Privacy Leakage Study and Protection for Virtual Reality Devices

Dirk Catpo Risco, Brody Vallier, Emily Yao

7 August 2024

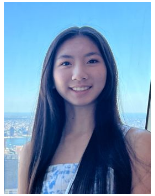
Project Advisor: Prof. Yingying (Jennifer) Chen
PhD Students as Mentors: Changming Li, Honglu Li, Tianfang Zhang

Introducing the Team Members

Students:

Dirk Catpo Risco
RU ECE MS

Brody Vallier
RU ECE UG



Emily Yao
HTHS HS

Mentors:

Changming Li
RU ECE PhD

Honglu Li
RU ECE PhD

Tianfang Zhang
RU ECE PhD

Advisor:

Prof. Yingying
(Jennifer) Chen

Motivation

- AR/VR devices have attracted millions of users and facilitate a broad array of emerging AR/VR applications
- As a key component for motion tracking, Inertial Measurement Unit (IMU) consists of an accelerometer for measuring acceleration and a gyroscope for detecting rotations
- Both sensors are present in each controller and the Head Mounted Display (HMD)

Gaming

Shopping

Banking

Education

Objectives

- Data from zero-permission motion sensors encodes various types of the user’s private information, such as activity information and preferences

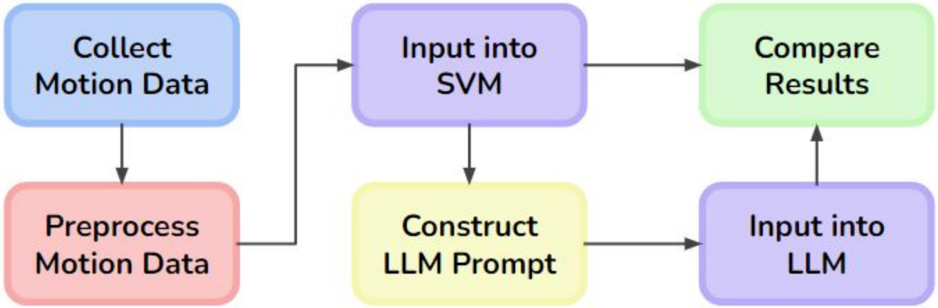
- This project aims to study the sensor data management in commercial AR/VR headsets and analyze the potential of private information leakage

Methodologies

- Investigate privacy leakage in Augmented Reality (AR)/Virtual Reality (VR) devices
- Extract data from the IMU on AR/VR headset and controllers for Human Activity Recognition (HAR)
- Use Support Vector Machine (SVM) and Large Language Model (LLM) to show how IMU data maliciously exposes activities of victim users

Attack Illustration

- Utilize SVM as a baseline model to identify effective statistical features (e.g., mean, max, etc.) from motion data to recognize human activity
- Design LLM prompts based on the effective statistical features
- If LLM achieves comparable accuracy to SVM on motion prediction, it validates that adversaries could expose victim's motion status without requiring data from victims

