AdCube: WebVR Ad Fraud and Practical Confinement of Third-Party Ads

Hyunjoo Lee[†], **Jiyeon Lee**[†], Daejun Kim[†], Suman Jana[‡], Insik Shin[†], Sooel Son[†]

[†] KAIST

[‡] COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Virtual Reality (VR)

- VR is the next computing revolution, it changes how we play, work, learn and live.

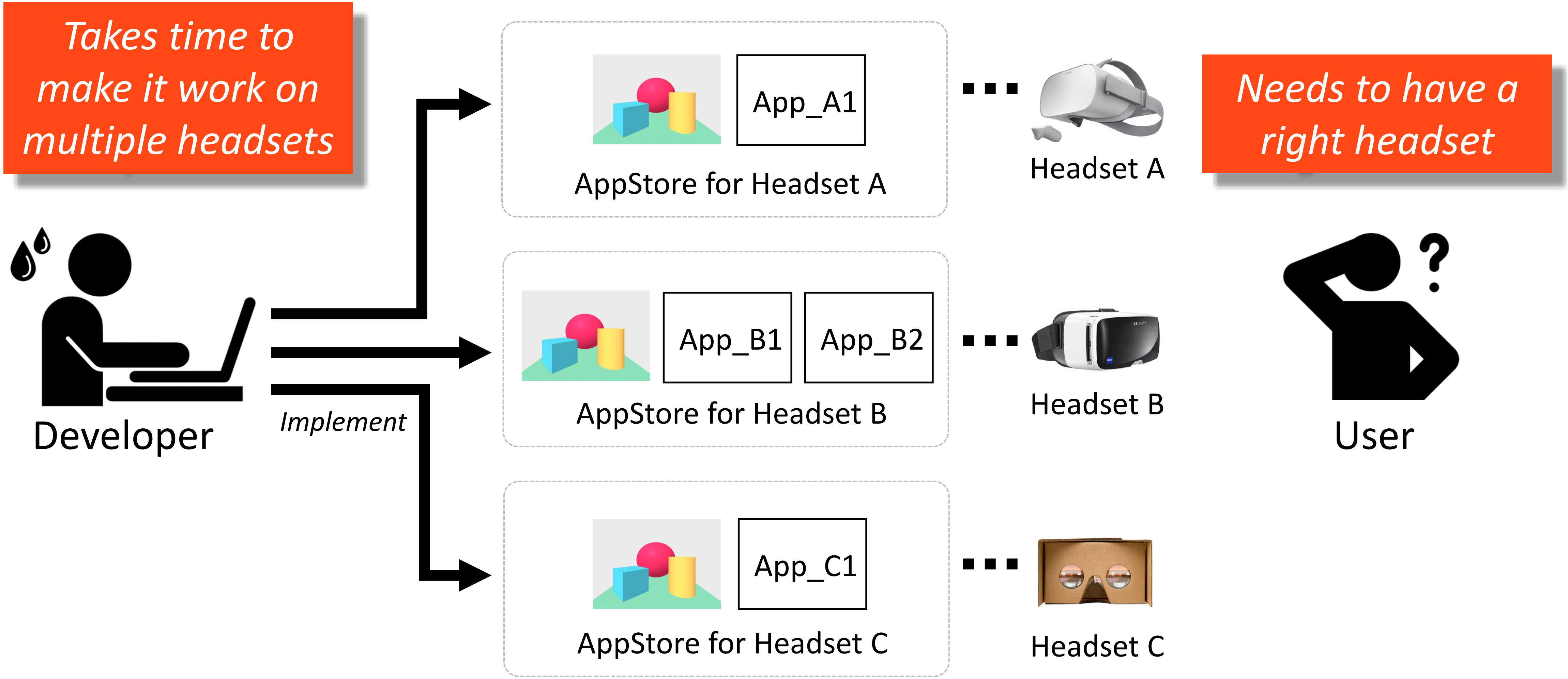
Game

Medical support

Fitness

Image Source:
https://www.amazon.com.au/Sony-PSVR-MegaPack-Bundle-2/dp/B07XLL6S5D
https://etech.iec.ch/issue/2019-03/virtual-reality-makes-real-life-even-better
https://www.wareable.com/vr/vr-fitness-holodia-one-big-problem

