# CSE 484 / CSE M 584: Emerging Technologies

Fall 2024

Franziska (Franzi) Roesner
franzi@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

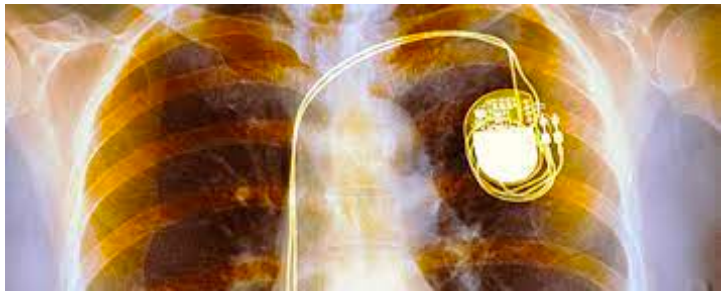
# Announcements

- Final **project Part A due** tomorrow @ 11:59pm (late days ok)
- Parts B+C due December 10 (no late days)

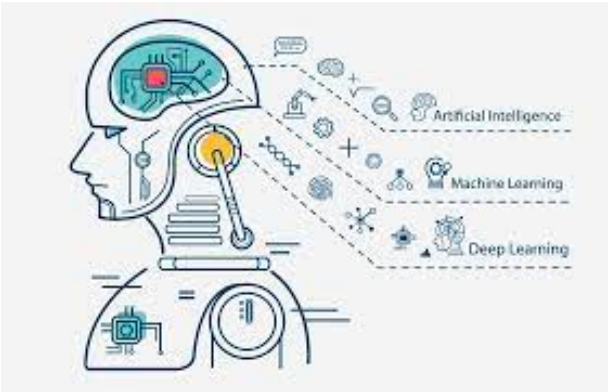
- Wednesday: physical security
  - **Not recorded, only some slides posted**

- **No section this week! Extended office hours in section rooms ☺**

- One last chance for an extra credit reading (due Thursday)



