BURGS Weekly Presentation

Broadening Undergraduate Research Groups

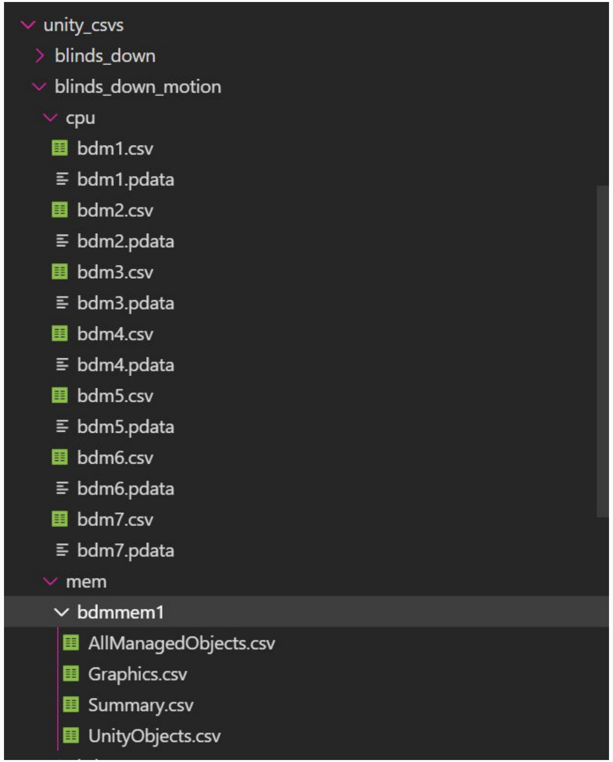
11/21/2025

Allie, Gayatri

Spatial Seer: Data Collection

Unity Profiler & Memory Profiler Data

- 120/120 Trials Collected
- Converted all 200 data points -> 500 CSVs
- Utilized 194 features for our model
    - Example: blinds_down_motion to the right



```
unity_csvs
  blinds_down
  blinds_down_motion
    cpu
      bdm1.csv
      bdm1.pdata
      bdm2.csv
      bdm2.pdata
      bdm3.csv
      bdm3.pdata
      bdm4.csv
      bdm4.pdata
      bdm5.csv
      bdm5.pdata
      bdm6.csv
      bdm6.pdata
      bdm7.csv
      bdm7.pdata
    mem
      bdmmem1
        AllManagedObjects.csv
        Graphics.csv
        Summary.csv
        UnityObjects.csv
```

Spatial Seer: Perfetto Model Pipeline

Data Source:

- Real-time telemetry CSVs from Meta Quest headset via Perfetto
- Time series data with 57 features including GPU metrics, CPU utilization, memory usage, frame timing, etc.
- 75 total scans across 4 room types (kitchen, hallway, lab, blinds/meeting_room)

Data Processing:

- Aggregated time series into summary statistics per scan:
    - Basic: mean, std, min, max, median
    - Spread: range, IQR (interquartile range)
    - Percentiles: p10, p25, p75, p90
    - Shape: skewness, kurtosis, coefficient of variation
    - Time series specific: first, last, diff_first_last, trend (slope), rolling_std, num_changes (direction changes)
- Total ~1,375 features per scan after aggregation

Spatial Seer: Perfetto Model Pipeline

Feature Selection:

- Compared every scan to every other scan (2,099 different-room comparisons, 676 same-room comparisons)
- Calculated discrimination score = diff_room_rate - same_room_rate
- Tested multiple thresholds (5%, 10%, 15%, 20%, 25%, 30%)
- Selected top 30 features with highest discrimination scores including:
    - `gpu_util_diff_first_last`, `Avg Preemption Delay_std`, `gpu_util_iqr`, etc.