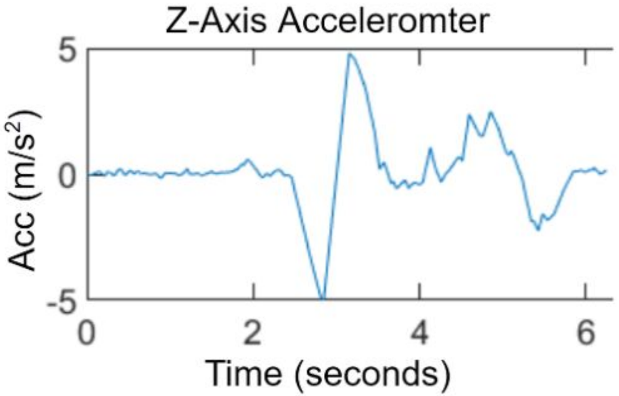


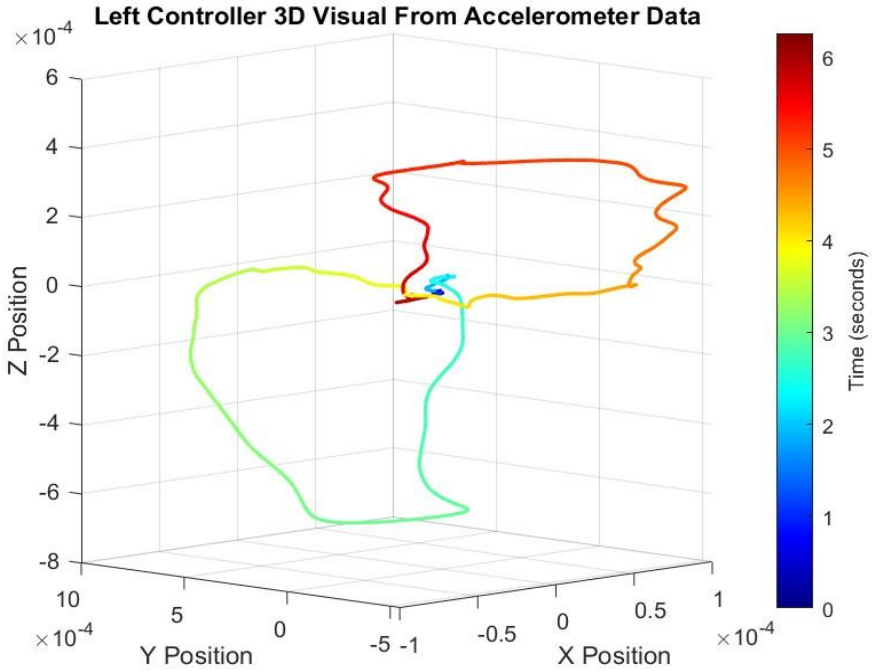
Motion Data Preprocessing

- Denoise and smooth data to generate accurate waveforms
- Compute 3D trajectories to visualize the motions