Limitations of the VR ecosystem



Takes time to make it work on multiple headsets

Developer

Implement

App_A1

AppStore for Headset A

App_B1

App_B2

AppStore for Headset B

App_C1

AppStore for Headset C

Headset A

Headset B

Headset C

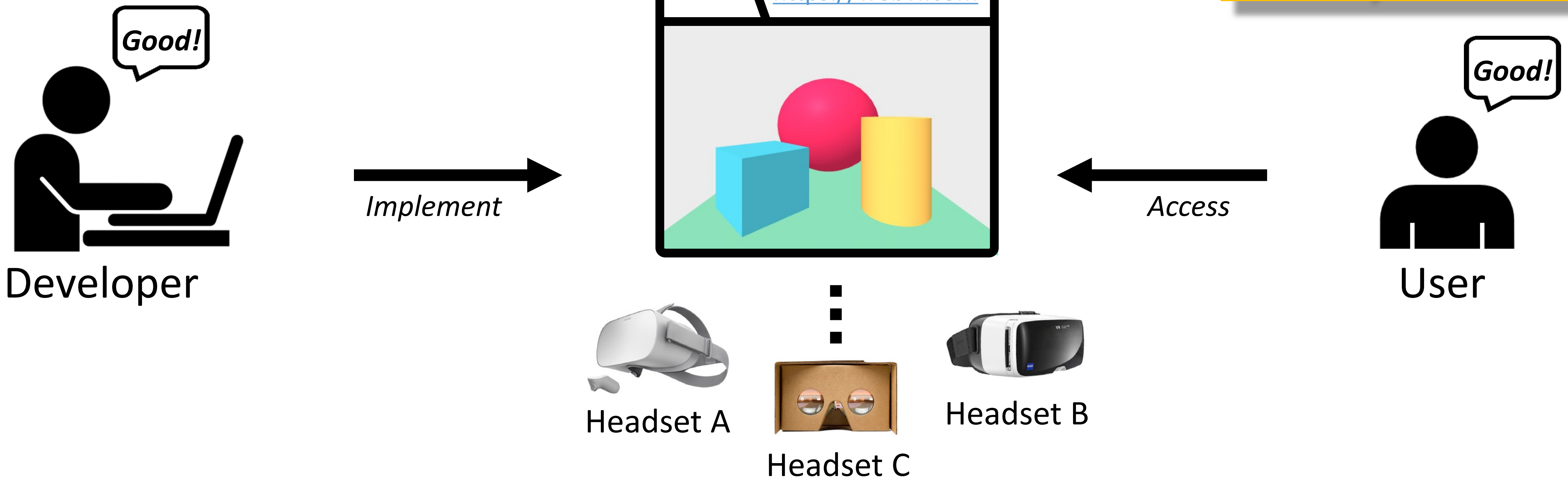
Needs to have a right headset

User

Enable VR on the Web

Easy to share

Any device through any browser



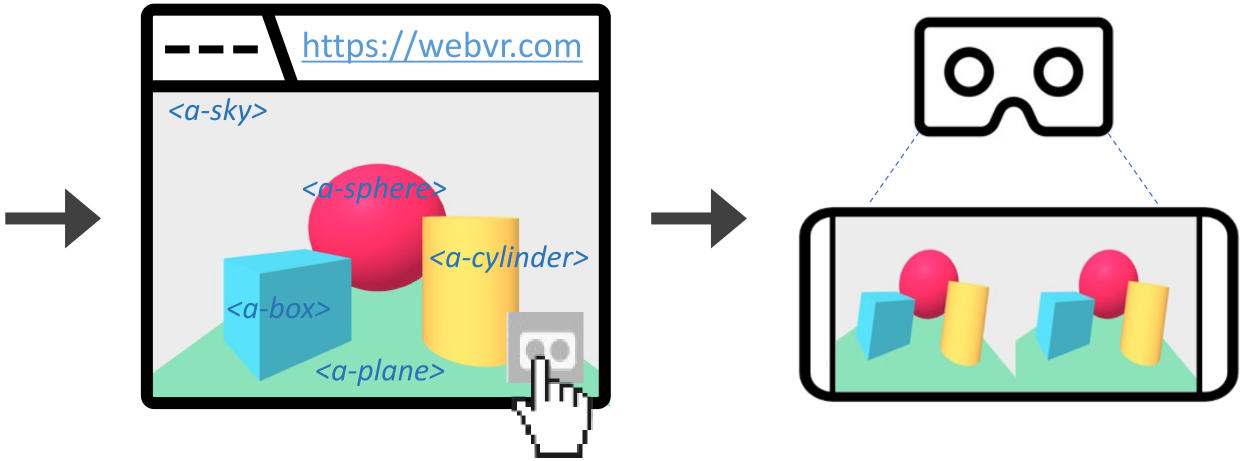
WebVR

- Enables VR on the Web, Supported by: Firefox 77+ Chrome 79+ Edge 79+
- Several frameworks (e.g., A-Frame) exist to help build a 3D world.

three.js React 360

A-Frame Example

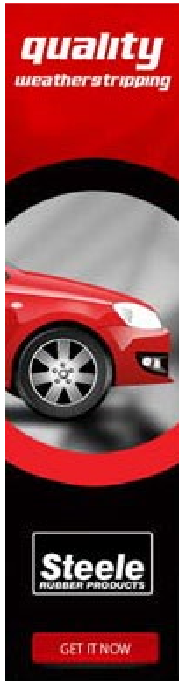
```
<head>
 <script src="aframe.js"></script>
 …
 <a-scene>
  <a-box position="-1 0.5 -3" color="#4CC3D9"></a-box>
  <a-sphere position="0 1.25 -5" color="#EF2D5E"></a-sphere>
  <a-cylinder position="1 0.75 -3" color="#FFC65D"></a-cylinder>
  <a-plane position="0 0 -4" color="#7BC8A4"></a-plane>
  <a-sky color="#ECECEC"></a-sky>
 </a-scene>
 …
```

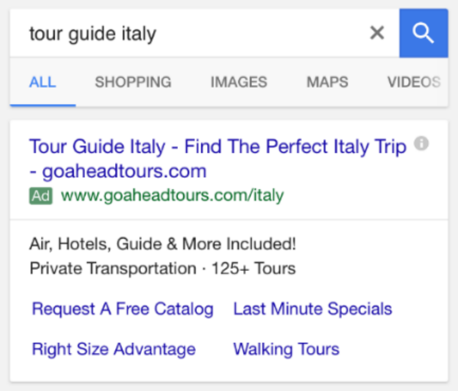


- Use cases: News, e-commerce, VR films, education, Custom business solutions

Motivation

- Online advertising is essential for the benefit of Web hosts.
- Recently, advertising has been applied to 3D world.




tour guide italy

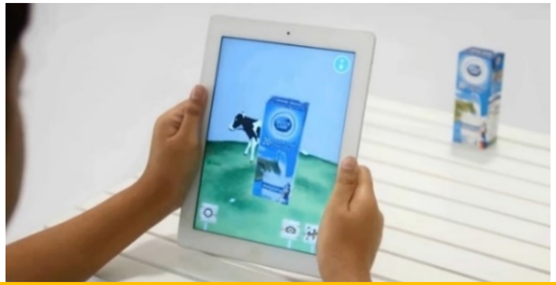
ALL SHOPPING IMAGES MAPS VIDEOS

Tour Guide Italy - Find The Perfect Italy Trip - goaheadtours.com
Ad www.goaheadtours.com/italy

Air, Hotels, Guide & More Included!
Private Transportation · 125+ Tours

Request A Free Catalog Last Minute Specials
Right Size Advantage Walking Tours

2D Advertising

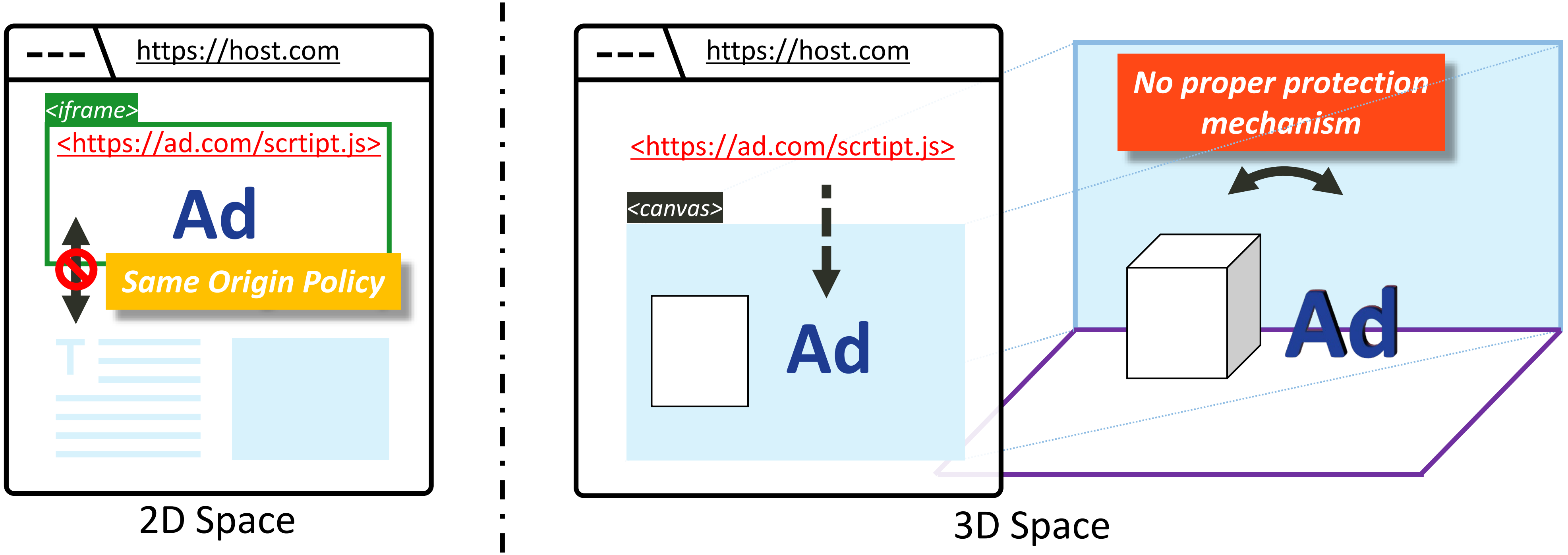


500% increase in the click-through rate due to the VR ad campaigns

3D Advertising

Problem

- There is no iframe-like primitive to isolate third-party ads in WebVR



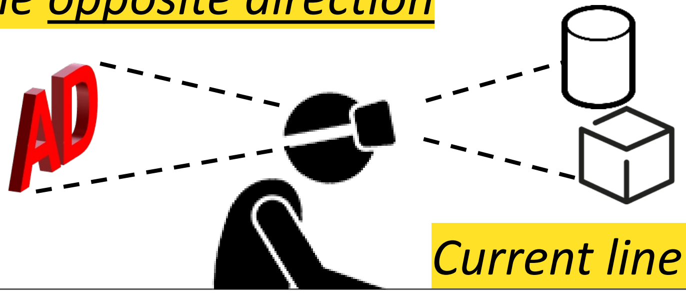
➔ Abusive third-party ads share the canvas with the first-party webpage

