EEG-MFA: On Step, Seamless Multi-Factor Authentication Using EEG Signals

Team Members

Name: Sindhu Reddy

Research Area:

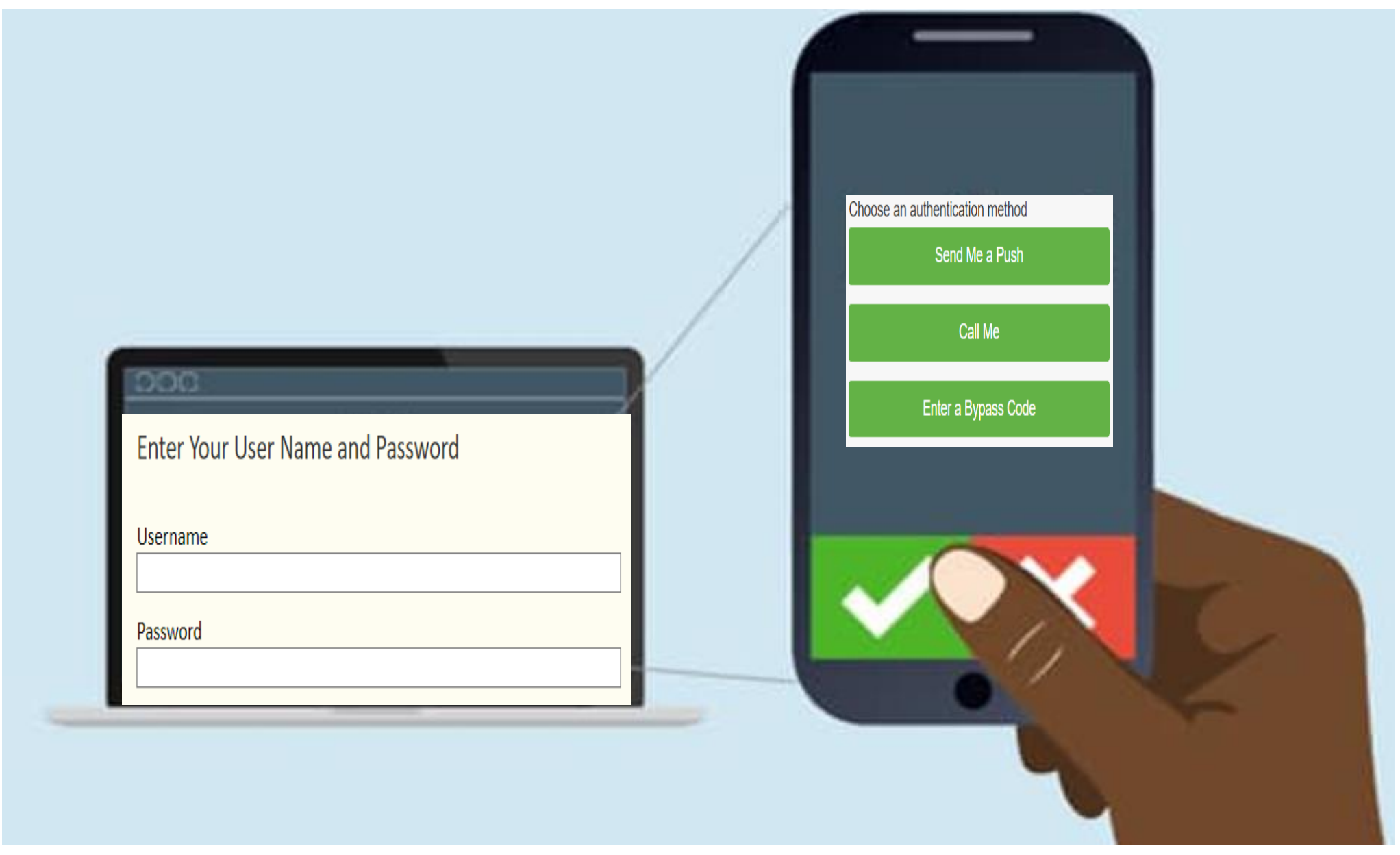
- Behavioral Biometrics for Authentication
- Side-Channel Attacks

Name: Dr. Diksha Shukla

Research Area:

- Behavioral Biometrics for Authentication
- Side-Channel Attacks
- Trustworthiness of Social Media network

