AR PRIVACY & SECURITY: FALL FINAL UPDATES

Casie Peng & Allie Craddock

REVIEW

- **Exploit Location Types of AR Users**
- **Use Performance Indicators of the AR Headset to Predict Location Features**
- **Magic Leap 2 Headset**
- **Two Avenues of Exploration:**
  - “Breaking into” the headset (develop spyware program which creates mesh scans)
  - Analyzing data once access is given

RELATED RESEARCH

It’s All In Your Head(set):

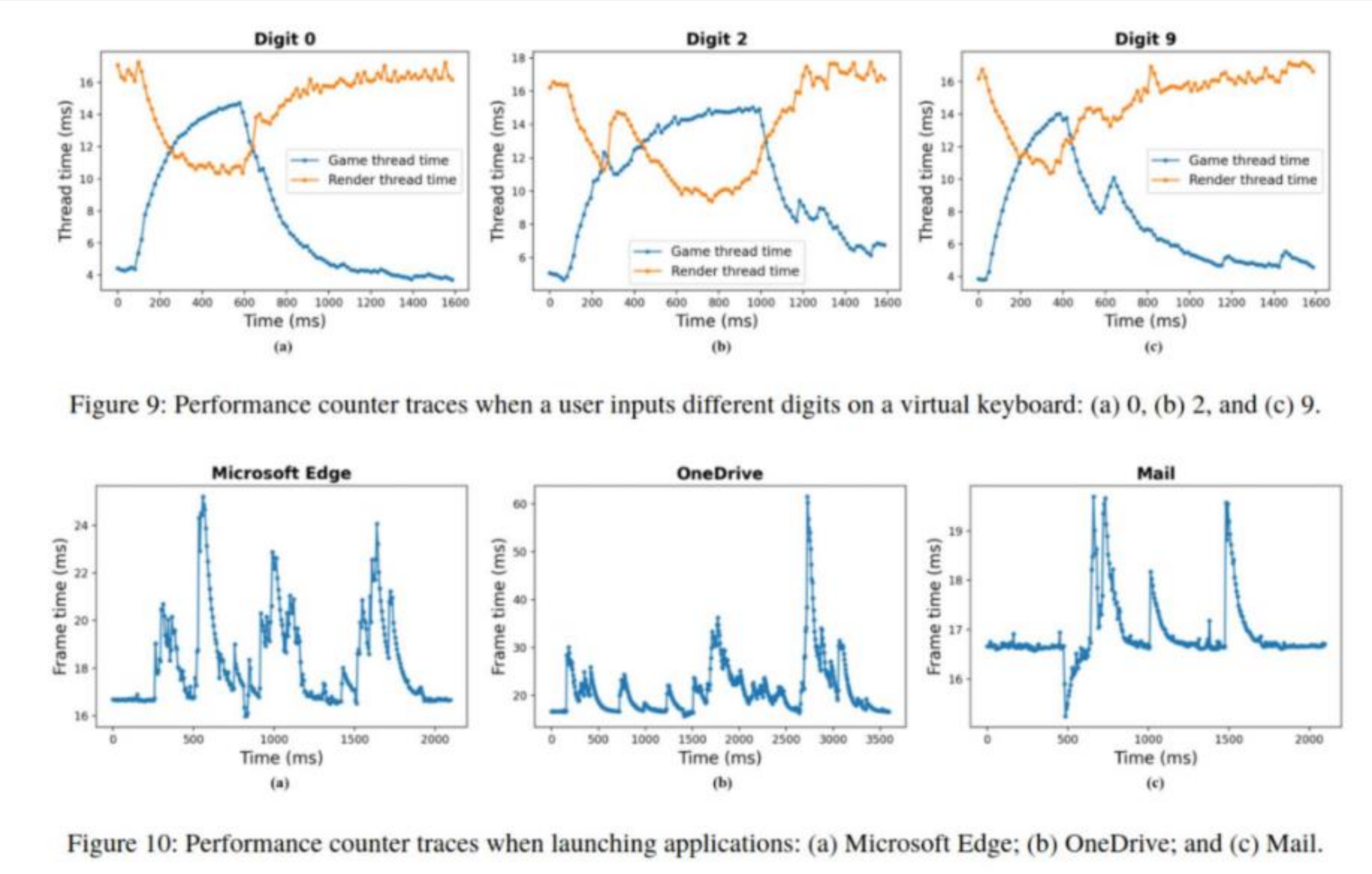


Figure 9: Performance counter traces when a user inputs different digits on a virtual keyboard: (a) 0, (b) 2, and (c) 9.

