MobiSec

NDSS'23 SYMPOSIUM

SoundLock

A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response

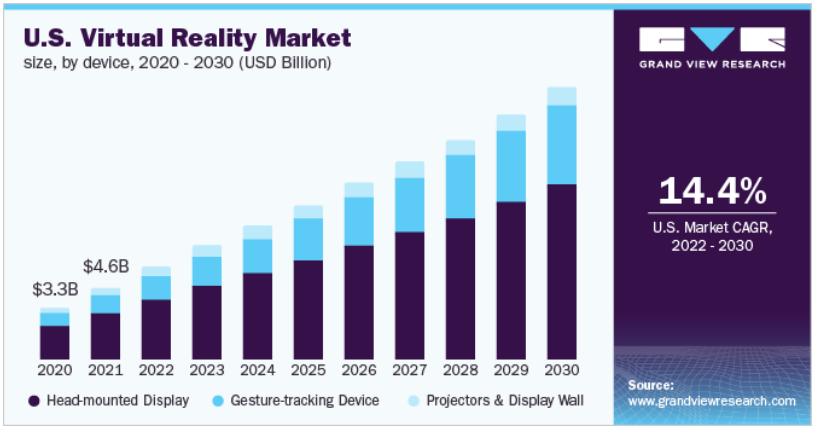
Huadi Zhu, Mingyan Xiao, Demoria Sherman, and Ming Li

The University of Texas at Arlington

UTA

Motivation

- Development of VR market
  $28 billion in 2022
  $87 billion in 2030



[1] https://www.grandviewresearch.com/industry-analysis/virtual-reality-vr-market

- VR applications

◁ Entertainment

E-commerce ▷

◁ Healthcare

Education ▷

◁ Social media

Motivation

- Sensitive information is stored in and accessible through VR devices
  - Personal media
  - Bank information
  - Health status

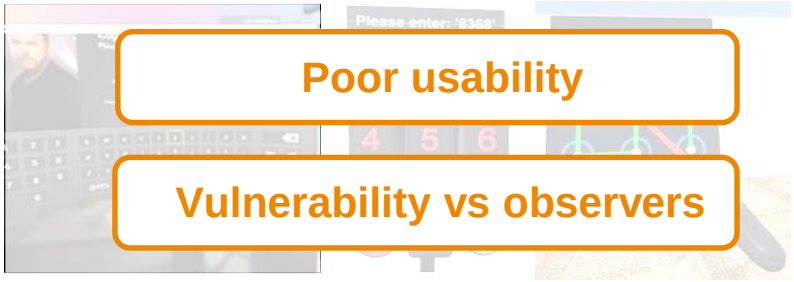
  ……

User authentication on VR is crucial

- VR applications

Related Work

Current solutions

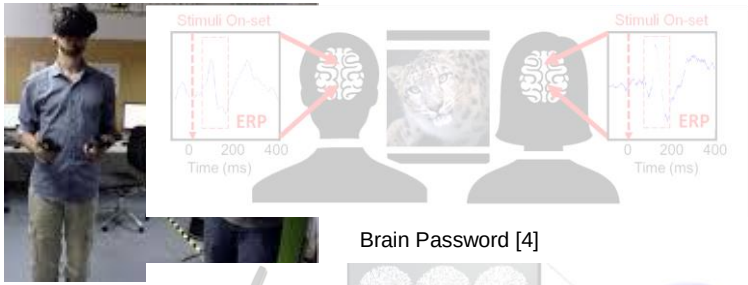


Password PIN [2] Pattern lock [3]

Poor usability

Vulnerability vs observers

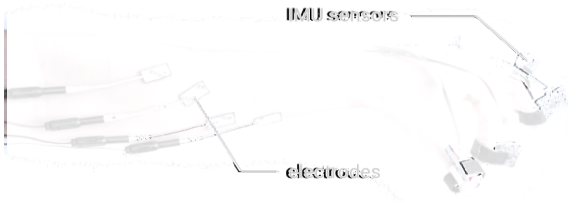
State-of-the-arts



Brain Password [4]