We introduce
four ad fraud techniques
specific to the WebVR environment

WebVR ad Frauds

Blind Spot Tracking Attack

Hide an ad entity
in the opposite direction



Current line of sight

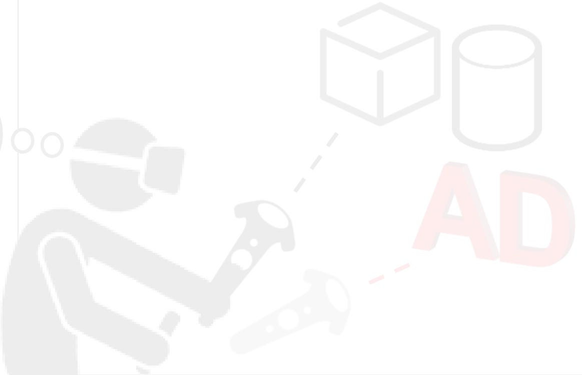
Abuse Auxiliary Display Attack

Display an Ad entity on the auxiliary display

Gaze Cursor Jacking Attack

Create a fake gaze cursor
and hide the original cursor

Controller Jacking Attack



Introduce an
additional fake
controller cursor

WebVR ad Frauds

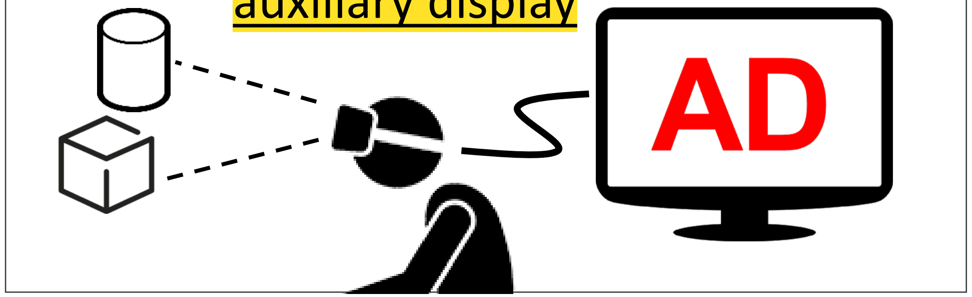
Blind Spot Tracking Attack

Hide an Ad entity
in the opposite direction

Current line of sight

Abuse Auxiliary Display Attack

Display an ad entity on the auxiliary display



Gaze Cursor Jacking Attack

AD
I am pointing…

Create a fake gaze cursor
and hide the original cursor

Controller Jacking Attack

Introduce an
additional fake
controller cursor

WebVR ad Frauds

Blind Spot Tracking Attack

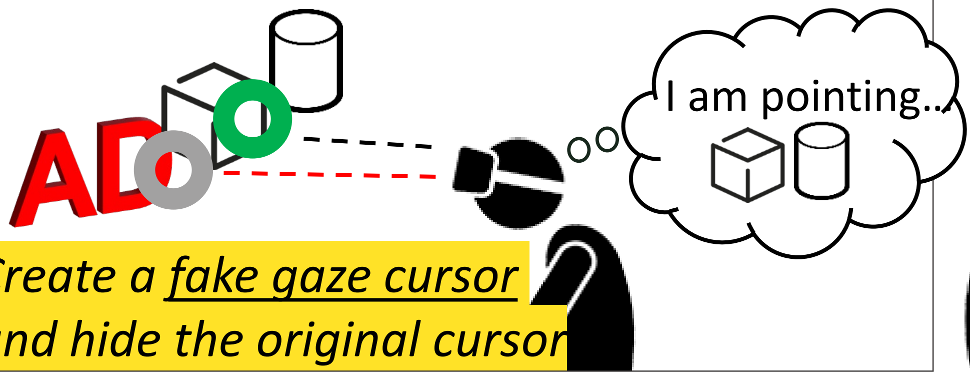
Hide an Ad entity in the opposite direction

AD
Current line of sight

Abuse Auxiliary Display Attack

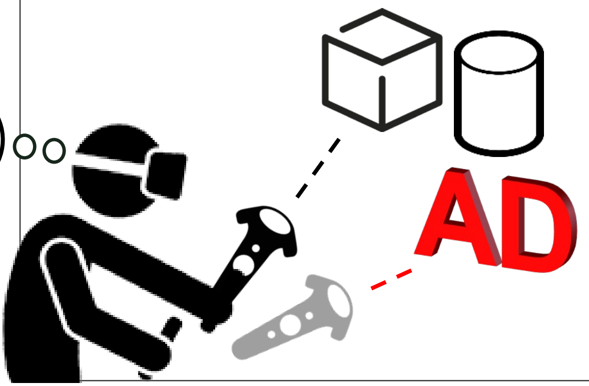
Display an Ad entity on the auxiliary display