# SECURITY AND PRIVACY FOR EMERGING TECHNOLOGIES



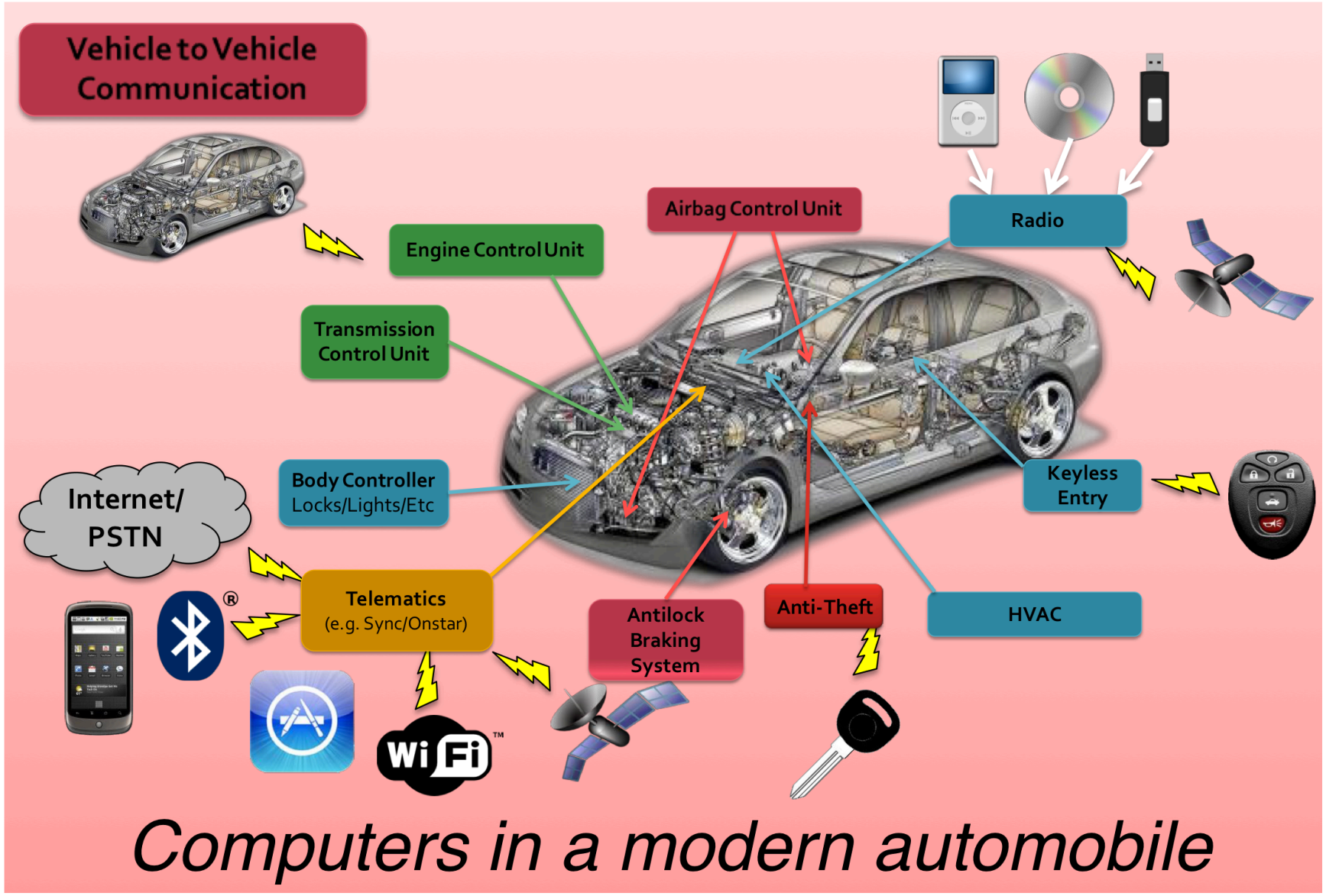


# (1) Connected Automobiles

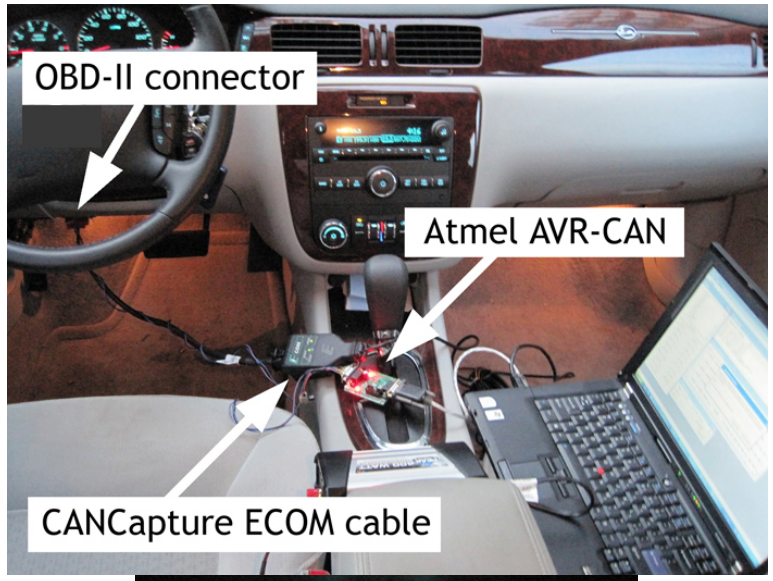
- Already "emerged" by now, but a fun story ☺

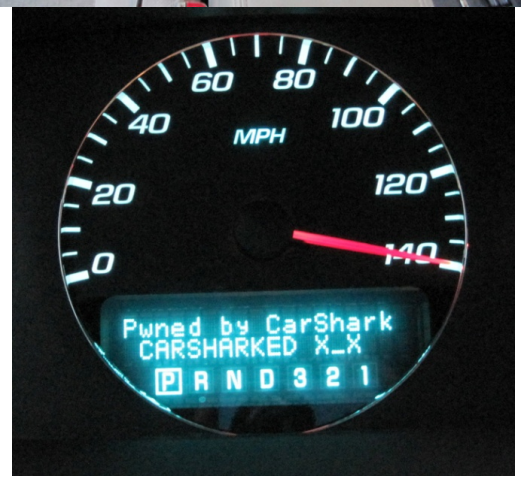
- Automobiles were only just being connected to the internet when we (UW+UCSD) studied them (~2009)
  - Had not faced significant adversarial pressure
  - Won a "Test of Time" Award in 2020

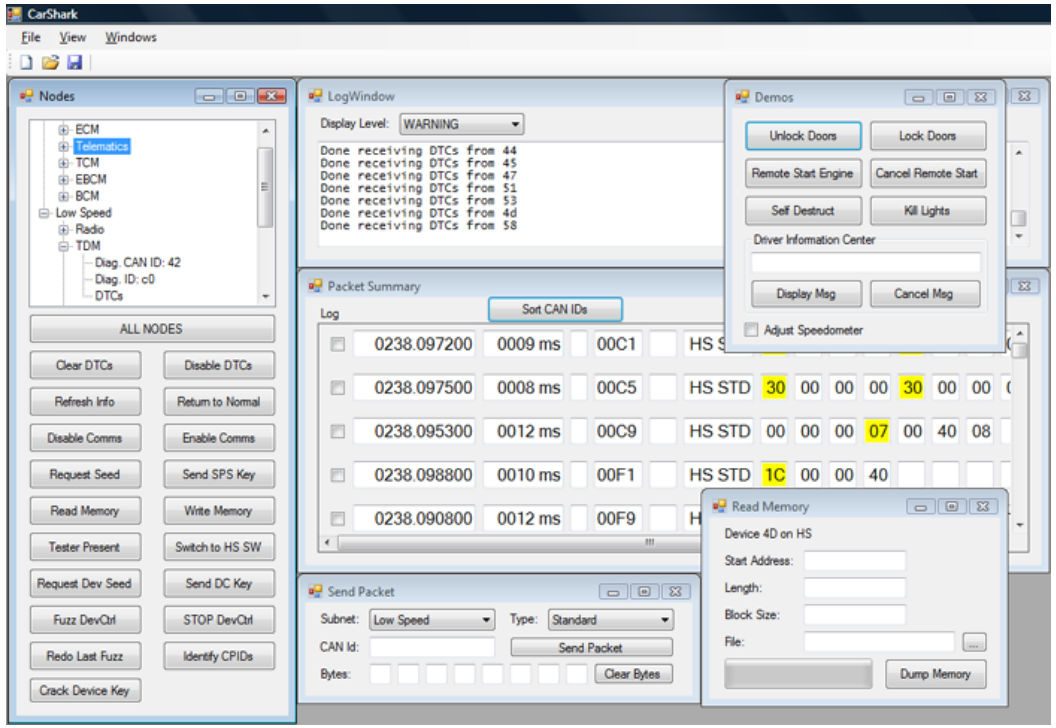
www.autosec.org


Vehicle to Vehicle Communication
Engine Control Unit
Airbag Control Unit
Radio
Transmission Control Unit
Body Controller Locks/Lights/Etc
Keyless Entry
Internet/ PSTN
Telematics (e.g. Sync/Onstar)
Antilock Braking System
Anti-Theft
HVAC
Wi Fi
Computers in a modern automobile

# Experiments with a Real Car



# Experiments with a Real Car

# Example: Force Brakes On/Off


https://www.youtube.com/watch?v=H6o0zuid1K4


https://www.youtube.com/watch?v=917VOx6tBKA

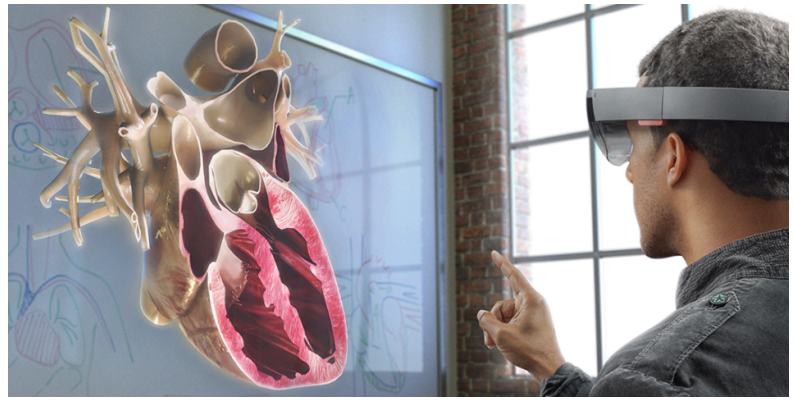
# Impacts

- Impact on automotive industry
  - Significant investment by automotive companies
  - Spurred vendor industry around automotive security
- Impact on standards, regulation, and legislation
  - SAE International (de facto standards body for the U.S. automotive industry) created committee and standards
  - Resources committed by NHTSA
  - U.S. bills on automotive cybersecurity
- Impact on research
  - New subfield of automotive security and significant DARPA and other funding efforts

