AR Security

Allie Craddock, Casie Peng

Problem

Location-detection attacks in AR systems using performance indicators

What is Augmented Reality (AR)?

Performance Indicators

- Indicate how well different parts of the system is working
  - CPU
  - GPU
  - Framerate
  - Battery Usage
  - Loading times
- Can be obtained by applications, application developers, cyber attackers, and networks

Literature Review

- It's all in your head(set): Side-channel attacks on AR/VR systems

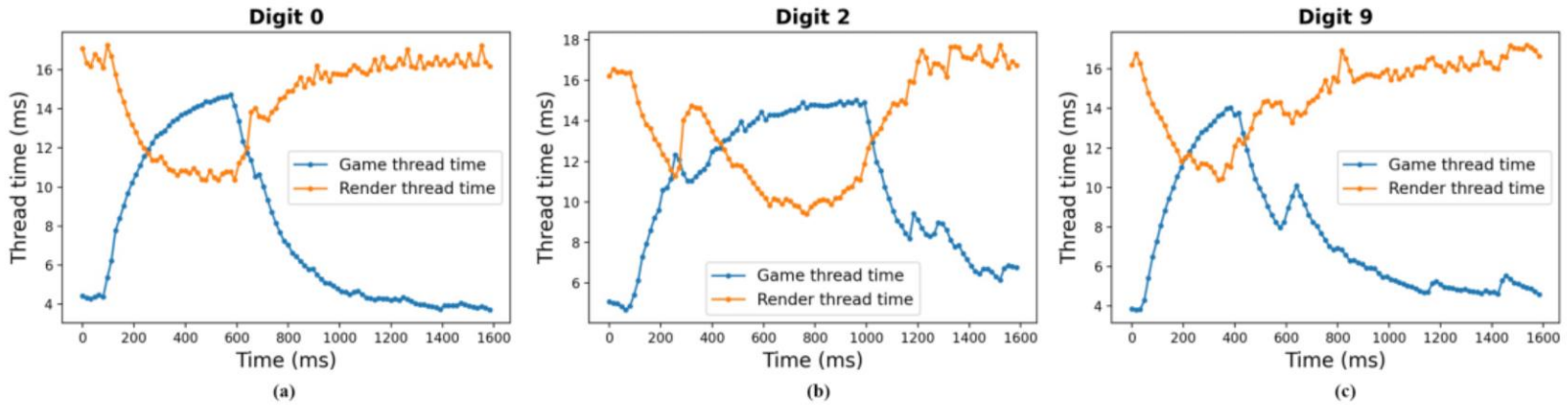


Figure 9: Performance counter traces when a user inputs different digits on a virtual keyboard: (a) 0, (b) 2, and (c) 9.