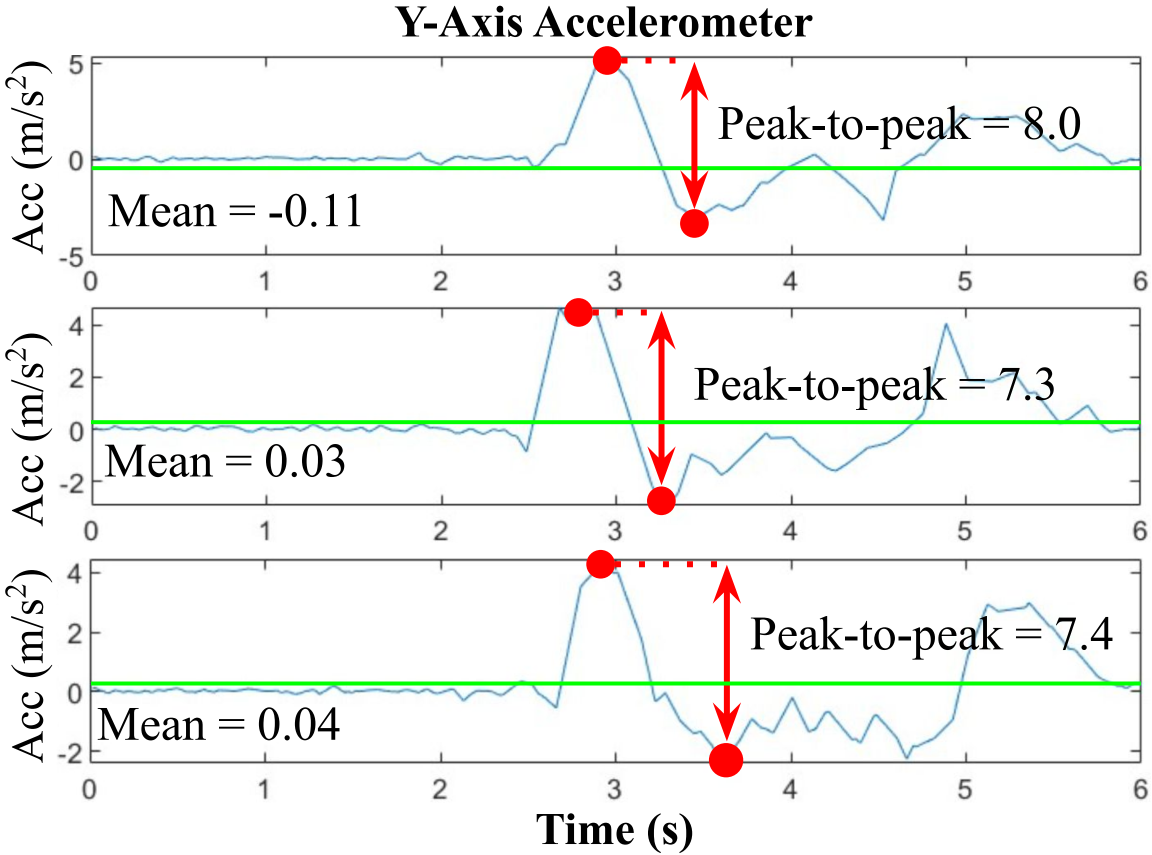
Example: Side Raise

Motion data matches activity pattern





Feature Extraction for SVM

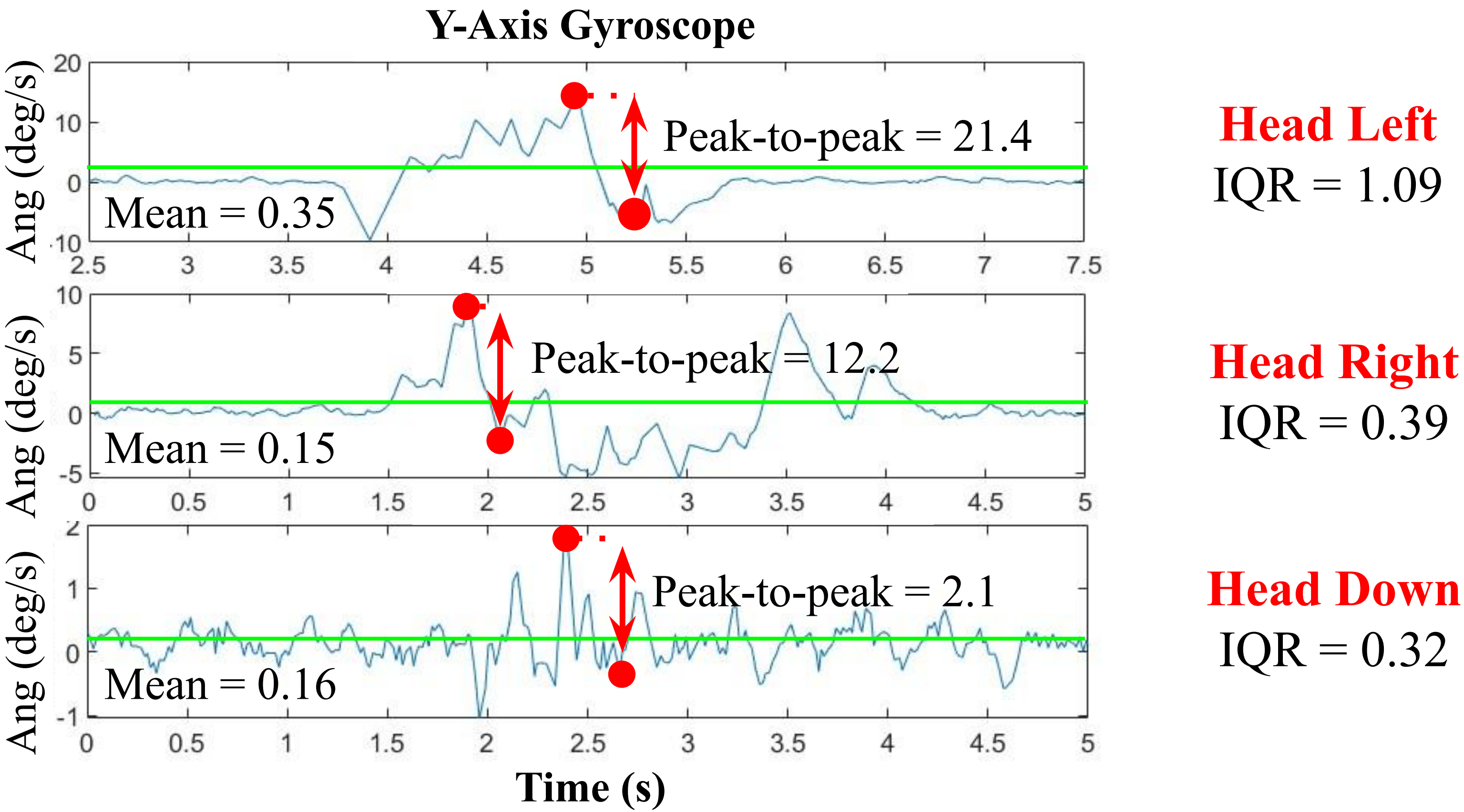


Front Raise #1
IQR = 0.16

Front Raise #2
IQR = 0.21

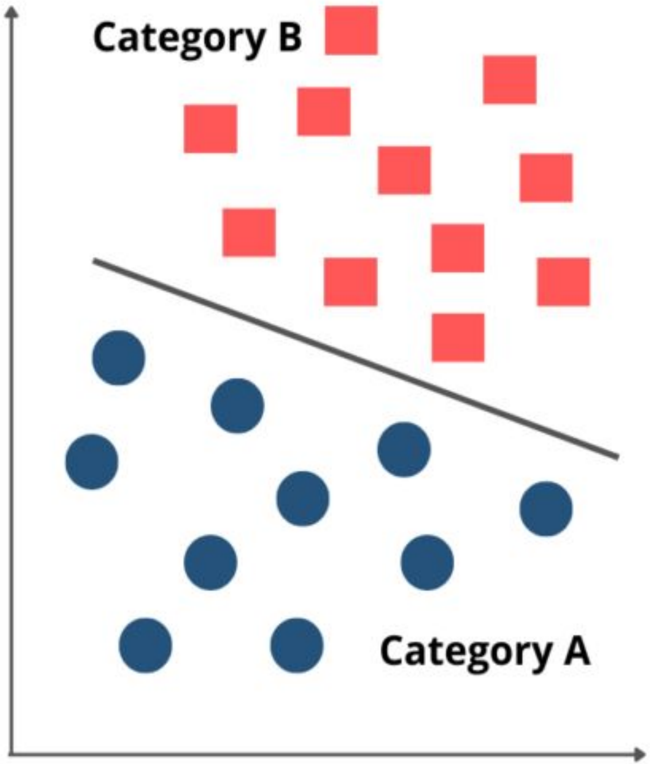
Front Raise #3
IQR = 0.21

Feature Extraction for SVM



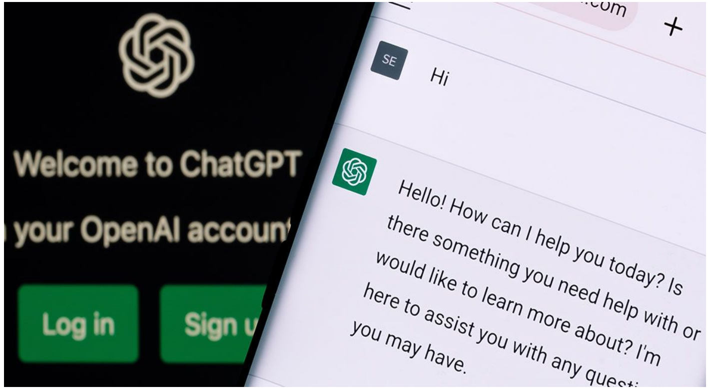
Support Vector Machine (SVM)

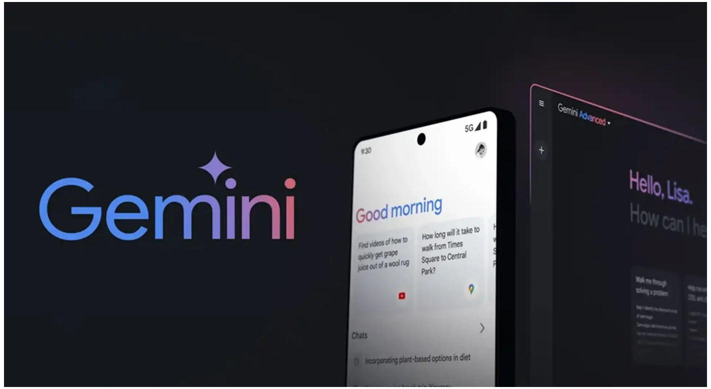
- An effective machine learning algorithm to find a hyperplane that separates classified data points
- Works well on accurately classifying motion sensor data
- Adversaries may require a huge amount of data from victim users during model training for accurate prediction



Large Language Model (LLM)

- Works well on recognizing human language and other complex tasks
- Can understand data and reproduce required outputs with designated prompts
- Pre-trained on vast amounts of data, adversaries may require no training data from victim users to accurately expose human motions





Experimental Setup

- Using Android Studio, we develop an application to extract data from the IMU sensors on Head-Mounted Display (HMD) and controllers of Meta Quest

```
    //ovrTracking2 tracking2 = vrapi_GetPredictedTracking2(appState->Ovr, current_time);
    ovrTracking tracking2 = vrapi_GetPredictedTracking(appState->Ovr, current_time);
    double x_acc = tracking2.HeadPose.LinearAcceleration.x;
    double y_acc = tracking2.HeadPose.LinearAcceleration.y;
    double z_acc = tracking2.HeadPose.LinearAcceleration.z;

    double x_gyro = tracking2.HeadPose.AngularAcceleration.x;
    double y_gyro = tracking2.HeadPose.AngularAcceleration.y;
    double z_gyro = tracking2.HeadPose.AngularAcceleration.z;

    ALOGV("Acceleration %f %f %f %f", current_time, x_acc, y_acc, z_acc);
    ALOGV("Gyroscope %f %f %f %f", current_time, x_gyro, y_gyro, z_gyro);

    prev = current_time;
};
```