Sensor deployment issue

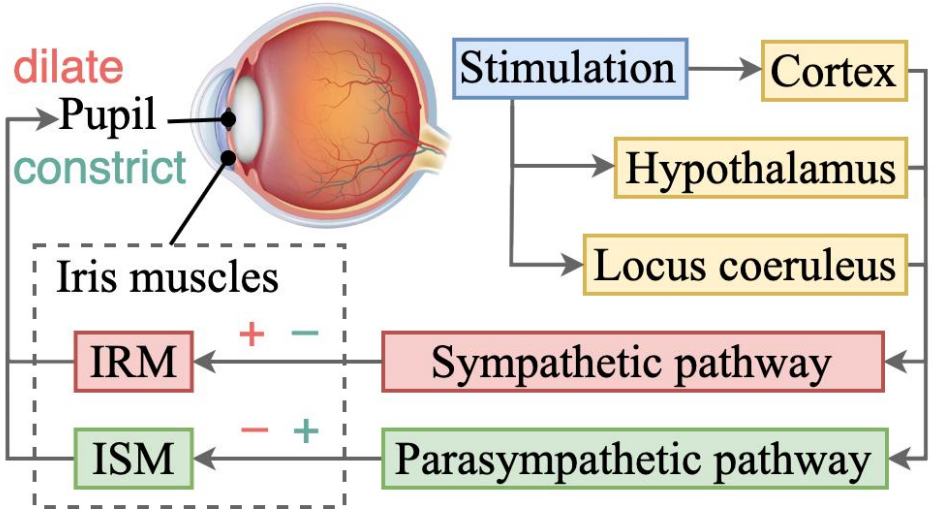
SkullConduct [5] OcuLock [6]



ElectricAuth [7]

A **convenient**, **robust** & **deployable** user auth scheme is in dire need!

Background: Auditory-Pupillary Response

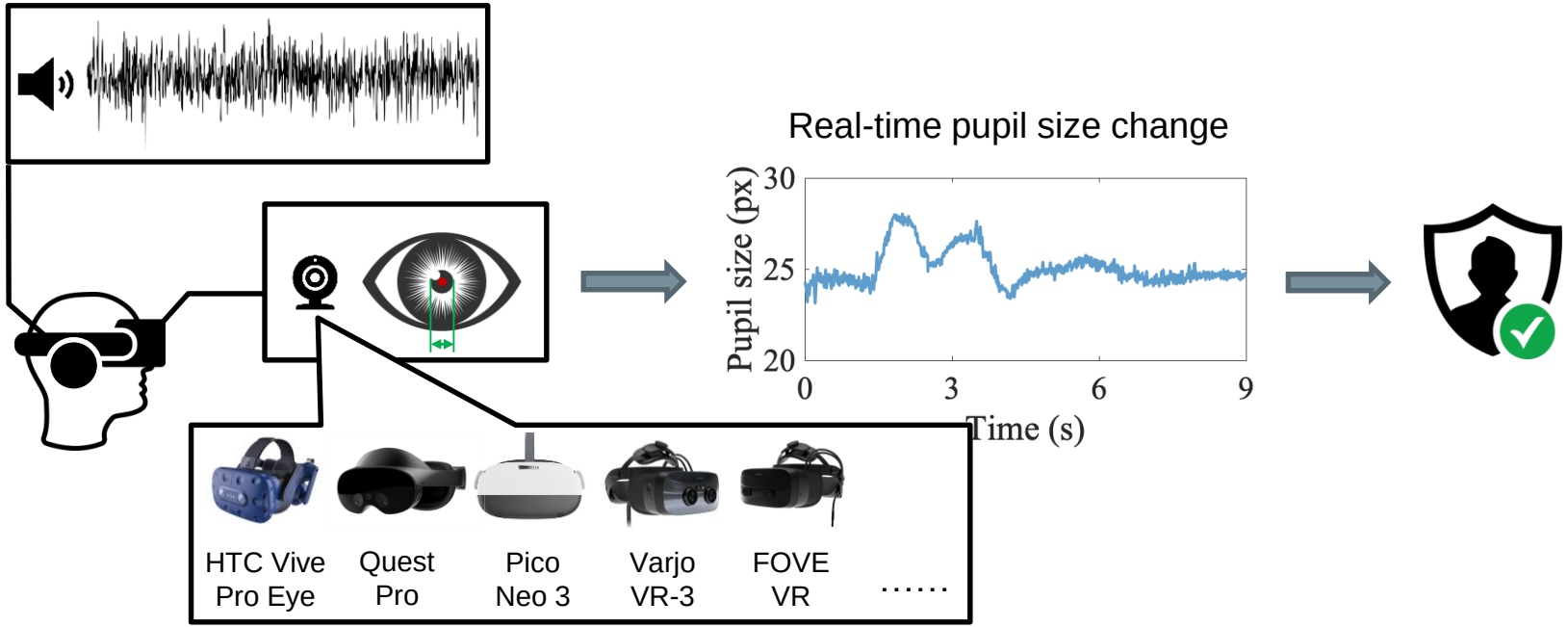


Auditory-pupillary response mechanism

The complex structure of neural pathways and iris muscles: **biological uniqueness**

