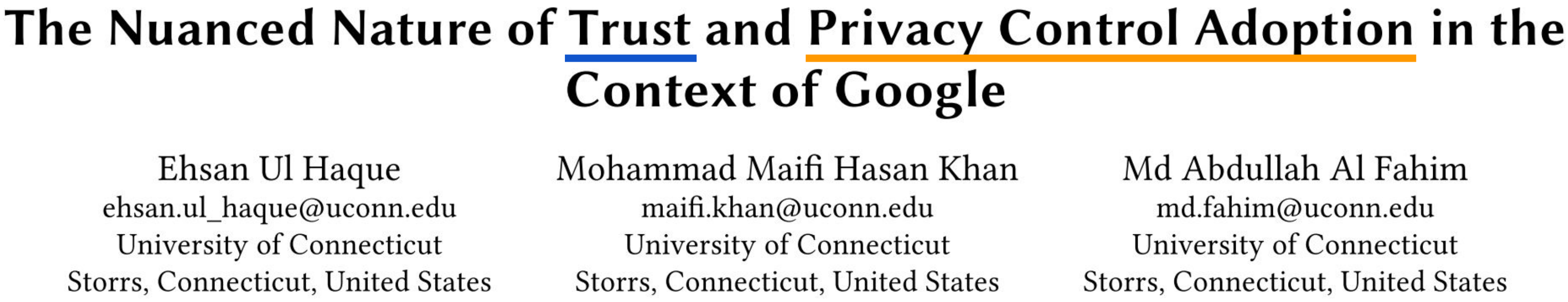
Discussion of Privacy and Security

INF232 Winter 2024
Ismat Jarin, Kenneth Pat, Kyuha Jung



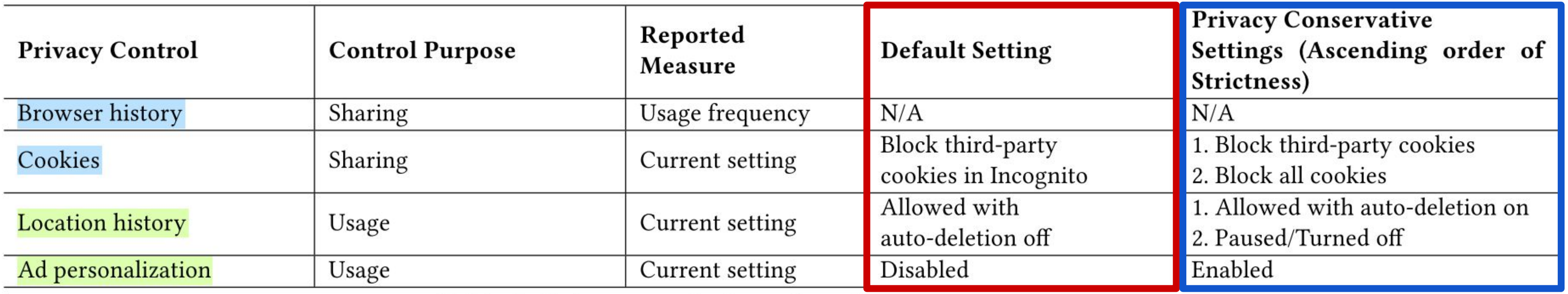
The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google

Ehsan Ul Haque
ehsan.ul_haque@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Mohammad Maifi Hasan Khan
maifi.khan@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Md Abdullah Al Fahim
md.fahim@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Google and the control over
sharing of data and usage of data



Privacy Control	Control Purpose	Reported Measure	Default Setting	Privacy Conservative Settings (Ascending order of Strictness)
Browser history	Sharing	Usage frequency	N/A	N/A
Cookies	Sharing	Current setting	Block third-party cookies in Incognito	1. Block third-party cookies 2. Block all cookies
Location history	Usage	Current setting	Allowed with auto-deletion off	1. Allowed with auto-deletion on 2. Paused/Turned off
Ad personalization	Usage	Current setting	Disabled	Enabled

