# Medusa3D: The Watchful Eye Freezing Illegitimate Users in Virtual Reality Interactions

**Aochen Jiao**\*, Di Duan\*, and Weitao Xu

City University of Hong Kong

MobileHCI 2024 | Melbourne

# Background

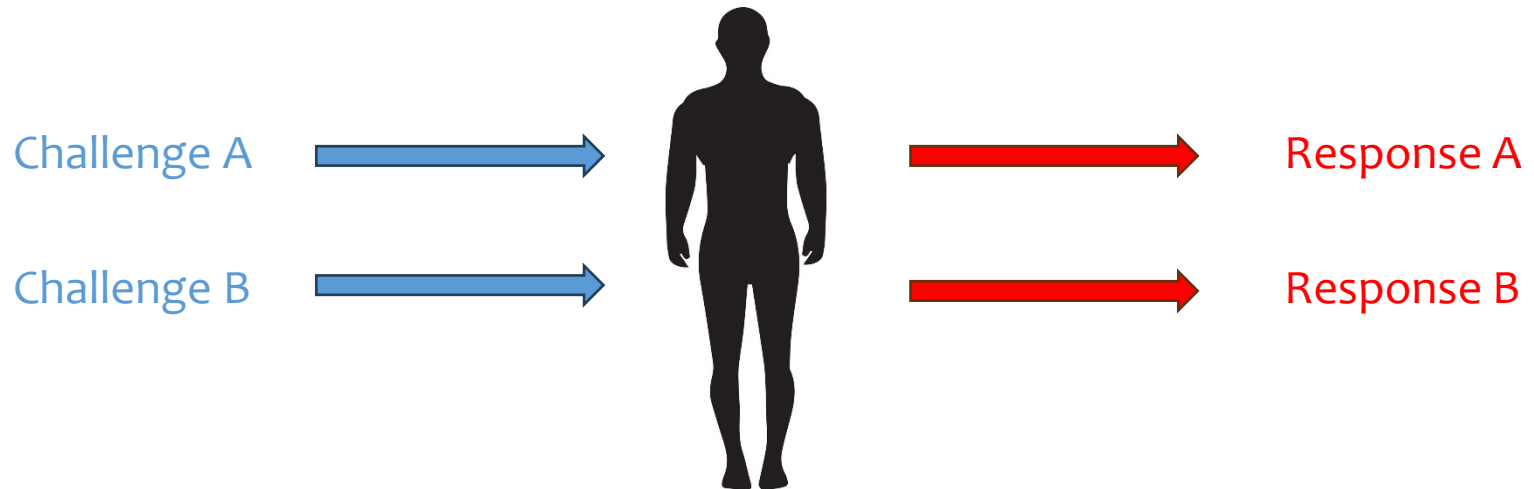## PIN / Password in VR

**Shoulder-surfing Attack**

# Background

**Static Biometric**

Vulnerable to **data leakage** and **replay attack**

Once stolen -> unrecoverable

# Background

## Active Biometric

Challenge A → 🚶 → Response A

Challenge B → → Response B

Response = H (Challenge)

Challenge-Response Method

Biometric is human's response **pattern** to challenge, but not specific challenge or response.

# Motivation

> *Reflexive eye movement is an activity that is driven by visual stimulation but does not require volitional control.*

*- R John Leigh and David S Zee. The neurology of eye movements. Contemporary Neurology*

❖ **VR headsets that already include integrated eye tracker**

| Primax Crystal | PlayStation VR2 | HP Reverb G2 | Pico Neo 3 Pro Eye | HTC Vive Pro Eye |