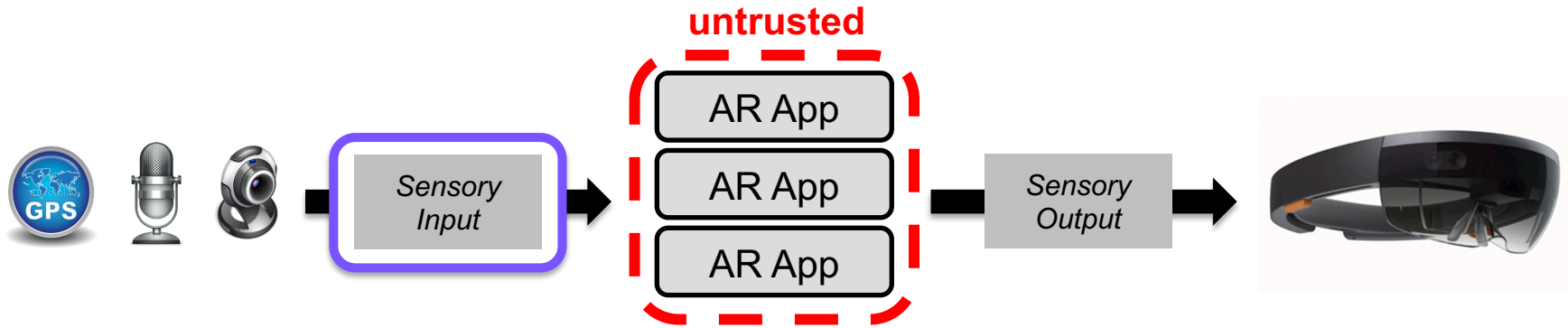
# (2) Security and Privacy for Augmented Reality







