Snooping Online Form Choice Privacy in Video Calls

Steven Seiden, Long Huang, Chen Wang

Department of Computer Science, Louisiana State University, Baton Rouge, LA 70803 USA

sseide3@lsu.edu, lhuang45@lsu.edu, chenwang1@lsu.edu

Motivation

- Since the pandemic, **online conference calls** have become extremely popular
- People are often **multitasking** while on conference calls
- e.g., a professor might ask students to fill out a survey while in class
- We are exploring if an attacker can **decipher a person's answers when voting in an online poll** while simultaneously in a conference call
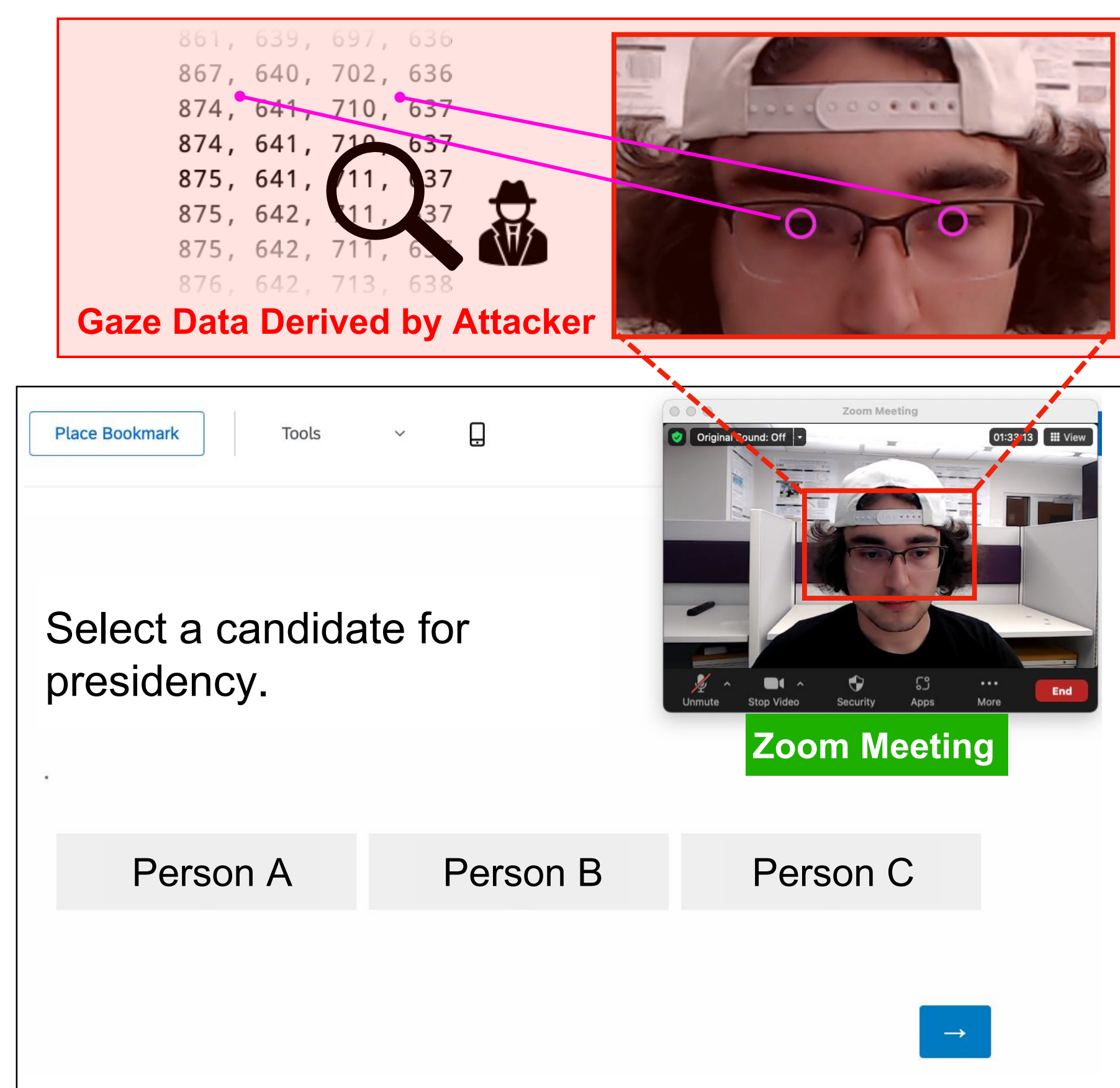
Basic Idea

Gaze Data Derived by Attacker

- **Attempting the attack:**
  - Complete the attack using the user's webcam footage
  - Track the user's eye gaze position
  - Attempt to derive the position of the screen in which the user is gazing

System Overview

Video Input From The User's Webcam 🎥

⬇

Pupil Location Extraction
- The user's web camera is analyzed by media pipe
- The location of the user's pupils within each video frame is recorded as a series of coordinates

⬇

Online Form Choice Derivation
- Features are derived from coordinates
- These features are fed into a linear regression model for model training
- The model can differentiate between different answer choices being selected based on a series of coordinates

⬇
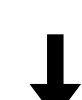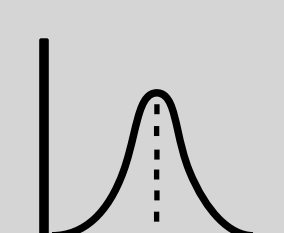
Online Form Privacy Revealed ✔