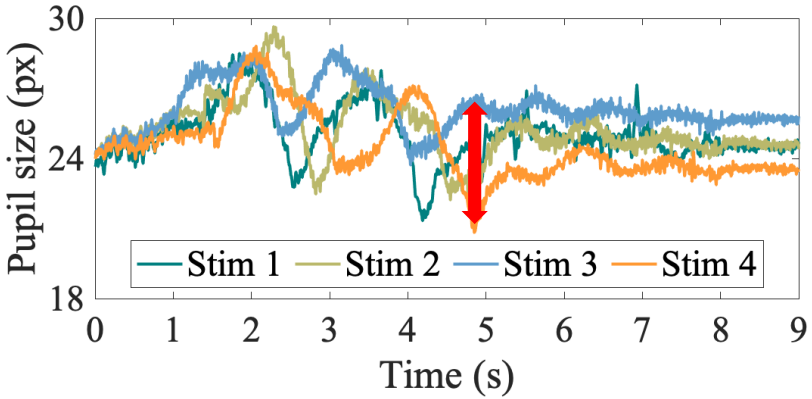
SoundLock: Basic Idea

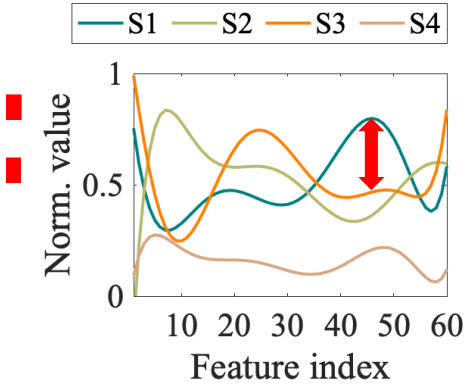
Leverage new biometric, **auditory-pupillary response**, for user authentication