# AR Input Privacy

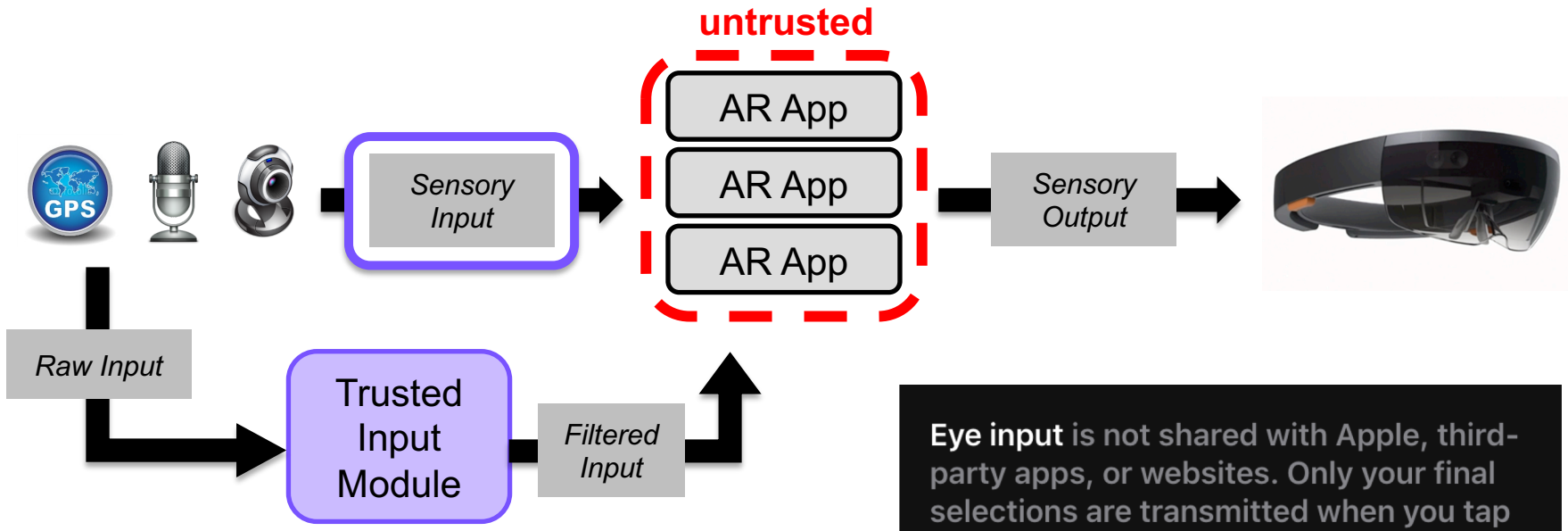



**Seattle dive bar becomes first to ban Google Glasses over privacy fears**

By NINA GOLGOWSKI

**PUBLISHED:** 00:43 EST, 10 March 2013 | **UPDATED:** 02:16 EST, 10 March 2013

# AR Input Privacy




**Input Privacy**

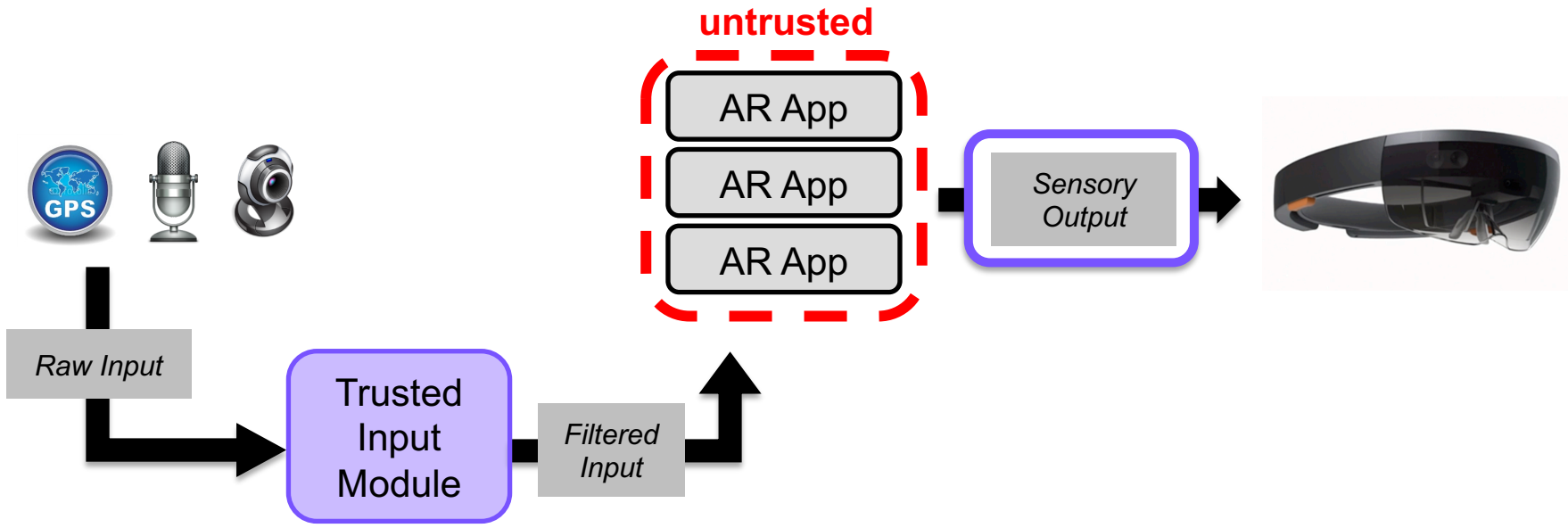
- Jana et al., USENIX Security '13
- T. Denning et al., CHI 2014
- Roesner et al., CCS '14
- Templeman et al., NDSS '14
- Raval et al., MobiSys '16

**Eye input** is not shared with Apple, third-party apps, or websites. Only your final selections are transmitted when you tap your fingers together.

Data from **cameras and sensors** is processed at the system level, so individual apps do not need to see your surroundings to enable spatial experiences.

https://www.apple.com/apple-vision-pro/

# AR Output Security

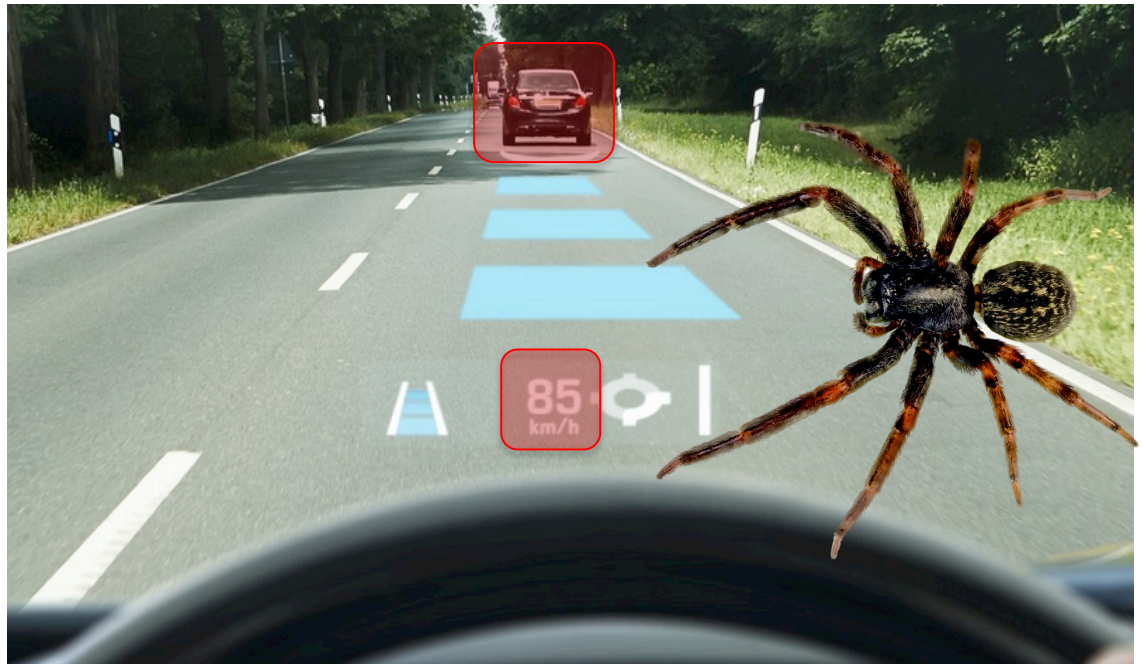



Hyper Reality (https://www.youtube.com/watch?v=YJg02ivYzSs)