Gaze Cursor Jacking Attack



Create a fake gaze cursor and hide the original cursor

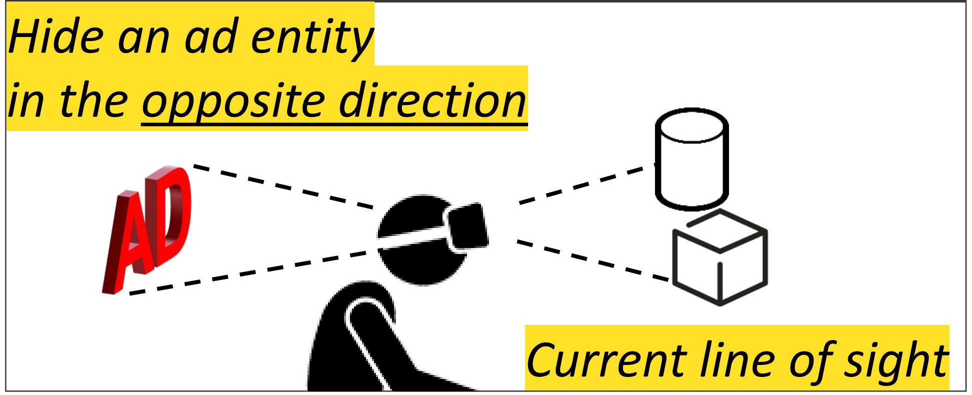
Controller Jacking Attack



Introduce an additional fake controller cursor

User Study on 82 Participants

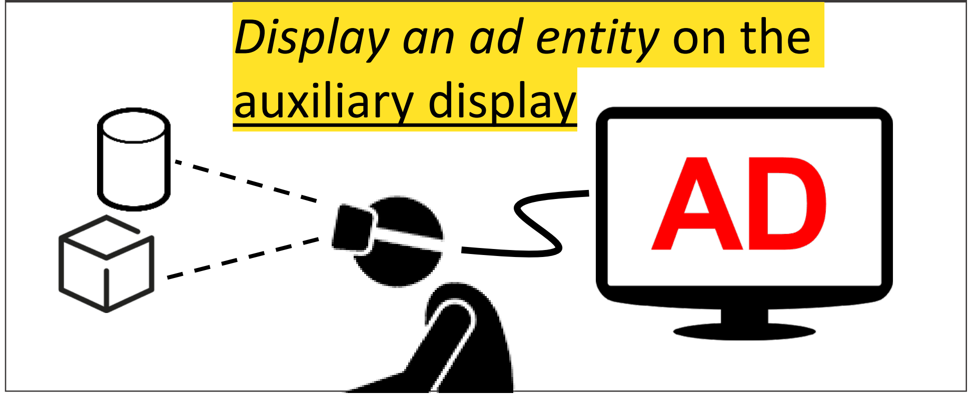
Blind Spot Tracking Attack



Hide an ad entity in the opposite direction

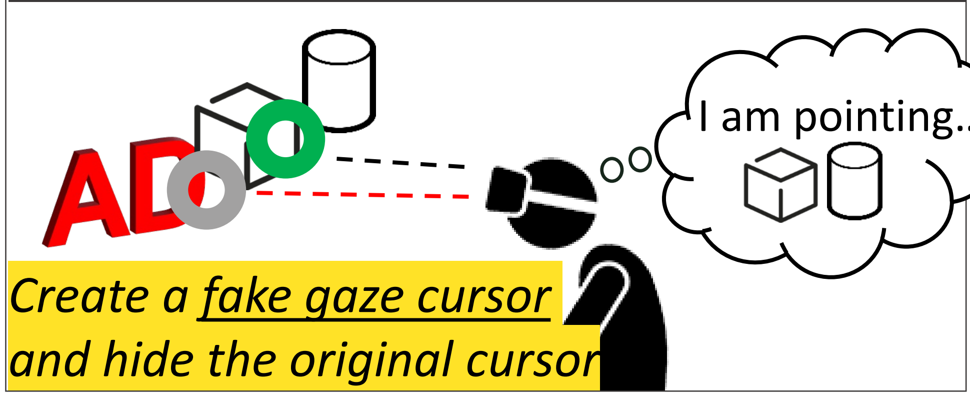
Current line of sight

Abuse Auxiliary Display Attack



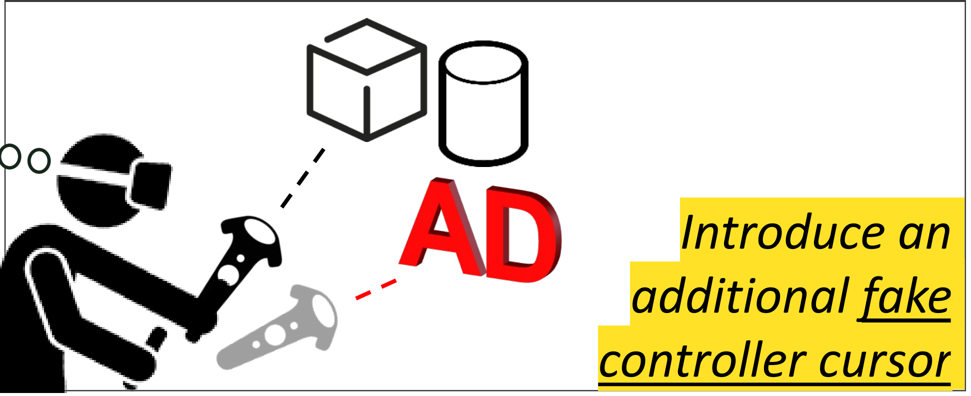
Display an ad entity on the auxiliary display

Gaze Cursor Jacking Attack



Create a fake gaze cursor and hide the original cursor

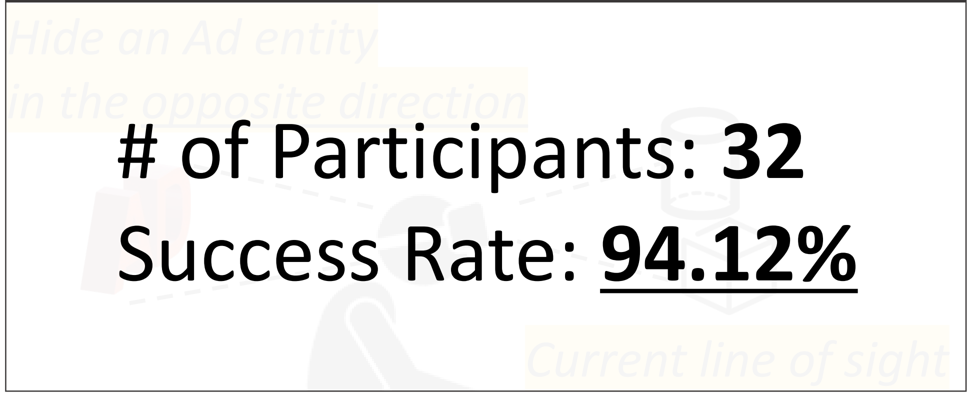
Controller Jacking Attack



Introduce an additional fake controller cursor

User Study Results

Blind Spot Tracking Attack

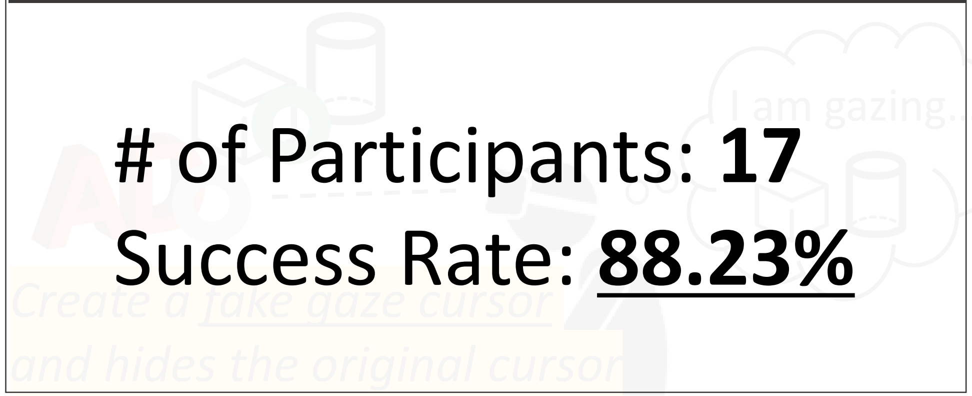


# of Participants: **32**
Success Rate: **<u>94.12%</u>**

Abuse Auxiliary Display Attack

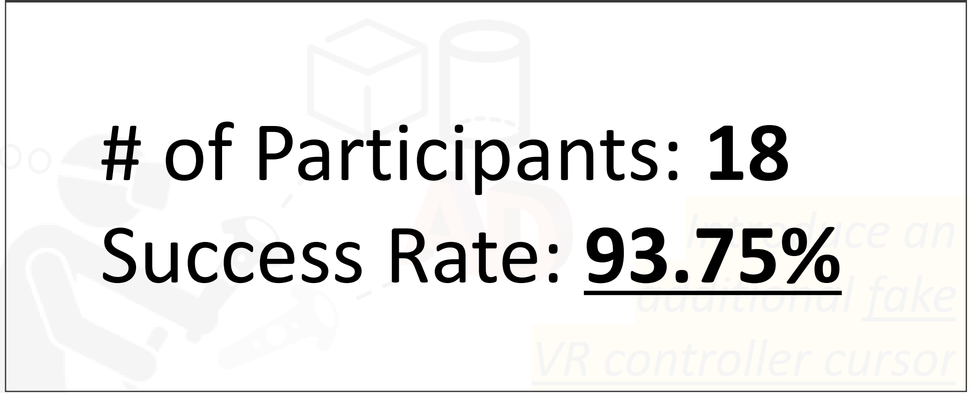
# of Participants: **32**
Success Rate: **<u>100%</u>**

Gaze Cursor Jacking Attack



# of Participants: **17**
Success Rate: **<u>88.23%</u>**

Controller Jacking Attack



# of Participants: **18**
Success Rate: **<u>93.75%</u>**

User Study Results

Blind Spot Tracking Attack

Hide an Ad entity in the opposite direction

# of Participants: **32**

Abuse Auxiliary Display Attack

Display an Ad entity on the auxiliary display

# of Participants: **32**

The four techniques are **effective in conducting click and impression fraud** in WebVR

I am gazing...