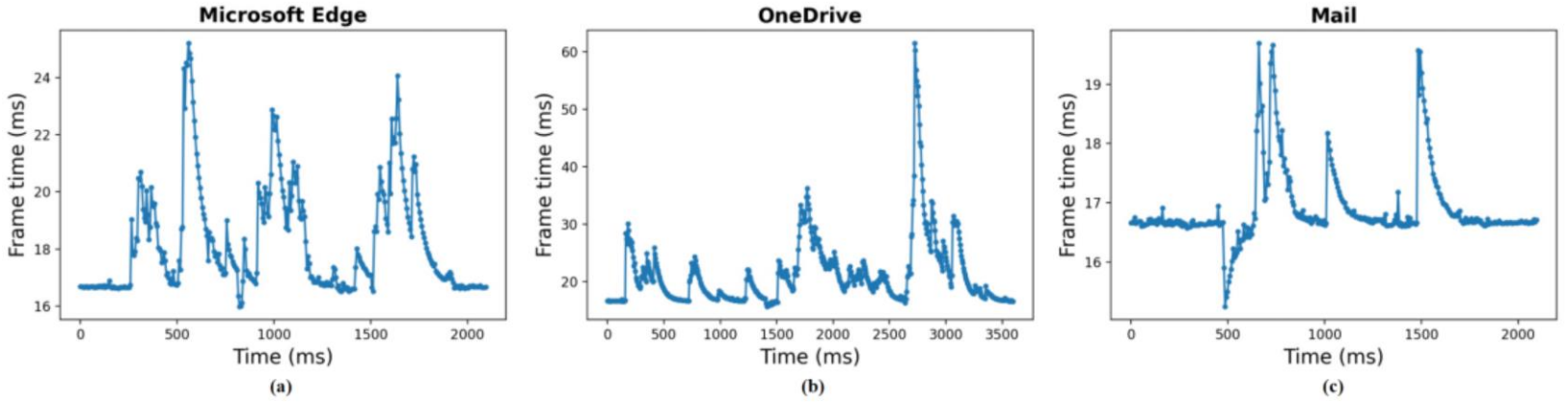


Figure 10: Performance counter traces when launching applications: (a) Microsoft Edge; (b) OneDrive; and (c) Mail.