Figure 10: Performance counter traces when launching applications: (a) Microsoft Edge; (b) OneDrive; and (c) Mail.

APPROACHES/ RESOURCES

“Breaking In” the ML2

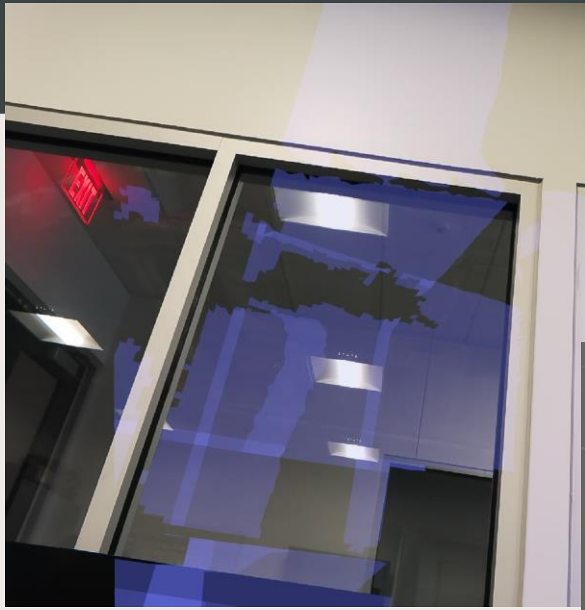
- Unity
- ML2
- Meshing Game Program
- Newman Library Virtual Environments Studio

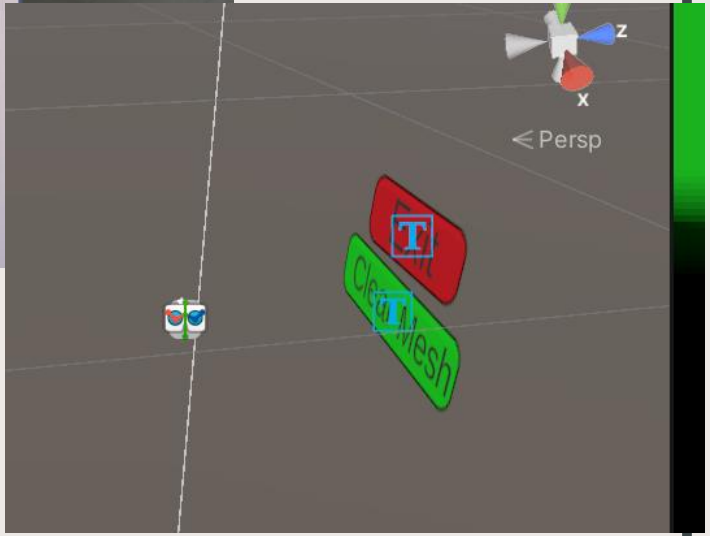
Analyzing Performance Indicators

- Matplotlib
- Pandas
- VSCode
- GitHub

UNITY: PROJECT BUILDING

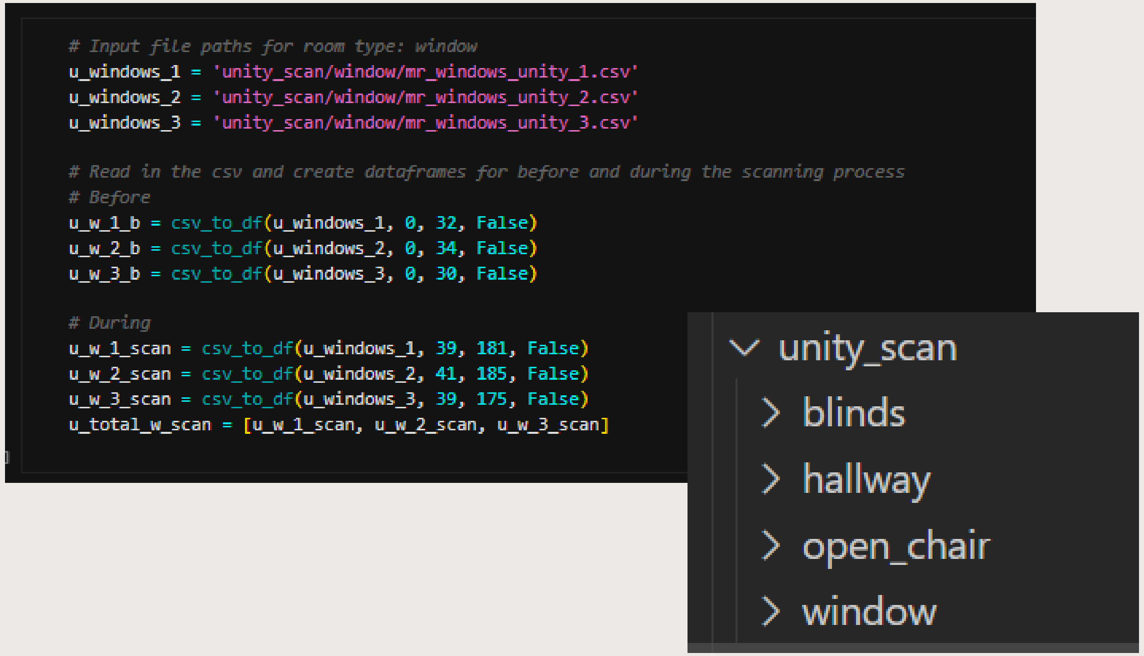
- Created Spatial Meshing App using Unity
- Redid the meshing color to be more visible
  - Blue transparent color
- Created exit and clear buttons in project
  - Will work on making them work