❖ **Can we use reflexive eye responses as biometric?**
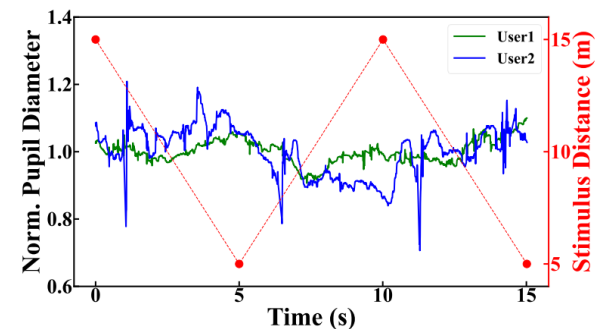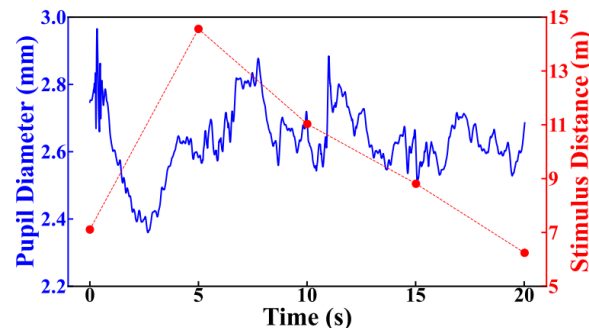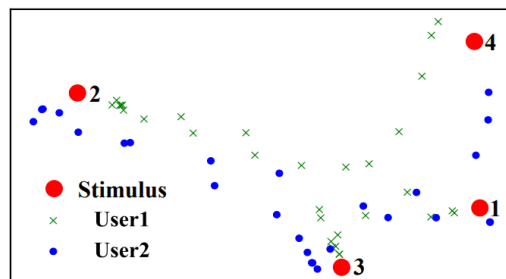
# Preliminary Study

❖ **What eye responses are reflexive?**
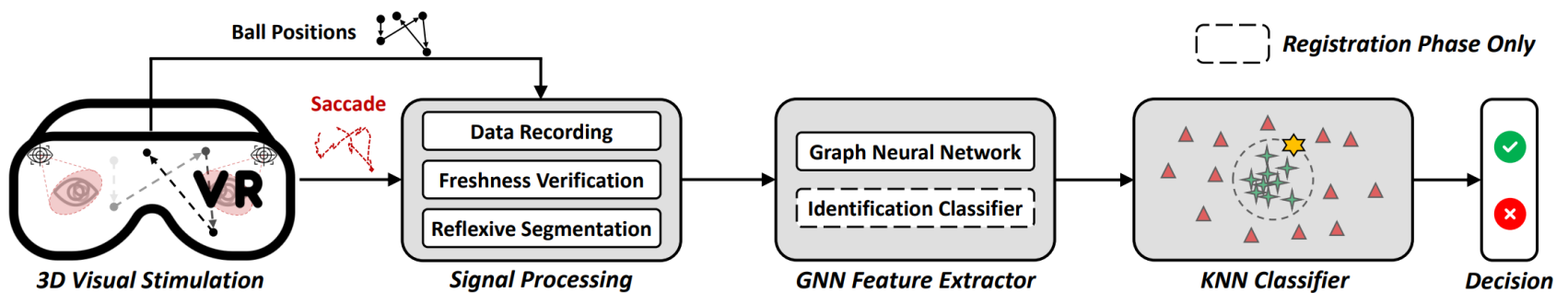
- Reflexive saccade

- Pupil diameter change

❖ **How to elicit the reflexive responses?**

- When a noticeable change occurs in the field of view

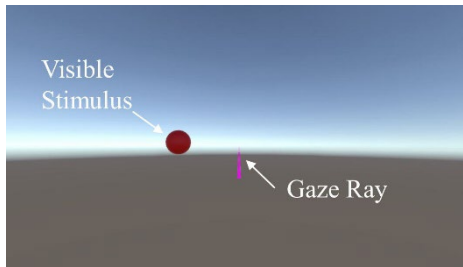- When focused object changes its depth

❖ **Overview**

- Visual stimulation

- Signal processing

- Feature extraction & Authentication
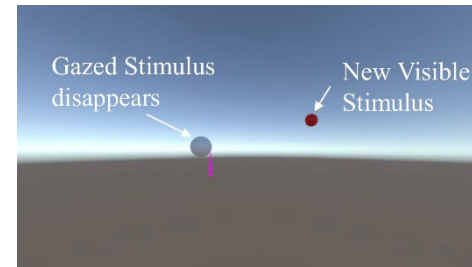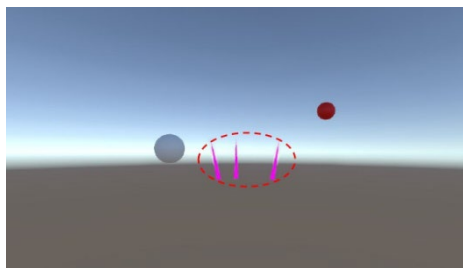
# System Design