Measurement Study

- Setup
  - 32 subjects × 20 audio tracks

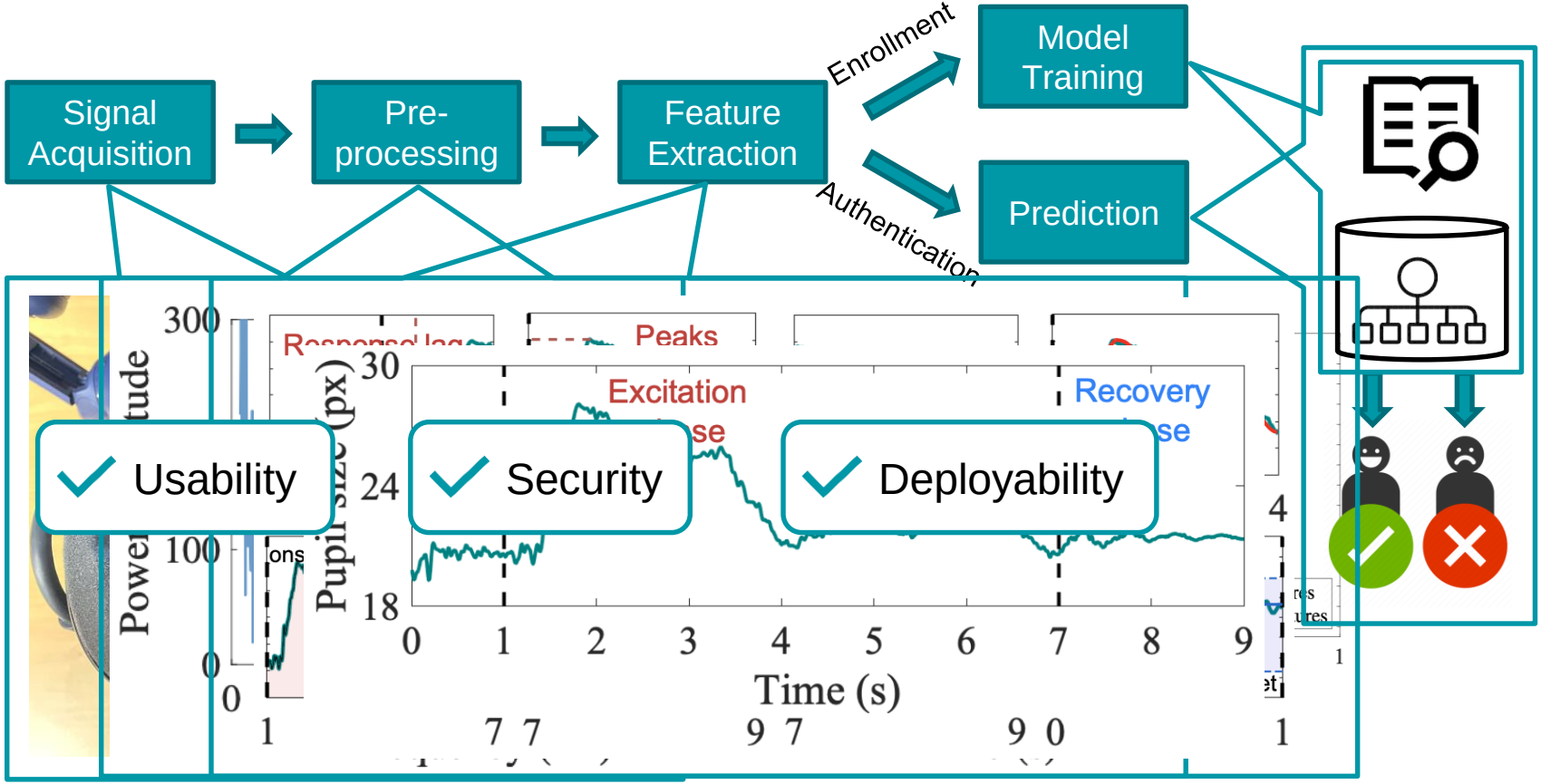




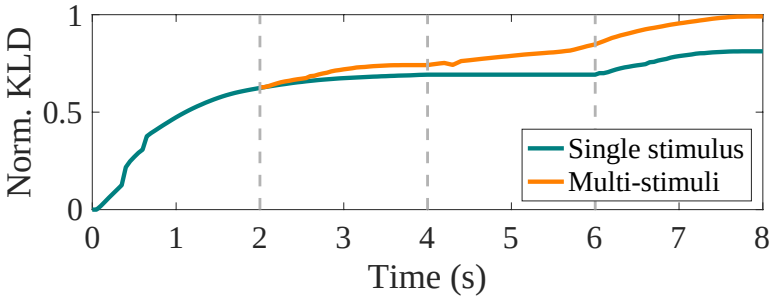
- Observations
  - Distinguishable responses across subjects
  - Consistent responses within a subject
  - Distinguishable responses across stimuli

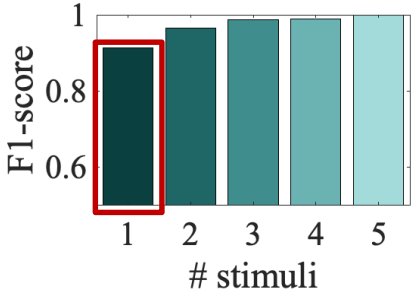
Auditory-pupillary response: **ideal biomarker**