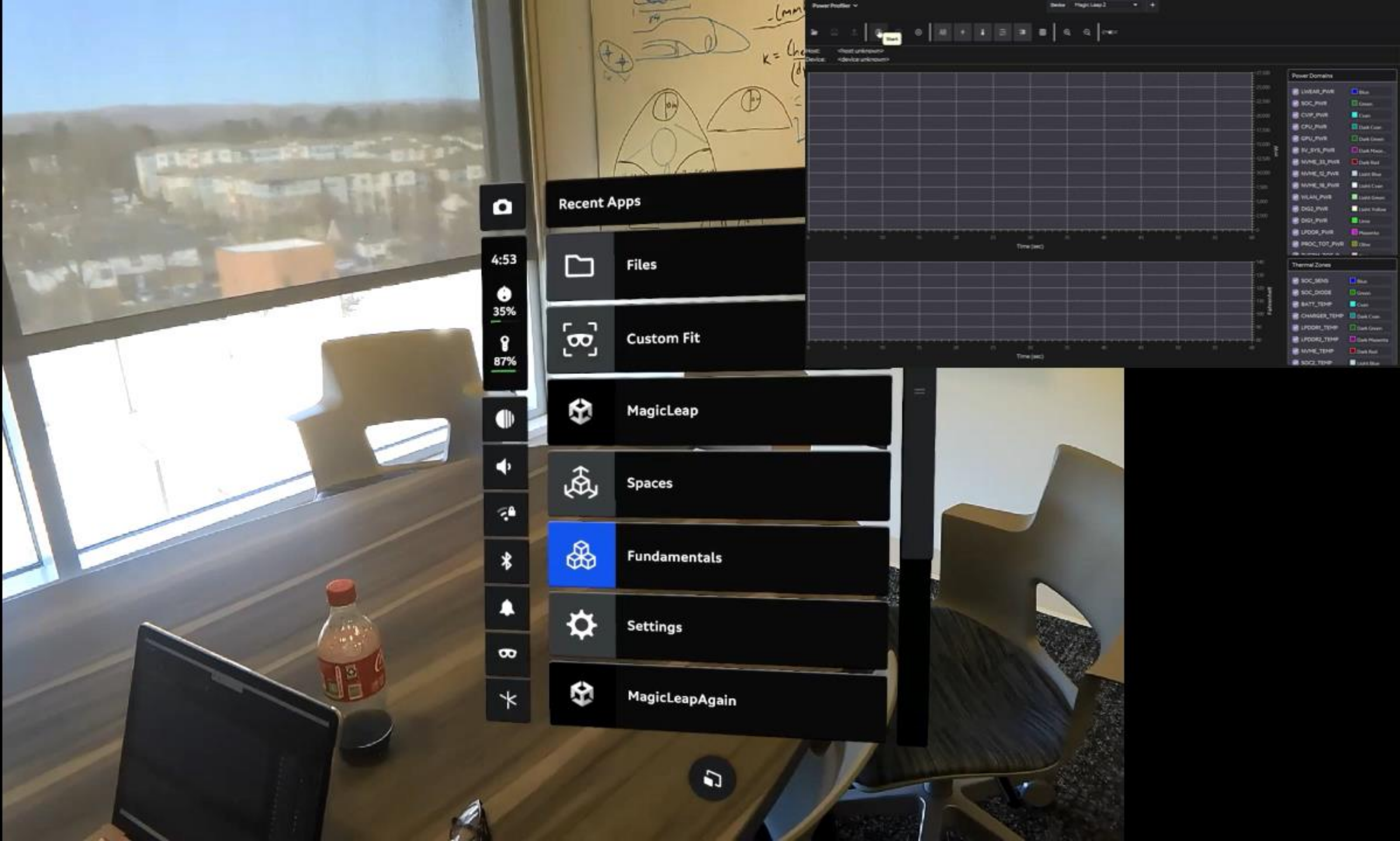
UNITY: DATA COLLECTION

- Scanned various areas (ex. Meeting rooms, hallways, etc)
- Sent the data into the shared VSCode to be compared with the Magic Leap Scanning feature and analyzed
  - CSV, PTP, and PNG (for time)