❖ **Visual Stimulation Design**

- **Salient change:** *elicit reflexive saccades.*
- **Variable depth:** *elicit pupil diameter changes.*
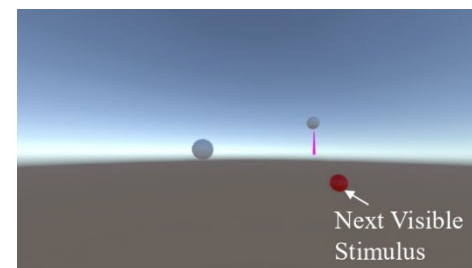- **Unpredictability:** *exclude the interference from memory.*
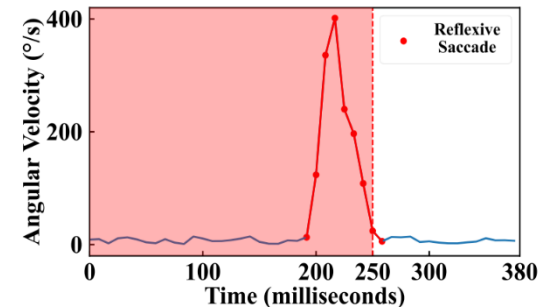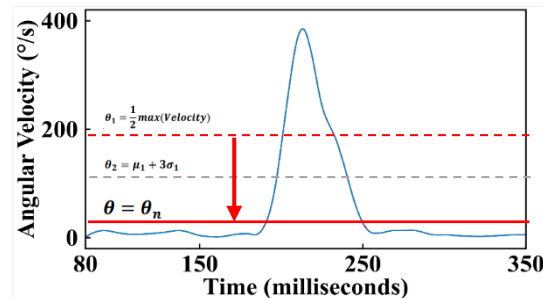


(a) Stim. appears in FOV



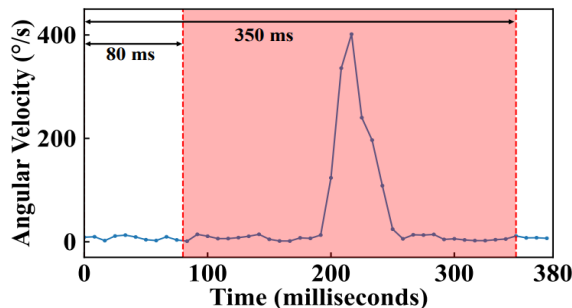(b) Gaze intersects stim.



(c) Saccades catch stim.



(d) New stim. is gazed.

❖ **Signal Processing**

- Reflexive saccades segmentation

    o *Determine the time interval reflexive saccades may occur.*

    o *Employ iteration method to adaptively search the threshold.*

    o *Verify the reflexivity of saccades extracted.*

# System Design

❖ **Feature Extraction & Authentication**

- Graph design
  - *We embed the spatial information of reflexive saccades into a graph.*

- GNN network design
  - *We design a graph-oriented network that can classify the users' feature*

- KNN classifier
  - *With the feature extracted, a user-specific KNN model is selected that can package legitimate user samples.*
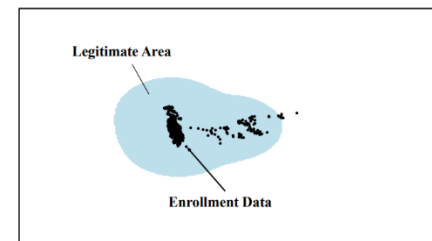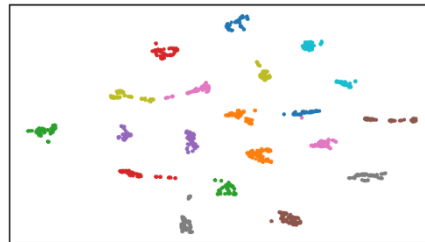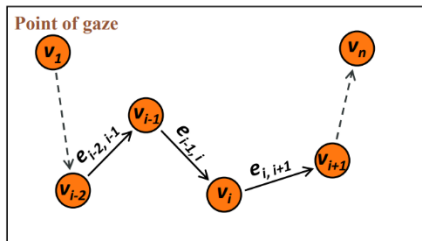
# Evaluation

## ❖ Set-up

- Device:
  - ○ *HTC VIVE Pro Eye*

- Threat model:
  - ○ *Zero-effort attack*
  - ○ *Replay attack*
  - ○ *Mimicry attack*