# of Participants: **17**

Success Rate: **88.23%**

Create a fake gaze cursor and hides the original cursor

# of Participants: **18**

Success Rate: **93.75%**

Introduce an additional fake VR controller cursor

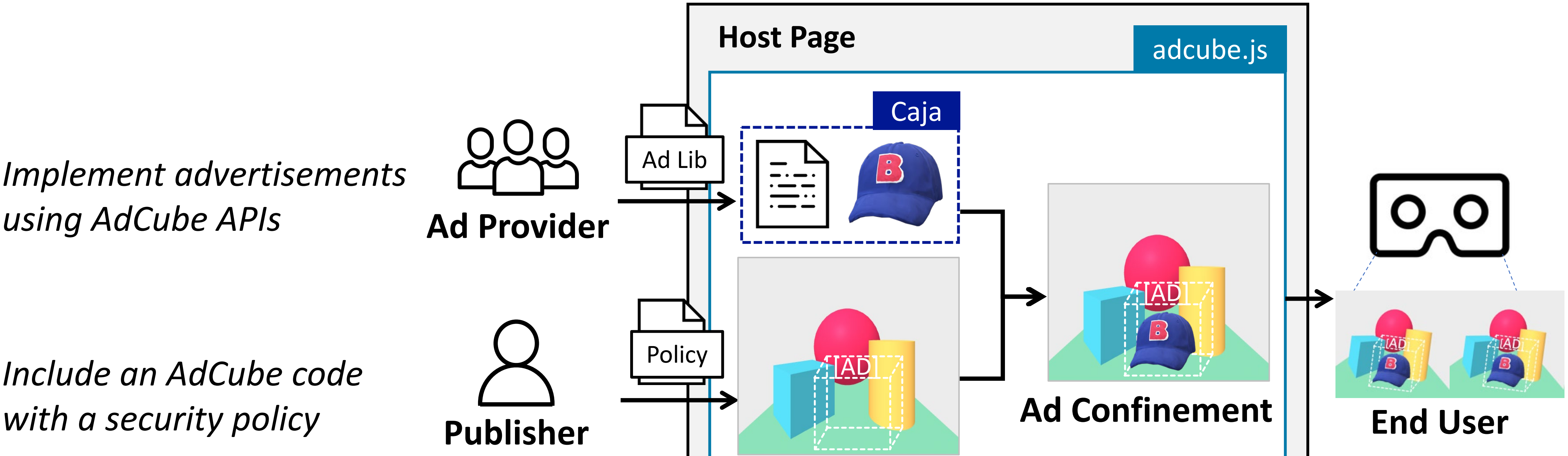
Defense Requirements

1. Third-party JavaScript code should place ad entities only within the confined area.

2. Third-party JavaScript code should not be able to alter DOM elements and sensitive entities (e.g., camera and controller).

AdCube Overview

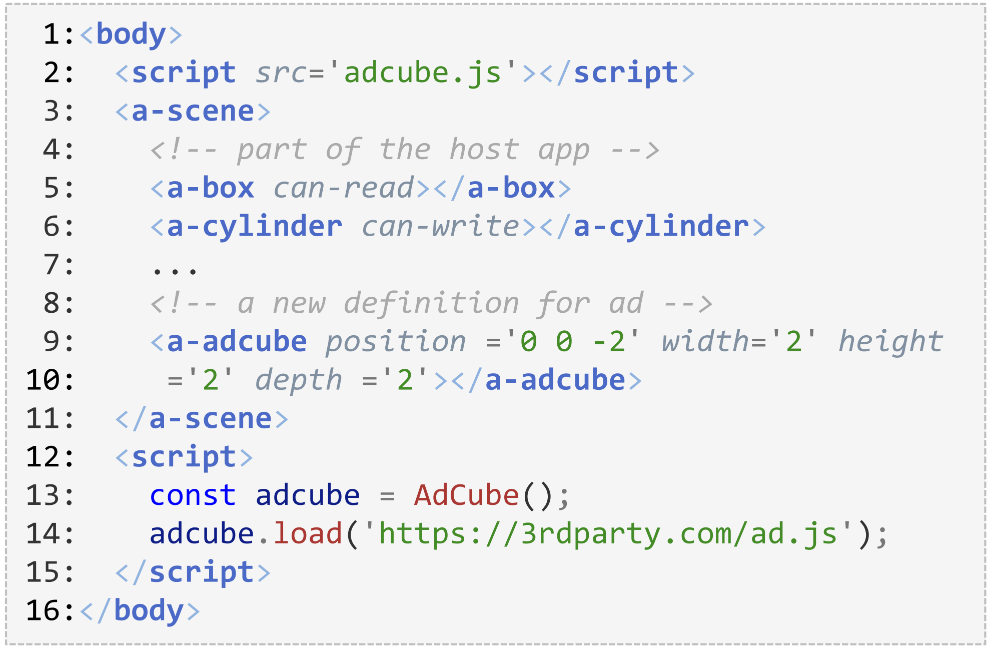
- AdCube is a JavaScript library, designed to confine the execution of third-party scripts rendering WebVR ads.



Implement advertisements using AdCube APIs
Ad Provider
Include an AdCube code with a security policy
Publisher
Ad Lib
Policy
Host Page
adcube.js
Caja
[AD]
Ad Confinement
End User