Background

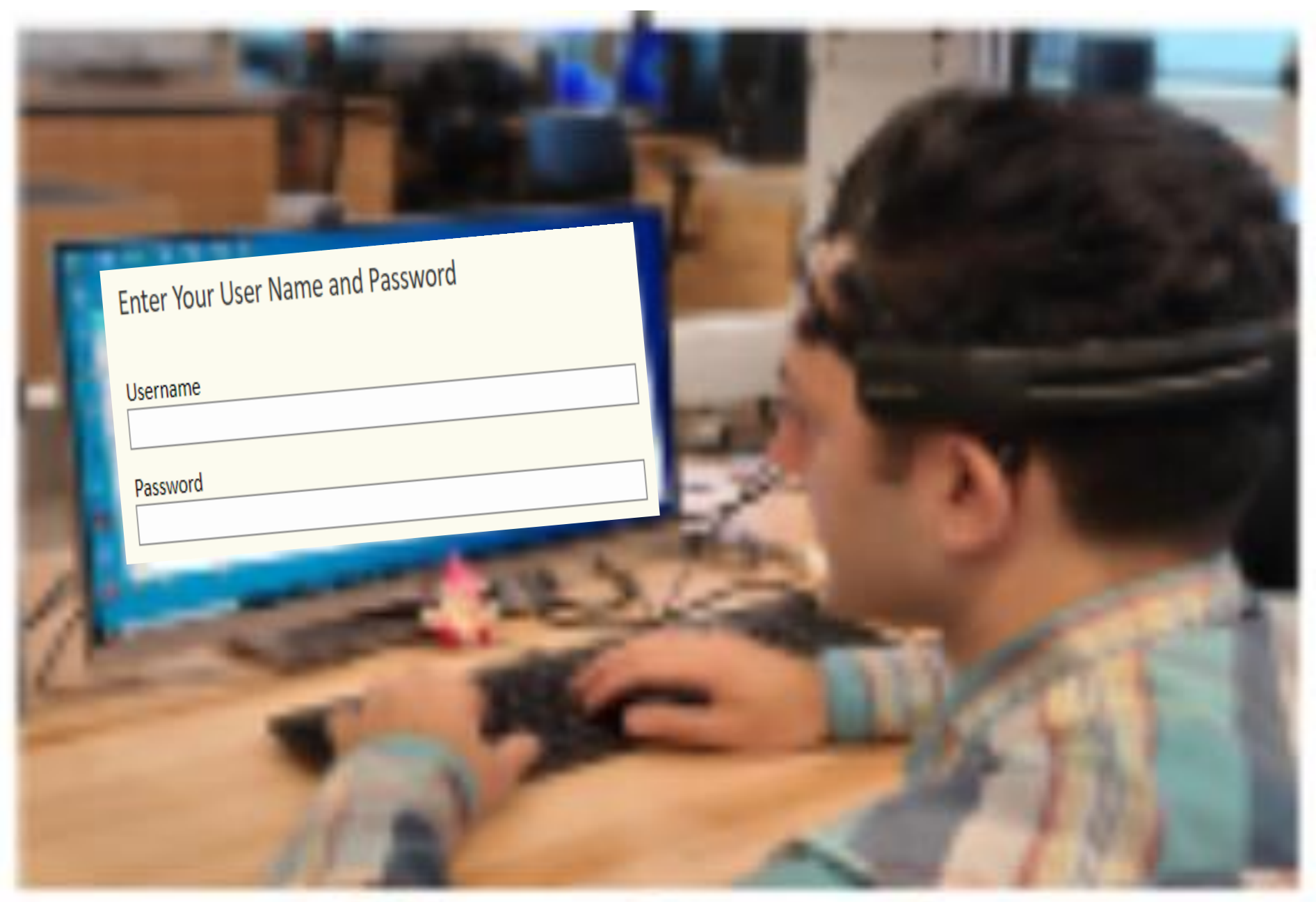

Choose an authentication method
Send Me a Push
Call Me
Enter a Bypass Code
Enter Your User Name and Password
Username
Password

- Verifies user based on two or more authentication factors.
- Examples of current MFA's first factor includes Passwords, pins, graphical lock-patterns.
- Second factors of current MFA can be OTP, hardware token, push notification.
- Example Applications: Duo Security, Microsoft Authenticator, Okta, etc.