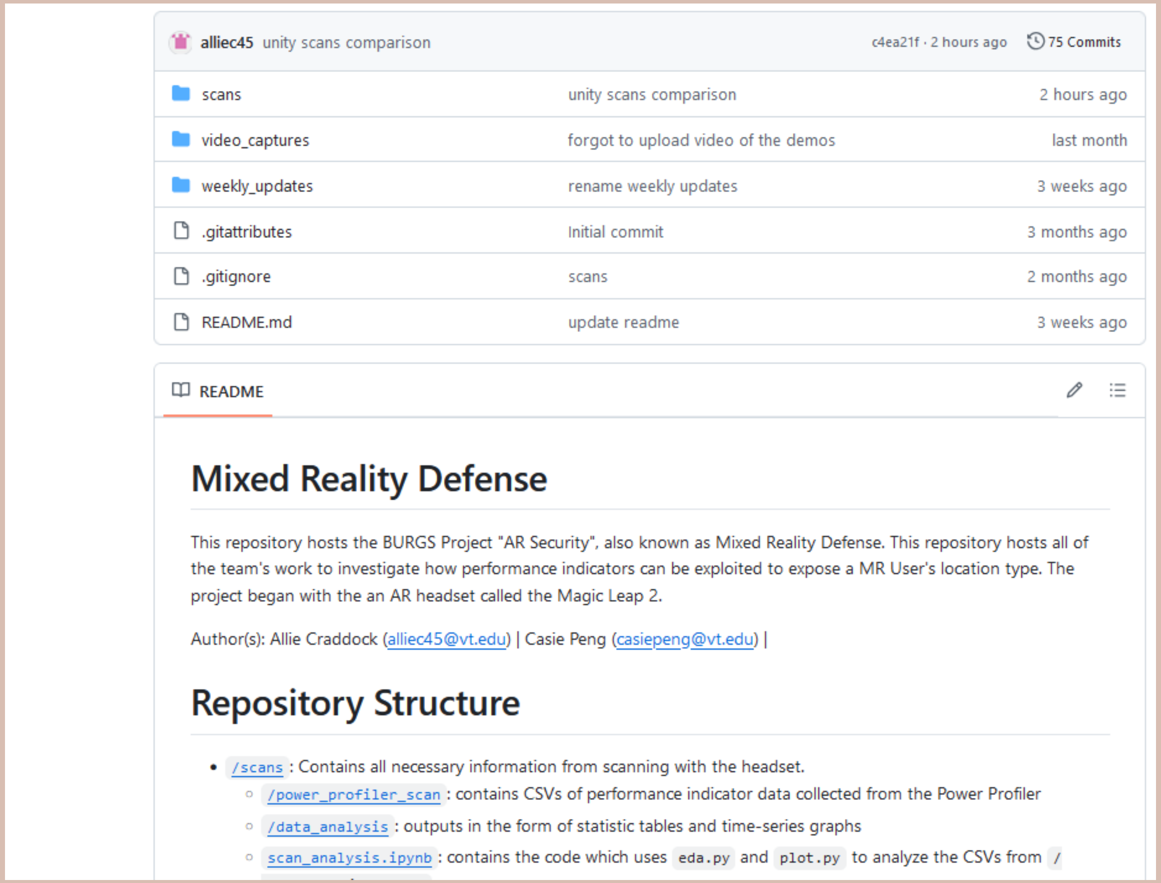


```
# Input file paths for room type: window
u_windows_1 = 'unity_scan/window/mr_windows_unity_1.csv'
u_windows_2 = 'unity_scan/window/mr_windows_unity_2.csv'
u_windows_3 = 'unity_scan/window/mr_windows_unity_3.csv'

# Read in the csv and create dataframes for before and during the scanning process
# Before
u_w_1_b = csv_to_df(u_windows_1, 0, 32, False)
u_w_2_b = csv_to_df(u_windows_2, 0, 34, False)
u_w_3_b = csv_to_df(u_windows_3, 0, 30, False)

# During
u_w_1_scan = csv_to_df(u_windows_1, 39, 181, False)
u_w_2_scan = csv_to_df(u_windows_2, 41, 185, False)
u_w_3_scan = csv_to_df(u_windows_3, 39, 175, False)
u_total_w_scan = [u_w_1_scan, u_w_2_scan, u_w_3_scan]
```

```
∨ unity_scan
  > blinds
  > hallway
  > open_chair
  > window
```