- Participants:
  - ○ *25 (20 users + 5 attackers)*
  - ○ *Various in demography and background*

- Evaluation metrics:
  - ○ *FAR: False Acceptance Rate*
  - ○ *FRR: False Reject Rate*

## ❖ Overall Performance

- Overall 0.21% FAR and 0.13% FRR
- Time required for authentication is about 5 s.

| Scheme | FAR (%) | FRR (%) | Authentication time(s) |
|---|---|---|---|
| OcuLock [1] | 3.55 | 3.55 | ≤10 |
| SkullConduct [2] | 6.90 | 6.90 | ≤23 |
| Brain Password [3] | 2.50 | 2.50 | ≈4.80 |
| ElectricAuth [4] | 0.83 | 2.00 | ≈1.30 |
| SoundLock [5] | 0.76 | 0.91 | ≤7 |
| VibHead [6] | ≈5 | ≈5 | ≤1 |
| **Medusa3D** | 0.21 | 0.13 | ≈5 |

[1] Luo et al. 2020. OcuLock. NDSS 2020.
[2] Schneegass et al. 2016. SkullConduct. CHI 2016.
[3] Lin et al. 2018. Brain Password. MobiSys 2018.
[4] Chen et al. 2021. ElectricAuth. CHI 2021.
[5] Zhu et al. 2023. SoundLock. NDSS 2023.
[6] Li et al. 2024. Vibhead. TOSN 2024.

# Evaluation
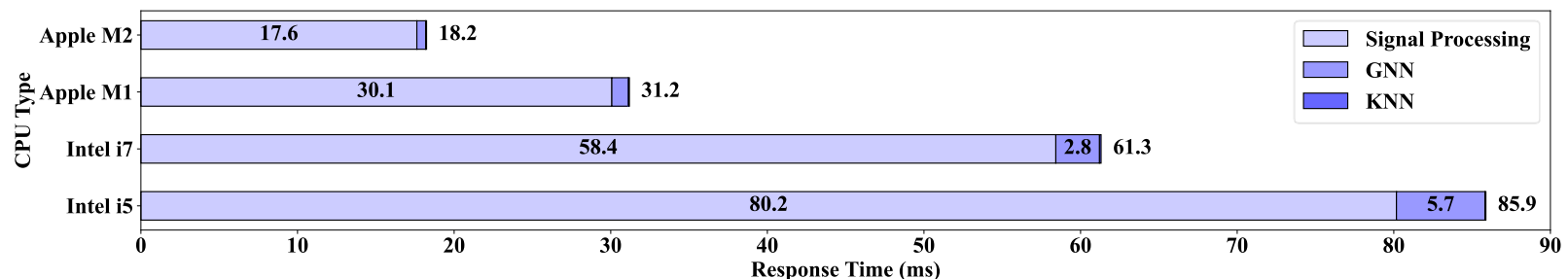
❖ **Zero-effort attack**

- Attackers attempt to unlock the device with their own biometrics as credentials
- FAR ~ 1%
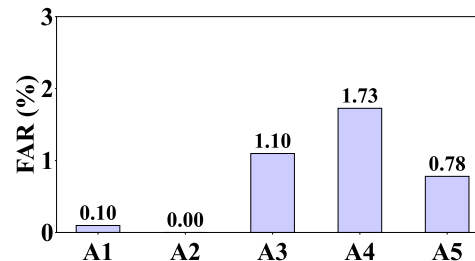


❖ **Replay attack**

- Attackers replay a pre-recorded eye movement response.
- Challenge is always new. Pre-recorded one cannot match the new challenge.

❖ **Mimicry attack**

- Attackers acquire and imitate the eye movement patterns
- Visual stimuli are random and new every time.
- Imitation is voluntary and will be excluded from the reflexive part.

# Conclusion

❖ **We propose Medusa3D, a challenge-response authentication system for VR based on reflexive eye responses.**

❖ **Medusa3D can utilize active biometric for authentication on users while keep safe against attackers.**

❖ **Future work will primarily focus on enhancing the system's robustness for long-term use.**

# *Thanks for your attention!*
## *Q&A*

I am actively looking for Ph.D. position starting 2025. Feel free to contact me if you have any relevant information.

Email: aochen.jiao@cityu.edu.hk

Personal Website