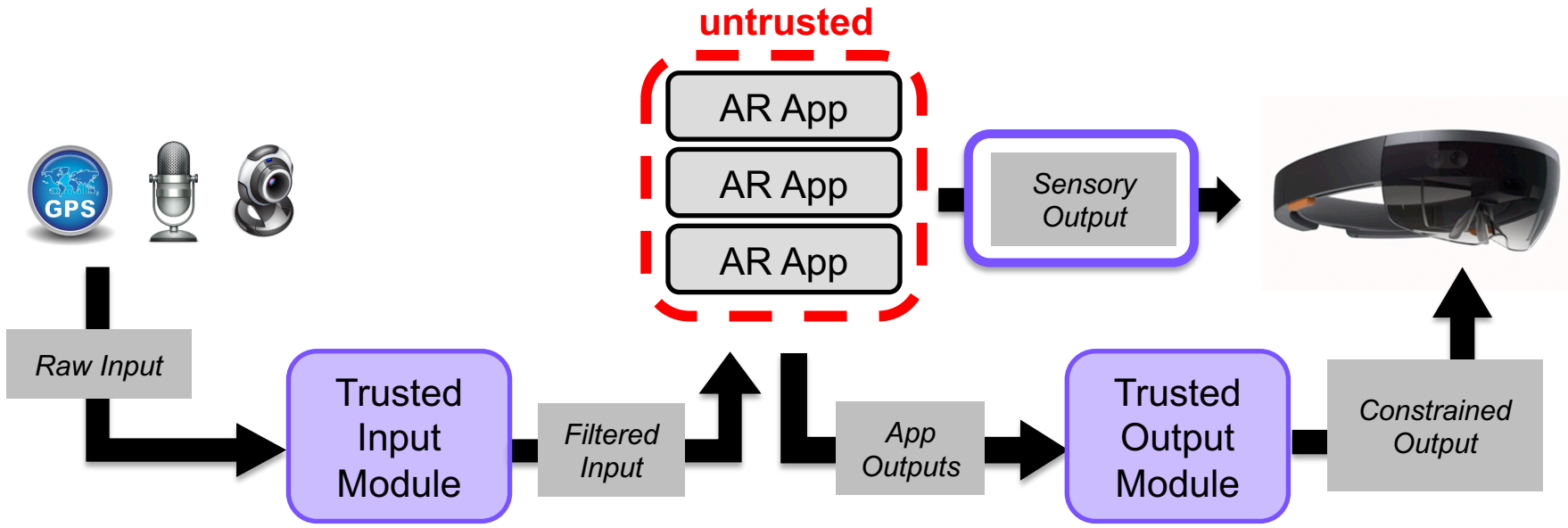
# AR Output Security

A buggy or malicious app might…

- **Obscure another app's virtual content** to hide or modify its meaning
- **Obscure important real-world content,** such as traffic signs or cars
- **Disrupt the user physiologically,** such as by startling them



# AR Output Security




**Output Security**

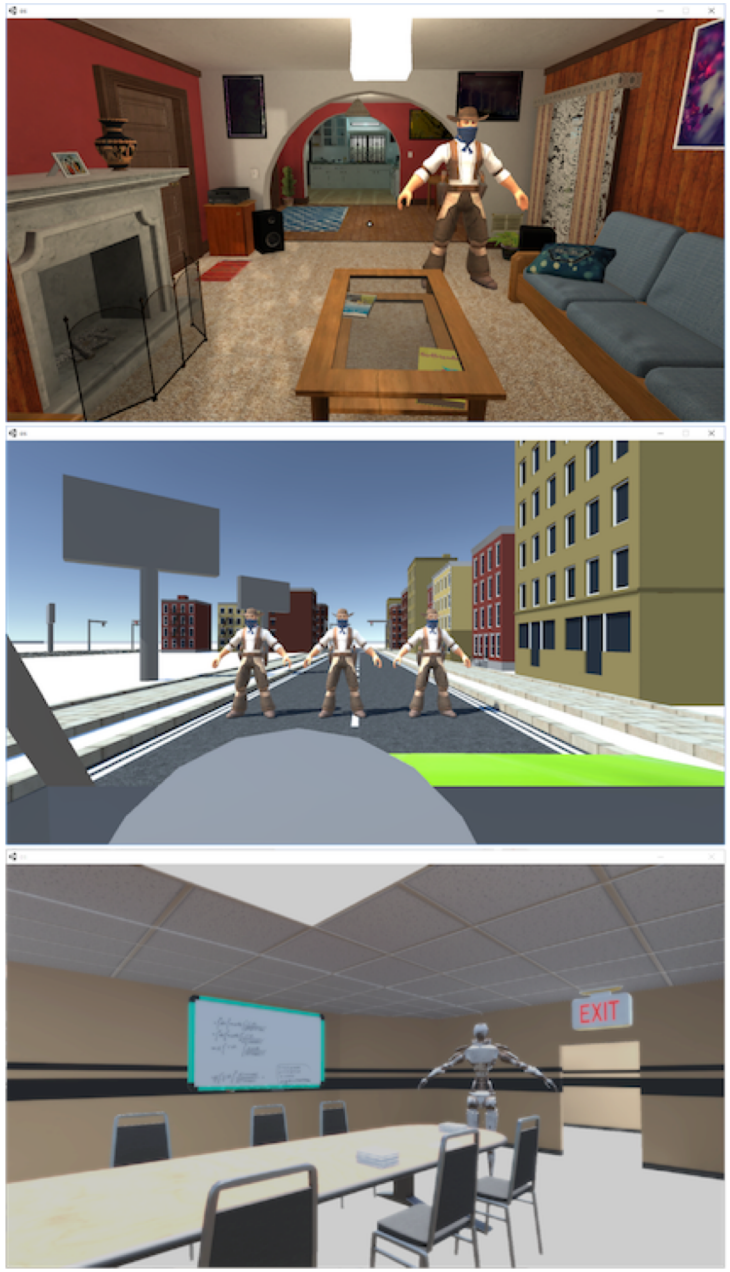
- Lebeck et al., HotMobile '16
- Lebeck et al., IEEE S&P '17
- Ahn et al., VR/AR Network '18
- Lebeck et al., HotMobile '19

# Arya: Securing AR Output

K. Lebeck, K. Ruth, T. Kohno, F. Roesner. "Securing Augmented Reality Output." IEEE Symposium on Security and Privacy 2017.

Key insight: Existing display abstraction (windowing model) doesn't work for AR.

"Real world"




"Real world" in our AR simulator

”Real world”