Power Profiler
Magic Leap 2
Host: <host unknown>
Device: <device unknown>
Time (sec)
Time (sec)
Power Domains
LWEAR_PWR Blue
SOC_PWR Green
CVIP_PWR Cyan
CPU_PWR Dark Cyan
GPU_PWR Dark Green
5V_SYS_PWR Dark Magen...
NVME_33_PWR Dark Red
NVME_12_PWR Light Blue
NVME_18_PWR Light Cyan
WLAN_PWR Light Green
DIG2_PWR Light Yellow
DIG1_PWR Lime
LPDDR_PWR Magenta
PROC_TOT_PWR Olive
Thermal Zones
SOC_SENS Blue
SOC_DIODE Green
BATT_TEMP Cyan
CHARGER_TEMP Dark Cyan
LPDDR1_TEMP Dark Green
LPDDR2_TEMP Dark Magenta
NVME_TEMP Dark Red
SOC2_TEMP Light Blue
4:53
35%
87%
Recent Apps
Files
Custom Fit
MagicLeap
Spaces
Fundamentals
Settings
MagicLeapAgain

AR SECURITY REPOSITORY PROJECT



alliec45 unity scans comparison c4ea21f · 2 hours ago 75 Commits

scans	unity scans comparison	2 hours ago
video_captures	forgot to upload video of the demos	last month
weekly_updates	rename weekly updates	3 weeks ago
.gitattributes	Initial commit	3 months ago
.gitignore	scans	2 months ago
README.md	update readme	3 weeks ago

README

Mixed Reality Defense

This repository hosts the BURGS Project "AR Security", also known as Mixed Reality Defense. This repository hosts all of the team's work to investigate how performance indicators can be exploited to expose a MR User's location type. The project began with the an AR headset called the Magic Leap 2.

Author(s): Allie Craddock (alliec45@vt.edu) | Casie Peng (casiepeng@vt.edu) |

Repository Structure

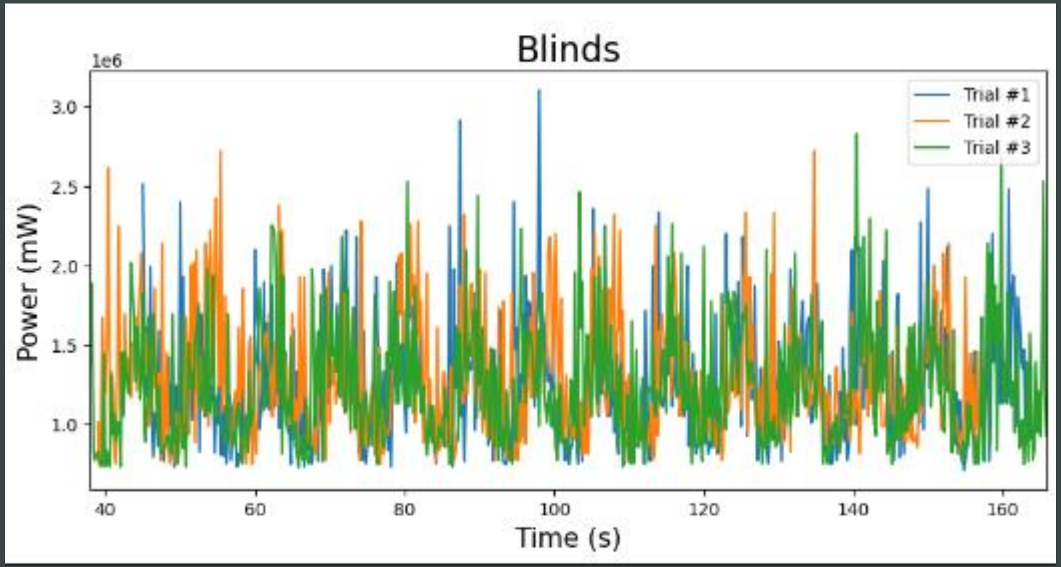
- `/scans` : Contains all necessary information from scanning with the headset.
  - `/power_profiler_scan` : contains CSVs of performance indicator data collected from the Power Profiler
  - `/data_analysis` : outputs in the form of statistic tables and time-series graphs
  - `scan_analysis.ipynb` : contains the code which uses `eda.py` and `plot.py` to analyze the CSVs from `/`

Completed:

