Security and Privacy Challenges of AR and VR

By: Redell Fair, Jessica Morales-Deleon, Nyla Blackwell

PERSPECTIVE

AR/MR:

Virtual objects behave based on user's perspective in the real world

VR:

Virtual objects will change their position and size according to user's perspective in the virtual world

What is AR?

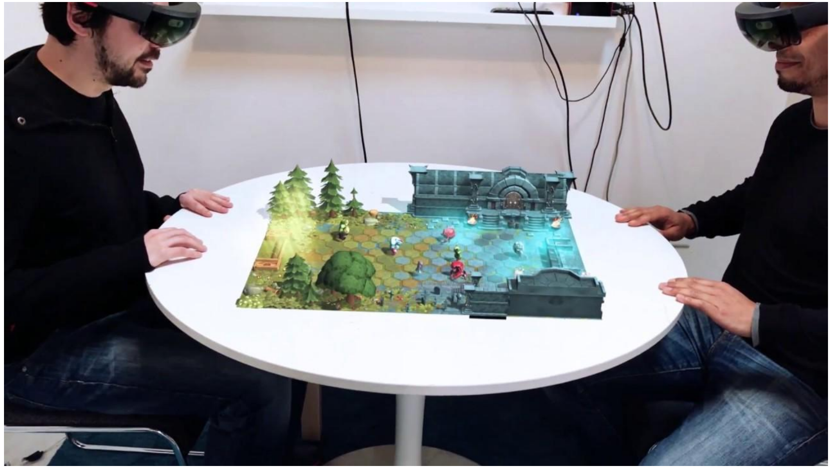
- Demonstrates virtual content on our perceptions of the physical world
- A commercial reality
- New and Improving

Gaps in Previous Studies

- Security and Privacy Problems:
    - Multi-user
    - Still new, still emerging

Single vs Multi-User Applications

- Single: One user interacting with their own AR device; done locally like from a mobile phone
- Multi: Multiple Users interacting within the same space



Risks

- Unknown Actions - hacker may alter the reality/environment in a way that is not familiar to the user.
- Physical Safety - one may not understand the true space around; may lead to dangerously accommodating new areas.
- Privacy - hacker may decipher other users’ private conversations.

Physiological Attacks and Deception

- Displaying Content on People - deceiving others with a sense of masquerade; not truly knowing who exactly you're talking to.
- Other Users' Obscure Actions - placing inappropriate virtual objects on an otherwise innocent user.
- Epilepsy - along with other visual holdings, flashing lights from a malicious user may dangerously affect another.

Security Mechanisms Targeted

- Ownership - determining which virtual objects truly belongs to you, or perhaps, the public.
- Access Control - controlling your own personal space, defending against unwanted circumstances.

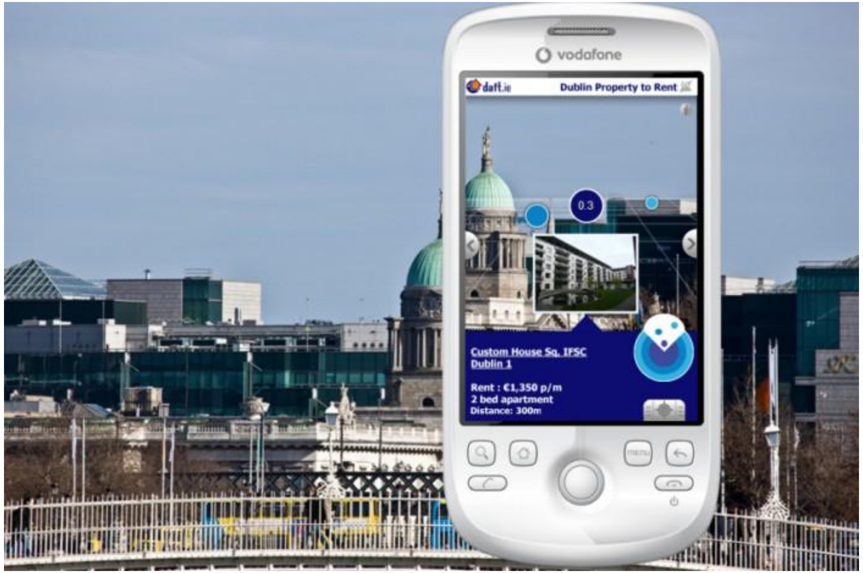
Security and Privacy of Multi-User AR

- Controlling other users’ access to personal objects
  - view/edit permissions to control a shared space
- Restraining Undesired content from other users
  - Controlling clutter (for example, huge block impeding your way) and inappropriate visuals
- Managing content between users
  - Avoiding spam and focusing on distributing information among the intended users
- Exploring Shared Environments
  - Intended sharing
- Access Control UIs
  - Design concept for organizing permissions
- Personal Space
  - No colliding objects nor people within your virtual space

No Escape from Reality:
Security and Privacy of Augmented Reality Browsers

Introduction

- Augmented reality (AR) browsers add interactive virtual objects to the user’s view of the physical world
- Popular AR browser are Junaio, Layar and Wikitude