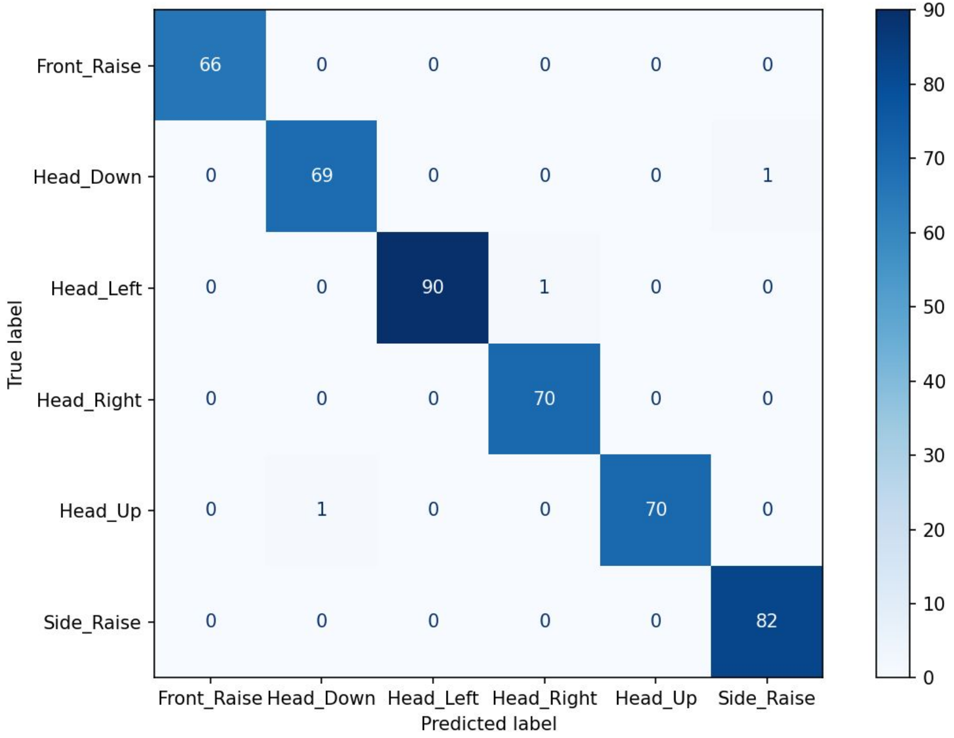
Experimental Setup

- We designed 6 activities for evaluation, including two hand-related activities and four head-related activities

Activity Inference Using SVM

- 3 statistic features (mean, peak-to-peak, and interquartile range) are extracted from the motion sensor data

- The overall accuracy of exposing 6 types of activities using SVM achieves 99.33%



Activity Inference Using LLM

- Developed a prompt for Gemini Advanced to understand the motion data
  - Explained the goal of the task and data types to be received
  - Asked LLM to extract features from the data and provided specific knowledge about how to utilize the features
  - Provided a response structure for results

1. **HMD Accelerometer**: Measures linear acceleration.

Data: Time (s); x, y, and z-axis coordinates (m/s^2).

Interpretation: Acceleration values between -0.8 m/s^2 and 0.8 m/s^2 indicate the head is stable. Values below -0.8 m/s^2 and above 0.8 m/s^2 indicate head movement.

Example prompt for specifying accelerometer readings

Activity Inference Using LLM

- Using our prompt with Gemini Advanced, we achieve 90.6% accuracy

Gemini Advanced Accuracy						
Trial #	**Front Raise**	**Side Raise**	**Head Left**	**Head Right**	**Head Up**	**Head Down**
1					H	
2			H		H	
3					L	
4				H	H	
5				H	H	
6				H	H	
7			H	H	H	
8			H	R		
9				H		
10				H		
Accuracy (%)	100	100	90	76.7	76.7	100
Key	Accurate (3/3)	Partial (2/3)	Inaccurate (1/3)	None (0/3)	**Total (%)**	90.6

H = Head L = Left Hand R = Right Hand

Conclusion and Future Work

- With designated prompt, LLM achieves an accuracy similar to SVM, indicating the potential activity information leakage without training effort using LLM

- With further prompt fine-tuning, the adversaries could realize stronger activity exposure attack using LLM

Thank You for Your Time

Scan for
Project Website
$\rightarrow \rightarrow \rightarrow$

Questions?