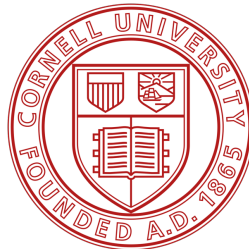# SoK: Authentication in Augmented and Virtual Reality

Sophie Stephenson, Bijeeta Pal, Stephen Fan,

Earlence Fernandes, Yuhang Zhao, Rahul Chatterjee

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

CORNELL UNIVERSITY · FOUNDED A.D. 1865

MAD S&P
Security and Privacy Research Group
at UW-Madison

AR and VR devices need authentication.

Why not passwords?

⚠️ Poor usability ➡️ ⚠️ Poor security

AR/VR present unique possibilities
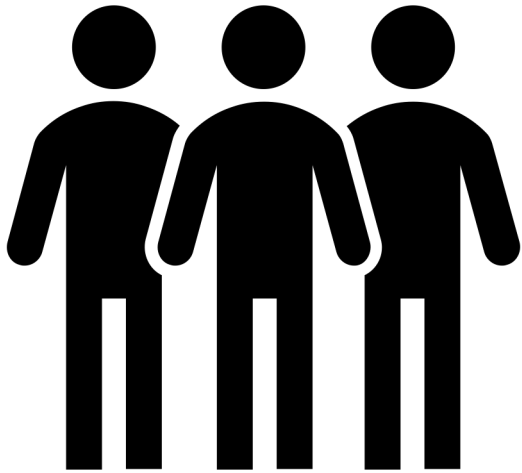
microphone

touchpad

IMU sensor

audio feedback

haptic feedback

inward camera

outward camera

controllers
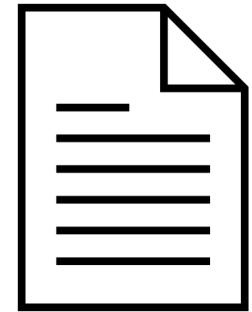
visual feedback

4

Our work

Survey of 139 users, including 49 developers

evaluation criteria for AR/VR authentication

7 methods used in 178 current apps

43 methods proposed in 38 prior works

Our work

Part 1
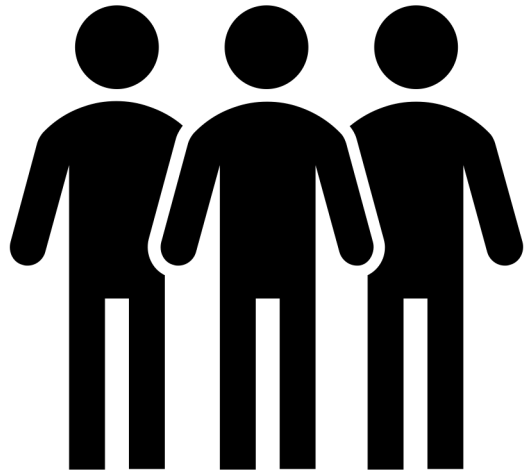
evaluation criteria for AR/VR authentication

Survey of 139 users, including 49 developers

7 methods used in 178 current apps

43 methods proposed in 38 prior works

Surveying users & developers

Designed a survey to ask:
- What do **users** think?
- Which authentication methods do **developers** choose? Why?

139 users **49** developers

Recruited participants on online platforms (e.g., Reddit, AR/VR Slack groups)

Defined evaluation criteria by coding qualitative responses

Properties for evaluation

Deployability

OS-Supported

Platform-Agnostic

Mature

Low-Power-Cons.

Usability

Efficient-to-Use

Physically-Effortless

Memorywise-Effortless

Easy-to-Learn

Nothing-to-Carry
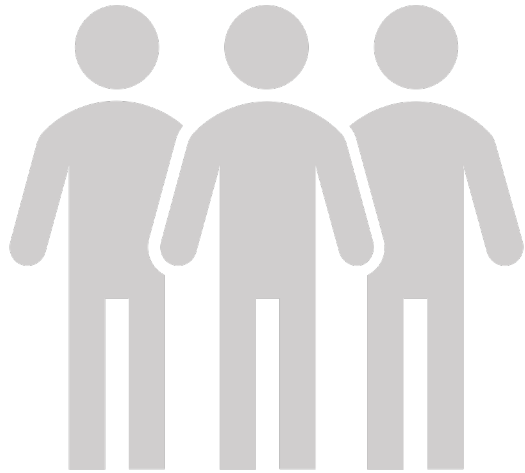
Infrequent-Errors

Acceptable-in-Public

Accessibility

Accessible-Visual

Accessible-Hearing

Accessible-Speech

Accessible-Mobility

Accessible-Cognitive

Security

Resilient-to-Guessing

Resilient-to-Observation

Protects-User-Privacy

Multi-Factor

See paper for details!