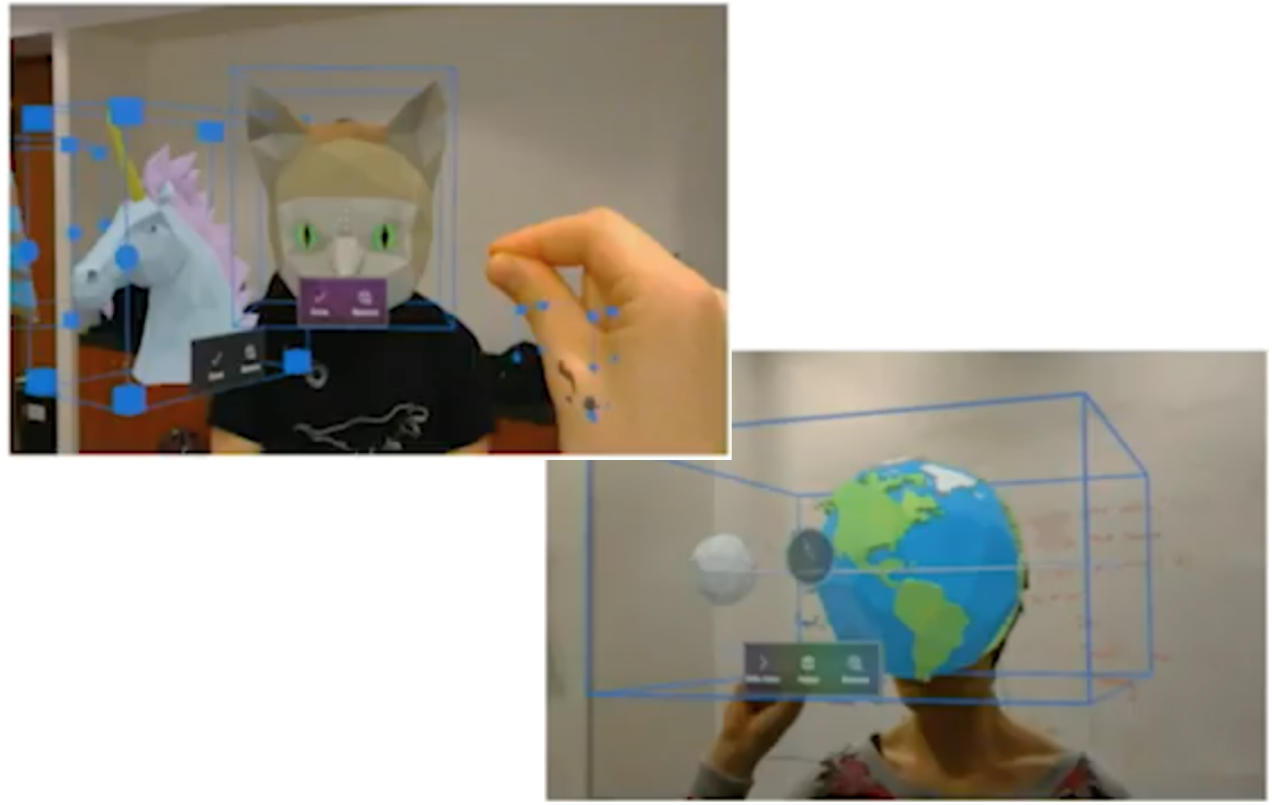
Buggy or malicious apps


Buggy or malicious apps


OS enforces output policies

# Challenge: Multiple Users

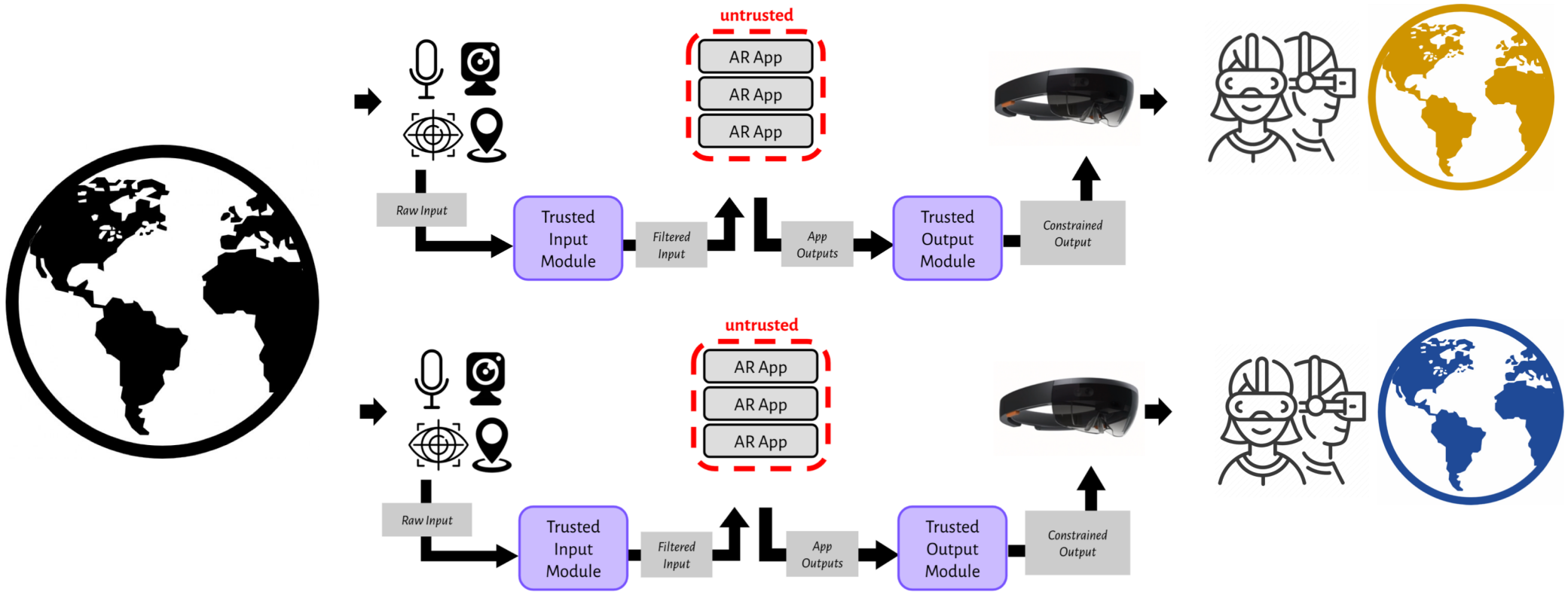
Study with pairs of participants and 2 Hololenses





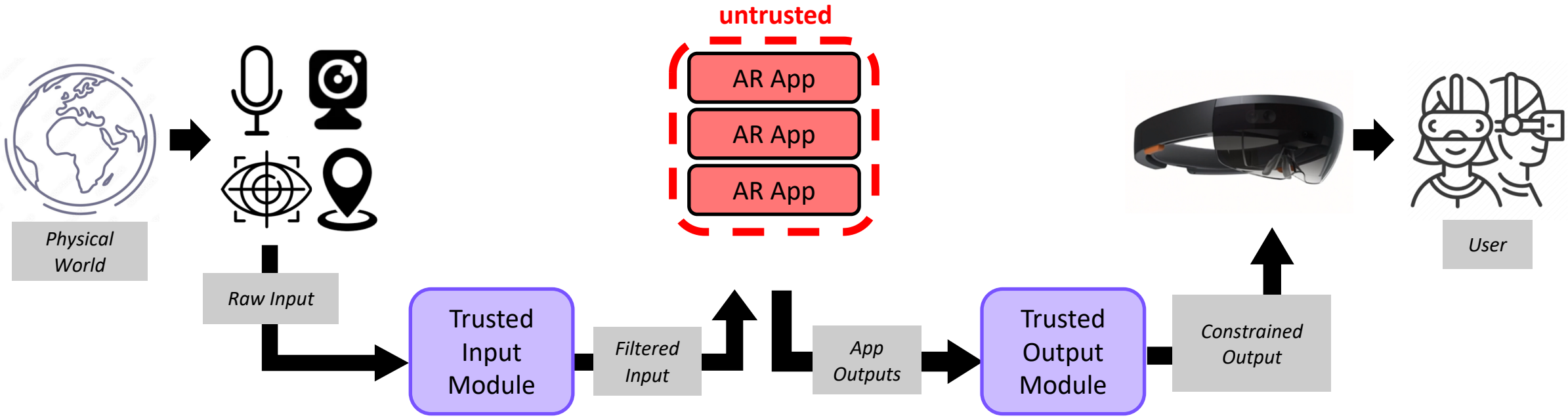
K. Lebeck et al., IEEE S&P (Oakland) 2018