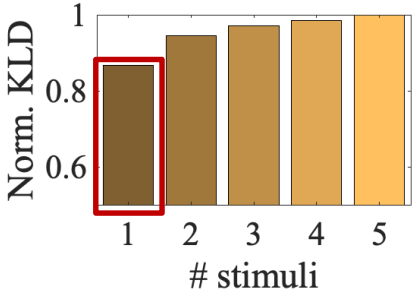
SoundLock: Workflow



Increasing System Entropy



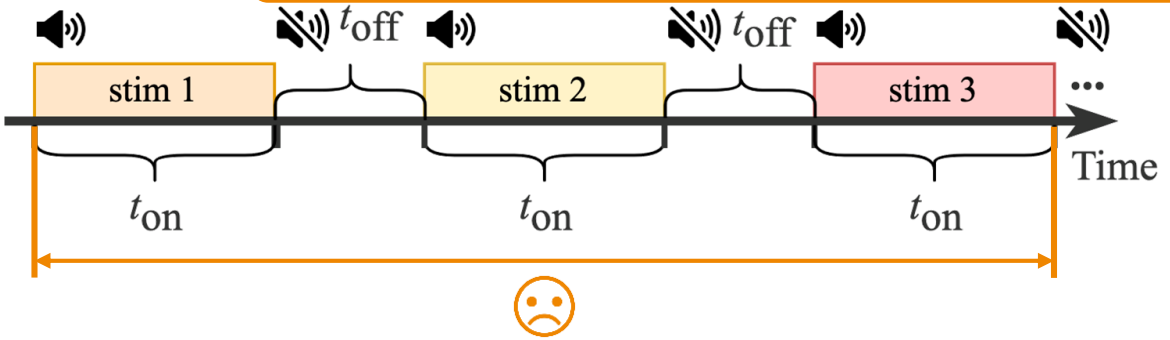




Strawman a

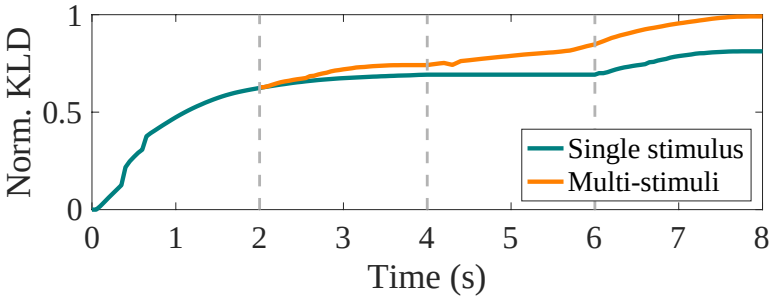
Single stimulus: limited biometric entropy and authentication accuracy

ses



Long authentication time!

Increasing System Entropy

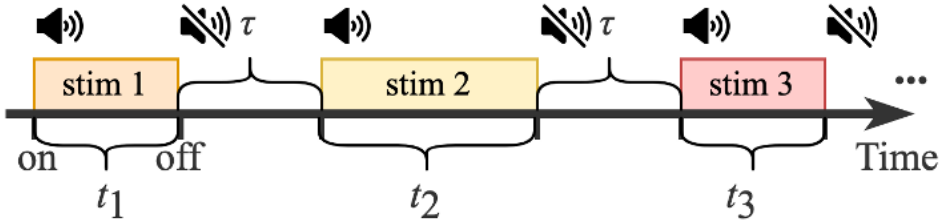


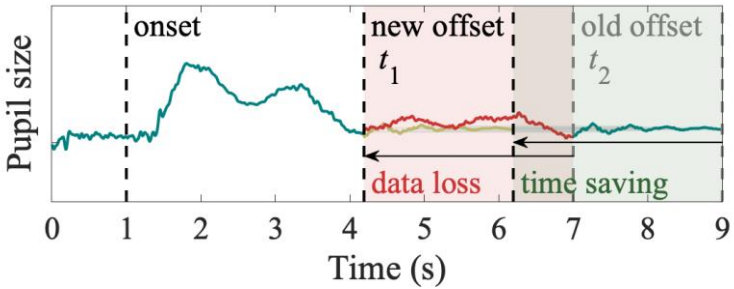
Performance indicator: Kullback-Leibler divergence (KLD)

$$D_{KL} = \sum_{x \in X} P(x) \log\left(\frac{P(x)}{Q(x)}\right)$$

KLD: non-uniform distribution → truncate stimuli

Our solution: concatenate truncated stimuli





Optimize **stimuli selection** and **duration** for the best performance-time tradeoff