Part 2

7 methods used in 178 current apps

Survey of 139 users, including 49 developers

evaluation criteria for AR/VR authentication

43 methods proposed in 38 prior works

Analyzing authentication in AR/VR apps

HoloLens 2 (AR)

HTC Vive (VR)

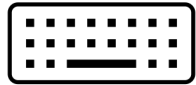🔍 Investigated authentication methods used in apps and devices
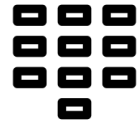
↳ 📋 Evaluated each method using our properties
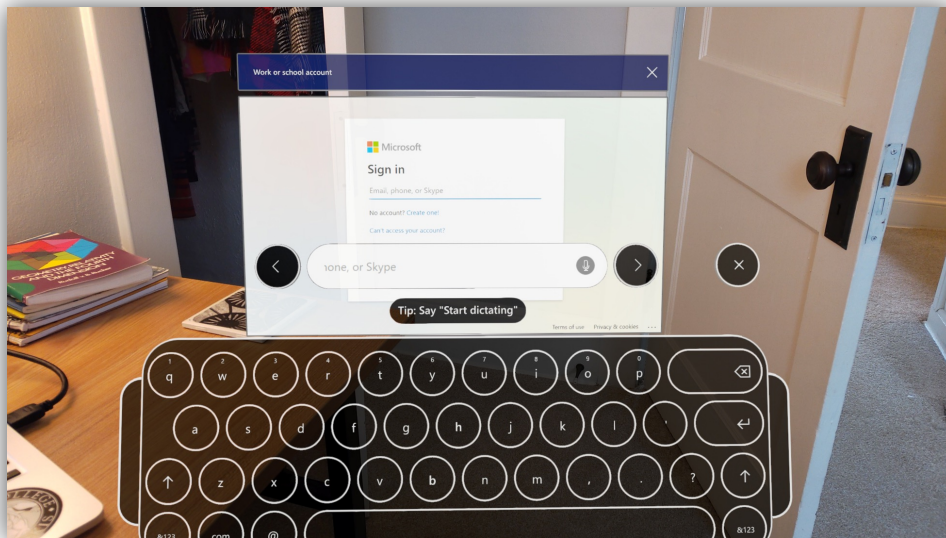
178 apps   **7** methods

Incumbent knowledge-based methods

password

PIN

paired account

+ Great **deployability** (*e.g., Platform-Agnostic*)

− Bad **usability** & **accessibility** (*virtual keyboard*)

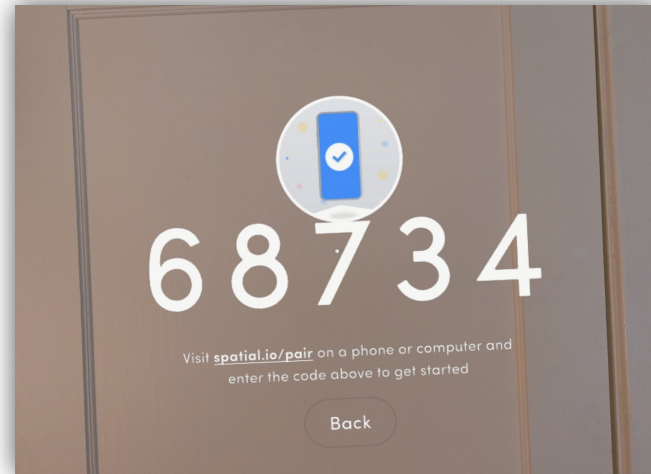**−** Worse **security** than on other devices (*e.g., shoulder surfing*)

Incumbent token-based methods

QR code

Short code

➕ Better **security**
(e.g., Resilient-to-Guessing)

➕ Better **usability**
(e.g., no virtual keyboard)

➖ Require a **secondary device**

Automatic paired account
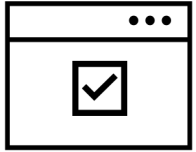

username: sophie
password: hunter2

You are logged in!

