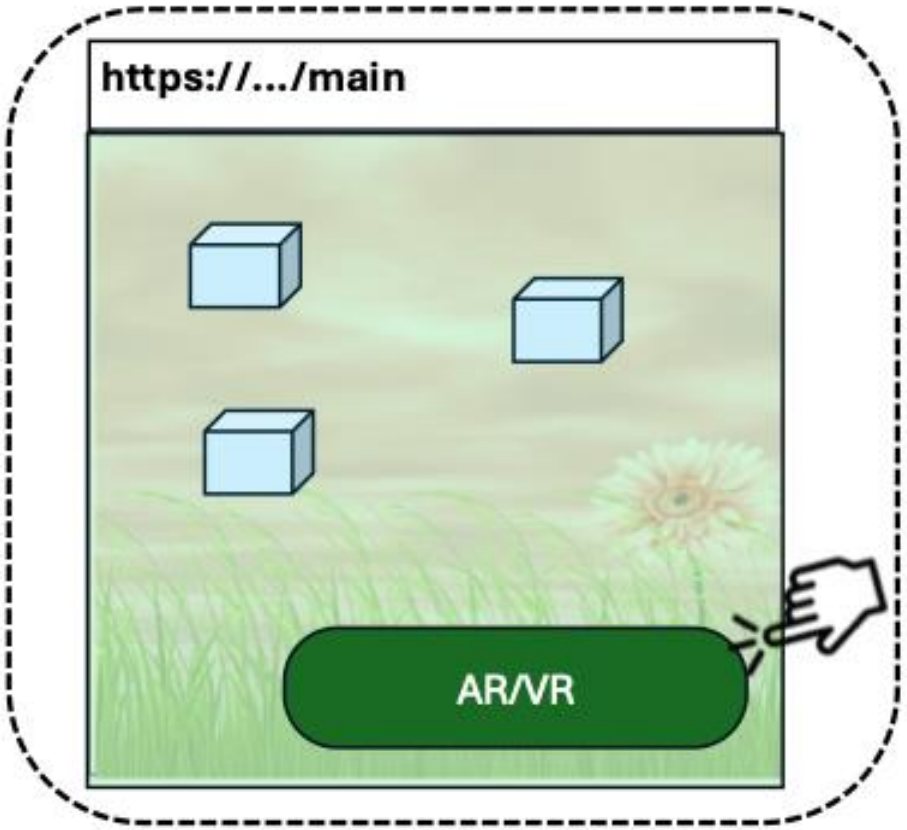




Example WebXR Scenes

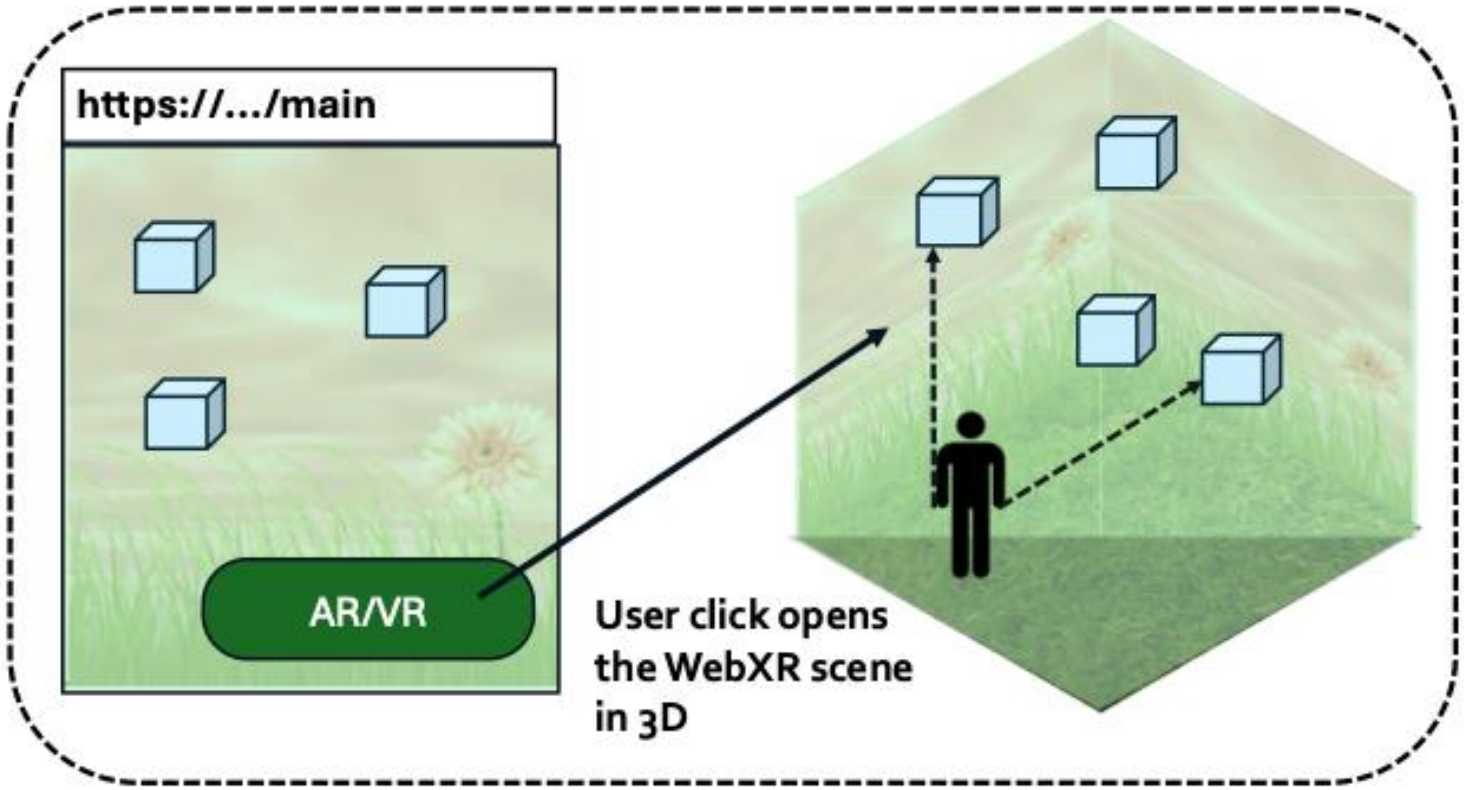
WebXR

WebXR allows users to interact with extended reality environments directly through the browser from their head-mounted display.



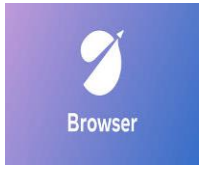
WebXR

WebXR allows users to interact with extended reality environments directly through the browser from their head-mounted display.

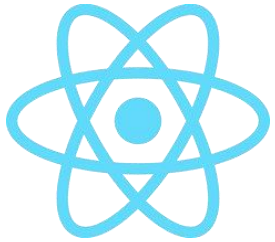


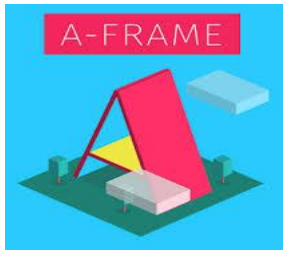
WebXR

A few lines of HTML and JavaScript code enables extended reality experiences.



Browsers Supported



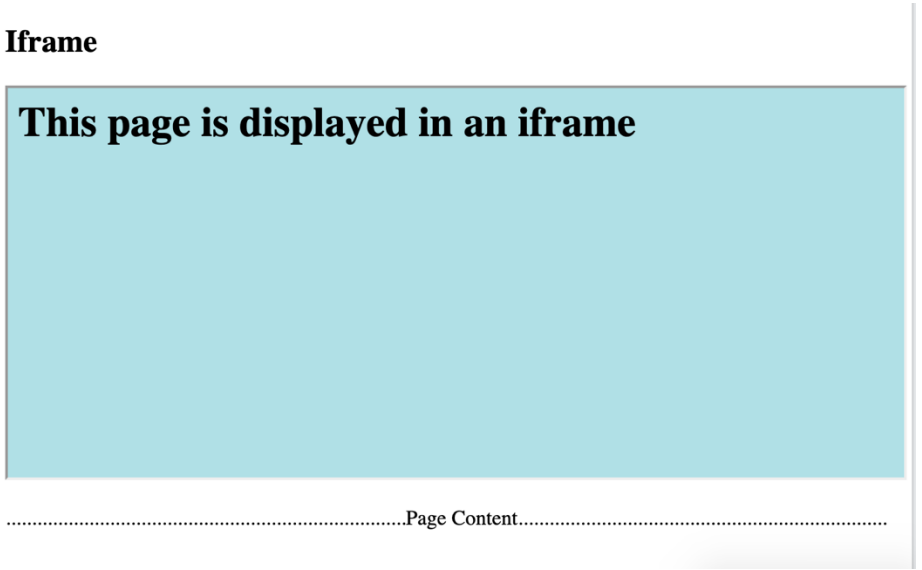


Libraries, Frameworks, Game Engines

No iframe in WebXR

- There is no iframe-like element to separate the third-party content from main content.

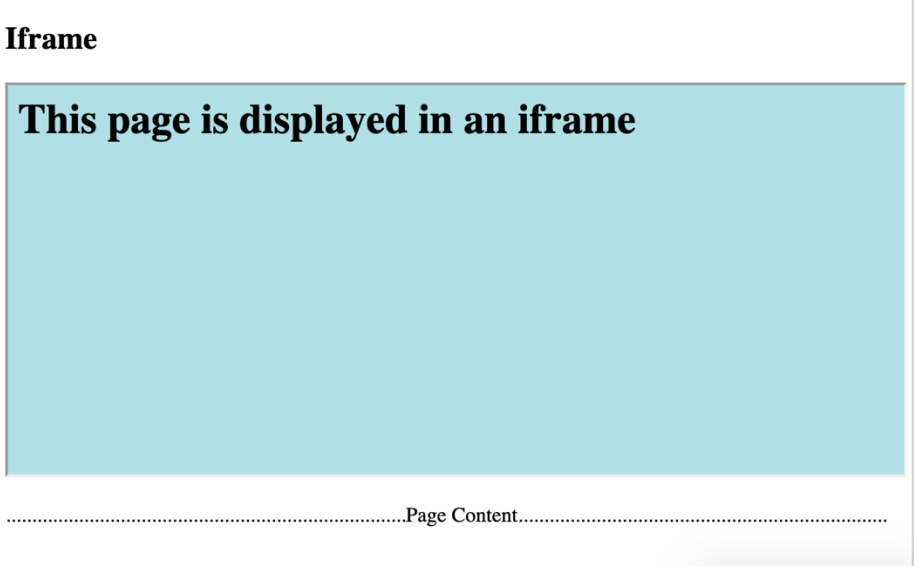
```
<!DOCTYPE html>
<html>
<body>

<h2>Iframe</h2>

<iframe src="demo_iframe.htm" name="iframe_a" height="300px" width="100%"
title="Iframe Example"></iframe>

<p> ..........................................................Page
Content..........................................................</p>
<p>

</body>
</html>
```



No iframe in WebXR

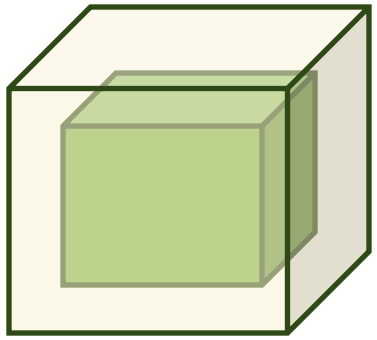
- There is no iframe-like element to separate the third-party content from main content.
- In standard web, **same-origin policy** blocks scripts from accessing resources across different origins.
  - No such mechanism in WebXR.

```
<!DOCTYPE html>
<html>
<body>

<h2>Iframe</h2>

<iframe src="demo_iframe.htm" name="iframe_a" height="300px" width="100%"
title="Iframe Example"></iframe>

<p> ..........................................................Page
Content..........................................................</p>
<p>

</body>
</html>
```

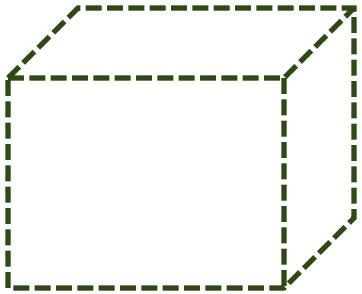


UI Properties

Various UI properties enhance immersion in WebXR. For example,



Overlapping objects



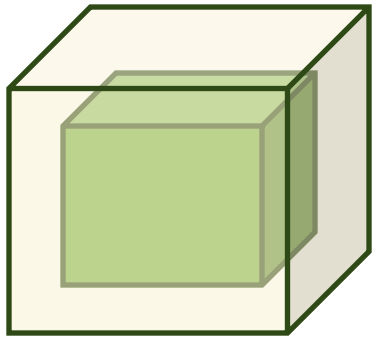
Transparency

```
var cube = this.el;
cube.emit('click');
```

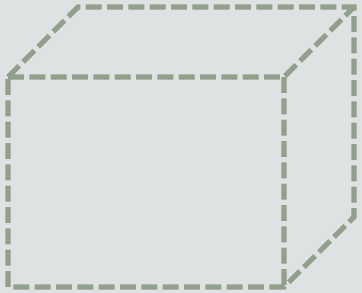
Synthetic input

UI Properties

Overlapping objects can be used to create complex scene architectures (city, office etc.)



Overlapping objects



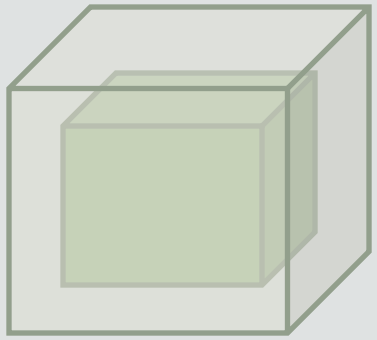
Transparency

```
var cube = this.el;
cube.emit('click');
```

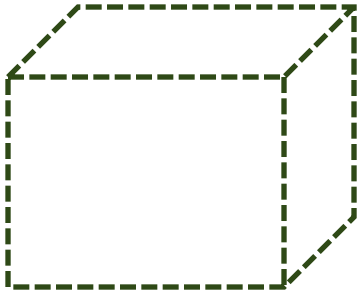
Synthetic input

UI Properties

Transparency is used to create visual effects such as depth, motion, shadow etc.



Overlapping objects



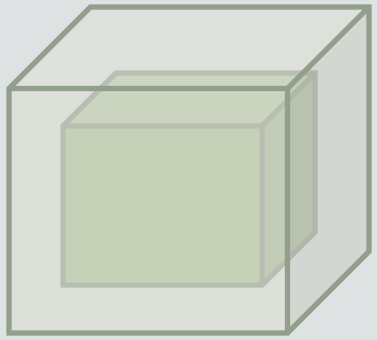
Transparency

```
var cube = this.el;
cube.emit('click');
```

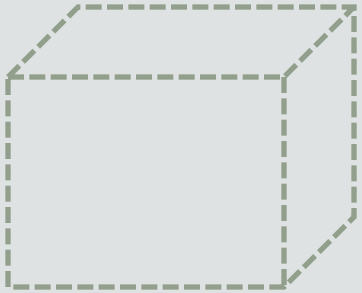
Synthetic input

UI Properties

Synthetic input is used to trigger dynamic object interactions between virtual objects without user's explicit input.



Overlapping objects



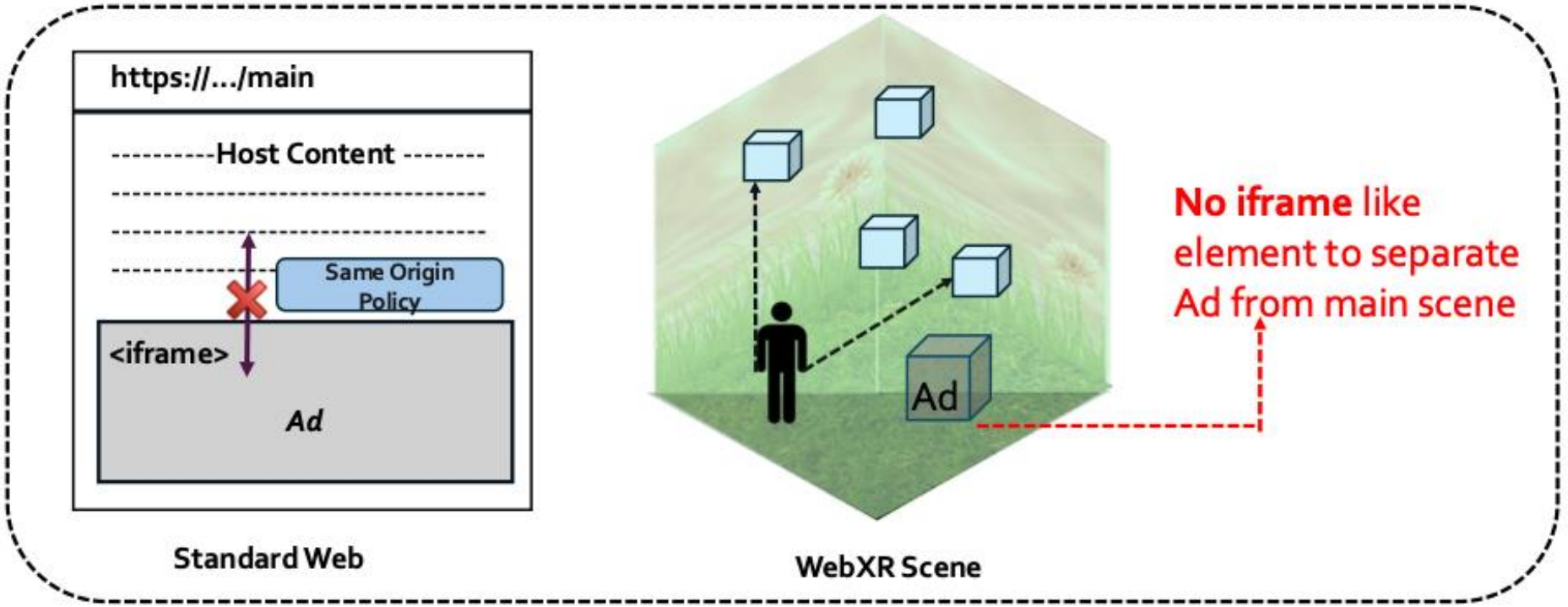
Transparency

```
var cube = this.el;
cube.emit('click');
```

Synthetic input

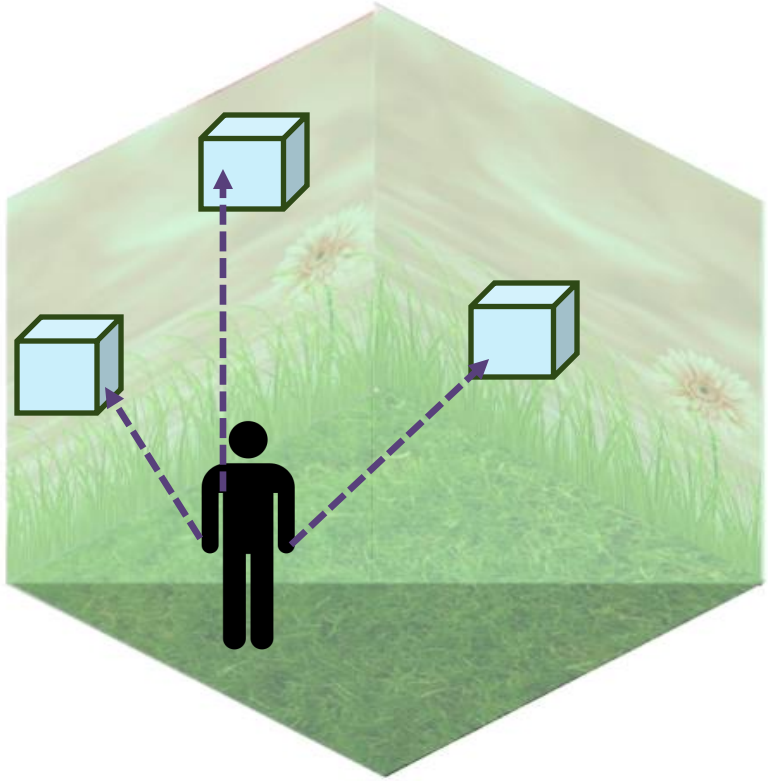
WebXR Advertising

WebXR advertising ecosystem (developer, ad service provider, and advertiser) can exploit the lack of iframe.



UI Properties

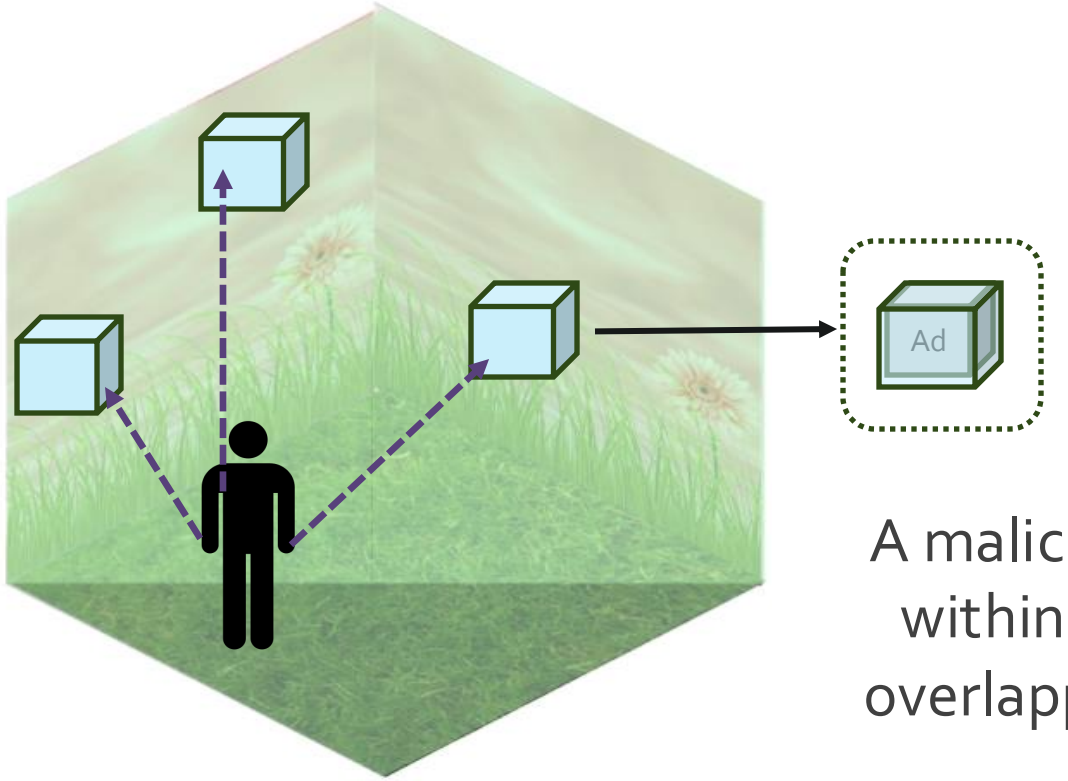
These properties may be exploited to deploy **dark patterns**, undermining user autonomy.



User Plays a Target Shooting Game

UI Properties

However, these properties may be exploited to deploy **dark patterns**, undermining user autonomy.

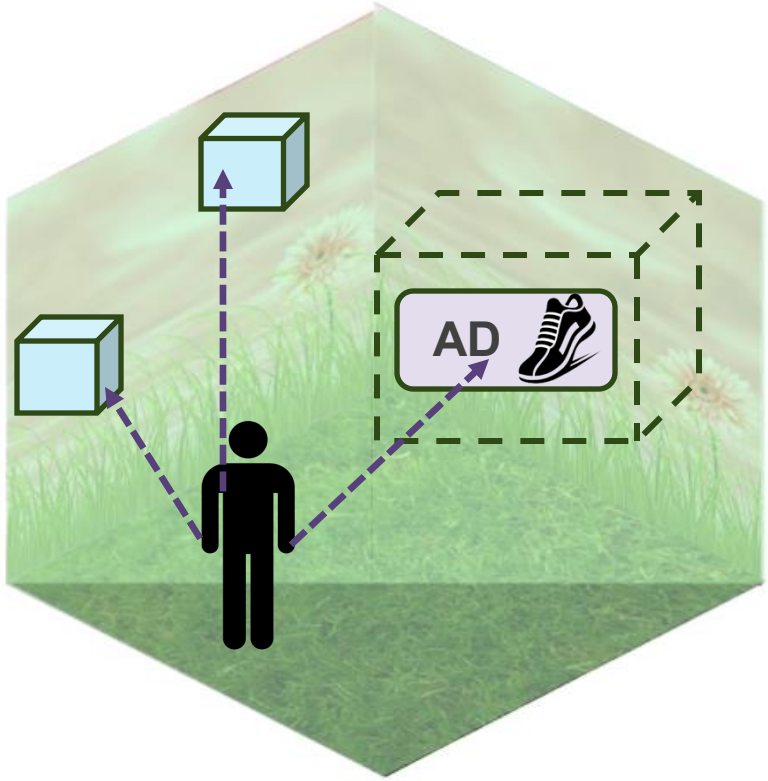


Exploiting Overlapping Objects

A malicious **developer** hides ad within a same size and shape overlapping object and receives clicks.

UI Properties

However, these properties may be exploited to deploy **dark patterns**, undermining user autonomy.



Exploiting Transparency

A malicious competing **ad service provider** blocks user actions on intended objects.

Harmful Consequences

Data theft

Malware Download

Financial Loss

Reputational Damage

Research Questions

RQ1: How do different UI properties contribute to the dark pattern designs in WebXR ad ecosystem?

RQ2: How do different deceptive design practices within WebXR impact the overall experience of users and their interaction with the app content?

Research Questions

RQ1: How do different UI properties contribute to the dark pattern designs in WebXR ad ecosystem?

RQ2: How do different deceptive design practices within WebXR impact the overall experience of users and their interaction with the app content?

Taxonomy of UI-based Attacks

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

Taxonomy of UI-based Attacks

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

Taxonomy of UI-based Attacks

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

Taxonomy of UI-based Attacks

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

Taxonomy of UI-based Attacks

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

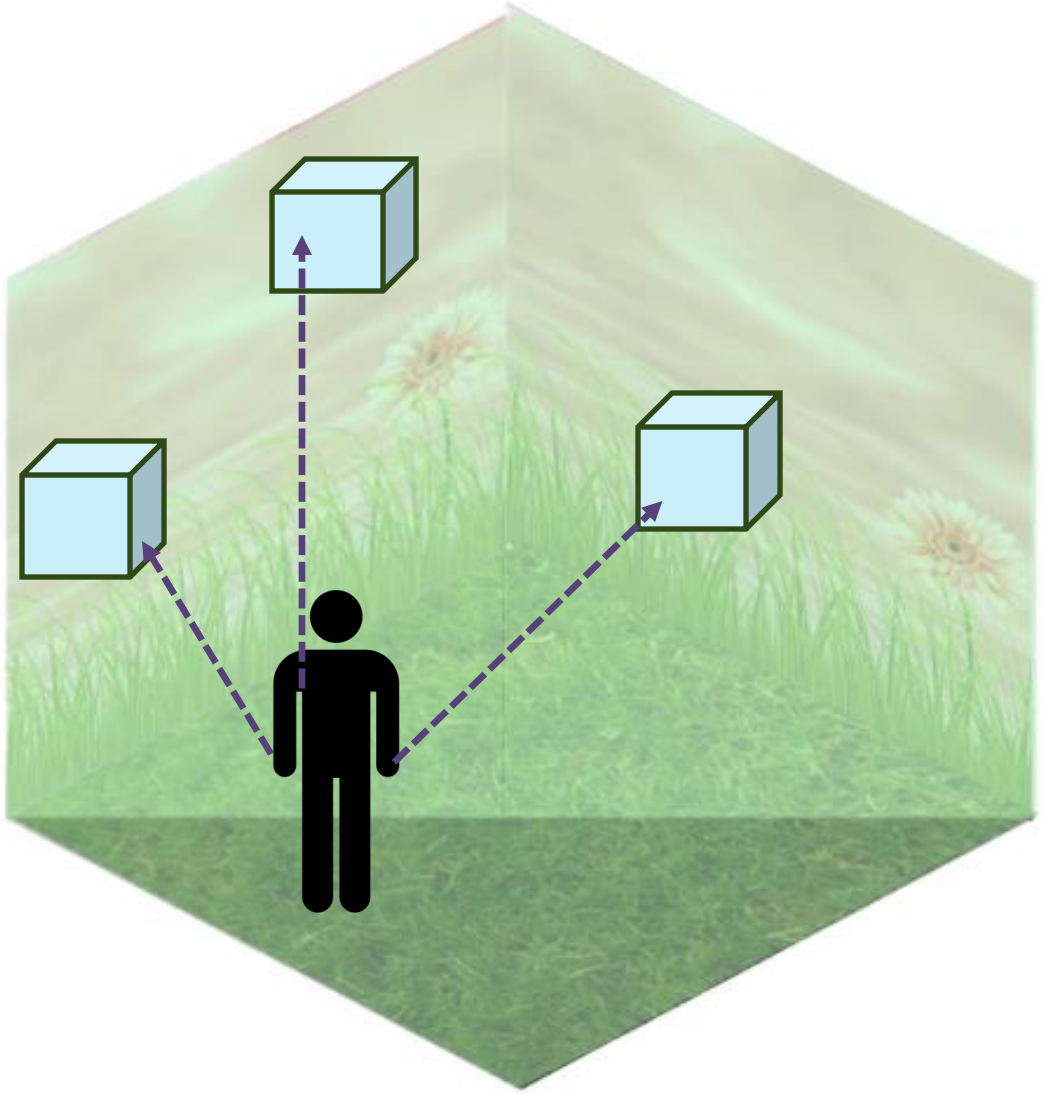
UI-based Privacy Leakage: Extracts sensitive user information

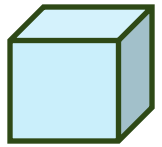
New Attacks in WebXR Ad Ecosystem

We proposed **five** novel UI-based attacks.

Category	Attack Name
Click Manipulation	Visual Overlapping
	Sequential Rendering
Peripheral Exploitation	Malvertising
UI-based Privacy Leakage	GUI Switch
Functionality Disruption	DoS through Overriding

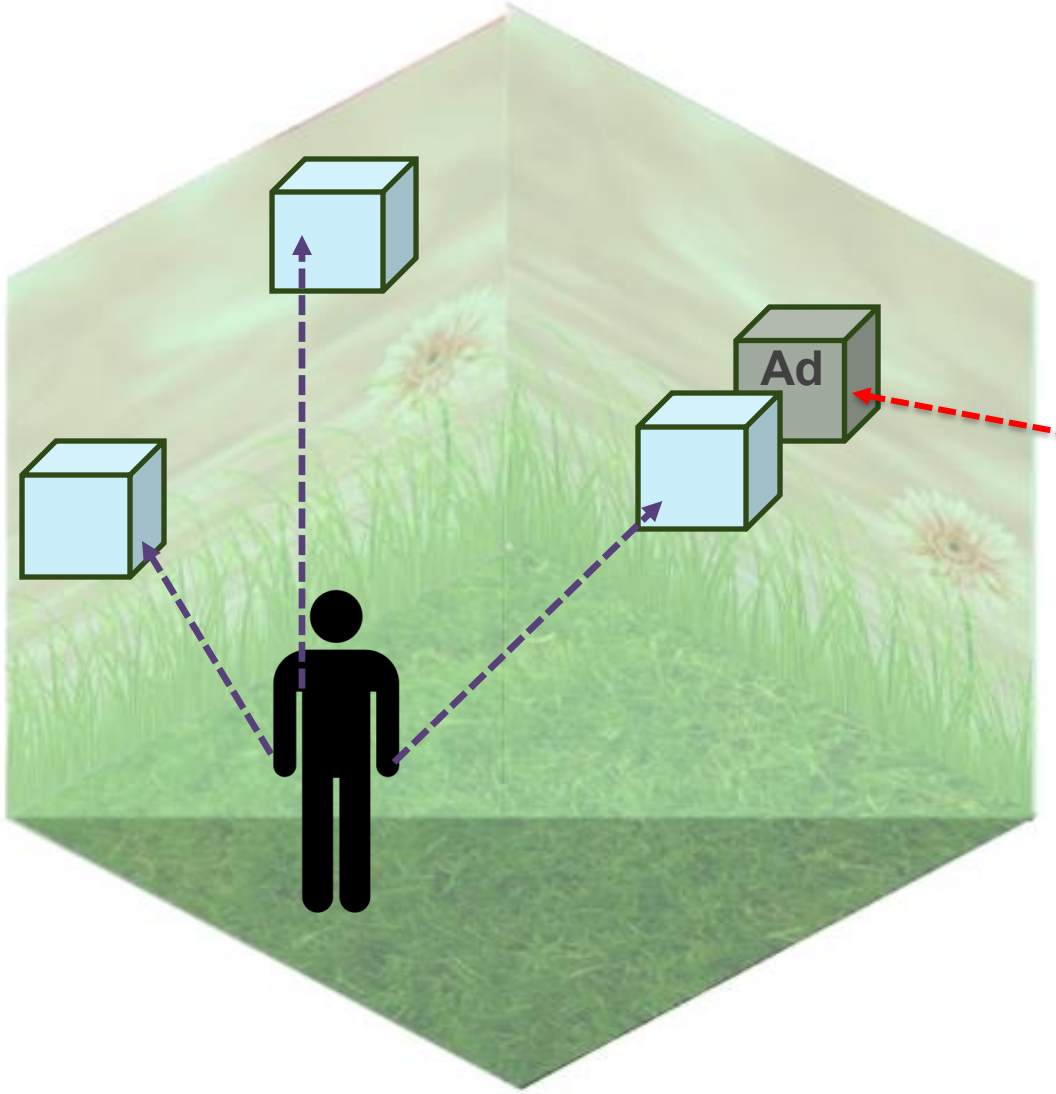
Visual Overlapping Attack





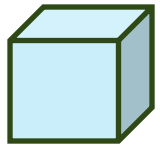
Interactive game object

Visual Overlapping Attack



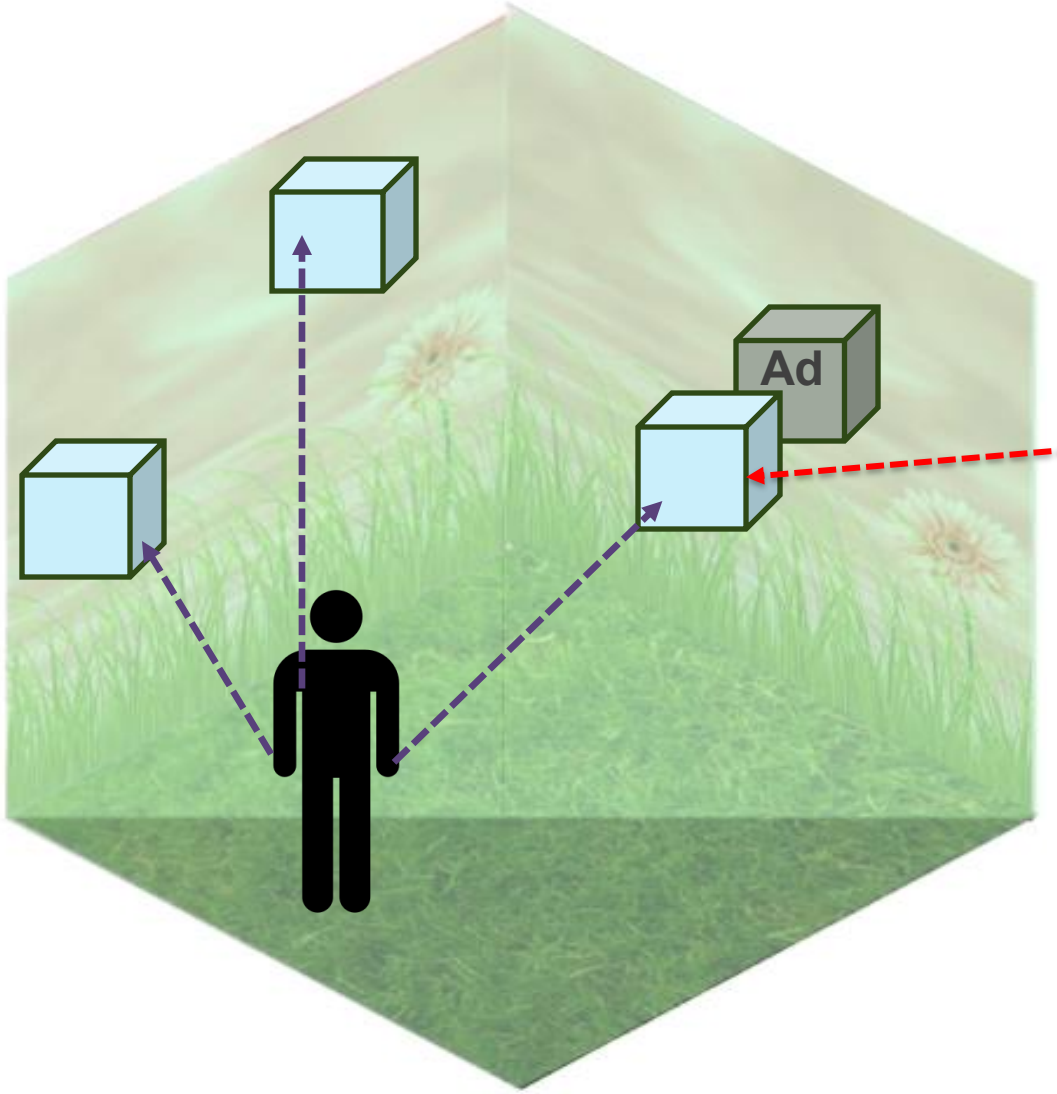
Malicious Developer

Ad placed strategically behind interactive object



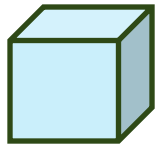
→ Interactive game object

Visual Overlapping Attack



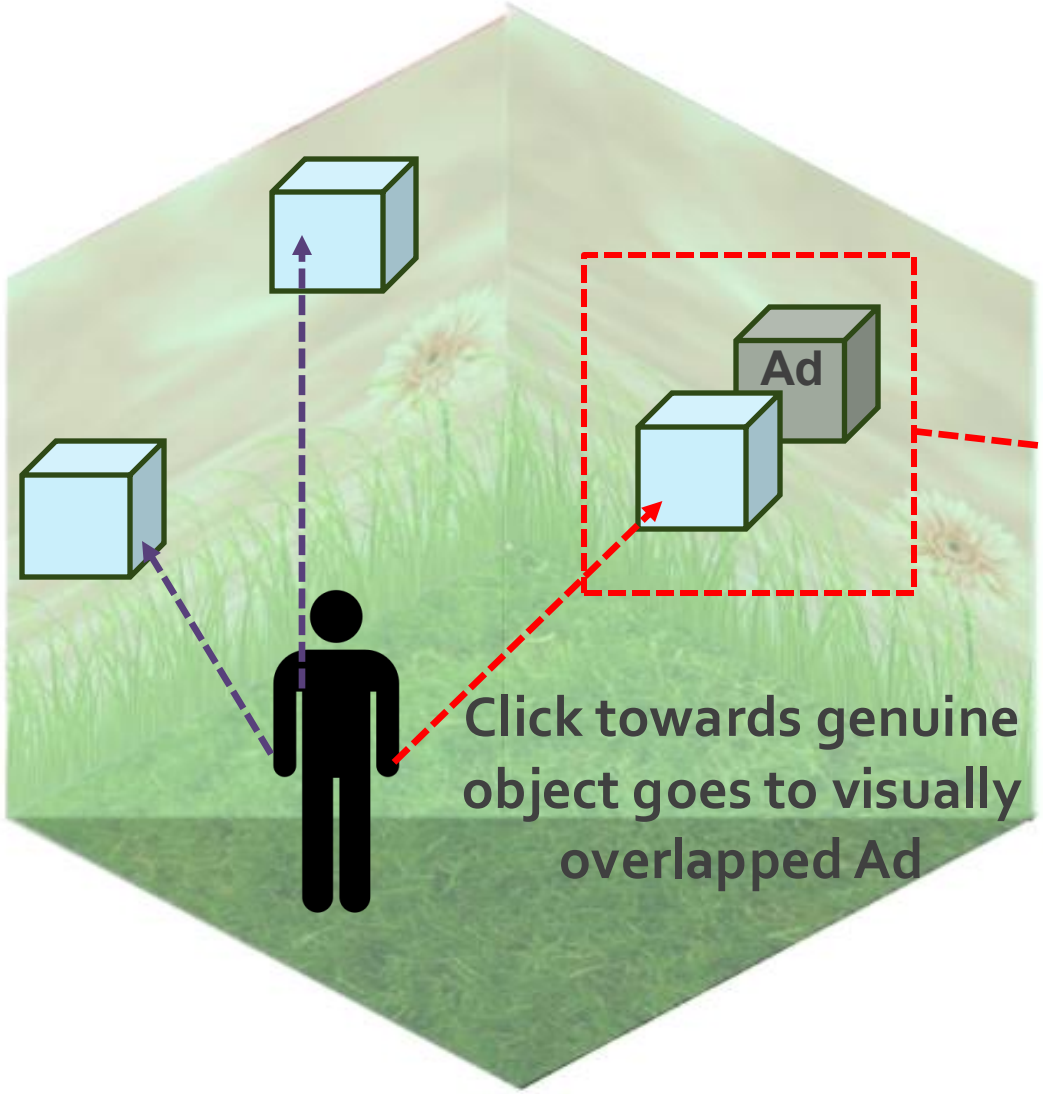
Malicious Developer

Target object is made unclickable.