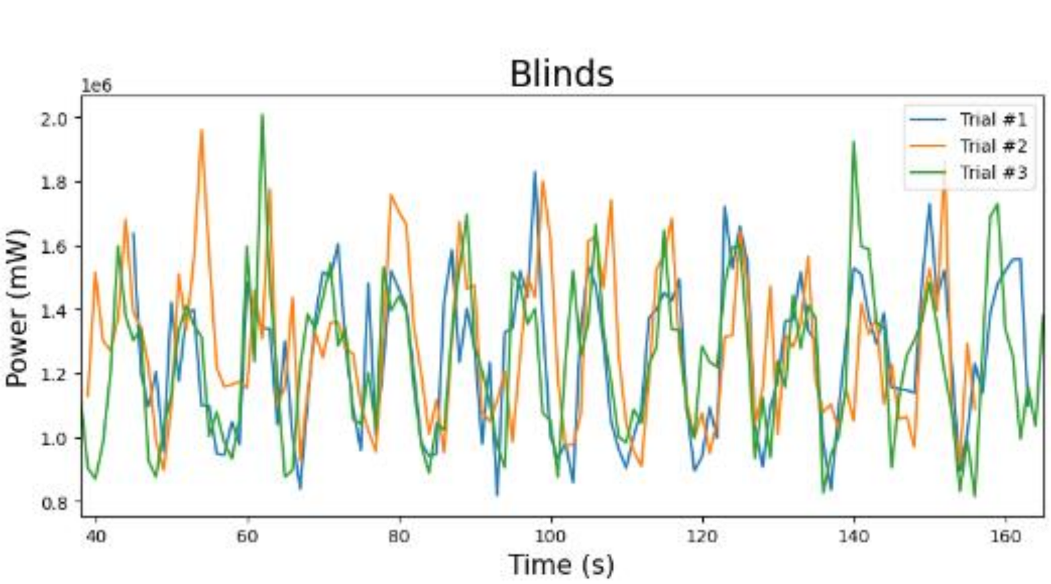
- Repository organization
- Documentation
- Separated Coding Functionality
  - Eda.py (pandas & exploratory analysis)
  - Plot.py (plotting functions)

WINDOW SLIDING

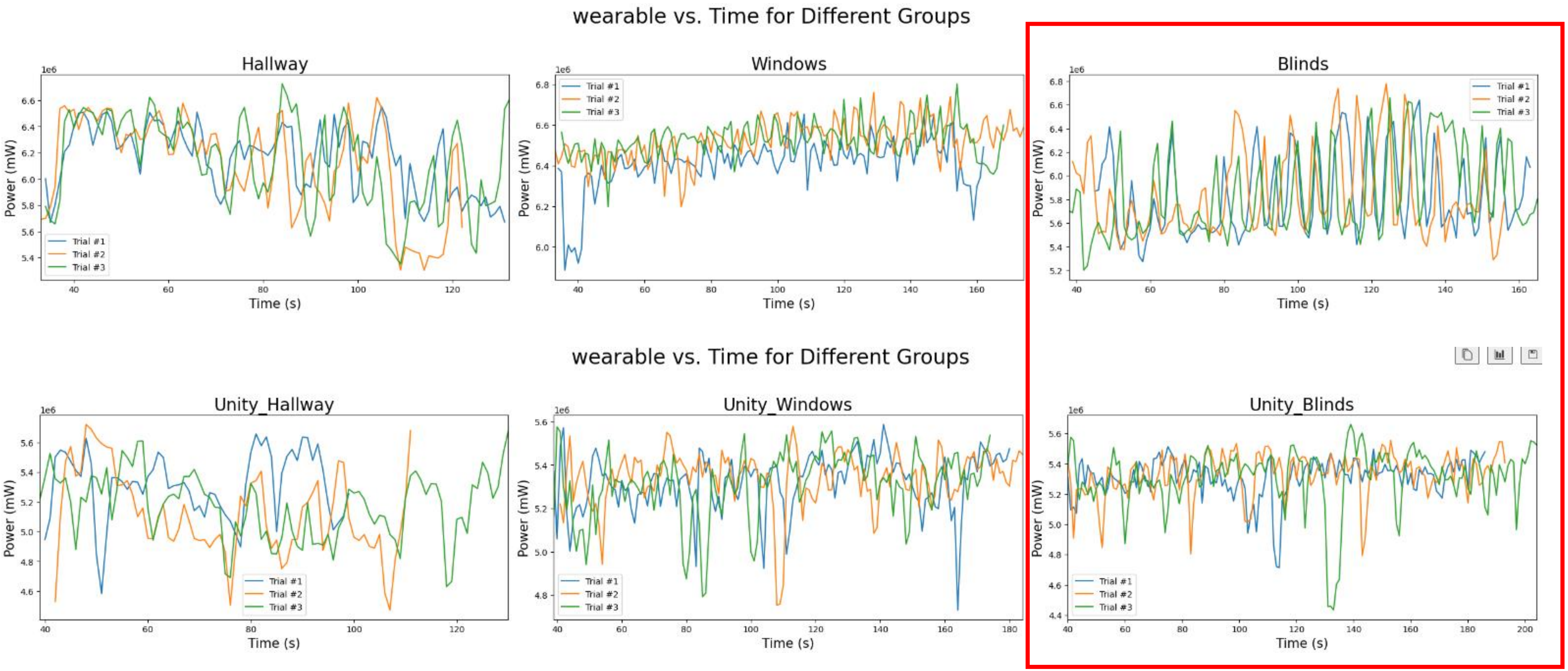
Before (CPU for Blinds Scan)