Approaches/Resources

1

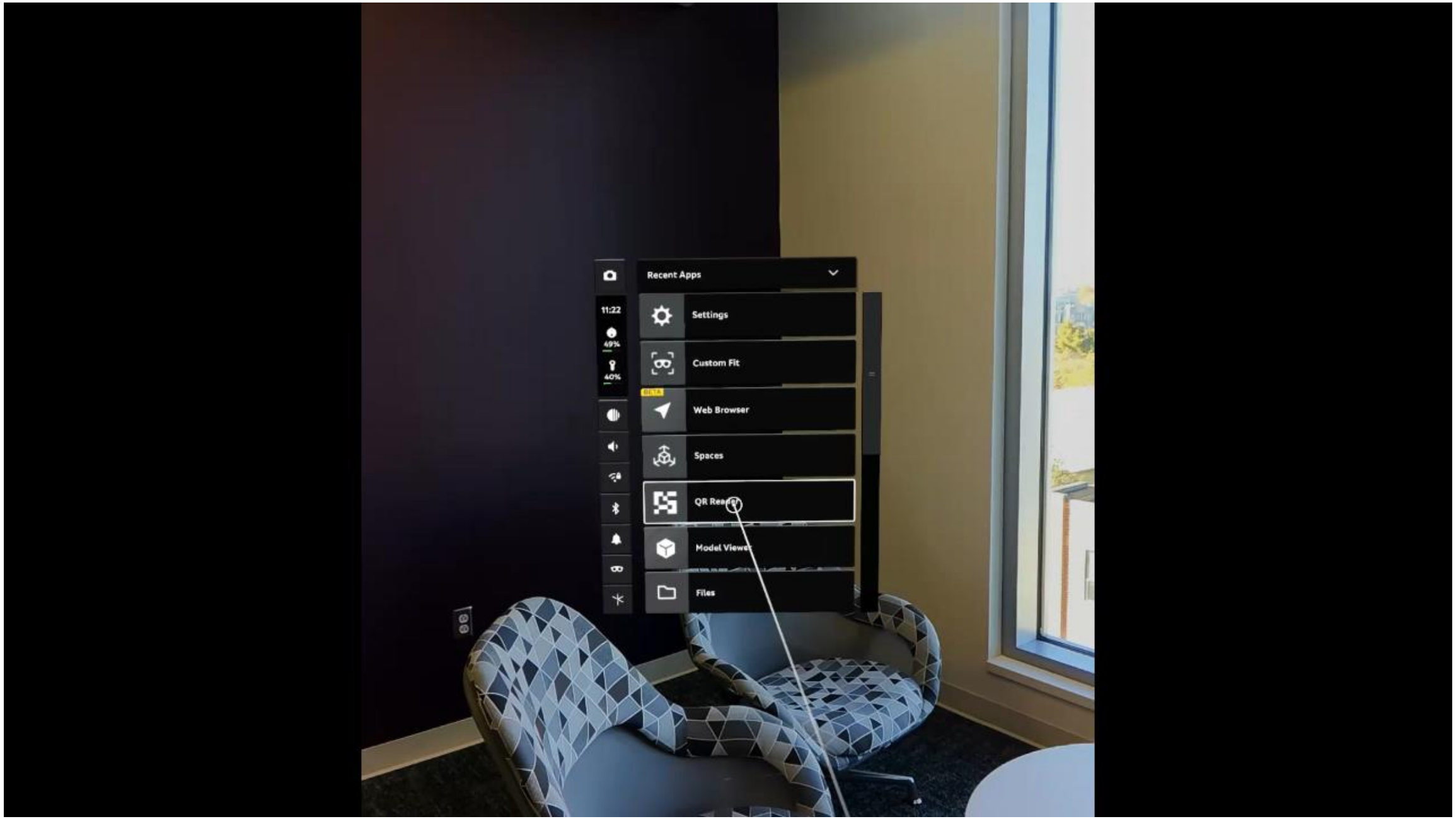
Analyzing Performance Indicators

- Magic Leap 2 Documentation
- ML2H3 Developer Forum
- Power Profiler
- Radeon GPU Profiler
- Pandas
- Matplotlib

2

Accessing the Headset

- VR Library Consultants
- Used Unity courses, documentations, online tutorials
- Magic Leap Documentation
- Unity Profiler


Recent Apps
11:22
49%
40%
Settings
Custom Fit
BETA
Web Browser
Spaces
QR Reader
Model Viewer
Files


Magic Leap Power Profiler
Power Profiler
Device
Magic Leap 2
Host: CasiePC (2024-10-30 11:22:25 173)
Device: GB62XT1101DU (build B3E.230810.09-R.028)
Power Domains
No Entries
mW
Time (sec)
Thermal Zones
No Entries
Fahrenheit
Time (sec)

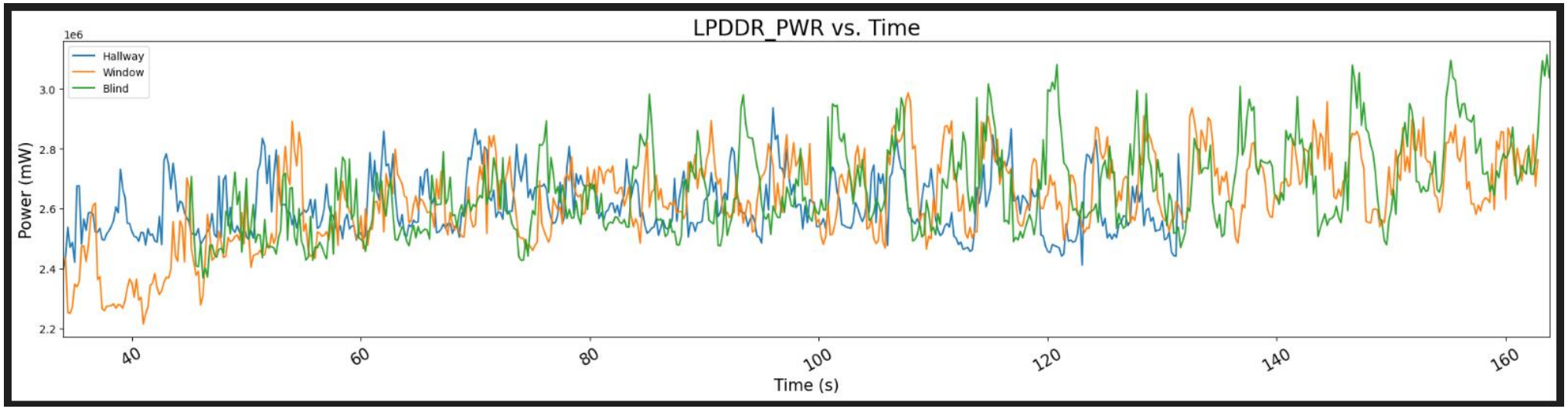
Data Analysis (Pandas)