1. User logs into Viveport account

2. User puts on headset and opens app

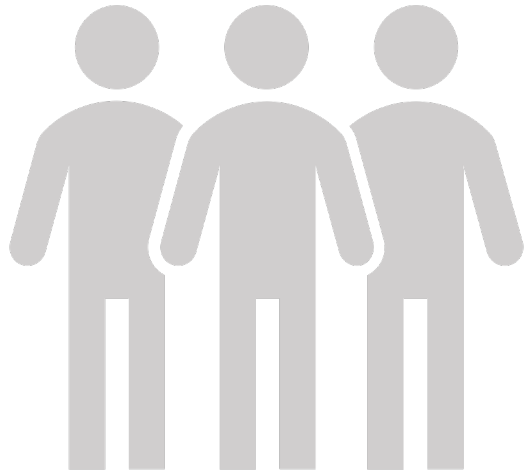3. User is automatically authenticated

Most promising incumbent methods

Automatic paired account

- ➕ Great **usability** & **accessibility**
- ➕ Strong **security** *(e.g., Resilient-to-Observation)*
- ➕ **Deployable**
- ➖ Potential privacy issues

Iris scan

- ➕ Great **usability** & **accessibility**
- ➕ Strong **security** *(e.g., Resilient-to-Guessing)*
- ➖ Not widely **deployable**
- ➖ Potential privacy issues

Survey of 139 users, including 49 developers

evaluation criteria for AR/VR authentication

7 methods used in 178 current apps

Part 3

43 methods proposed in 38 prior works

Evaluating proposed methods

Queried Google Scholar for papers which presented *new authentication mechanisms specifically for AR/VR*

38 papers   **43** mechanisms
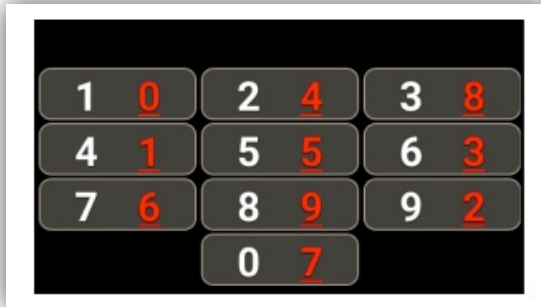
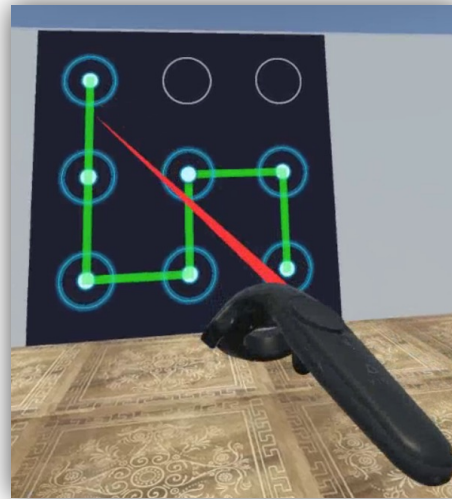Crawled references of the papers we found to identify more relevant work

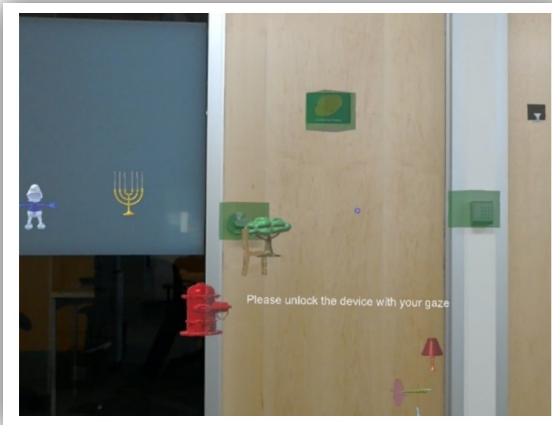Evaluated each method, relying on papers' reported results
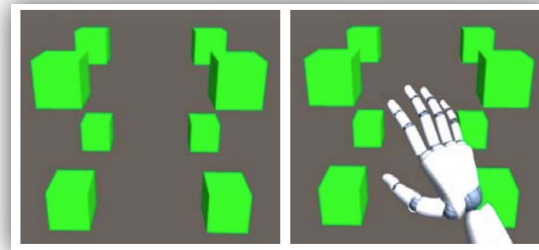
Proposed knowledge-based methods