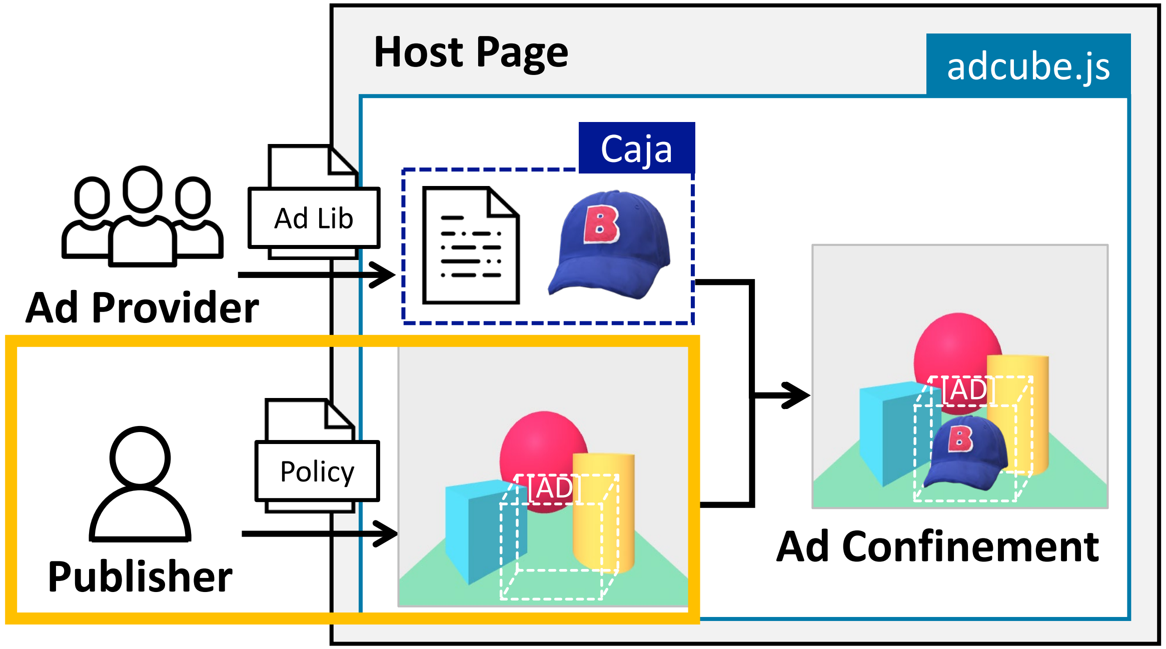
AdCube in Detail

1. The publisher defines ad in scene and writes a security policy.



```
<body>
  <script src='adcube.js'></script>
  <a-scene>
    <!-- part of the host app -->
    <a-box can-read></a-box>
    <a-cylinder can-write></a-cylinder>
    ...
    <!-- a new definition for ad -->
    <a-adcube position ='0 0 -2' width='2' height
     ='2' depth ='2'></a-adcube>
  </a-scene>
  <script>
    const adcube = AdCube();
    adcube.load('https://3rdparty.com/ad.js');
  </script>
</body>
```

An example of A-Frame host page with AdCube

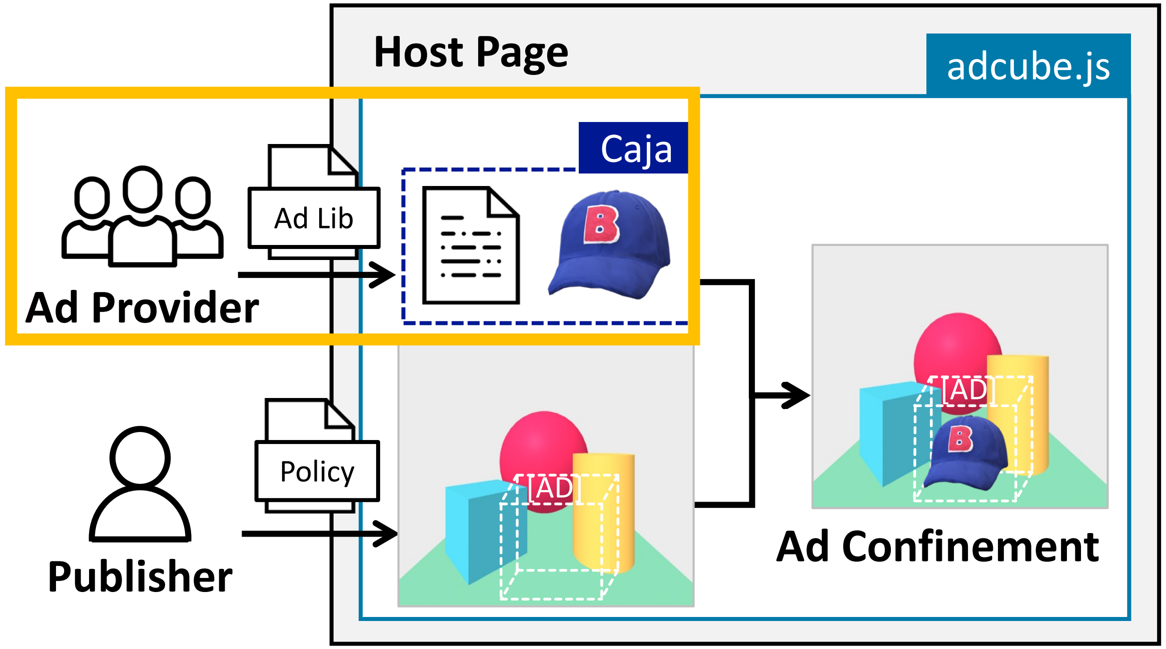


AdCube in Detail

2. The Ad provider implements advertising with AdCube APIs.

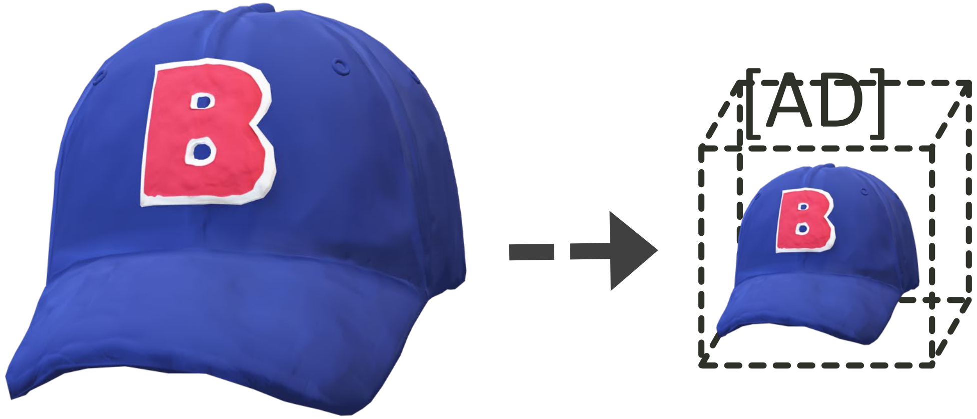
```
let e = createElement('a-gltf-model’);
e.setAttribute('src', 'product.gltf’);
e.addEventListener('click', onClick);
addElement('adcube-id', e);
function onClick(event){
  /** click event handler **/
}
```