Custom House Sq. IFSC
Dublin 1

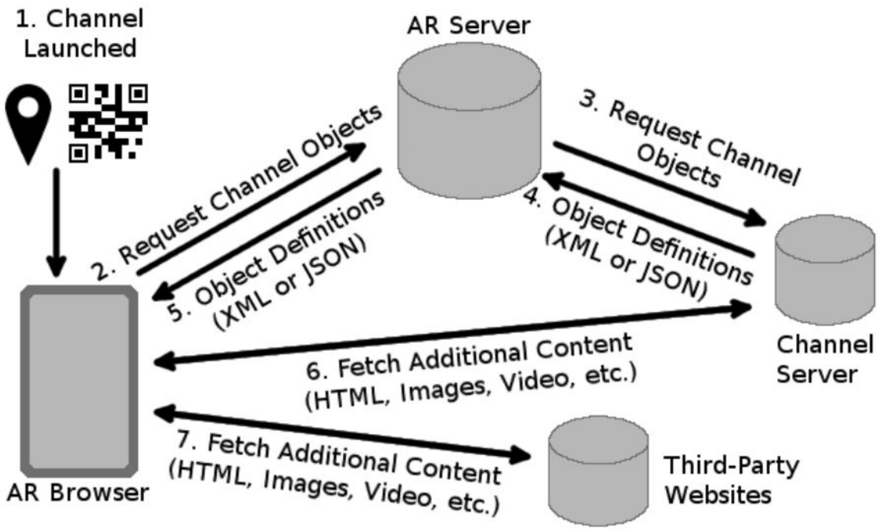
Rent : €1,350 p/m
2 bed apartment
Distance: 300m

AR Browser

- AR applications have three stages
- access sensors on mobile device (GPS, camera)
- Create and manipulate a variety of 2D and 3D interactive virtual objects
- Display virtual on top of the camera feed

Architecture of AR Services

- User access third party AR content through dedicated AR servers
- AR content providers host it in their servers and register their content with AR service providers
- AR content are channels

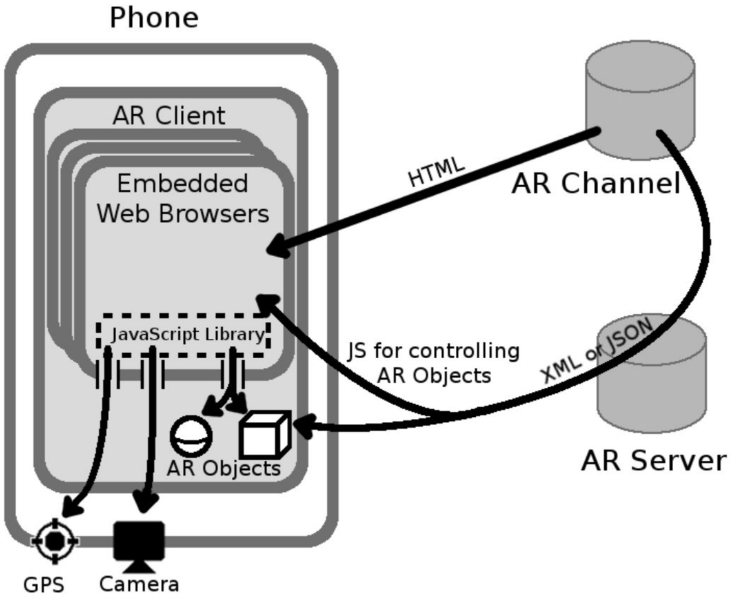

1. Channel Launched
AR Server
2. Request Channel Objects
3. Request Channel Objects
4. Object Definitions (XML or JSON)
5. Object Definitions (XML or JSON)
Channel Server
6. Fetch Additional Content (HTML, Images, Video, etc.)
7. Fetch Additional Content (HTML, Images, Video, etc.)
AR Browser
Third-Party Websites

AR Functional Requirements

- Access to native resources on the user’s device
  - Access to onboard camera and GPS location
- Support of interactive AR content
  - Channels include service specific XML or JSON
- Image-Triggered code execution
  - automatically recognize picture and launch channels
- Outsourced image processing
  - send images from phone’s camera to provider for processing
- Visual composition of AR content
- Indirect retrieval of AR content

Components of AR services

- AR browsers
- AR channels
  - specify AR content for display and how to display it
  - specify actions to take
- AR servers



Threat Model

- AR attackers
  - controls malicious contents and trick users into visiting them
- Ad attackers
  - tricks AR channels into incorporating malicious content
- Web attackers
  - controls own website and lure users to its via ads
- Curious AR services
  - privacy risks caused by user-specific visual data
- Network attackers
  - Man-in-the-middle attacks

Out-of-Sandbox Native Access

- Access network device resources
- Can be accessed by any web content regardless of origin
- Launching AR browsers through custom URLs
- execute native commands directly without user permission

Risks

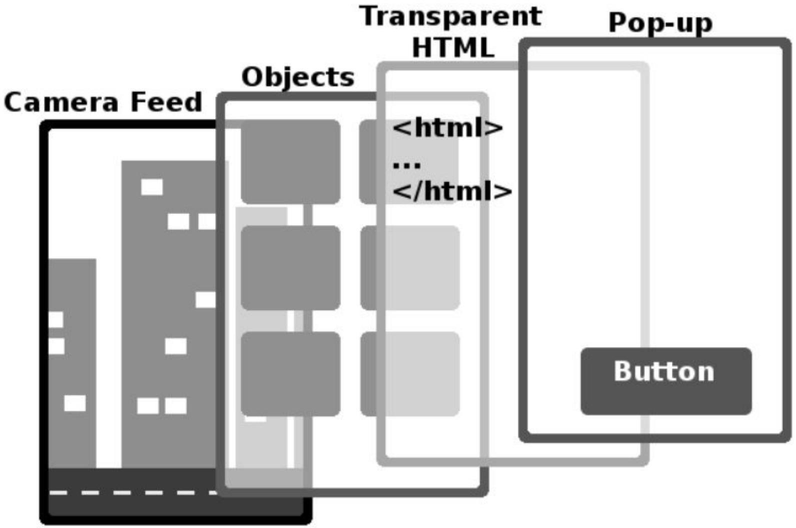
- Conventional web content breaking out of the sandbox
- Malicious ads breaking out of the sandbox
- Malicious AR content abusing access

Support for Non-HTML AR content

- AR objects such as 2D, 3D models, animations cannot be described in HTML alone and hence AR browsers rely on XML or JSON definitions
- AR browsers may combine content from different origins
- Conventional web browsers follow same-origin policy (SOP)
- Difficult to implement as objects must be described in XML or JSON which are not governed by SOP

Doing it wrong

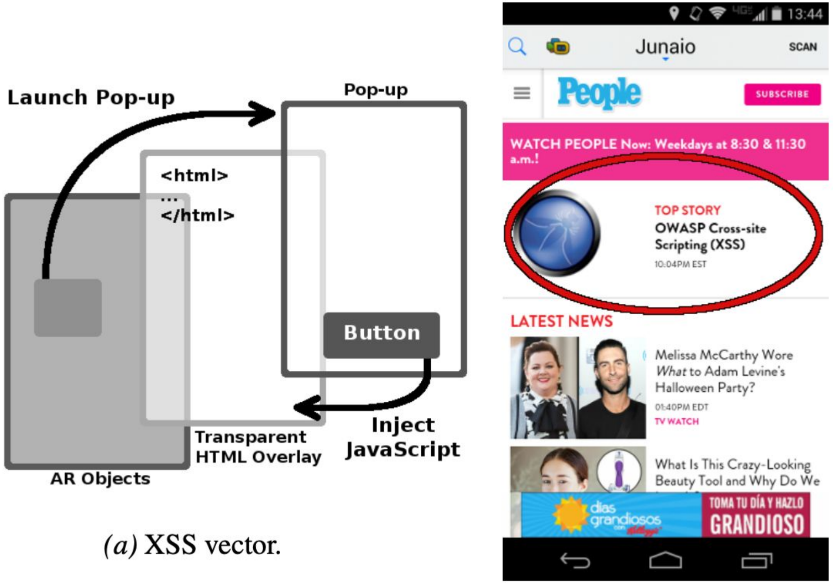
- AR objects defined in XML
- Transparent overlay provides GUI functionality
- Overlay may belong to a different origin



Junaio’s visual stack. AR objects are on top of the camera feed, the transparent overlay on top of the objects, if an object is clicked, a popup appears at the very top.

Risks

- Cross-site scripting
  - A malicious channel can specify any origin for the transparent page and associate arbitrary script with button
  - Clicking this button allows unrestricted access to all contents from page's origin



WATCH PEOPLE Now: Weekdays at 8:30 & 11:30 a.m.!

TOP STORY
OWASP Cross-site Scripting (XSS)
10:04PM EST

Melissa McCarthy Wore *What* to Adam Levine's Halloween Party?
01:40PM EDT
TV WATCH

What Is This Crazy-Looking Beauty Tool and Why Do We

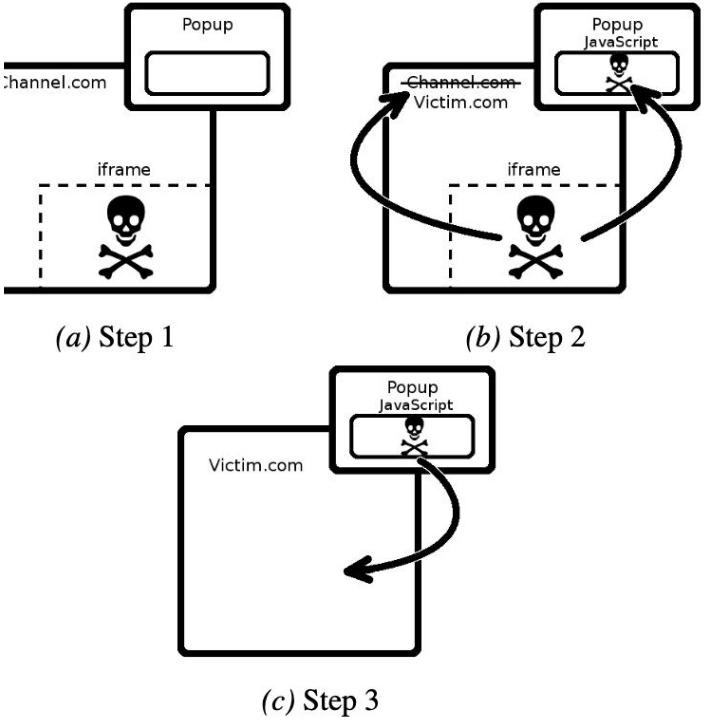
(a) XSS vector.

(b) Exploiting XSS.

Cross-site scripting (XSS) in Junaio

Risks (con't)

- Universal cross site scripting
  - Malicious javascript hidden in ad can associated with popup
  - Change URL of the transparent overlay



Universal XSS vulnerability in Junaio

Image-Triggered Code Execution

- AR service continuously analyze camera feed
- On recognizing an image associated with a channel it automatically launched channel content
- User cannot preview the URL or any other information

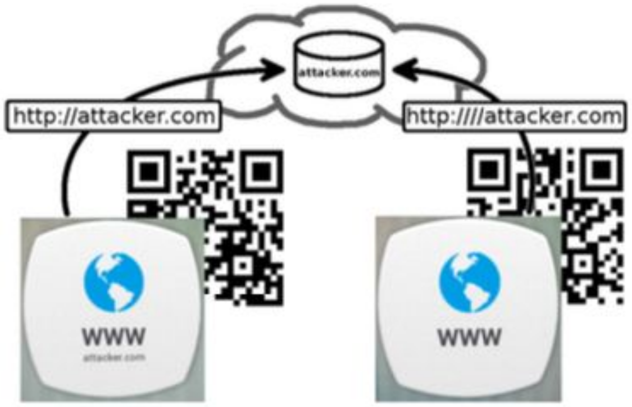


Figure 10: Both codes launch the same channel, but Layar fails to parse the

Both codes launch the same channel but Layar fails to parse the code on the right and does not show the URL

Risks

- Fully automated, stealthy, large-scale tracking
  - Used for automated stalking and tracking
- Automatically launching malicious content
  - attacker registers an image trigger similar to that of a trusted channel
  - AR browser may be tricked into automatically launching the malicious channel
  - same picture maybe associated with multiple channels

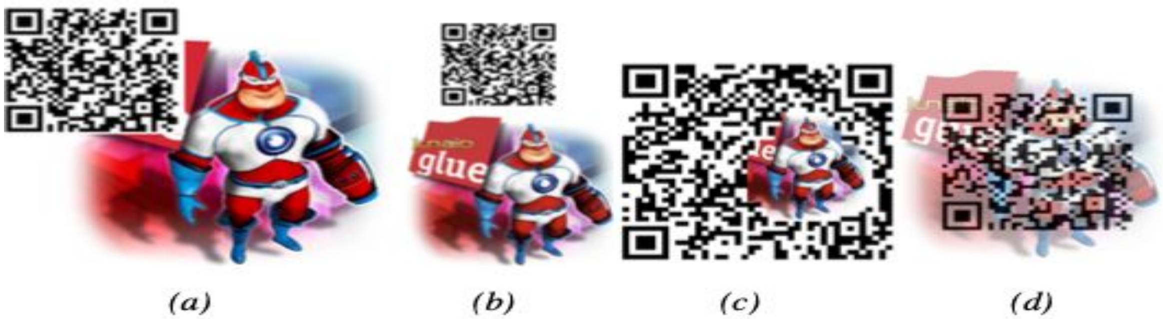


Figure 12: Different combinations of the Junaio mascot and QR code launch different channels.

Indirect retrieval of AR content

- Content requests must pass through the AR provider’s own server
- Some AR browsers enable third-party channels to authenticate users or keep track of preferences
- When the browser first loads the channel, the cookies are set by the channel’s authentication page and thus correctly bound to the channel’s origin at that time
- If the origin changes, the server notes the change and forwards requests accordingly
- Server does not notify the browser of the change

Risks

- AR attackers lie about their channel’s URL
- By “desynchronizing” the Layar browser’s and the Layar server’s understanding of the channel’s origin, a malicious channel can steal cookies from any origin

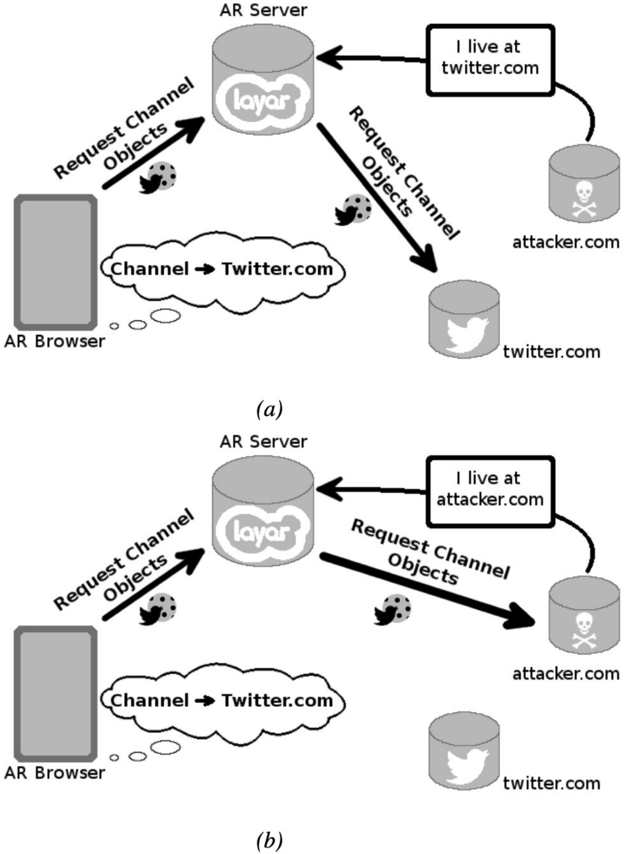


Figure 17: Layar cookie stealing attack.

Security and Privacy in Virtual Reality

What is a XR, VR, AR & MR

- Extended Reality (XR) is a paradigm that refers to different types of human-machine interaction within real and virtual environments, enabled by computer technology and wearable devices.
- Virtual Reality (VR) is a computer-generated simulation of a 3D environment that enables realistic physical interactions by means of technology and wearable devices.
- In Augmented Reality (AR), virtual objects are added to the real environment for enriching it;a notable example is pointing a smartphone to an art piece and getting information about the piece itself
- Mixed Reality (MR) is a combination of VR and AR, where the interactions do not happen exclusively in the virtual space nor in the real one, but in a hybrid fashion

How do Vrs Work?

- Different sensors are included into VR devices that capture both verbal and nonverbal cues. The VR engine then uses this data to create a virtual environment that responds to the user's activities.
- A VR has the ability to gather a lot of non-verbal data, including user motions, biometrics, and usage patterns.
- Additionally, information gathered when using the VR headset contains potential security and vulnerability risks.

Privacy Issues in VR

There is a combination of VR and social network privacy issues:

- Associational Privacy: The power to invite or reject people from events or the global village, where everyone may acquire both important and irrelevant information about others;
    - An example of this comes from Facebook. Facebook has a history of demonstrating how removing good or bad news from feeds influenced people's moods. They also pointed out that the Oculus regulations were written in a way that Facebook could carry out comparable trials.
    - The sensors in head-mounted displays (HMDs) allow for thorough recording of a user's physiological and psychological reactions to stimuli.These responses could be analyzed automatically and used for targeting users with tailored advertising, a method known as neuromarketing.

Privacy Issues in VR (cont.)

- Informational Privacy: The increased vulnerability of data or its misuse.
  - VR users are not sufficiently protected by the US legal system under its present laws against online identity theft. Plaintiffs have no party to suit due to the combination of many laws. Identity theft victims in virtual reality environments are unable to even file lawsuits in US courts.
- Physical Privacy: The prevalence of recording devices or the unintended revelation of physical information such as physical reactions to ads and the loss of anonymity.
  - Personal space is easy to detect and use to infer information about VR users, and this poses the nontrivial problem of how to collect and treat this type of data. An example of this would be an attack called ReAvatar which uses only movement to discover who is hiding behind a avatar. This does not require any malicious code.

The Solution for Privacy Issues in VR

- Method to assess the cognitive load of users during a driving simulation experience, while preserving their privacy.
- Using critical and noncritical time frames, trained multiple classifiers and validated their proposal with a leave-one-person-out cross-validation (LOOCV) approach.
- To combat eye tracking technology, images of the iris may be blurred with Gaussian filters, rendering the iris patterns unidentifiable while retaining the ability to detect gaze.
    - A hardware approach to this is to use an eye tracker which would be attached to a short telescoping arm, enabling users to freely manually defocus photographs of the iris.

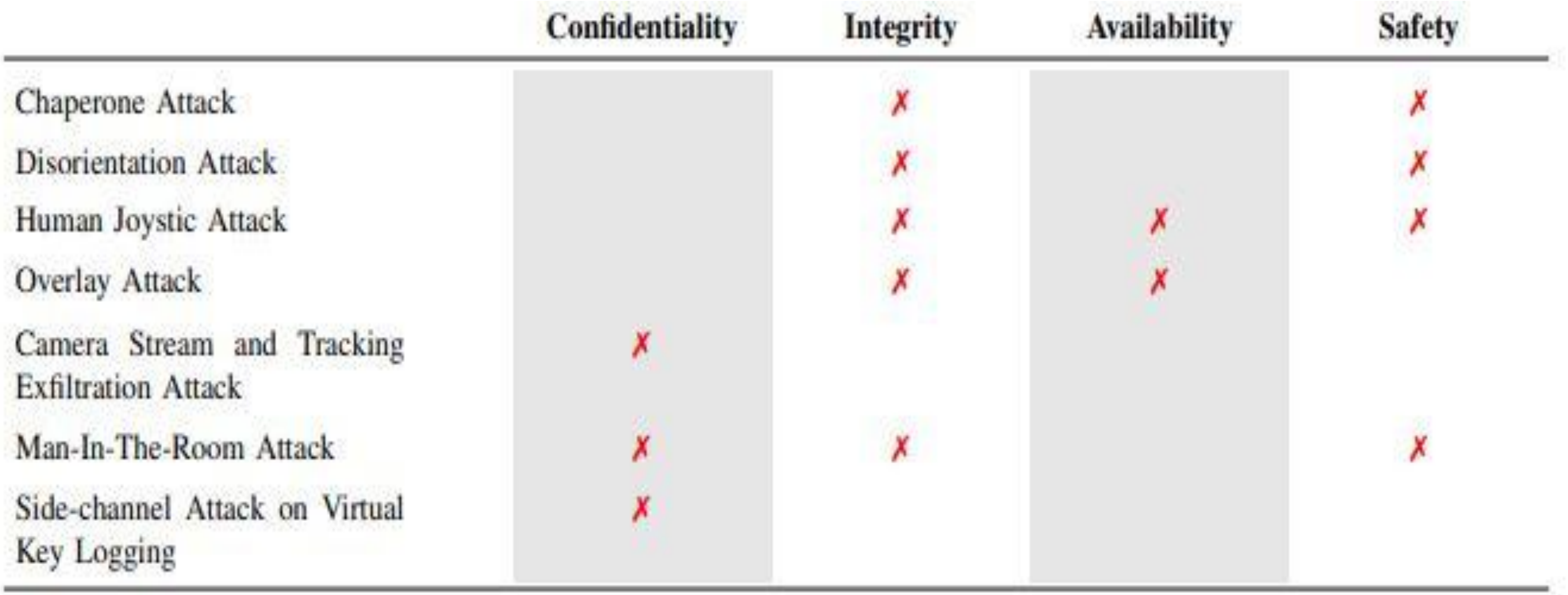
Specific Attacks to VR Security

- Chaperone Attacks
  - Manipulate the Virtual Environment (VE) boundaries (i.e., tampers with the walls drawn in the VR scene) to make the collision avoidance fail and put users’ safety at risk.
- Disorientation attacks
  - Aim to cause dizziness and confusion in VR users, causing a condition referred to as cybersickness. Cybersickness is a form of motion and simulation sickness due to physiological factors of the users, in correlation with their immersion and presence in VR environments;
- Human Joystick Attacks
  - Aim to control the physical movement of a user, such that they move to a predefined spot without realizing it;

Specific Attacks to VR Security (cont.)

- Overlay Attacks
  - Where an attacker inserts in the VE unwanted objects, such as images and videos.
- Camera Stream and Tracking Exfiltration attacks
  - attacker gains access to the HMD live stream and the HMD front facing camera stream.
- Man-In-The-Room attack
  - Attacker joining the target's VR environment while remaining invisible, allowing to extract information regarding the user or maliciously manipulate the environment.
- Side-channel Attack on Virtual Key Logging
  - Attackers can extract gesture patterns from channel state information (CSI) waveforms of Wi-Fi signals and then, by applying machine learning, recognize keystrokes from such patterns.

Specific Attacks to VR Security (CIAS Table)



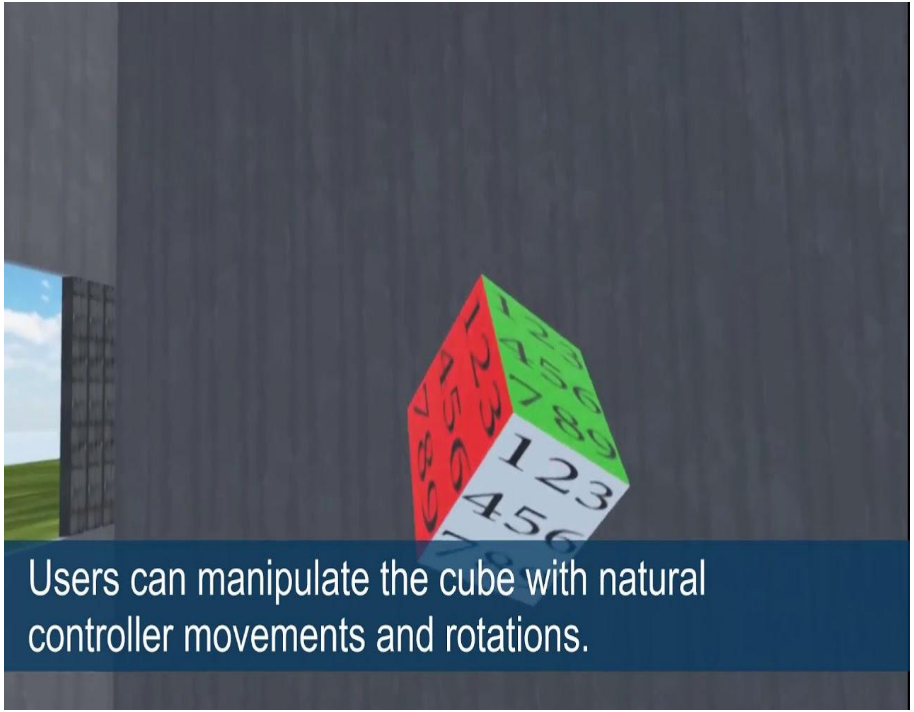
	Confidentiality	Integrity	Availability	Safety
Chaperone Attack		✗		✗
Disorientation Attack		✗		✗
Human Joystic Attack		✗	✗	✗
Overlay Attack		✗	✗	
Camera Stream and Tracking Exfiltration Attack	✗			
Man-In-The-Room Attack	✗	✗		✗
Side-channel Attack on Virtual Key Logging	✗			

Generic Attacks to VR Security

- VR systems may be exposed to more general security vulnerabilities in addition to those that affect VR particularly because of its features.
- The results of an experiment in which the traffic rate was artificially altered demonstrate that these attacks significantly impair several aspects that lead to cybersickness, such as nausea and pain.
    - The authors went on to show that security and privacy problems, whether brought on by assaults, errors, or a mix of both, might be linked to cybersickness.

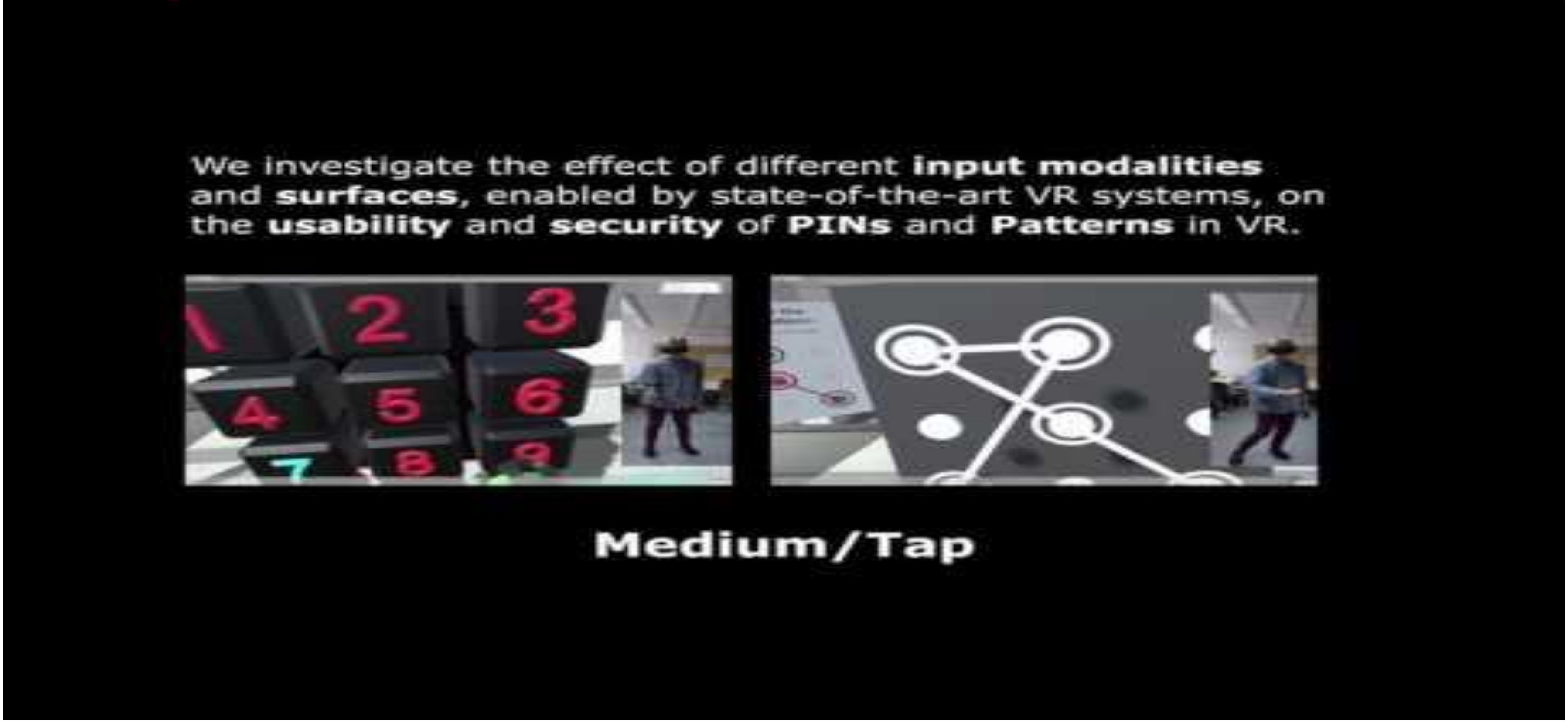
VR Authentication (Traditional Authentication)

- There are a few different ways of authentication when it comes to VRs. One of them being called traditional authentication.
- Traditional authentication includes PINs and swipe patterns.
- RubikAuth: a threedimensional authentication method, consisting in a five-faced cube that exhibits 1 colour and 9 digits per face.
  - For authenticating themselves, the user rotates the cube with the left HHC and selects n digits as their chosen password.



Users can manipulate the cube with natural controller movements and rotations.

Example of Traditional Authentication



We investigate the effect of different **input modalities** and **surfaces**, enabled by state-of-the-art VR systems, on the **usability** and **security** of **PINs** and **Patterns** in VR.

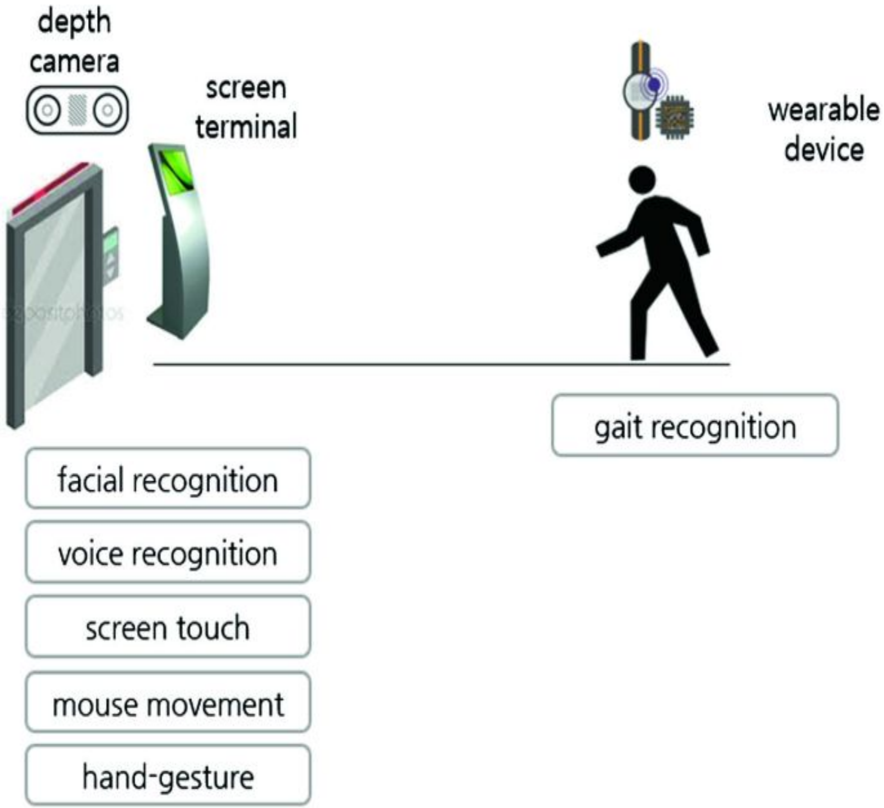
Medium/Tap

Biomechanics-based Authentication

- Some tend to think that traditional authentication methods such as PINs and swipe passwords not only can be stolen by malicious attackers, but they also allow a legitimate user to hand-over control to a third party.
- Body movement can be used for authentication purposes when it is universal, distinctive, repeatable, and collectible. VR sensors can be used to capture movement patterns.
- Head movements, steps, positions of hands and body movement all play a part in biomechanic-based authentication.

Experiments on Biomechanics-based Authentication

- There has been a number of experiments testing out this type of authentication.
- One of the first experiments done recording the headbanging of an individual as a way of authentication.
- From headbanging, trajectory movements were being record and used as authentication until we reached what is referred to as GaitLock.
- GaitLock: Can authenticate users during walking tasks from the on-board inertial measurement units of a Google Glass to protect VR and AR systems.
  - Dynamic-SRC fuses data information from both the HMD accelerometer and the HMD gyroscope reaching an accuracy of 95% based off 5 steps.



Authentication with eye-tracking sensors

- VR authentication with eye-tracking sensors uses not only eye blinking but the rhythmic pattern in the blinks as well as the pupil movement as a way of authentication.
- OcuLock: involves the complete human visual system (HVS), which is made up of several parts, including eyelids and extraocular muscles, that display characteristics that could be used for identification.
- BioMove is a technique for identifying biomechanical behavior patterns and employing them for user authentication. A study demonstrates that while completing controlled tasks like grab, rotate, and drop, 15 users employed their heads, hands, and eyes.
- BlinKey, an authentication method created for virtual reality headsets with eye-tracking technology, attempts to solve the issue by relying exclusively on users' eyes, which are by nature covered when using a VR HMD. BlinKey's central concept is to encode a password as a series of blinks that are executed in a rhythm that is known only to the user.

Other Methods of VR Authentication

- RubikBiom: The application of behavior-based, knowledge-driven authentication in the VR space. Two distinct authentication elements were used in a proof of concept that was created. a password that is only known by the user and the movement patterns that result from entering it in virtual reality.
- In RubikBiom, the password is a 4-digit PIN selected on a 5-faced cube. Each face has a different colour and exhibits 9 digits.
- Man-in-the-room (MITR) attack defenses may also be successful when using multiattribute authentication techniques. Their authentication system's fundamental premise is that real-world objects are defined by a wealth of attributes.

Let’s Play Jeopardy

https://codd.cs.gsu.edu/~jmoralesdeleon1/JeopardyClone-arshad_branch/index.php