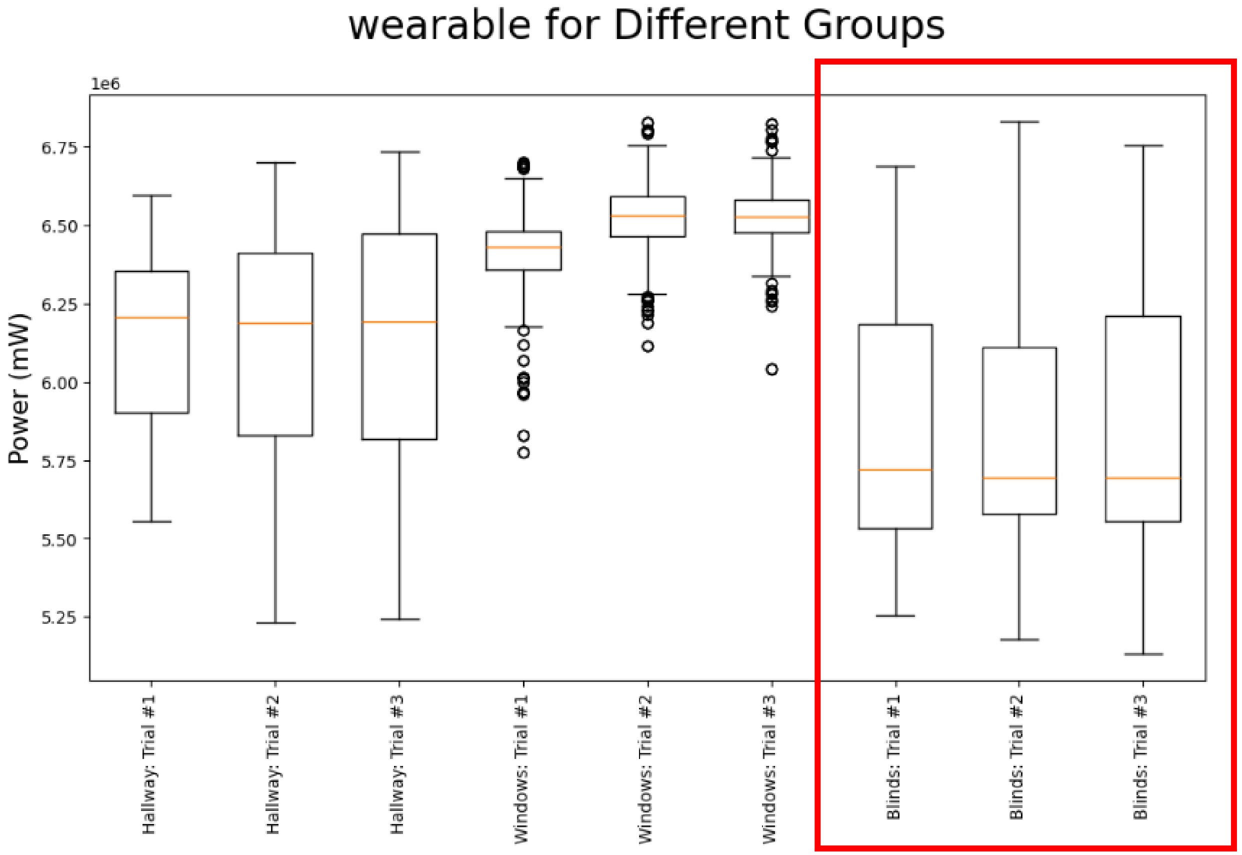
After (CPU for Blinds Scan)