An example of ad-serving JS script

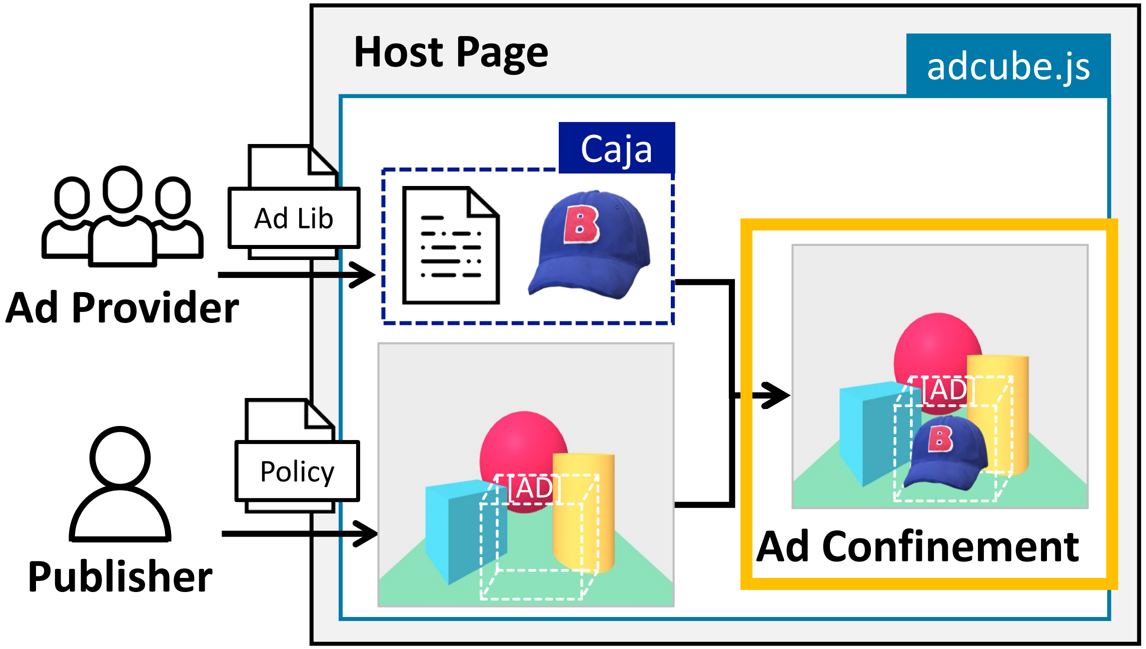


AdCube in Detail

3. AdCube confines an ad in the space provided by the publisher.

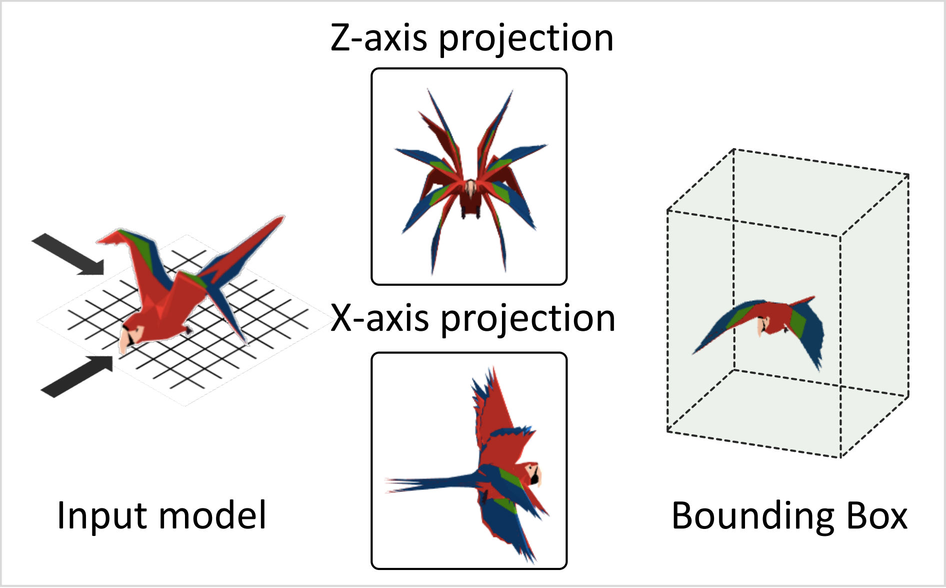


Resizing the ad entity to fit within
the space allowed by the publisher

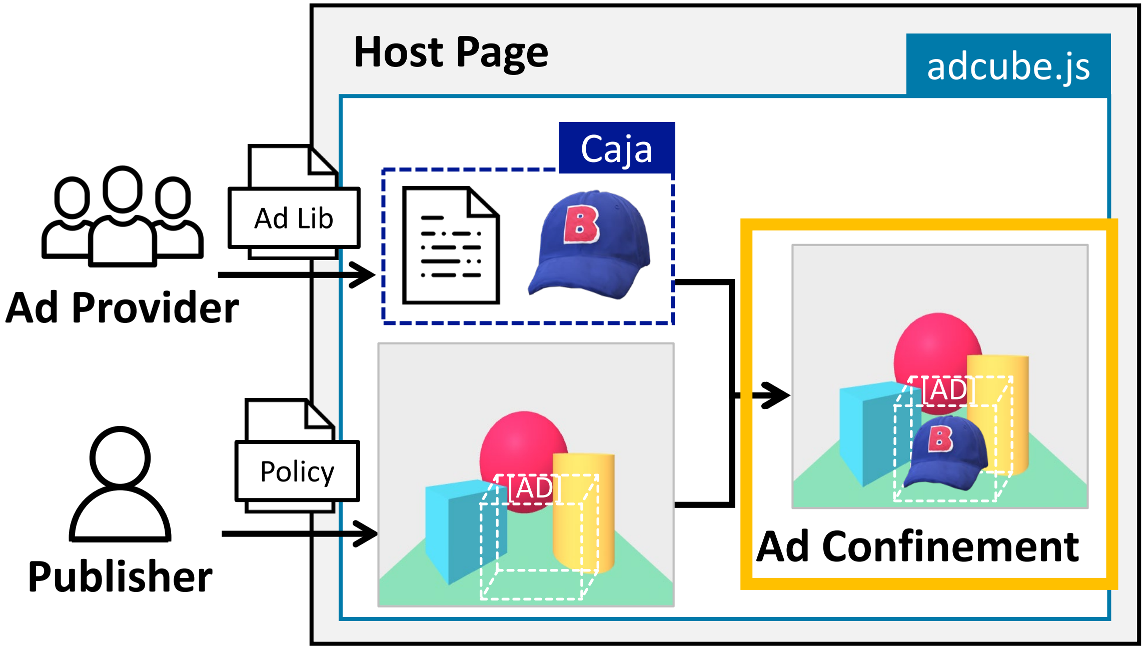


AdCube in Detail

3. AdCube confines an ad in the space provided by the publisher.



Calculating the maximum size of a bounding box including animation actions

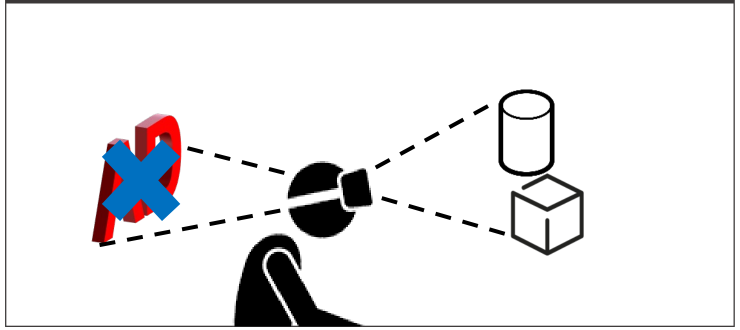


Security Evaluation

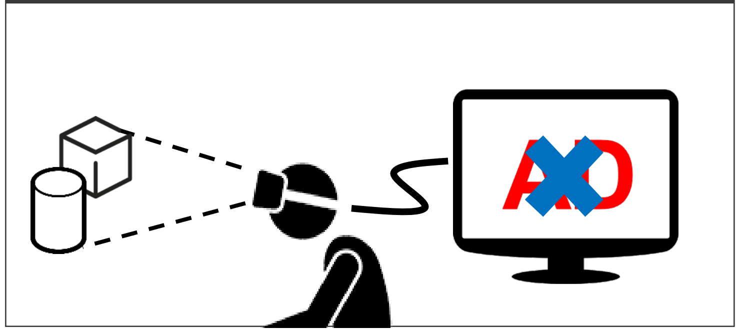
- AdCube blocks all four of the attacks by:

