Attack Model of YOU CAN'T HIDE BEHIND YOUR HEADSET: USER PROFILING IN AUGMENTED AND VIRTUAL REALITY

Kyu Park, Dingyi Sun, Kendrick Xie

Part 1: Topic Review

- SoK: Data Privacy in Virtual Reality
  - In VR, individual's sensitive data attributes are at risk of exposure. Unlike other internet platforms defenses like Tor, VPNs, proxies, and incognito mode are not commonplace.
- FaceMic: Inferring Live Speech and Speaker Identity via SUbtle Facial Dynamics Captured by AR/VR Motion Sensors
  - Leverage speech-associated facial dynamics captured by zero-permission motion sensors in AR/VR headsets to infer sensitive information (gender, identity, speech content) from individuals using voice interfaces
  - Defenses: Disabling motion sensors is not practical. Use sensory noises or ductile materials to obfuscate facial vibrations and limit sampling rate of accelerometer and gyroscope. Still may have usability issues and low-frequency facial movements can still be used to derive sensitive information.
- You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality
  - Profile users based on VR motion data (i.e., age, gender)
  - Defenses: no direct defense presented, but suggest supporting privacy by default such as through incognito metaverse or privacy-preserving measures on daily usage systems
- Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality
  - Infer user identity from a group of users based on VR body motion and relations
  - Defenses: Identification is framed as a feature for authentication or environment adaptation so none are presented. General support for privacy by default still applies.

Part 2. Summary of the Attack Model

- The paper “You Can’t Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality” demonstrates the feasibility of user profiling in AR and VR motions leveraging machine learning to identify users and infer their individual attributes (i.e., age, gender)
- Users’ head, controller, and eye movements, we investigate the ease of pro- filing on several tasks (e.g., walking, looking, typing) under different mental loads. Our contribution gives significant insights into user profiling in virtual environments.
- We use the same attack model from “You Can’t Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality”, attempt to infer one’s personal information, gender, from user’s captured VR motion.

Attack Model Process

1. Data Collection
    a. Total 54 data sets from 9 male and 9 female were collected
    b. Participants were asked to walk normally drawing a circle
    c. Their head position, angVel, controller position and angVel were collected
2. Data Processing
    a. Raw data were processed into mean, standard deviation, quantile and entropy
    b. All data sets were randomly distributed into training/test sets
3. Machine Learning
    a. Random Forest ML model was trained using the training sets
    b. The ML model predicted one's gender given one's walking data

Evaluation

- Total 41 sets (22 Female, 19 Male) were used to train the model
- Total 13 sets (5 Female, 8 Male) were used to test the accuracy of the model
- The accuracy of the model and F1 score was measured to assess the effectiveness of the attack model

Results

```
Training time: 0.7308773994445801 seconds
Testing time: 0.2119276523590088 seconds

Random Forest accuracy: 0.8461538461538461

Confusion Matrix:
 [[7 1]
 [1 4]]

F1 score: 0.8000000000000002
```

	True Class		
Predicted Class		Male	Female
	Male	7 (TP)	1 (FP)
	Female	1 (FN)	4 (TN)

Conclusion/Limitation

- **We were able to demonstrate the feasibility of the attack model, predicting one's gender from one's VR activity**
- Low number of sample
- Unlike the paper, we only used one ML algorithm of Random Forest method instead of using all four of Logistic Regression, Ridge, Decision Tree and Random Forest
- Unlike the paper, we only focused on one simple task of walking, and only predicted one's gender
- Unlike the paper, we could not leverage the eye tracking sensor (Oculus Quest 2 does not have eye tracking sensor)