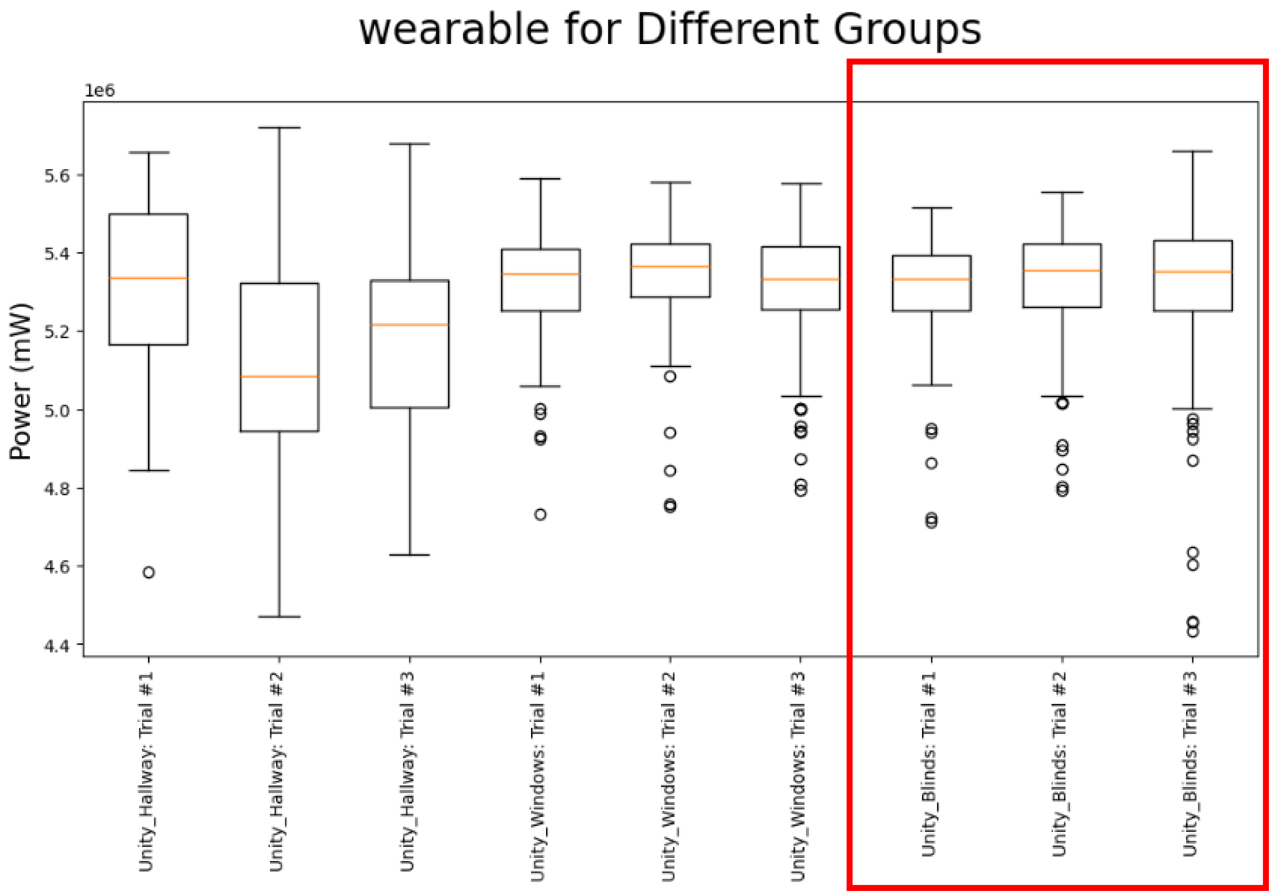


DATA ANALYSIS – TIME SERIES



DATA ANALYSIS – BOXPLOT





CURRENT ISSUES

High-Level Scans / Data Analysis

- Radically different room types result in different performance indicators
- Small changes do not reflect in performance indicators
  - Too much systematic variability
  - Noise greatly affects small scans with minute differences

Technical

- Compatibility issues with headset
- Headset scanning application routinely updates/changes
- Unity documentation outdated
  - ○ ML Unity features deprecated

FUTURE GOALS

“Hacking In” to AR Headset

- Finish Meshing Saving/Clearing/Boundary options for Unity
- Create data collection feature for spyware (Unity) application
- Explore other cyber attacks (EX: Network attacks)

Data Collection & Analysis

- Eventually bring the headset outside
- Add moving objects to rooms
- Narrow on how performance indicators change from headsets with different system components
- Isolate low-level changes in performance indicators
- Use ML models to predict location type

THANK YOU