# Offensive and Defensive Analysis of Behavioral Biometrics on Smart Wearables

Sindhu Reddy Kalathur Gopal, Diksha Shukla

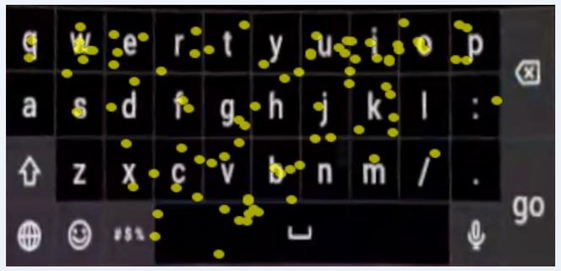
University of Wyoming

## VULNERABILITIES: TRADITIONAL PASSWORD/ PIN/TOKEN-based AUTHENTICATION SYSTEMS

- PINs and Passwords may be forgotten or stolen
- Susceptible to different attacks such as phishing attack, dictionary attack, shoulder surfing, side-channel attack, replay attack, forgery attack such as key loggers, etc.
- Traditional authentication systems performs entry point authentication which can lead to security threats such as session hijacking [1], etc.

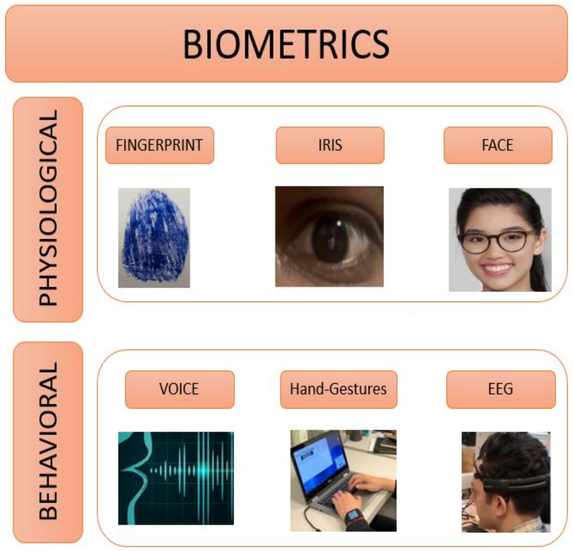
### Example of Side-channel Attack

**Adversary's view** of a target user while the user types on the virtual keyboard in an immersive VR environment on Oculus Quest.



**Experimental Results**: Plotting of the click location data and mapping it to the keyboard geometry for inferring the typed characters.

## BIOMETRICS CLASSIFICATION




## CONS: PHYSIOLOGICAL BIOMETRICS

- Physiological biometrics such as fingerprints and iris can be acquired stealthily and are susceptible to some attacks similar to those of the traditional authentication systems
- Requires an additional step to verify the liveness of the person

## SHORTCOMINGS OF EXISTING RESEARCH

- **Pre-defined tasks** leading to mimicry attacks
- Examples of pre-defined tasks: Typing defined text, perform arithmetic operations, etc.
- **Unobtrusive tasks**: Takes user's time away from their work to perform authentication

## OUR WORK


Light-weight Low-cost

## BEHAVIORAL BIOMETRICS-based CONTINUOUS AUTHENTICATION

- Continuous Authentication (CA): Verifies user continuously to overcome attacks such as session hijacking
- Behavioral Biometrics such as EEG is hard to be stolen and spoofed [2]
- EEG satisfies liveness criteria [3]

**1. Temporal Memory-based CA [5]:**

- Unobtrusive Task.
- Does not take time away from the user's work
- *Feature Temporalization:*

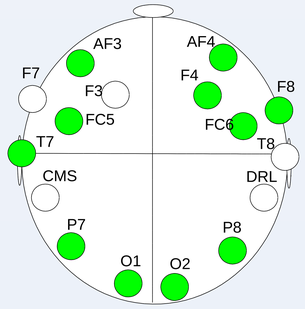
$$v_{fnew} = [v_{f1} \,||\, v_{f2} \,||\, v_{f3} \,||\, \ldots\ldots \,||\, v_{fn}]$$

where temporalized feature: $v_{fnew}$

and feature at previous time stamp: $v_{fn}$

**2. Concealable Biometrics-based CA [4]:**

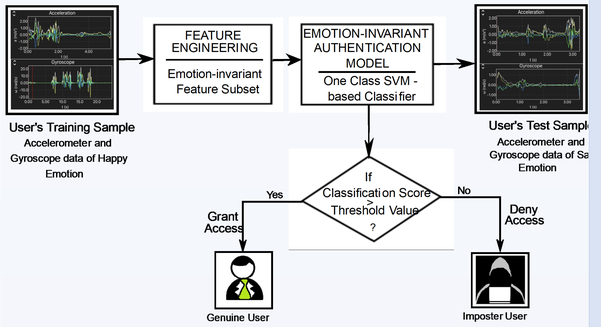
- Authenticates user unobtrusively using electroencephalogram (EEG) signals
- Learns the user's unique biometric signature based on his/her brain activity.
- Optimal feature subset is constructed using a minimal number of EEG electrodes/channels




**Channels of Emotiv Device**

Illustration of the Placement of EEG Electrodes on the user's head is shown in the Channels of Emotiv Device figure. Electrode locations that Contributed in Optimal Features Subset are Highlighted with Green Color

**3. Emotion-invariant CA:**




- Train the model while the user is in any of the emotional state
- Verify the user irrespective of the emotional state the user is

## REFERENCES

1. Shukla, P. P. KUNDU, R. Malapati, S. Poudel, Z. Jin, and V. V.Phoha. Thinking unveiled: An inference and correlation model toattack eeg biometrics.Digital Threats: Research and Practice, 1(2),May 2020
2. J. Galbally, S. Marcel, and J. Fierrez. Image quality assess-ment for fake biometric detection: Application to iris, fin-gerprint, and face recognition.IEEE Transactions on ImageProcessing, 23(2):710–724, 2014.
3. T. Kathikeyan and B. Sabarigiri. Countermeasures againstiris spoofing and liveness detection using electroencephalo-gram (eeg). In2012 International Conference on Computing,Communication and Applications, pages 1–5, 2012.
4. S. R. K. Gopal and D. Shukla. Concealable biometric-based contin-uous user authentication system an eeg induced deep learning model.In2021 IEEE International Joint Conference on Biometrics (IJCB),pages 1–8, 2021.
5. S. R. Kalathur Gopal and D. Shukla. A temporal memory-basedcontinuous authentication system. In2021 IEEE International JointConference on Biometrics (IJCB), pages 1–7, 2021.