Table 1: Privacy controls and available choices/options

Q. How do you set your privacy controls?

Survey with Amazon MTurk users (N = 209)

1. Technical literacy: *technical* or *non-technical* user

2. Adoption of privacy controls: *adopter* or *non-adopter*

- *Adopter*: someone who changed the control’s default setting (less or more strictly)
- *Browser history*: calculated by frequency of proactively using the feature
  - “using within a week, within a month, and within three months”

3. Trust towards Google: *competence, benevolence, integrity*

- Competence: “*Google is competent and effective in providing the services I need*”
- Benevolence: “*Google does its best to help me if I need help*”
- Integrity: “*Google is truthful in its dealings with me*”

Finding: Adoption of Privacy Controls

Most participants are likely to **keep the defaults as their current settings** for the chosen privacy controls.

Among the four controls, non-technical participants significantly differ from technical participants in changing the default settings for the **Cookies control only.**

- 42.3% of non-technical users kept the default setting compared to 76.5% of technical users did (non-technical users tend to change the default setting more)

Q. Why do you think there was a difference between non-technical and technical users?

Q. Why a significant difference only in Cookies control?

Finding: Trust Perceptions towards Google

Technical users show **lower trust in integrity and benevolence** of Google than non-technical users.

But **no significant difference for trust in competence.**

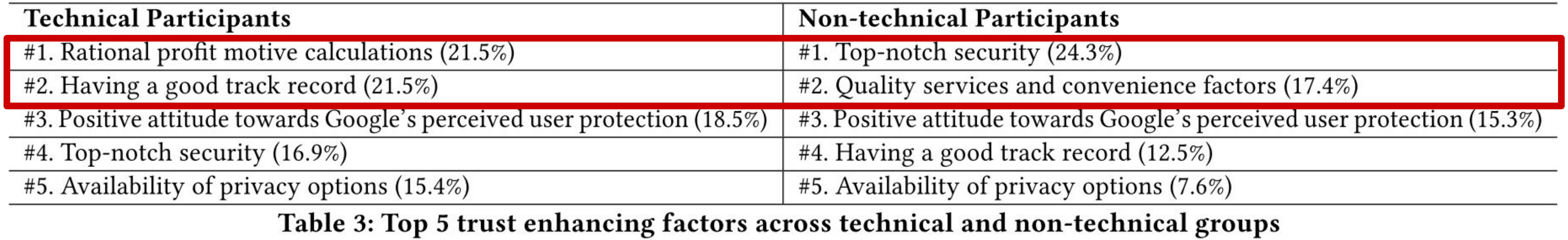
- Competence: "*Google is competent and effective in providing the services I need*"
- Benevolence: "*Google does its best to help me if I need help*"
- Integrity: "*Google is truthful in its dealings with me*"

Q. How would you explain this finding?

Finding: Trust Perceptions towards Google

Trust works as an crucial antecedent for non-technical users' adoption decision of privacy control

- **"sharing" controls:** non-technical adopters pose **higher trust** (integrity and benevolence) towards Google compared to non-technical non-adopters of such controls
- **"usage" controls:** non-technical adopters pose **lower trust** (integrity and benevolence) towards Google compared to non-technical non-adopters of such controls
- For "sharing" controls, adopters indicate **higher trust** (integrity and benevolence) in Google, whereas for "usage" controls, adopters indicate **lower trust** (integrity and benevolence) in Google



Technical Participants	Non-technical Participants
#1. Rational profit motive calculations (21.5%)	#1. Top-notch security (24.3%)
#2. Having a good track record (21.5%)	#2. Quality services and convenience factors (17.4%)
#3. Positive attitude towards Google's perceived user protection (18.5%)	#3. Positive attitude towards Google's perceived user protection (15.3%)
#4. Top-notch security (16.9%)	#4. Having a good track record (12.5%)
#5. Availability of privacy options (15.4%)	#5. Availability of privacy options (7.6%)