Optimization Approach

- Problem formulation

$$\max_{\boldsymbol{m},\boldsymbol{t}} D_{KL}(P||Q)$$

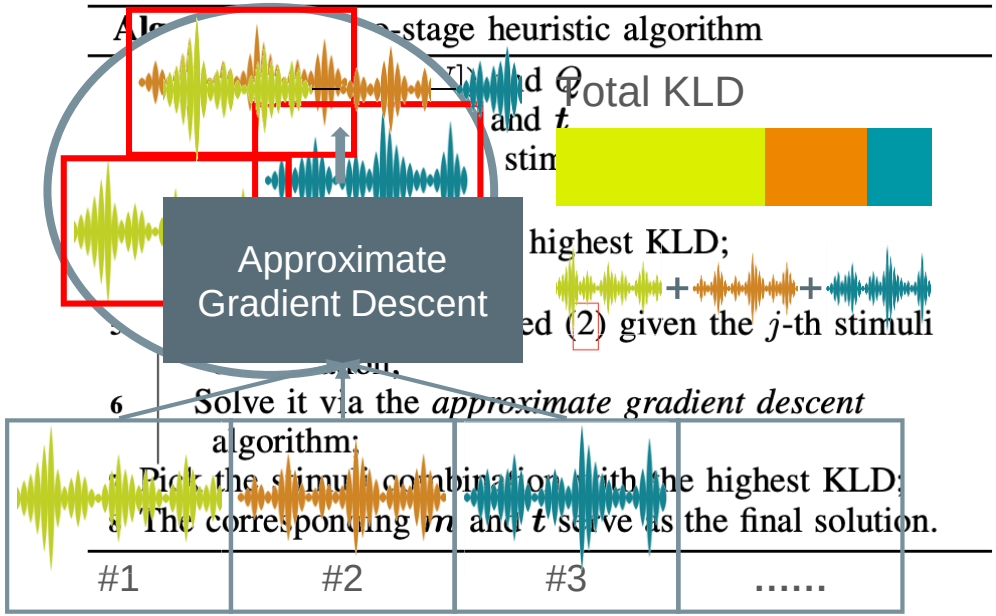
$$\text{s.t.} \sum_{i=1}^{N} (t_i + \tau) \times m_i \leq T_0$$

$$m_i \in \{0,1\}$$

Correlation between variables

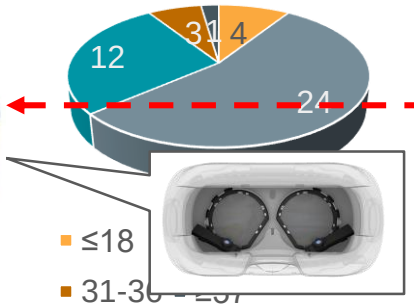
Non-linearity

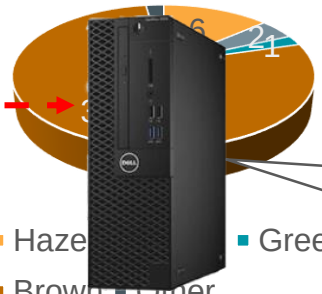
- Two-stage heuristic optimization algorithm
  - **Stage 1** approximately optimize $\boldsymbol{m}$
  - **Stage 2** optimize $\boldsymbol{t}$ via AGD

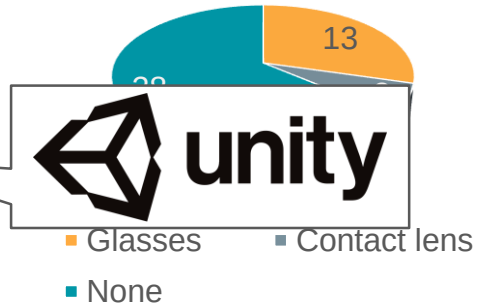


Experiment Setup

- Prototype apparatus
  - VR headset: HTC VIVE Pro
  - Eye tracker: Pupil Labs add-on
  - Server: Exxact desktop
    - Processor: Intel Core i7 CPU
    - GPU: 2x NVIDIA GeForce RTX
    - Operating system: Windows 10
  - Software platform: Unity
- Recruitment
  - 44 participants from UT Arlington
- Procedure
  - Enrollment
  - Authentication
  - Impersonation attack
  - Consistency tests
  - User study







Overall Performance

- Comparison with state-of-the-arts

Approach	FAR (%)	FRR (%)	F1-score	Auth time
PIN* [2]	-	>1.14	-	2.54-2.95
Drawing pattern* [2]	-	>5.19	-	2.82-3.87
OcuLock [6]	3.55	3.55	0.983	≤10
SkullConduct [5]	6.90	6.90	-	≤23
Brain Password [3]	2.50	2.50	0.955	≈4.80
ElectricAuth [7]	0.83	2.00	-	≈**1.30**
SoundLock (this work)	**0.76**	**0.91**	**0.984**	≤7