Problem Statement

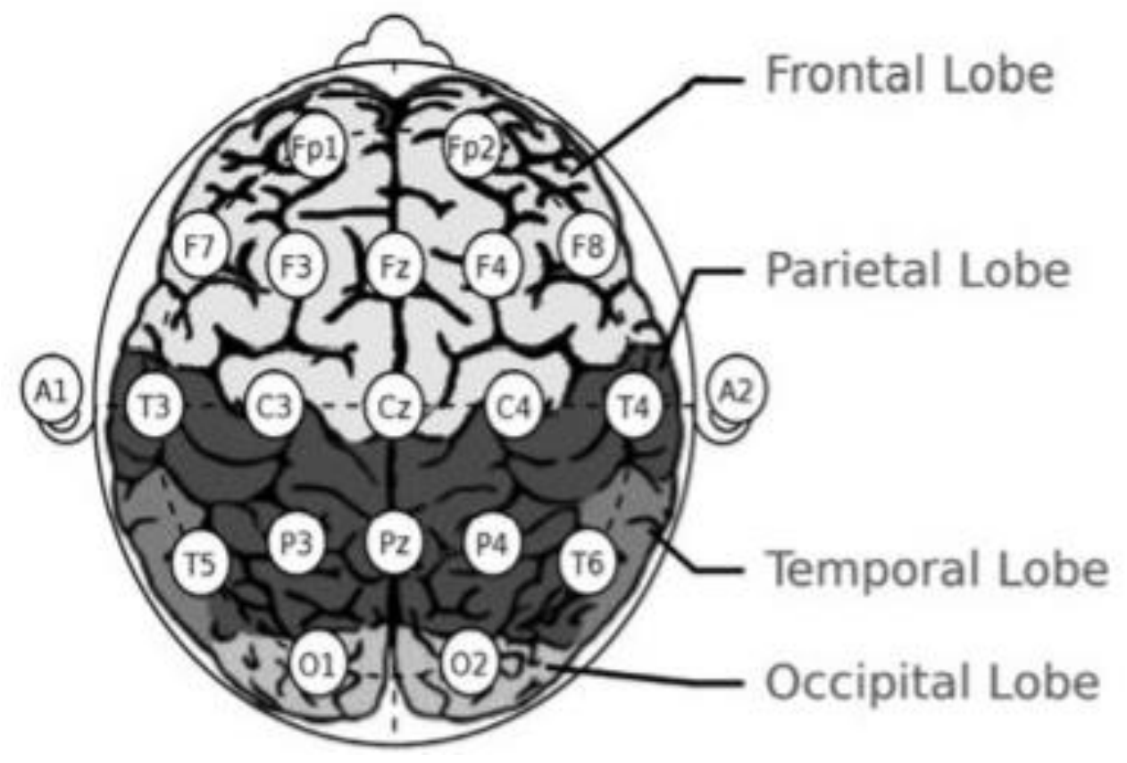
- Does the current multi-factor authentication verify user or imposter ?
- What if the user's device is stolen?
- Is the current MFA secure against impersonation attacks [1] [2] ?
- Usability Concerns: e.g., Take time off their work to enter OTP or accept the push notification.
- Is there a method to overcome the security threats and usability issues?

Proposed Solution



- User performs authentication using password or pin or graphical-lock pattern
- Relies only on familiarity factor in concealable electroencephalogram (EEG) signals
- Seamless identification of the user without taking time off their work.

EEG as a Biometric



Functions
Memory, concentration, emotions.
Problem Solving, attention, grammar, sense of touch.
Memory, face recognition, hearing, word recognition, social clues.
Reading, vision.
Motor control, balance.
Attention, mental processing, fine motor control, sensory integration.

Source for Table: Demos, John. (2005). Getting Started with Neurofeedback; Source for Figure: A survey on methods and challenges in EEG based authentication in Computers & Security

- EEG Signals: Brain signals acquired from users' scalp by using EEG devices
- Unique to an individual [3] [4].
- Cannot be obtained unobtrusively [5].
- Secure against spoofing or presentation attacks
- Intrinsic liveness detection [6]

References

[1] D Shukla, R Kumar, A Serwadda, VV Phoha . Beware, your hands reveal your secrets! in Proceedings of the ACM SIGSAC Conference on Computer and Communication Security, 2014.

[2] Diksha Shukla, Vir V Phoha. Stealing passwords by observing hands movement in IEEE Transactions on Information Forensics and Security, 2019.

[3] Sindhu Reddy Kalathur Gopal, Diksha Shukla. Concealable Biometric-based Continuous User Authentication System An EEG Induced Deep Learning Model in IEEE International Joint Conference on Biometrics, 2021

[4] Diksha Shukla, Partha Pratim Kundu, Ravichandra Malapati, Sujit Poudel, Zhanpeng Jin, Vir Phoha. Thinking Unveiled: An Inference and Correlation Model to Attack EEG Biometrics in ACM Digital Threats: Research and Practice, 2020.

[5] QiongGui, Maria V. Ruiz-Blondet, Sarah Laszlo, and ZhanpengJin. A survey on brain biometrics. ACM Comput.Surv., 51(6), feb2019

[6] E. F.Wijdicks, "Determining brain death in adults",Neurology, vol. 45, no. 5, pp. 1003-1011, 1995.

University of Wyoming

UW College of Engineering and Physical Sciences

UW Cybersecurity Education and Research Center

UW School of Computing

UW College of Engineering and Physical Sciences Electrical Engineering and Computer Science

CEDAR
Cybersecurity Education And Research Center