Online Form Choice Inference Algorithm

- Many algorithms for eye tracking through a standard web camera are inaccurate or require user training
- After experimenting with several algorithms, we selected Google's Mediapipe
- This algorithm allows a real-time video feed to be analyzed
- The location of the user's pupils from within the video feed is exported as a series of coordinates

Preliminary Experiments & Results

- Experiment Setup:
  - The user is asked to fill out an online poll while their video camera is on
  - The video feed is analyzed in real time by Mediapipe
    - Mediapipe uses facial recognition to find the user's pupils within the video feed
  - The algorithm outputs a series of gaze coordinates that can be used to estimate where on the screen user is gazing

- Data Analysis:
  - Using MATLAB for data interpretation
  - Eye motion features are extracted to capture the user's eye behaviors of making different answer choices
  - Extracted features fed into a Support Vector Machine-based algorithm
  - The user's choices can then be inferred based on their eye gaze data
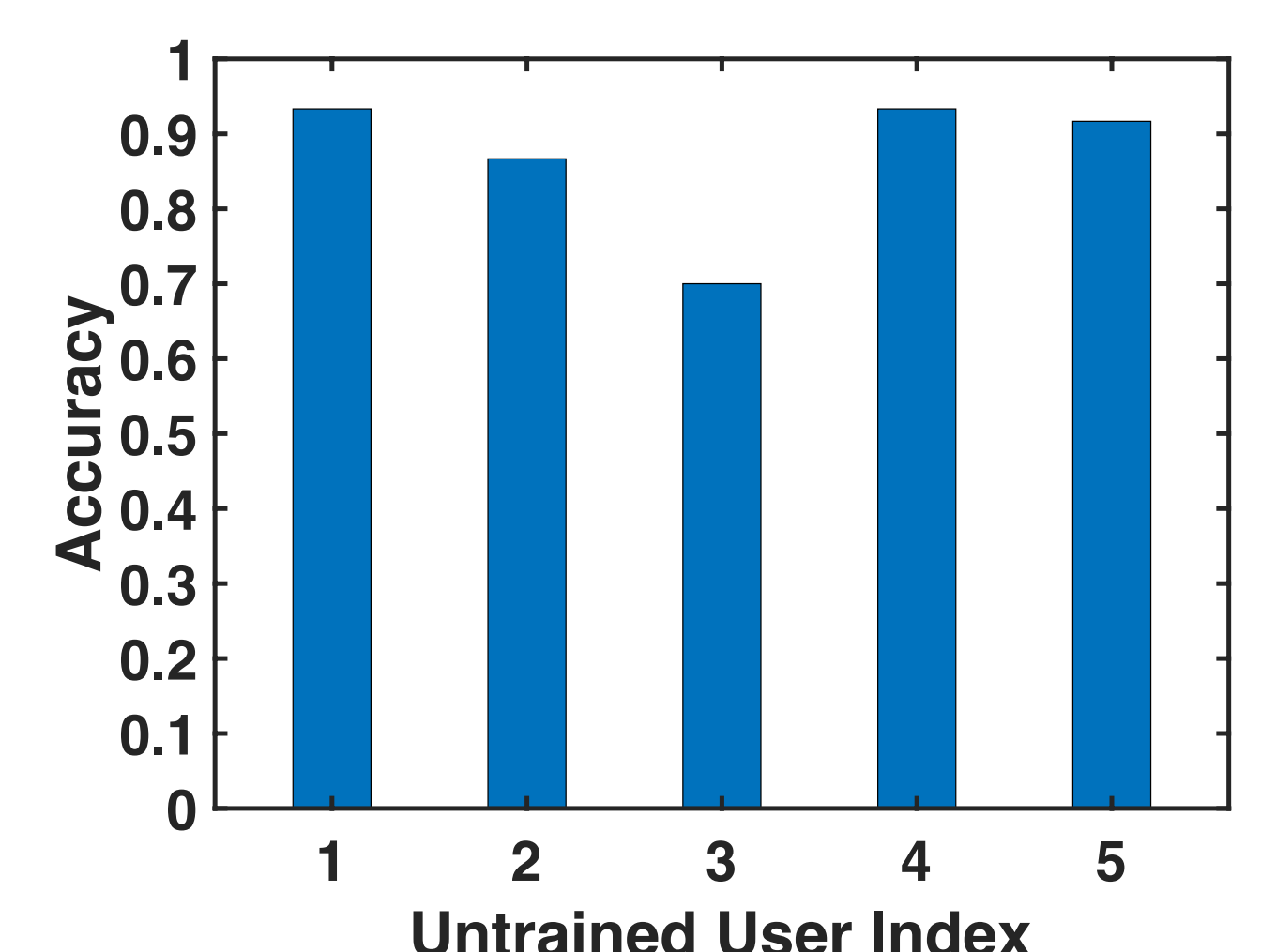
- Experiment Results:
  - We can infer the online form choices with an overall 89.3% accuracy
  - Inferring accuracies for choice A, B, and C are 86%, 86%, and 96%
  - We can observe our system achieves accuracies of 93.3%, 86.7%, 70%, 93.3%, and 91.7% when excluding one user for training and testing their data against our model

Preliminary Conclusion

- Analysis of eye gazing patterns thus far has proved to be very accurate
- Based on the location of the next button on the screen, we can see which answer the user selects prior to moving to the next question
- We are currently analyzing other algorithms to attempt to improve our results