1. Spoken, obfuscated PIN
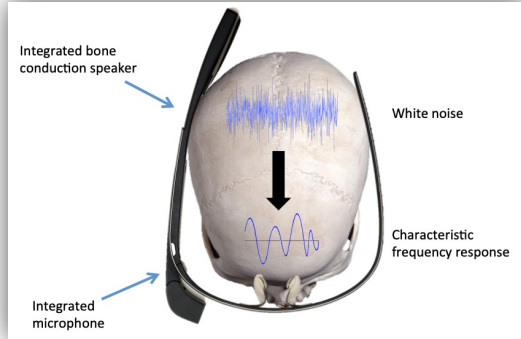*(Cheng et al., 2017)*

2. Swipe pattern
(Olade et al., 2020)

3. Environment-based PIN
(Funk et al., 2019)

4. Cube PIN
(Yu et al., 2016)

+ Good **deployability**
(e.g., Platform-Agnostic)

+ Improved **security**
(e.g., Resilient-to-Observation)
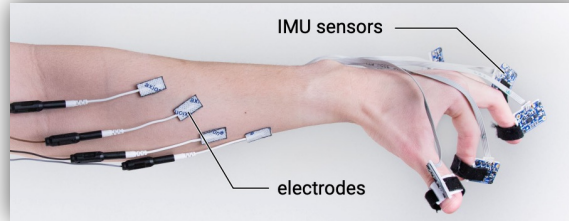
– Improved **usability**; still poor

Proposed physical/behavioral biometrics

5. Sound conduction
(Schneegass et al., 2016)

6. Muscle stimulation
(Chen et al., 2021)

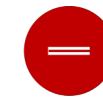

7. Head movement
(Li et al., 2016)

8. Moving virtual balls
(Olade et al., 2020)

+ [Physical]
Usable & **accessible**

− [Behavioral]
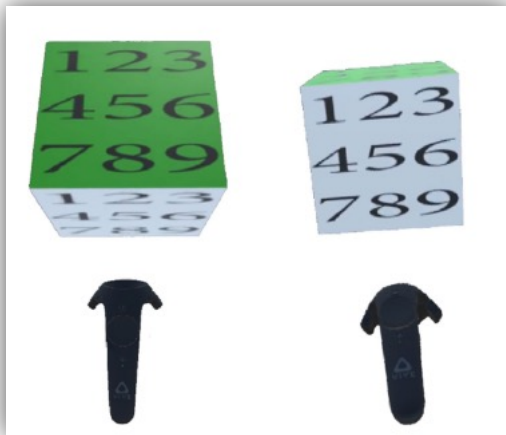Less **usable,** less **accessible**

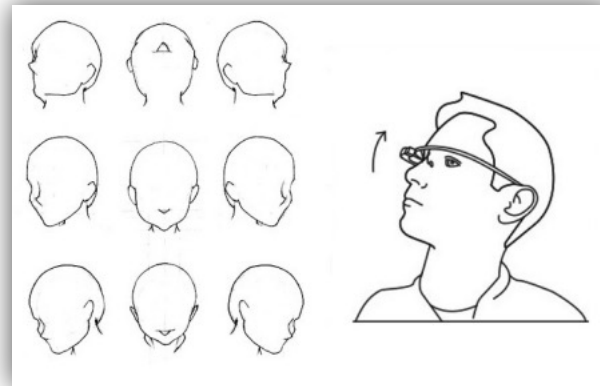− Not **deployable**
(e.g., not Platform-Agnostic)

− Need improved accuracy

Proposed multi-factor methods

9. Rubik's Cube PIN + controller biometrics
(Mathis et al., 2020)

10. Security questions + head movement biometrics
(Yi et al., 2016)

➕ Best **security**!

➕ Quasi-*Platform-Agnostic*

➖ Security reduced on other platforms

Future directions

Focus on **deployability**

Unify the authentication stack with **federated login**

Strengthen **biometrics**: accuracy, privacy, and platform support

Password managers for AR and VR devices

SoK: Authentication in Augmented and Virtual Reality

Created user- & developer- desired properties for any AR/VR authentication method

Evaluated the authentication methods currently on AR/VR

Evaluated proposed AR/VR authentication methods

Sophie Stephenson

srstephenso2@wisc.edu

sophiestephenson.notion.site

@sophxstephenson