✓ The default policy of AdCube specifies no read and write access

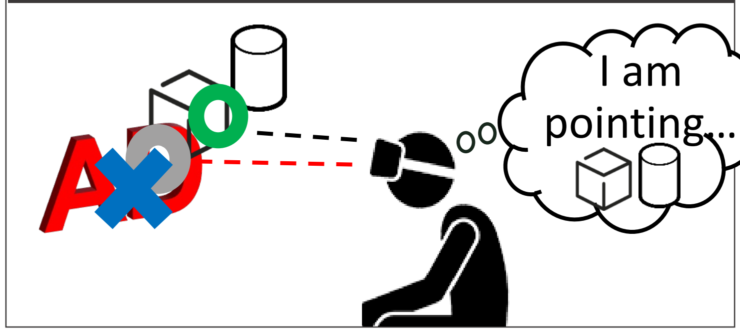
Blind Spot Tracking Attack



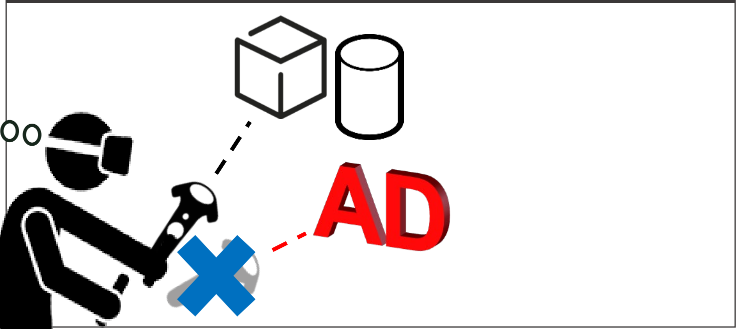
Abuse Auxiliary Display Attack



Gaze Cursor Jacking Attack



Controller Jacking Attack

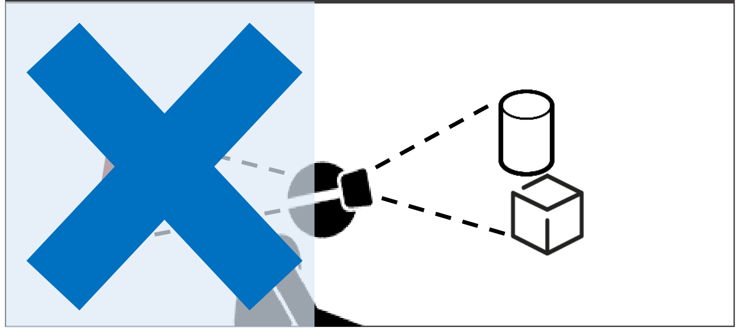


Security Evaluation

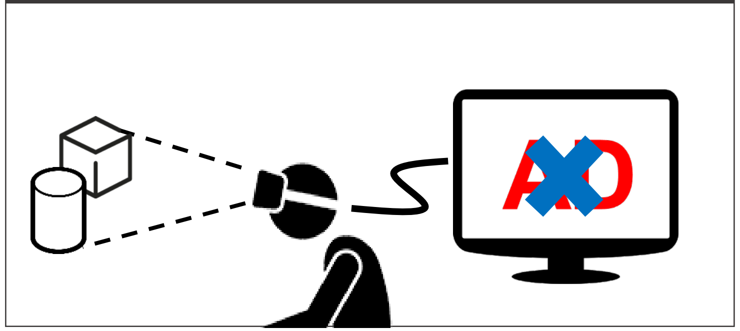
➔ ***<u>AdCube effectively defends all attack scenarios</u>***

- ✓ The default policy of AdCube specifies no read and write access
- ✓ AdCube prohibits advertising behind the camera
- ✓ All fake cursors are visually distinguishable with the [AD] label

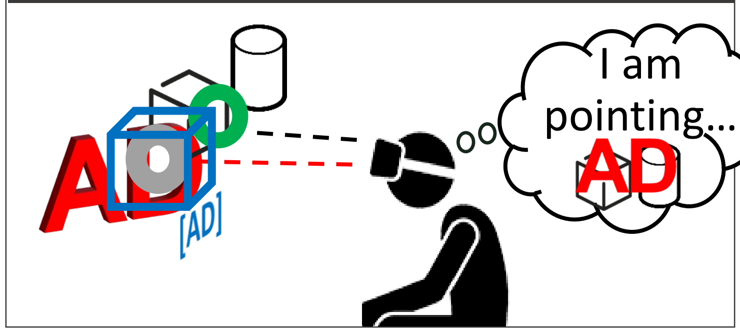
Blind Spot Tracking Attack



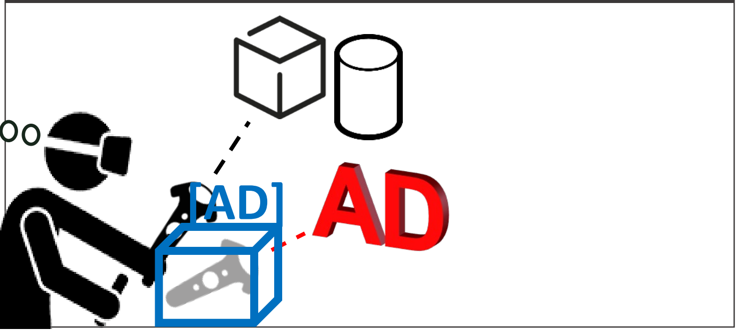
Abuse Auxiliary Display Attack



Gaze Cursor Jacking Attack



Controller Jacking Attack



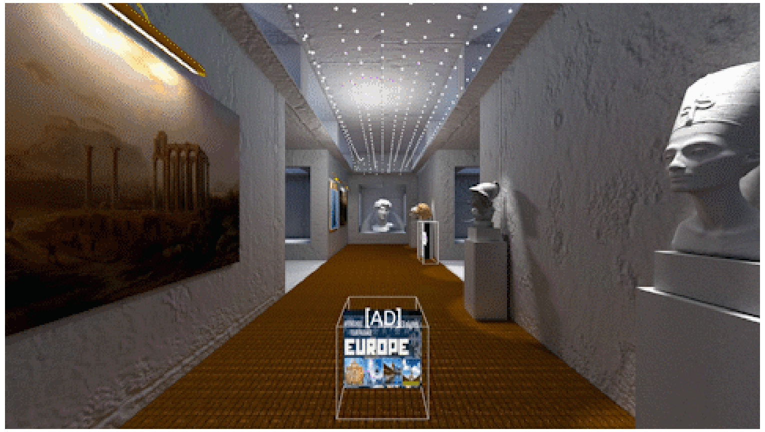
Performance Evaluation

- Two other methods
  - **Baseline**: run third-party scripts without any underlying security defense
  - **Mirroring**: run the third-party script in a separate origin different from its host
- Experiment
  - Measured 1) the average page loading times ran on the nine WebVR sites and 2) FPS change for 12 events

Performance Metric	Baseline	Mirroring	AdCube
Average Loading Time (s)	0.55	0.95	0.78
FPS (drop rate)	56.70 (-)	53.12 (6.32%)	55.79 (1.60%)

Conclusion

- We have devised four new attack variants to conduct WebVR ad fraud.
- We propose AdCube that allows publishers to confine third-party ad entities.
- AdCube is able to block ad fraud threats with negligible overheads.



A Showcase of WebVR ads with AdCube

Thank You

Jiyeon Lee (jy.lee@kaist.ac.kr)

KAIST

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK