Spatial Seer: Exploiting Telemetry to Expose XR User Environment

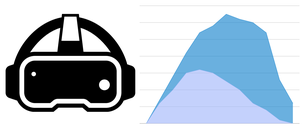
Allie Craddock Gayatri Kamtala
Bo Ji Brendan David-John Margaret Ellis

Motivation

Extended Reality (XR) systems are increasingly being used in healthcare, retail, education, and entertainment industries. Sensitive location information is tracked by these headsets.

Problem: Attackers can exploit side-channel leaks in XR systems to obtain information about a user's location, threatening the privacy and security of the user and surrounding systems.

Cyberattack Intent



Build Virtual Environment

Parallel Profiling

Event-Based API

Exploit Data Leak

Methodology

We tested on the **Meta Quest 3** and **Magic Leap 2** with Unity scan applications.

We scanned 4 or 5 room types, each with 4 different trial conditions:

- Base room architecture
- Object manipulation
- Human interference
- Headset in motion

Implementation

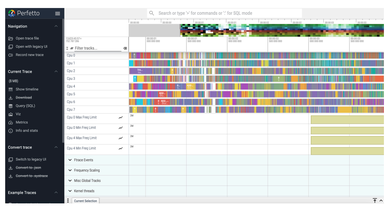
System-Wide Profiling

Perfetto

Traces: time-series telemetry data

↓

Aggregated time series into summary statistics per scan

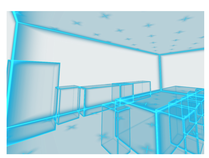


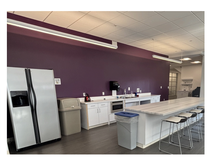
Application-Based Profiling

Unity

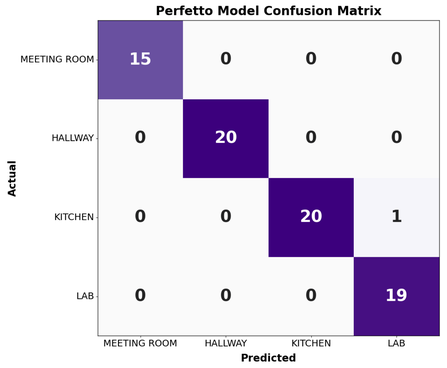
Unity Profiler: tabled performance data

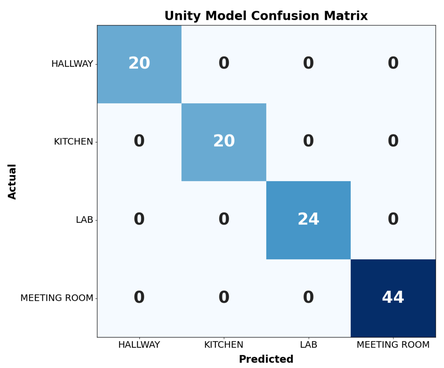
Unity Memory Profiler: snapshots containing memory usage counters





Results





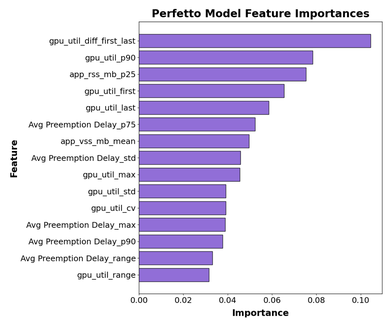
Random Forest Model (300 trees, 30 features)

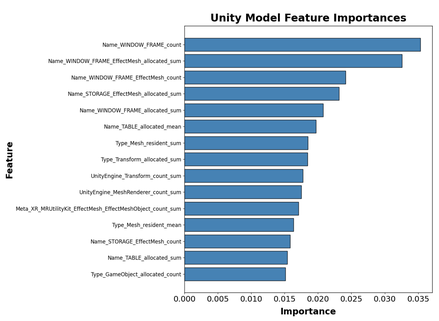
5-Fold Cross-Validation Accuracy:
98.67% ± 2.67%

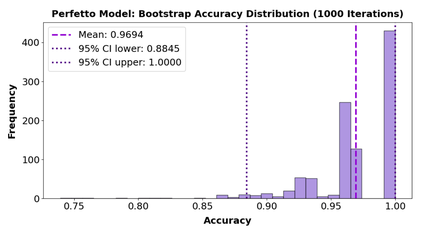
Random Forest Model (100 trees, 194 features)

5-Fold Cross-Validation Accuracy:
100.00% ± 0.00%

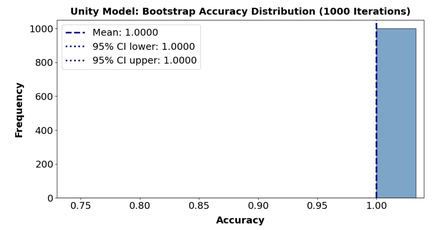
Analysis & Validation







Bootstrapped Mean Accuracy (1000 iterations):
96.94% ± 3.53%



Bootstrapped Mean Accuracy (1000 iterations):
100.00% ± 0.00%

Conclusions

We have high test accuracy for system-wide profiling (98.7%) and application-based profiling (100%), demonstrating noise-robust performance. An attacker with only these metrics could identify a user's room over 98% of the time.

Thus, we can predict room type across multiple headsets and profilers accurately, proving a major risk for XR privacy.

Future Work

- Validate findings across MR and VR applications
- Finalize event-based API to remotely extract profiler data
- Publish workshop paper to relevant conferences

References

[1] Matthew Corbett, Brendan David-John, Jiacheng Shang, and Bo Ji. 2024. ShouldAR: Detecting Shoulder Surfing Attacks Using Multimodal Eye Tracking and Augmented Reality. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 8, 3, Article 97 (September 2024), 23 pages. https://doi.org/10.1145/3678573

[2] Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh. 2023. It's all in your head(set): side-channel attacks on AR/VR systems. In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC '23). USENIX Association, USA, Article 223, 3979–3996.