Best authentication performance

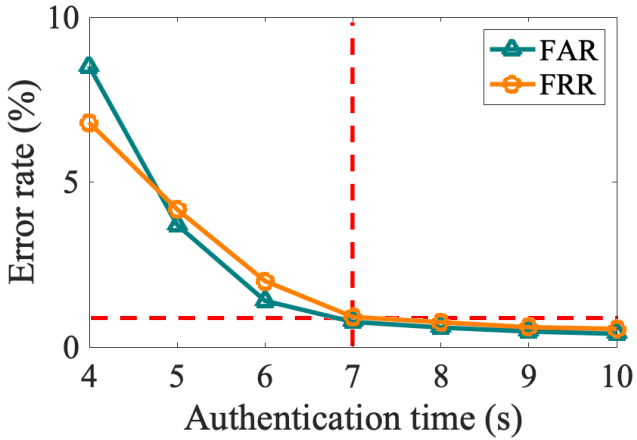
Entropy Analysis

- Comparison with existing generic authentication systems

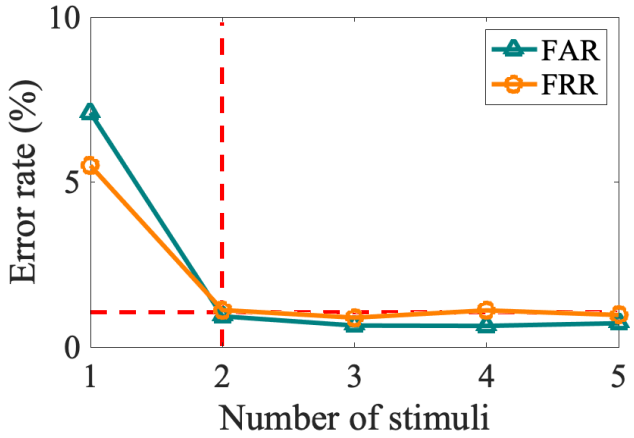
Work	Authentication method	Entropy (bits)
Wang et al. [8]	Password	$20 - 23$
Wang et al. [9]	PIN (4-digit[1], 6-digit[2])	$8.41^{[1]}, 13.21^{[2]}$
Sae-Bae et al. [10]	Keystroke	$3.48 - 4.62$
Youmaran et al. [11]	Iris	$278 - 288$
Takahashi et al. [12]	Fingerprint	18.6
Adler et al. [13]	Face	$37.0 - 55.6$
SoundLock (this work)	Pupillometry	81