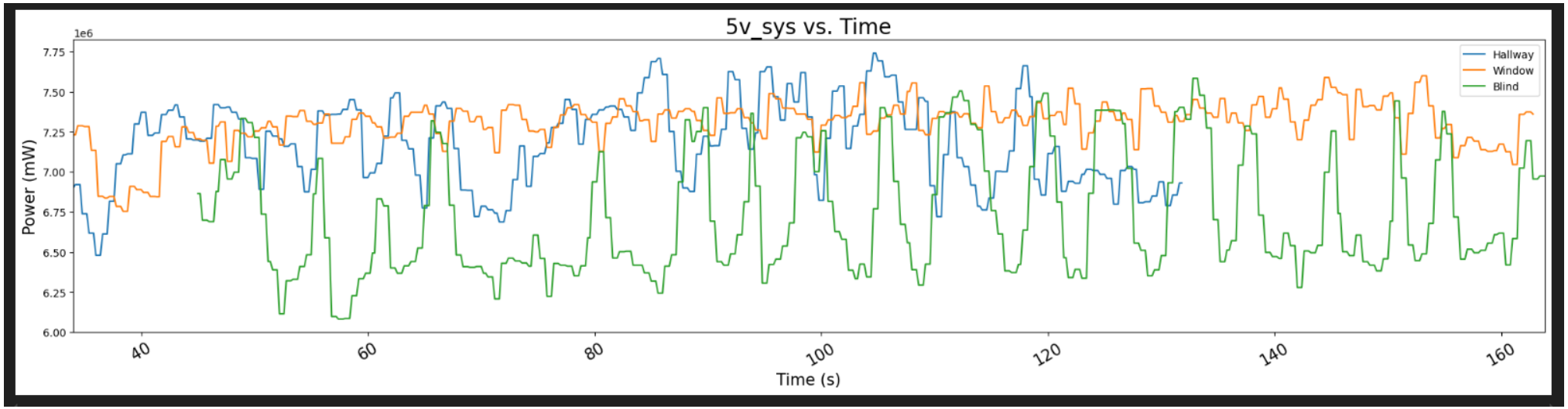
blinds_comb.txt

data_analysis > blinds_comb.txt

Metric	Mean	Median	Standard Deviation
wearable	5.85e+06	5.70e+06	3.84e+05
soc	1.26e+06	1.24e+06	1.64e+05
cvip	1.70e+06	1.63e+06	3.13e+05
cpu	1.26e+06	1.18e+06	3.84e+05
gpu	1.76e+06	1.05e+05	2.31e+06
5v_sys	6.84e+06	6.75e+06	4.13e+05
wlan	2.38e+05	2.33e+05	2.50e+04
nvme_pwr1	1.62e+03	0.00e+00	9.68e+03
nvme_pwr3	3.30e+04	5.00e+03	1.04e+05
nvme_pwr2	6.28e+03	4.00e+03	4.29e+03
vddp_run	6.90e+04	6.80e+04	3.33e+03
vddp_s5	6.84e+04	6.80e+04	1.28e+03
LPDDR_PWR	2.68e+06	2.67e+06	1.48e+05
PROC_TOT_PWR	6.01e+06	4.87e+06	2.35e+06
THERM_TOT_PWR	8.69e+06	7.64e+06	2.36e+06
THERM_TOT_PWR-throttle	2.50e+07	2.50e+07	0.00e+00
Tboard_soc1tmp	1.25e+02	1.24e+02	1.84e+00
Tdiode_soc1tmp	1.23e+02	1.22e+02	2.21e+00
battery	9.12e+01	9.12e+01	3.98e-01
chrgr	1.17e+02	1.17e+02	1.78e+00
ddr1	1.23e+02	1.23e+02	1.95e+00
ddr2	1.21e+02	1.21e+02	1.99e+00
mem	1.14e+02	1.14e+02	1.53e+00
mero2	1.24e+02	1.24e+02	1.99e+00
vrm	1.21e+02	1.20e+02	1.95e+00

Data Analysis (Matplotlib)





Approaches/Resources

1

Analyzing Performance Indicators

- Magic Leap 2 Documentation
- ML2H3 Developer Forum
- Power Profiler
- Radeon GPU Profiler
- Pandas
- Matplotlib