Interactive game object

Visual Overlapping Attack

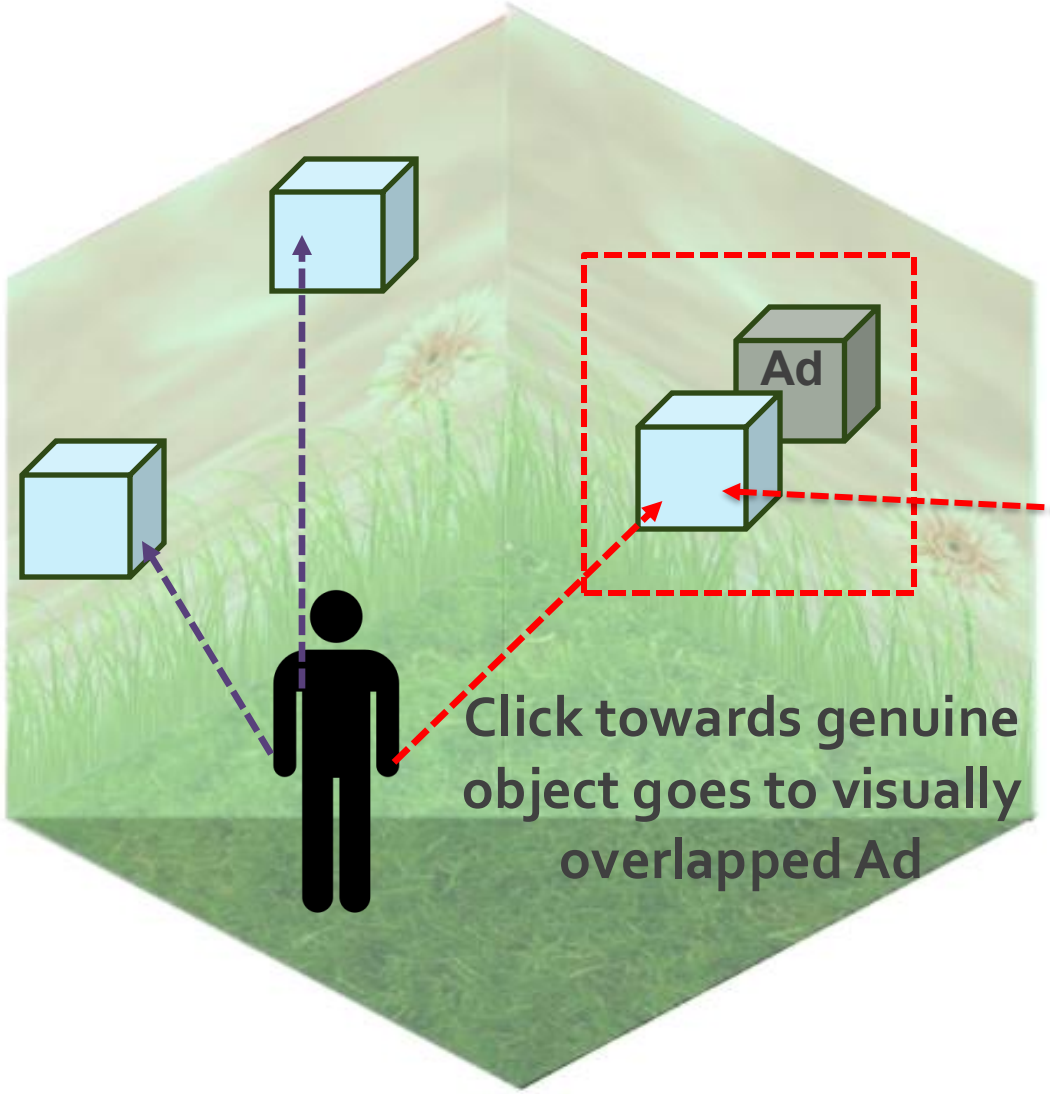


Malicious Developer

Visually overlapped two objects.

Interactive game object

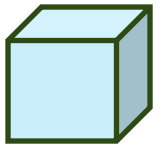
Visual Overlapping Attack



Malicious Developer

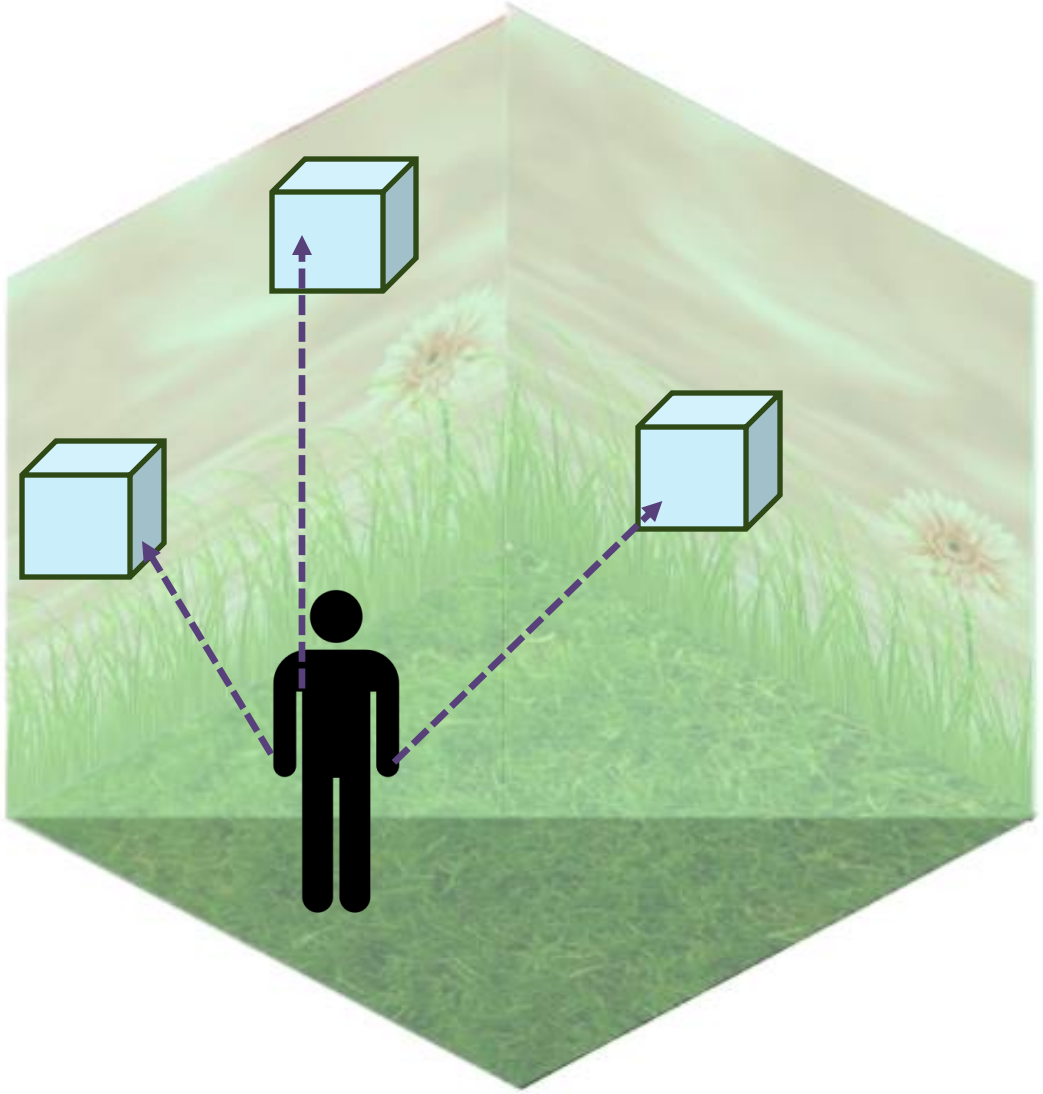
Synthetic input on target object keeps the functionality intact.

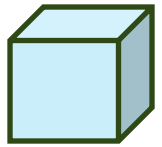
```
target.emit('click')
```



→ Interactive game object

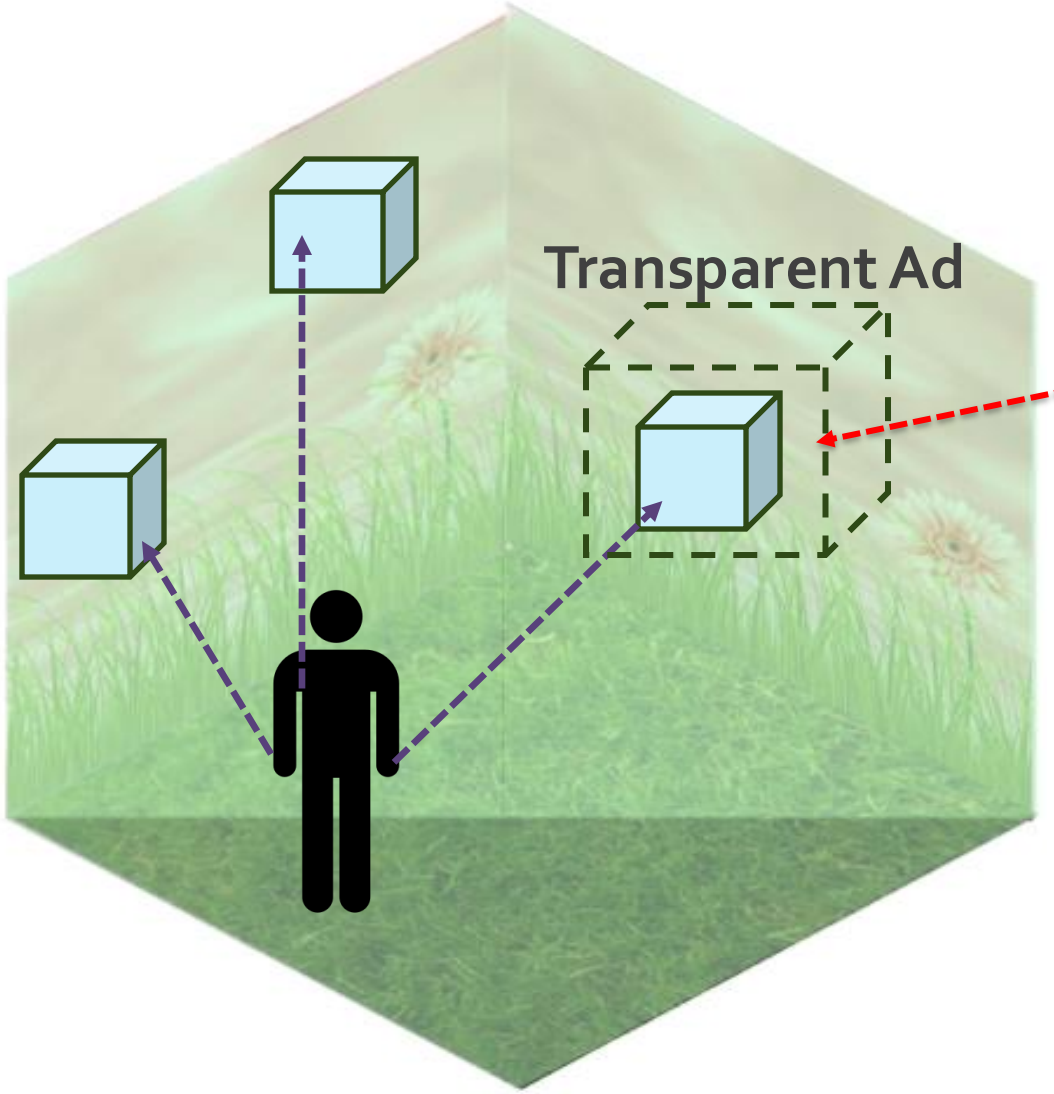
Malvertising Attack





Interactive game object

Malvertising Attack

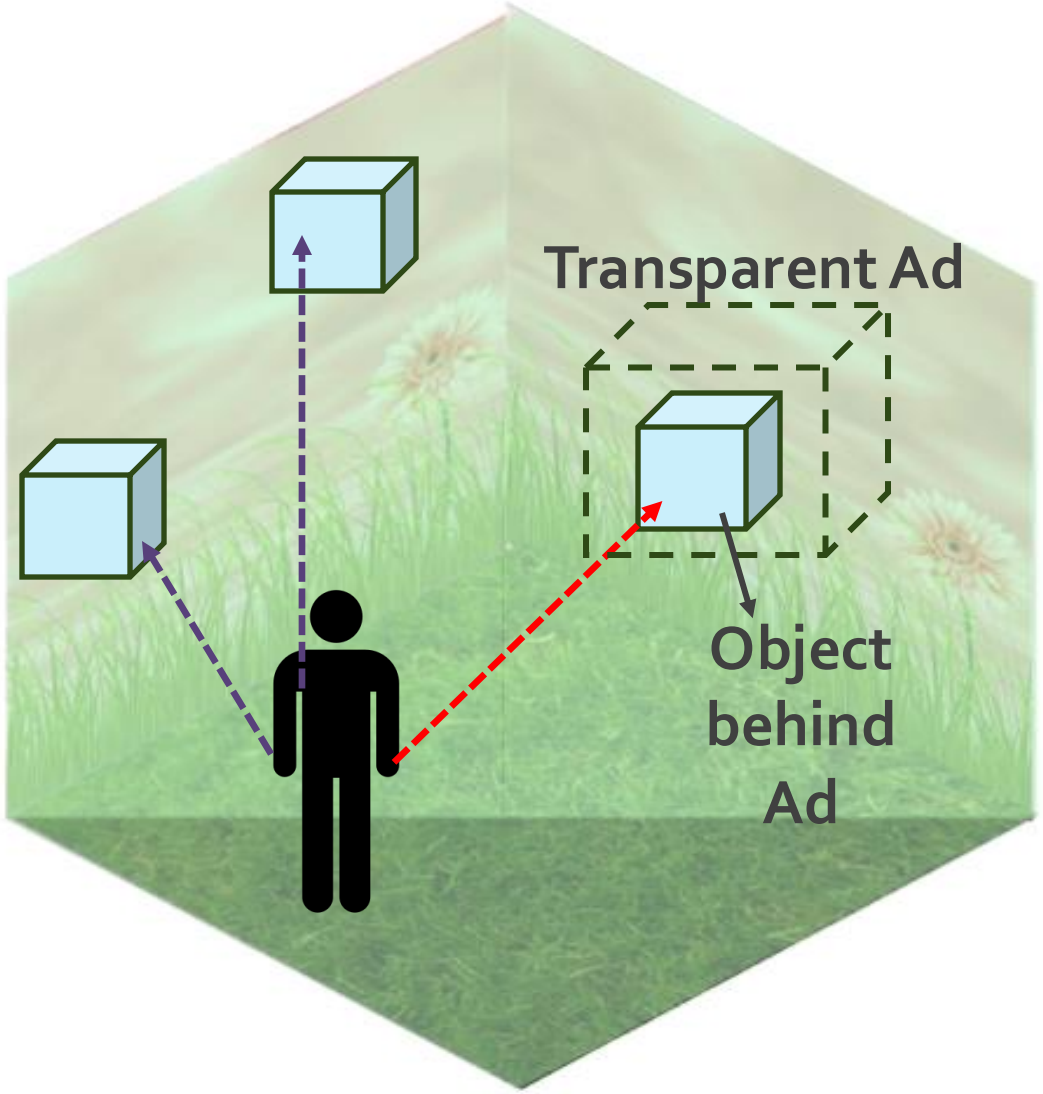


Malicious Advertiser

Provides transparent or partly transparent advertisement

Interactive game object

Malvertising Attack

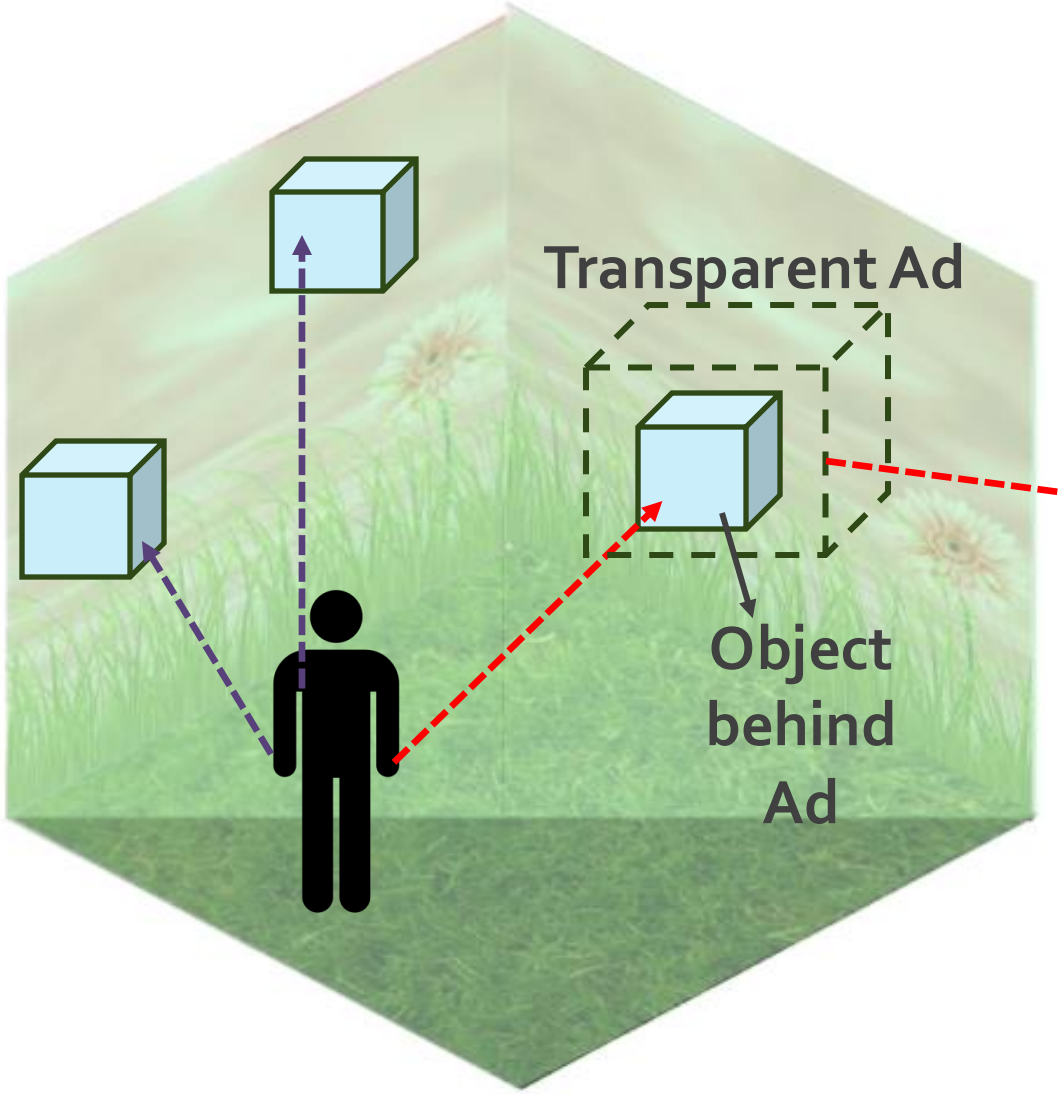


Malicious Advertiser

- User still sees the object behind the advertisement
- Click towards genuine object goes to the Ad

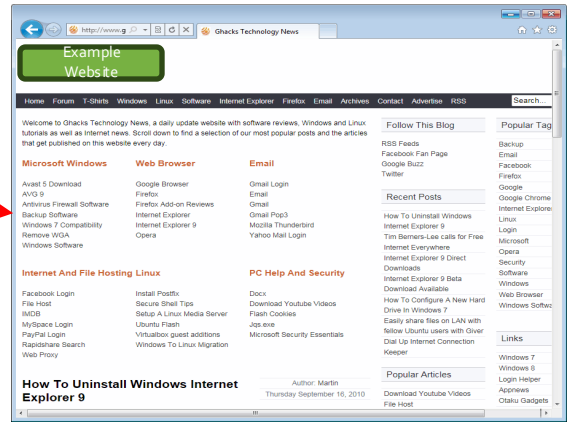
Interactive game object

Malvertising Attack



Malicious Advertiser

Redirected web page in the HMD's browser (auxiliary screen)



→ **Interactive game object**

Research Questions

RQ1: How do different UI properties contribute to the dark pattern designs in WebXR ad ecosystem?

RQ2: How do different deceptive design practices within WebXR impact the overall experience of users and their interaction with the app content?

Understand Impact of Attack Categories on Users

- Capture granular 3D interaction data, identifying intentional and unintentional events.

Understand Impact of Attack Categories on Users

- Capture granular 3D interaction data, identifying intentional and unintentional events.
- Determine if impact varies while interacting with apps with different context and interaction demands.

Understand Impact of Attack Categories on Users

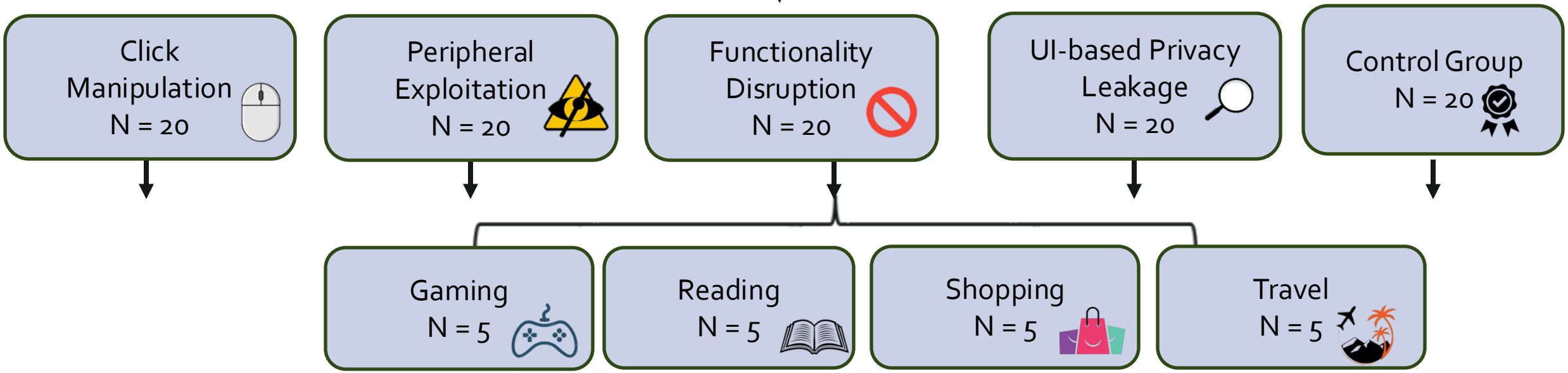
- Capture granular 3D interaction data, identifying intentional and unintentional events.
- Determine if impact varies while interacting with apps with different context and interaction demands.
- Design a between-subjects user study
  - Comparing attack categories with each other and control group
  - Two factors (app and attack category/control group)

Between-Subjects User Study Design

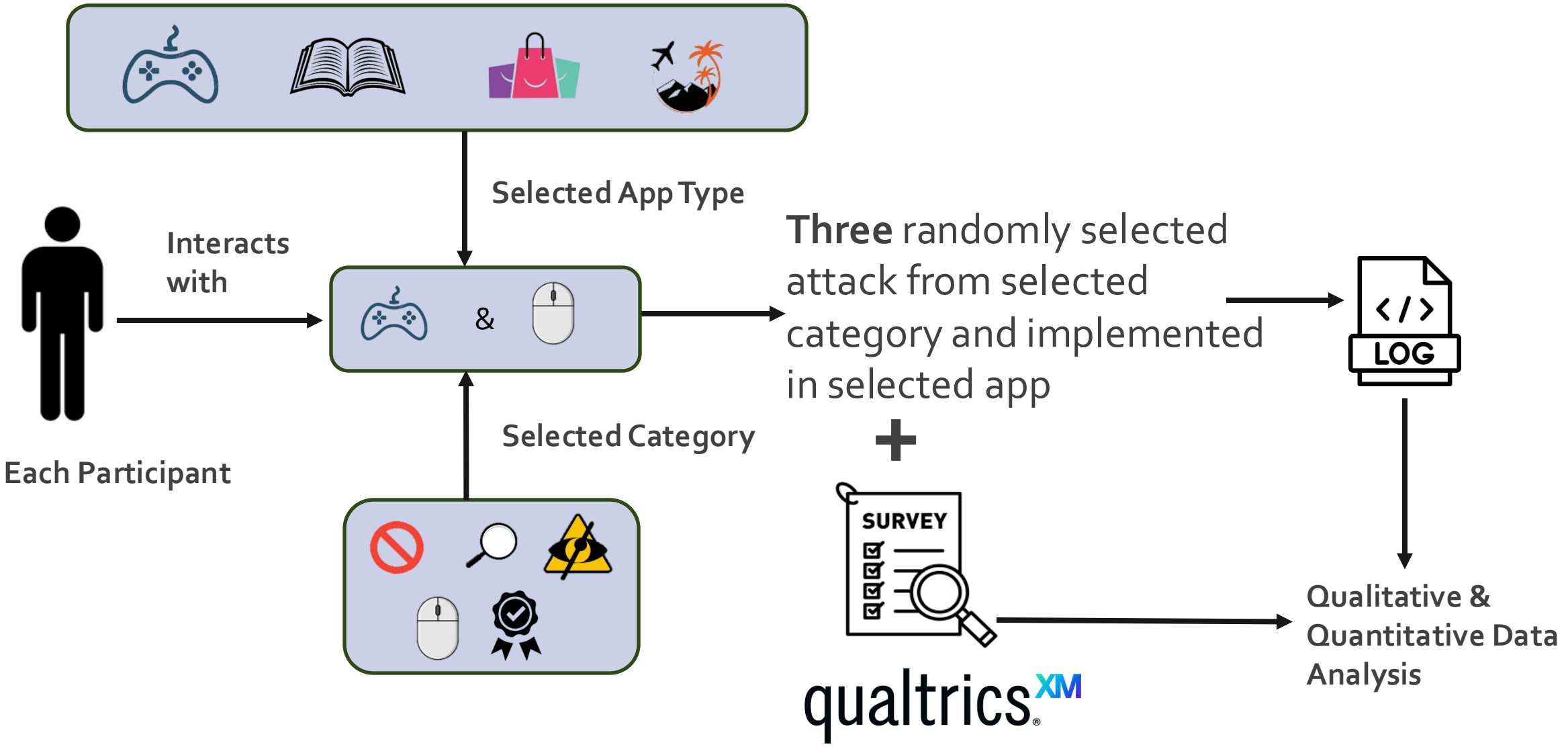
Two Factors –
App & **Attack** Category/ **Control** Group

IRB Approved

N = 100 participants (age>18 years)



Between-Subjects User Study Design



User Study Framework

Log Framework: Capture user intended and unintended interactions with objects part of main scene (T_{obj}) and others such as advertisement (DP_{obj}).

Interaction Metrics: Obtain meaningful insights from collected logs.

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

User Study Framework

Log Framework: Capture user intended and unintended interactions with objects part of main scene (T_{obj}) and others such as advertisement (DP_{obj}).

Interaction Metrics: Obtain meaningful insights from collected logs.

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

Logging Framework

- Single entry point and consists of four components.
- Developed using A-Frame and Three.js

Environment Scanner: Continuous monitoring of objects in the scene

T_{obj} or DP_{obj} Logger: Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional

Cursor Event Logger: Captures simultaneous interactions by single cursor

Camera and Gaze Logger: Estimates user's position and attention

Logging Framework

- Single entry point and consists of four components.
- Developed using A-Frame and Three.js

Environment Scanner: Continuous monitoring of objects in the scene

T_{obj} or DP_{obj} Logger: Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional

Cursor Event Logger: Captures simultaneous interactions by single cursor

Camera and Gaze Logger: Estimates user's position and attention

Logging Framework

- Single entry point and consists of four components.
- Developed using A-Frame and Three.js

Environment Scanner: Continuous monitoring of objects in the scene

T_{obj} or DP_{obj} Logger: Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional

Cursor Event Logger: Captures simultaneous interactions by single cursor

Camera and Gaze Logger: Estimates user's position and attention

Logging Framework

- Single entry point and consists of four components.
- Developed using A-Frame and Three.js

Environment Scanner: Continuous monitoring of objects in the scene

T_{obj} or DP_{obj} Logger: Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional

Cursor Event Logger: Captures simultaneous interactions by single cursor

Camera and Gaze Logger: Estimates user's position and attention

Logging Framework

- Single entry point and consists of four components.
- Developed using A-Frame and Three.js

Environment Scanner: Continuous monitoring of objects in the scene

T_{obj} or DP_{obj} Logger: Captures 3D spatial data related to click and focus events, identifies events as intentional or unintentional

Cursor Event Logger: Captures simultaneous interactions by single cursor

Camera and Gaze Logger: Estimates user's position and attention

User Study Framework

Log Framework: Capture user intended and unintended interactions with objects part of main scene (T_{obj}) and others such as advertisement (DP_{obj}).

Interaction Metrics: Obtain meaningful insights from collected logs.

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

Interaction Metrics

- **Presence (P):** User's focus on task.

Interaction Metrics

- **Presence (P):** User's focus on task.
- **Safe Engagement (E_s):** Impact on user interaction with task under attack conditions.

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.

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 Framework

Log Framework: Capture user intended and unintended interactions with objects part of main scene (T_{obj}) and others such as advertisement (DP_{obj}).

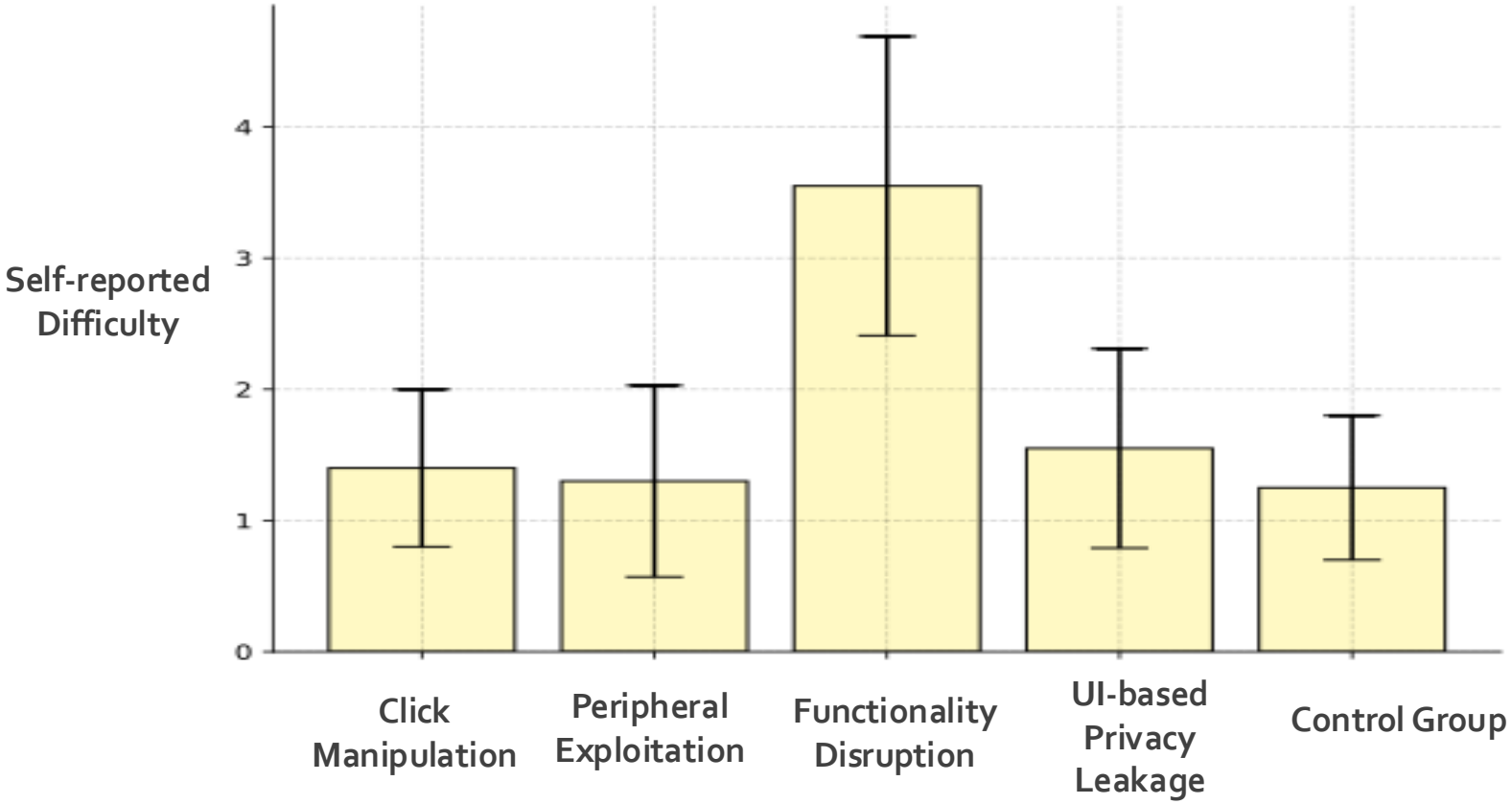
Interaction Metrics: Obtain meaningful insights from collected logs.

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

User Study Findings - 1

How do WebXR UI attacks influence the quality of users' experience?

Most of the attack categories go unnoticed by users.



User Study Findings - 2

Do these attacks influence user attention and alter interaction behavior, diverting them from their tasks?

- User's Presence is
  - Influenced by the app type.
  - Not by attack categories.

User Study Findings - 2

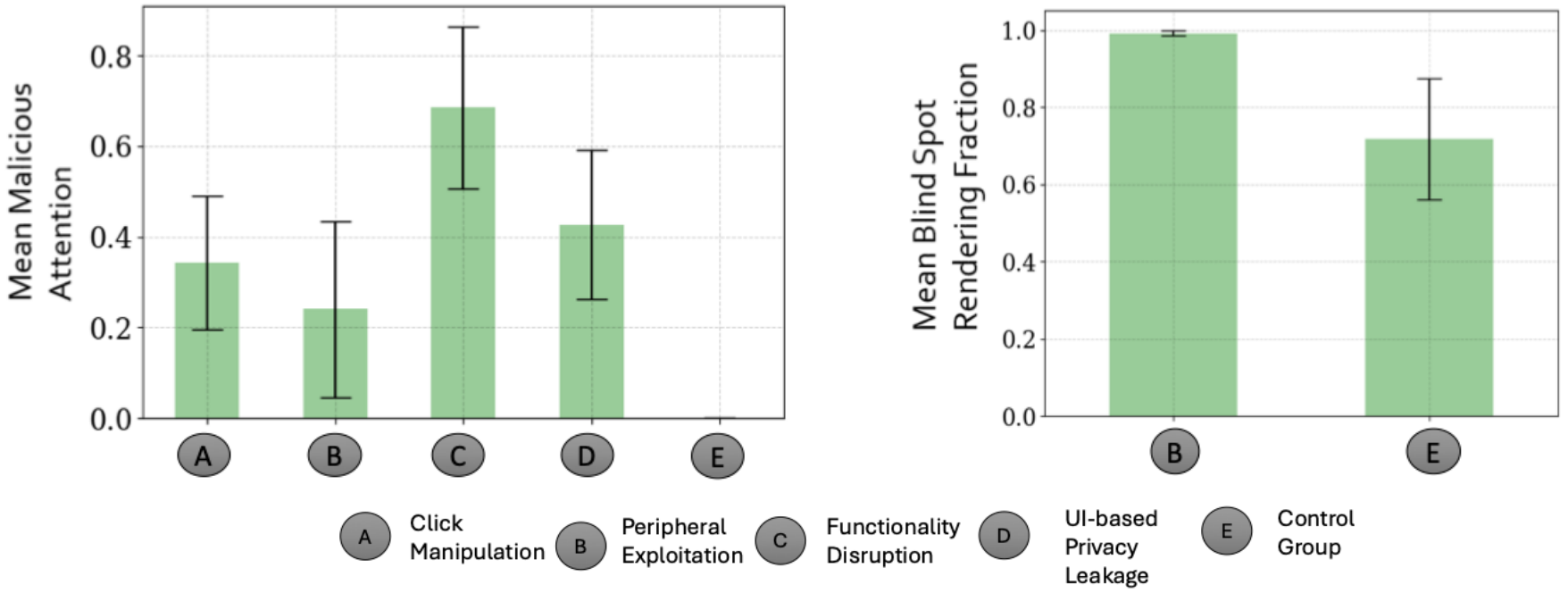
Do these attacks influence user attention and alter interaction behavior, diverting them from their tasks?

- User's Presence is
  - Influenced by the app type.
  - Not by attack categories.
- Safe Engagement suggests
  - Attacks force users to shift their engagement with the given task.

User Study Findings - 3

Do these attacks achieve their intended objectives?

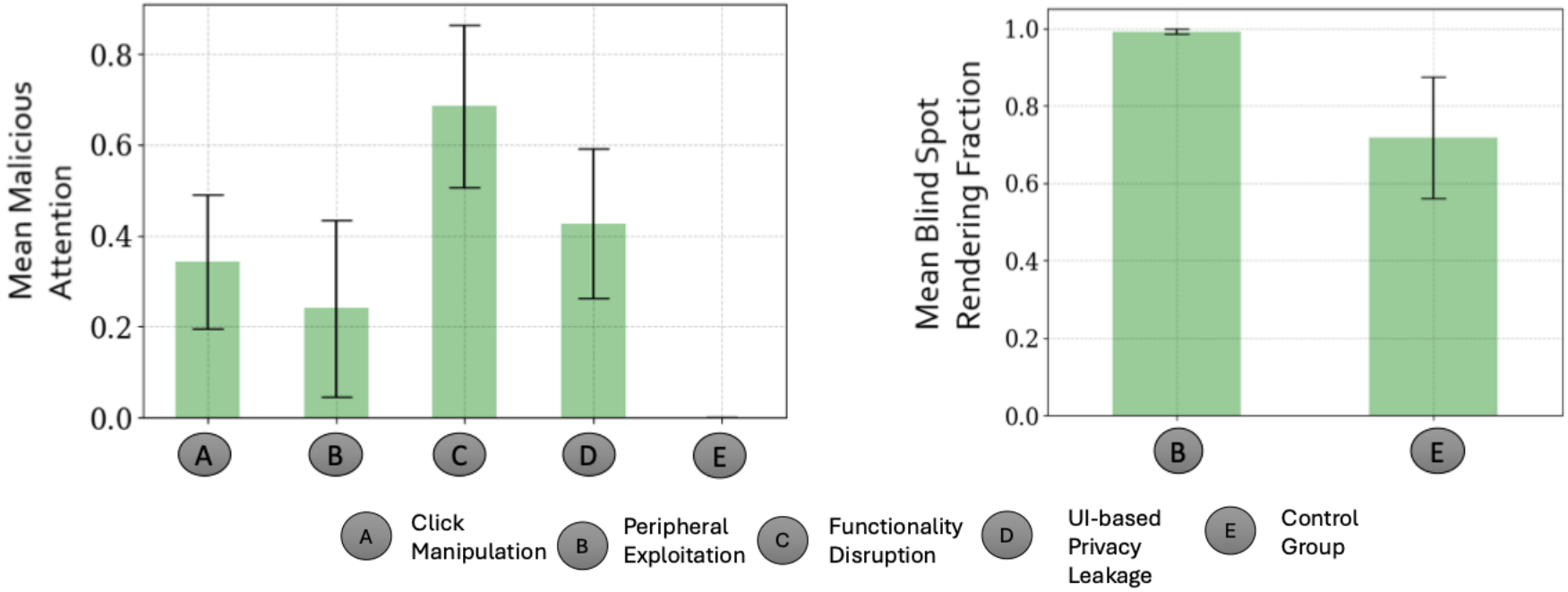
- Attacks are effective in achieving their objectives.



User Study Findings - 3

Do these attacks achieve their intended objectives?

- Attacks are effective in achieving their objectives.
- Generalization to different applications.



Summary

- WebXR
  - Easily available, deployable, can be seamlessly used in various HMD devices.
  - Beneficial UI properties can also be exploited to integrate dark patterns.

Summary

- WebXR
  - Easily available, deployable, can be seamlessly used in various HMD devices.
  - Beneficial UI properties can also be exploited to integrate dark patterns.
- Contributions
  - Five novel UI-based attacks.
  - Four-category taxonomy identifying contributing UI properties.
  - Open source: Logging Framework, Interaction Metrics, Apps.

Summary

- WebXR
  - Easily available, deployable, can be seamlessly used in various HMD devices.
  - Beneficial UI properties can also be exploited to integrate dark patterns.
- Contributions
  - Five novel UI-based attacks.
  - Four-category taxonomy identifying contributing UI properties.
  - Open source: Logging Framework, Interaction Metrics, Apps.
- Developers and platform owners can use the list of identified properties and attacks to secure user interactions in WebXR.

Thank You! Questions?

cmukherj@purdue.edu

PURDUE UNIVERSITY

AUS American University of Sharjah

UCI

CERIAS

PurSec Lab