Performance-Usability Tradeoff

- Error rate vs authentication time



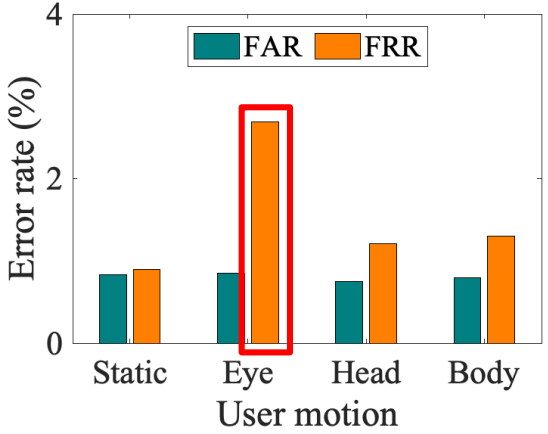
- Error rate vs number of stimuli



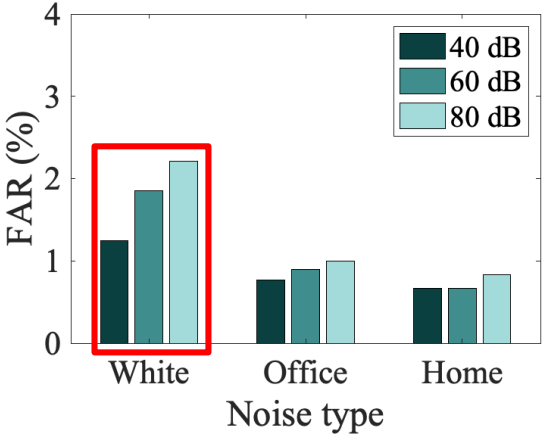
Optimal tradeoff

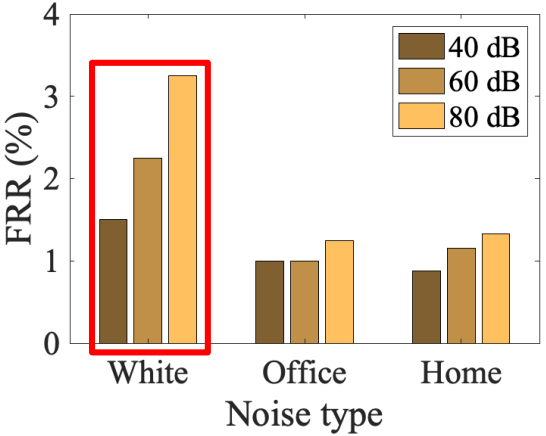
Performance Under Various Scenarios

- Impact of user motion



- Impact of ambient noise





Eye movement: highest impact on FRR

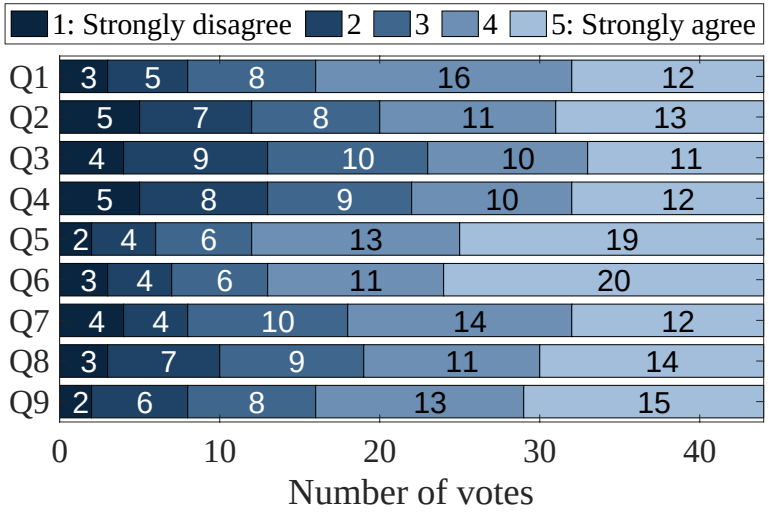
Minimal impact on FAR: no security degradation

White noise: highest impact

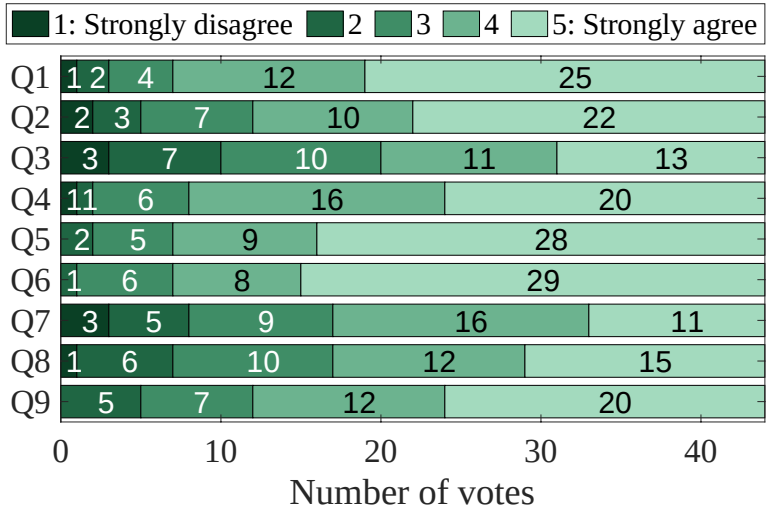
Consistent in real-world scenarios

User Study

- Closed questionnaire design
- User feedback



Pre-study results



Post-study results

Well perceived by users in both studies

Improvement in post-study: exceeds expectations

User Study

- Open questionnaire
  - What's your overall experience with SoundLock?
    - *"It was a **fun** experience!"* (P9)
    - *"The idea of using pupil for authentication is **smart**."* (P35)
    - *"I **don't need to do anything** and the authentication is automatically done."* (P40)
  - Do you have any concerns or did you notice any potential issues of SoundLock?
    - *"Will **twins or siblings be able to hack** into each other's profile?"* (P35)
    - *"Will my pupillary response be used to **infer what I'm thinking**?"* (P38)
  - Do you have any suggestions to improve SoundLock in the future?
    - *"I think the system can be **extended to smartphones**, which will prove a valuable addition. The speaker can emit a sound and the eye image can be captured by the camera."* (P1)

Conclusion

- ✓ We investigate auditory-pupillary response, a novel reflexive physiological biometric, for user authentication on VR devices
- ✓ We formulate an optimization problem and propose a two-stage heuristic algorithm to efficiently optimize the accuracy-usability tradeoff
- ✓ We prove via extensive in-field experiments that SoundLock outperforms state-of-the-art solutions and is well received among users

THANK YOU

Check our SoundLock paper

Find out about our MobiSec group