2

Accessing the Headset

- VR Library Consultants
- Used Unity courses, documentations, online tutorials
- Magic Leap Documentation
- Unity Profiler

Profiler

Profiler Modules | Play Mode | Frame: 0 / 0 | Clear | Clear on Play | Deep Profile | Call Stacks

CPU Usage

0.1ms (10000FPS)

- Rendering
- Scripts
- Physics
- Animation
- GarbageCollector
- VSync
- Global Illumination
- UI
- Others

Rendering

- Batches Count
- SetPass Calls Count
- Triangles Count
- Vertices Count

Memory

- Total Used Memory
- Texture Memory
- Mesh Memory
- Material Count
- Object Count

Timeline | Live

againscene1
- Directional Light
- Mapping Permissions
- Meshing Subsystem
- Mesh Parent
- Cube
- XR Rig

Project

Assets > Scripts

MeshingC...

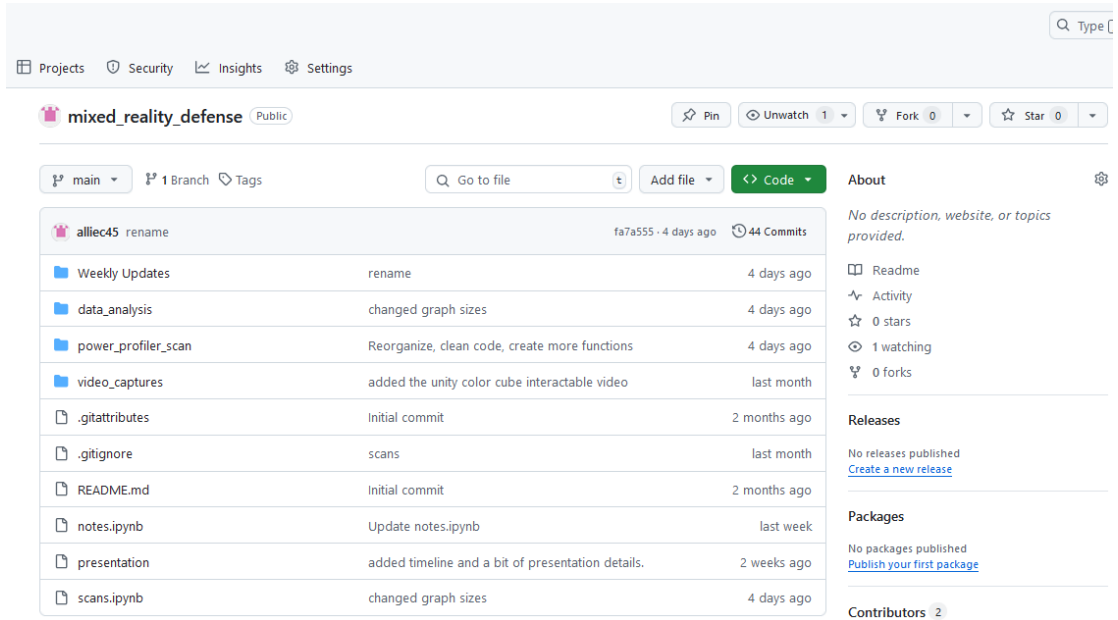
SpatialMa...

Persp

Game

Game | Display 1 | Free Aspect

Documentation



- VSCode
- JupyterNotebook
- GitHub

Current Challenges

- Cleaning visual data
- Power Profiler performance indicator names unclear
  - Requires android-specific profilers
- Debugging my spatial meshing project in Unity
- Magic Leap 2 being discontinued -> many features are being discontinued
  - Incompatible with Unity features & some Profilers
  - Documentation is outdated

Future Goals

- End of Semester Goals:
  - Finalize Unity project that forces the headset to create spatial meshes and record performance indicators
  - Isolating most influential environmental features which cause data leaks
- Future Endeavors:
  - Training an ML Model to predict which room type a user is located based on performance indicators