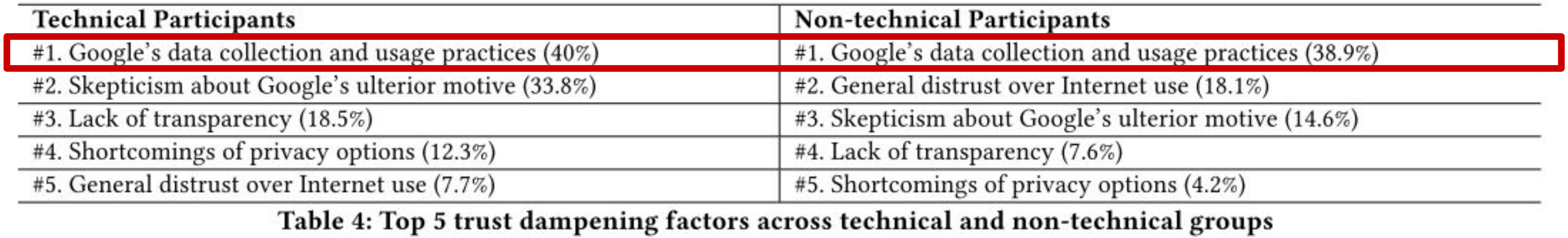
Table 3: Top 5 trust enhancing factors across technical and non-technical groups

*Google's **business model should protect** its users so that it can keep earning profit*

*Google has a pretty **good track record with security** and I've their services for over 10 years and I trust them highly*

*Google is one of the **topmost search-engine** in the world. Google offers high security to our data and protects our data.*

***I search many results in Google Chrome.** I trust this search engine for 90% percent.*



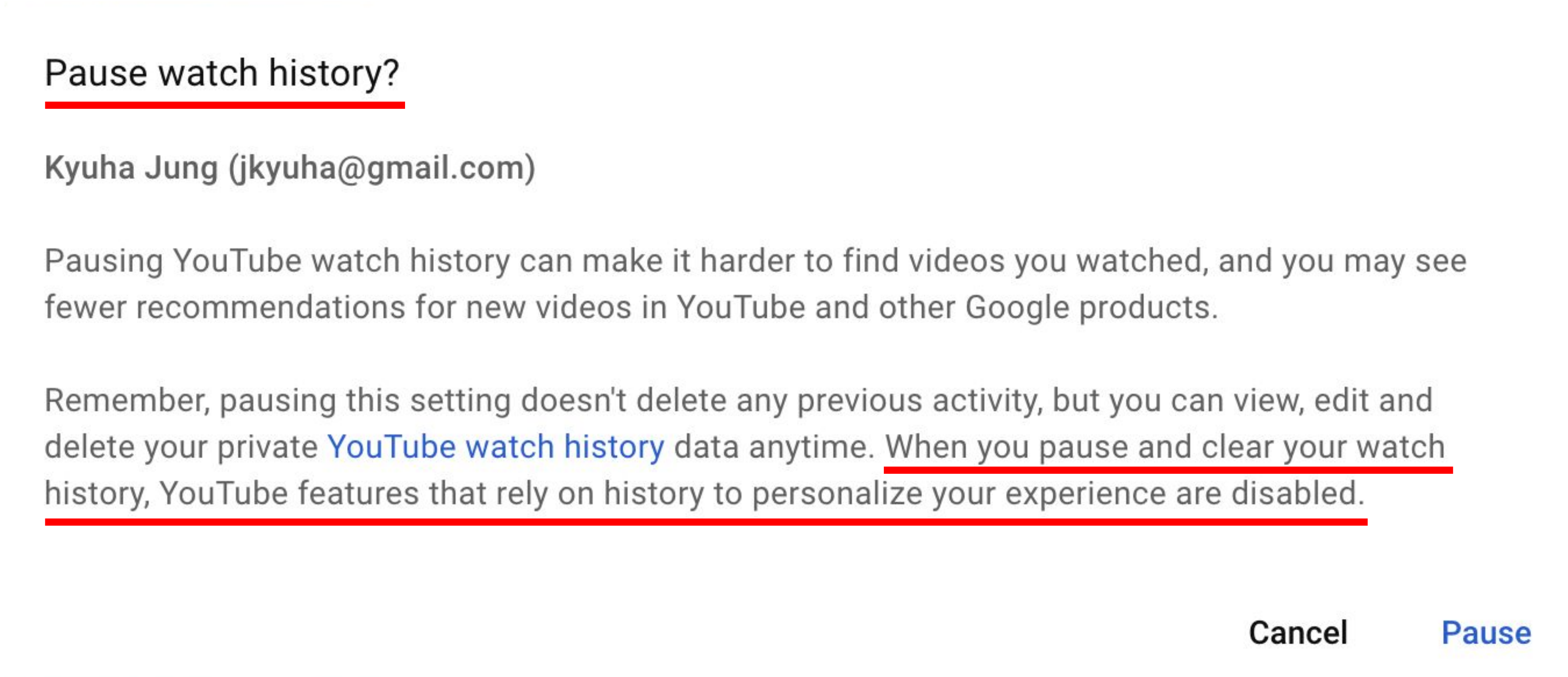
Technical Participants	Non-technical Participants
#1. Google's data collection and usage practices (40%)	#1. Google's data collection and usage practices (38.9%)
#2. Skepticism about Google's ulterior motive (33.8%)	#2. General distrust over Internet use (18.1%)
#3. Lack of transparency (18.5%)	#3. Skepticism about Google's ulterior motive (14.6%)
#4. Shortcomings of privacy options (12.3%)	#4. Lack of transparency (7.6%)
#5. General distrust over Internet use (7.7%)	#5. Shortcomings of privacy options (4.2%)

Table 4: Top 5 trust dampening factors across technical and non-technical groups

*"**I don't trust Google at all.** I am sure it stores and shares data that I have given them either willingly or without knowing."*

*"**Tracks what websites I visit and targets ads to me.** Sells or shares information with other companies and advertisers. "*

Dark patterns of privacy controls

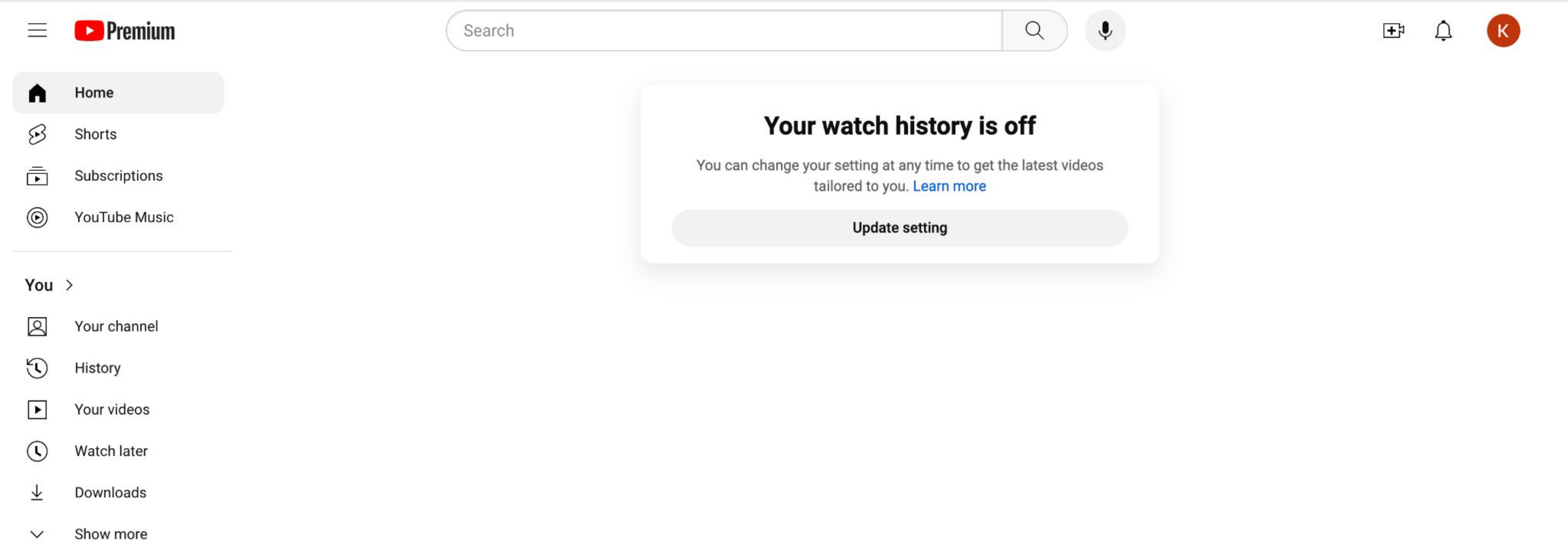


Pause watch history?

Kyuha Jung (jkyuha@gmail.com)

Pausing YouTube watch history can make it harder to find videos you watched, and you may see fewer recommendations for new videos in YouTube and other Google products.

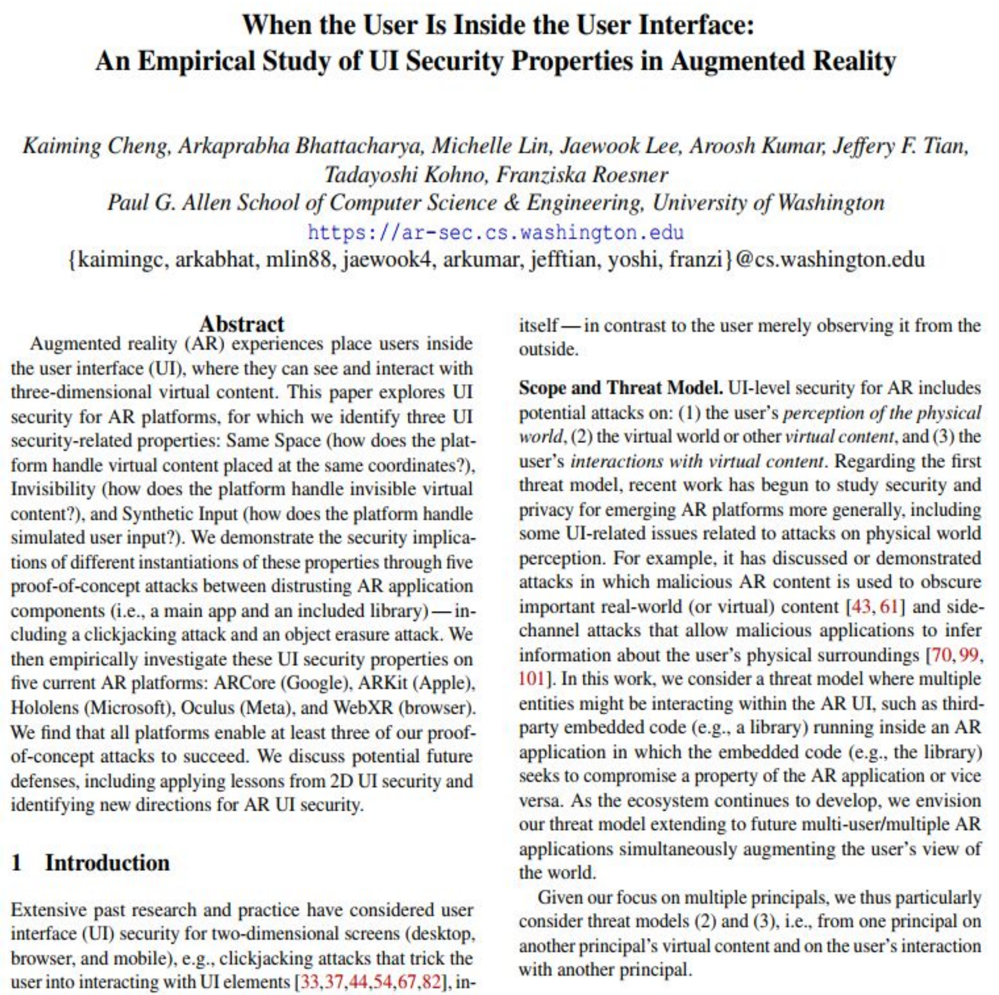
Remember, pausing this setting doesn't delete any previous activity, but you can view, edit and delete your private YouTube watch history data anytime. When you pause and clear your watch history, YouTube features that rely on history to personalize your experience are disabled.



Your watch history is off

You can change your setting at any time to get the latest videos tailored to you. Learn more

Update setting



When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality

Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F. Tian, Tadayoshi Kohno, Franziska Roesner
Paul G. Allen School of Computer Science & Engineering, University of Washington
https://ar-sec.cs.washington.edu
{kaimingc, arkabhat, mlin88, jaewook4, arkumar, jefftian, yoshi, franzi}@cs.washington.edu

Abstract

Augmented reality (AR) experiences place users inside the user interface (UI), where they can see and interact with three-dimensional virtual content. This paper explores UI security for AR platforms, for which we identify three UI security-related properties: Same Space (how does the platform handle virtual content placed at the same coordinates?), Invisibility (how does the platform handle invisible virtual content?), and Synthetic Input (how does the platform handle simulated user input?). We demonstrate the security implications of different instantiations of these properties through five proof-of-concept attacks between distrusting AR application components (i.e., a main app and an included library) — including a clickjacking attack and an object erasure attack. We then empirically investigate these UI security properties on five current AR platforms: ARCore (Google), ARKit (Apple), Hololens (Microsoft), Oculus (Meta), and WebXR (browser). We find that all platforms enable at least three of our proof-of-concept attacks to succeed. We discuss potential future defenses, including applying lessons from 2D UI security and identifying new directions for AR UI security.

1 Introduction

Extensive past research and practice have considered user interface (UI) security for two-dimensional screens (desktop, browser, and mobile), e.g., clickjacking attacks that trick the user into interacting with UI elements [33,37,44,54,67,82], in-itself — in contrast to the user merely observing it from the outside.

Scope and Threat Model. UI-level security for AR includes potential attacks on: (1) the user's *perception of the physical world*, (2) the virtual world or other *virtual content*, and (3) the user's *interactions with virtual content*. Regarding the first threat model, recent work has begun to study security and privacy for emerging AR platforms more generally, including some UI-related issues related to attacks on physical world perception. For example, it has discussed or demonstrated attacks in which malicious AR content is used to obscure important real-world (or virtual) content [43, 61] and side-channel attacks that allow malicious applications to infer information about the user's physical surroundings [70, 99, 101]. In this work, we consider a threat model where multiple entities might be interacting within the AR UI, such as third-party embedded code (e.g., a library) running inside an AR application in which the embedded code (e.g., the library) seeks to compromise a property of the AR application or vice versa. As the ecosystem continues to develop, we envision our threat model extending to future multi-user/multiple AR applications simultaneously augmenting the user's view of the world.

Given our focus on multiple principals, we thus particularly consider threat models (2) and (3), i.e., from one principal on another principal's virtual content and on the user's interaction with another principal.

⚠ The AR Technology is here! But are we ready?

Overview

Gray Zone

- What are the relationships between Users, User-Interface & the environment?
- Is AR ready? Privacy-wise, Security-wise & Safety-wise?

?

How User-Object Interactions Happen in these scenarios?

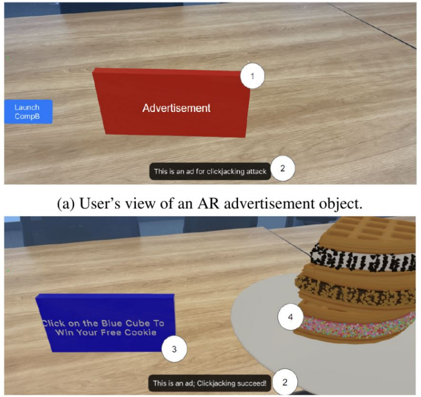
1. Same Space
2. Transparent Object
3. Synthetic Input

Let's Link Together:

- If two objects are same size and take same space, which object the users will interact 1st?(results: interaction without knowledge clickjacking)
- Can invisible objects take users input? (results: Invisible object can place between user & desired object -disable user interaction)
- Is there any difference in real or fake users input? (result: overwrite real users input)

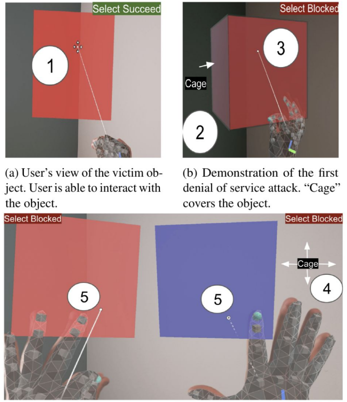
Examples: Plausible Security Attacks in AR-UI

- **ClickJacking:** Tricking Users to interact with Malicious Object
- **DOS:** Block Users from Interacting with VO
- **Input Forgery:** Deceptive User Interaction


1
Launch CompB
Advertisement
This is an ad for clickjacking attack
2
Click on the Blue Cube To Win Your Free Cookie
3
4
This is an ad; Clickjacking succeed!
2

(a) User's view of an AR advertisement object.

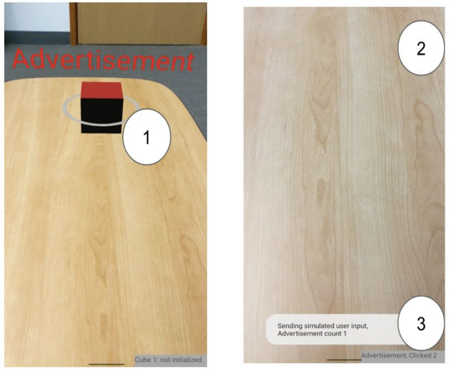
(b) Demonstration of the clickjacking attack



(a) User's view of the victim object. User is able to interact with the object.

(b) Demonstration of the first denial of service attack. "Cage" covers the object.

(c) Demonstration of the second denial of service attack. "Cage" covers the entire space.



(a) User's view of the victim app.

(b) Demonstration of the input forgery attack

Why This Study is Important?

“Click to advertisement that you don’t wanna see”

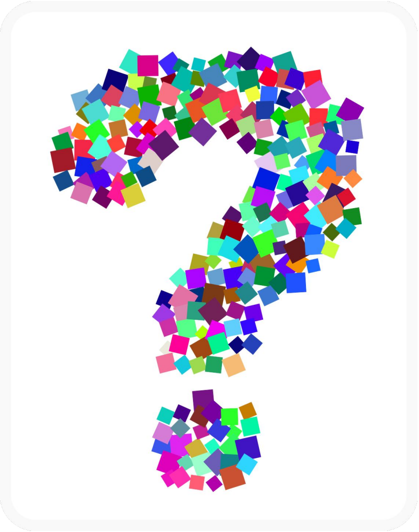
“Without Clicking any link, a violent video may appear!”

“Try to join a virtual meeting, can not join”

Imagine Everything is Happening in 3D around you-Not 2D Computer Screen!

So We need Solutions: Identify the Attacks and Countermeasures (Defense) against them!

What are the main findings of this study you think important for future AR/VR technology?



Contribution

Research Contribution wrt HCI?

‘Empirical’

- AR UI Property having Security Implications
- Identify Probable Security attacks inside AR UI-> Threat to Users
- Empirical Study on Commercial AR Platforms - Practical Use Cases (ex. Hololens, Oculus)
- Countermeasures/Defense

Research Scope of this Paper

Within HCI

- Augmented Reality
User Interface -AR UI
- AR UI Security Issues/Attacks
- Privacy/Defense for AR UI
- User-Object Interaction in AR

OutSide HCI

- AR Technologies/Devices
- Computer Graphics/ 3D Modeling/Virtual Objects
- Security Attacks (i.e clickjacking, DoS)

The End