# Challenge: Multiple Users




I. Sluganovic et al., ACSAC 2017
K. Lebeck et al., IEEE S&P (Oakland) 2018
K. Ruth et al, USENIX Security 2019

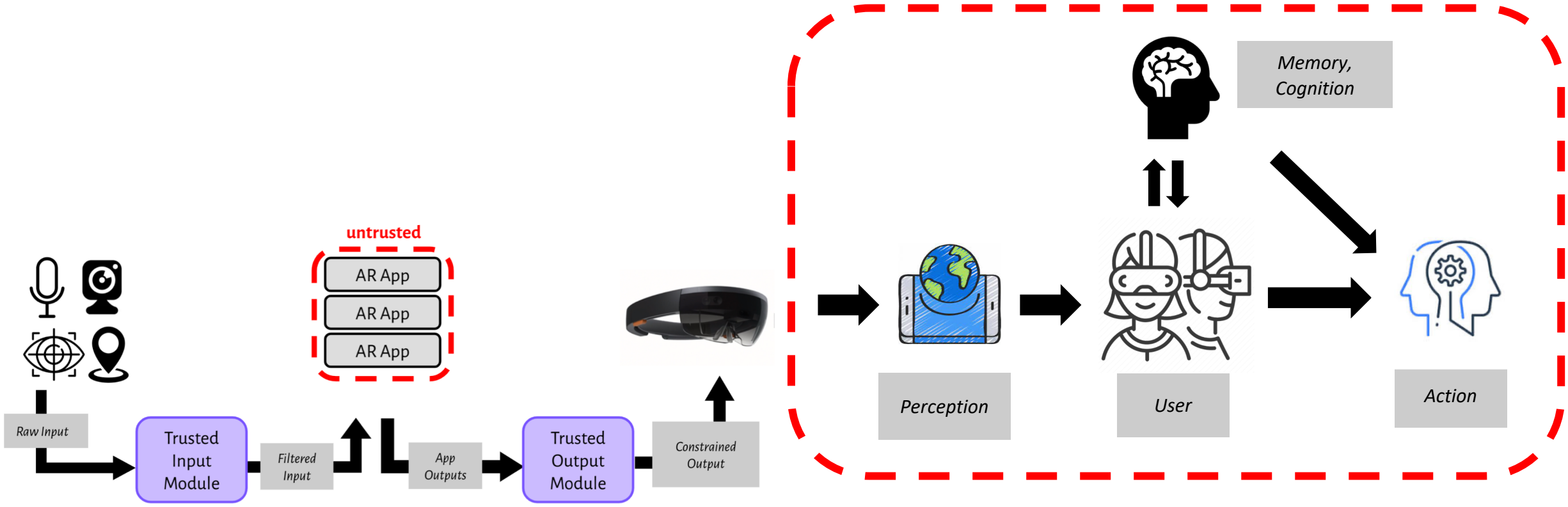
# Challenge: Multiple Apps






K. Lebeck et al, HotMobile 2019

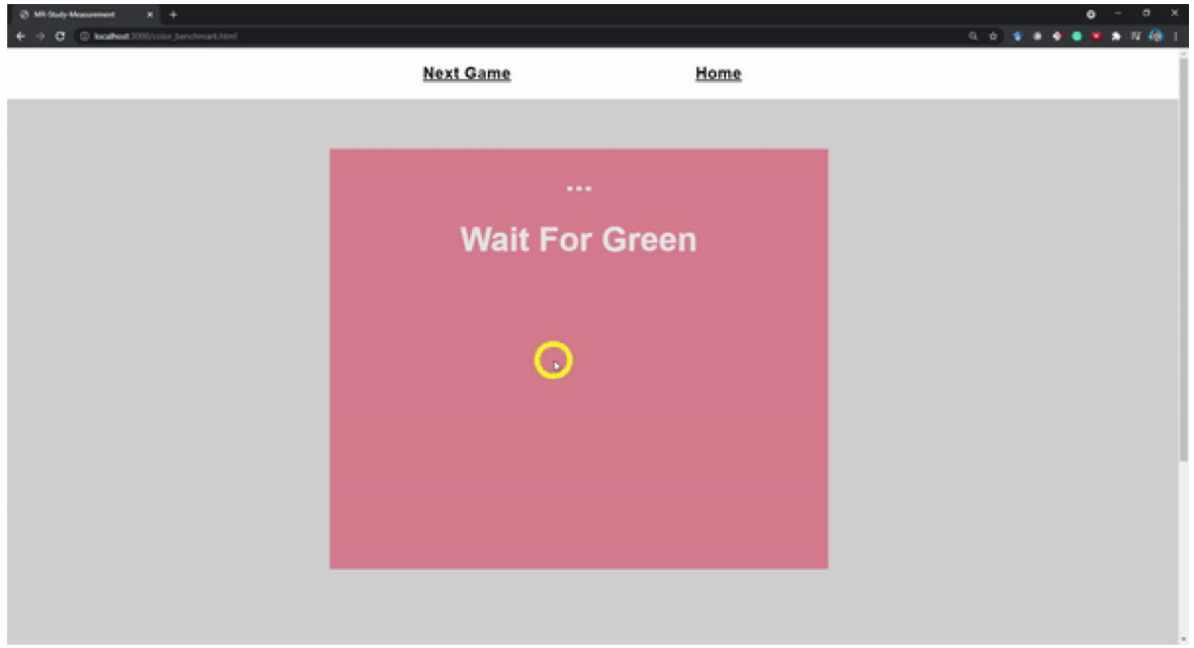
# Challenge: Human Brain as the Attack Surface




S. Baldassi et al, arXiv:1806.10557, 2018
P. Casey et al., IEEE Transactions on Dependable and Secure Computing 2019
J. R. Gordon et al., CHI 2021
W. Tseng et al., CHI 2022
Cheng et al., USENIX Security 2023

# Perceptual Manipulation Attack (PMA)

Can AR-based attacks be effective on users in practice, and how do people react?



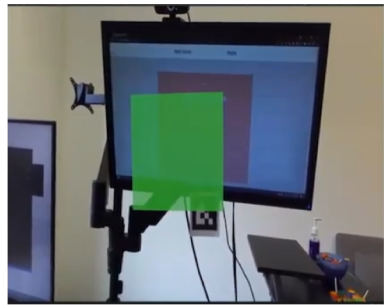



Cheng et al., USENIX Security 2023

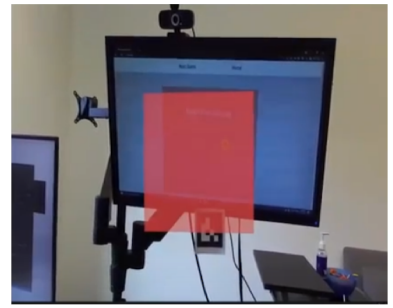
# Perceptual Manipulation Attacks (PMA)

**Example Visual PMA:**

Induce an incorrect reaction

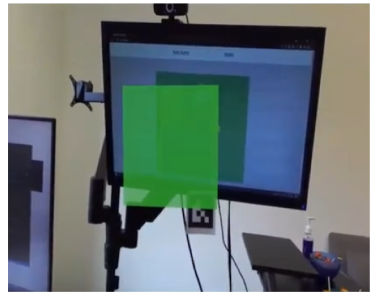


**FalseGreen Attack**

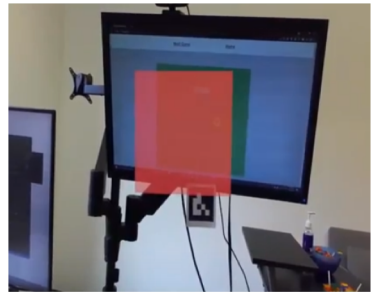


**DoubleRed Attack**

Delay a correct reaction



**DoubleGreen Attack**

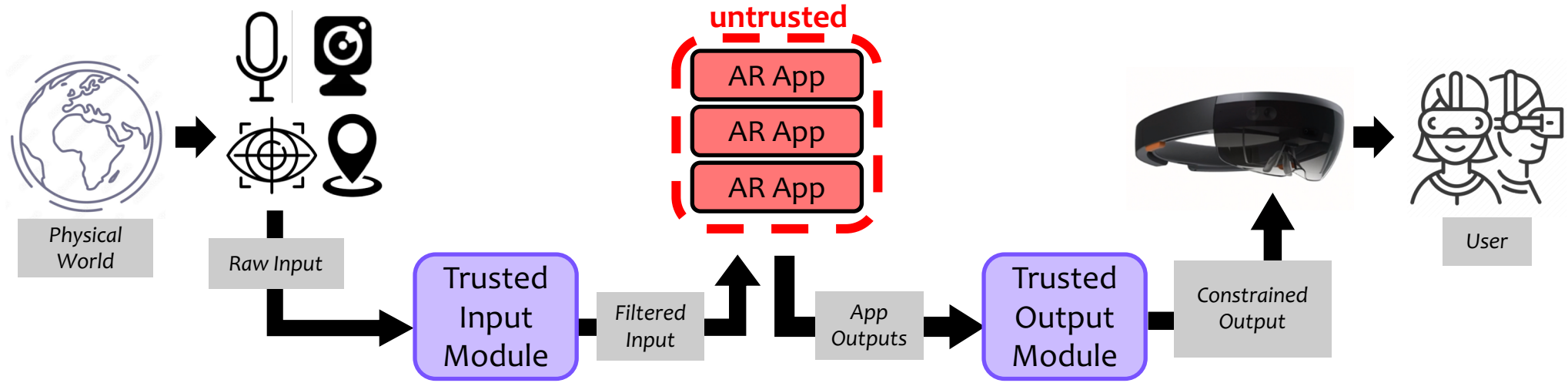


**FalseRed Attack**



Cheng et al., USENIX Security 2023

# Meanwhile: Advancing Platforms and Hardware




Unity

MRTK MIXED REALITY TOOLKIT

AR Foundation

Hololens

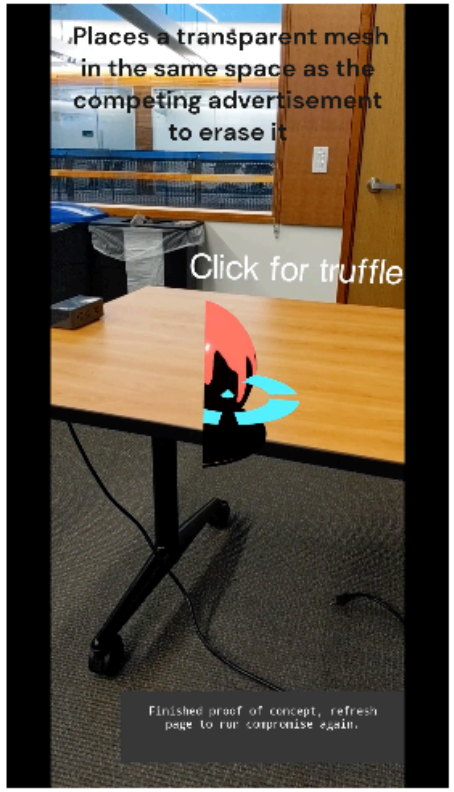
Magic Leap

Oculus

Glass

Snap

# UI-Level Security Example: Erasure Attack




**Implemented on WebXR - Exploited Invisibility Property**

When the user launches the application, it presents two competing third-party ad libraries. Code from one mock ad library then places a transparent mesh in the same space as the competing advertisement to erase it.



https://ar-sec.cs.washington.edu/ar_ui/

# Friday: Emerging Topics 2

- Adversarial machine learning
- Large language models
- Mis/disinformation