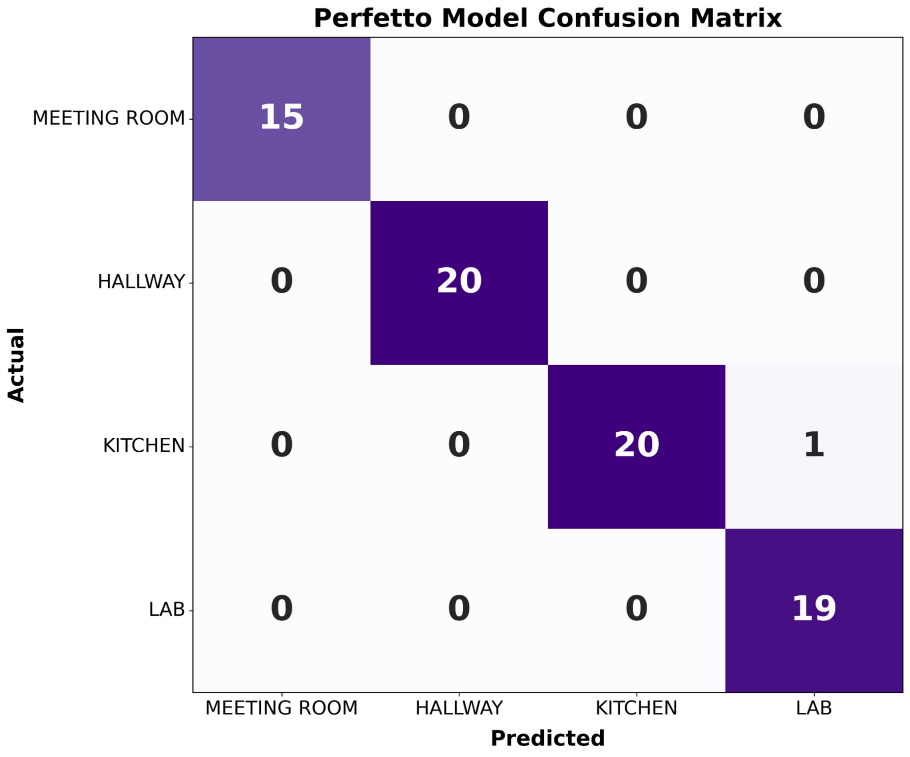
Model Comparison:

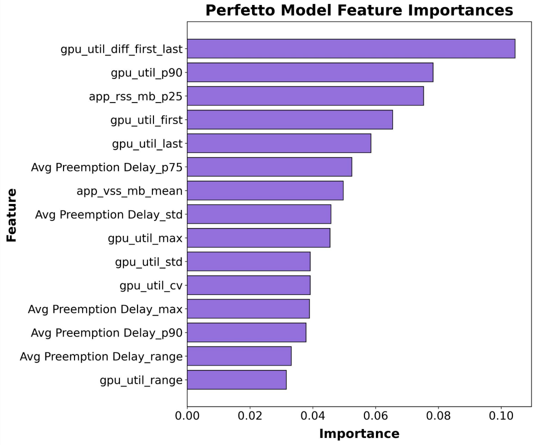
- Tested multiple classifiers: Random Forest (100, 200, 300 trees), Gradient Boosting, SVM (C=1, C=10), KNN (k=3, k=5)
- Tested 12 features vs 30 features
- Best combination: Random Forest (300 trees) with 30 features → 98.67% accuracy

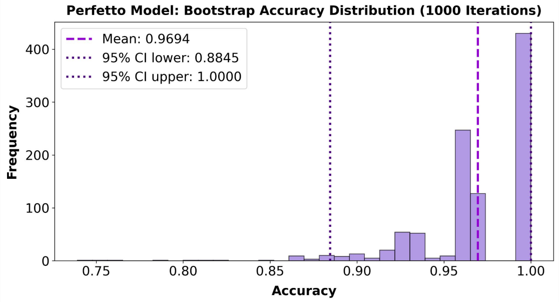
Model Training & Evaluation:

- 5-Fold Stratified Cross-Validation
- Bootstrap validation (1000 iterations) for confidence intervals
- Final model achieved ~96-98% mean accuracy with 95% CI [~83%, 100%]

Spatial Seer: Perfetto Random Forest Model







Spatial Seer: Unity Model Pipeline

Data Sources:

- CPU profiler CSVs (semicolon-delimited): Extracted median time for specific functions including `MRUK.Update()`, `ScriptRunBehaviourUpdate`, `BehaviourUpdate`, `CullResults.CreateSharedRendererScene`, etc.
- Memory profiler CSVs:
    - **UnityObjects.csv**: Aggregated by Type (Mesh, GameObject, MeshFilter, MeshRenderer, MonoBehaviour, Transform) for allocated/resident memory; aggregated by NameOfObject for furniture categories (BED, CEILING, COUCH, DOOR_FRAME, FLOOR, LAMP, STORAGE, WINDOW_FRAME, etc.)
    - **Graphics.csv**: Aggregated by NameOfObject for furniture categories with count, allocated sum, and allocated mean
    - **AllManagedObjects.csv**: Aggregated by Type for Meta XR MRUtilityKit-specific types (EffectMesh, MRUKAnchor, etc.)

Data Processing:

- Extracted features from 19 room/scan type combinations × 5-10 trials each = 108 total scans
- Each scan became one row with ~194 features
- Combined `blinds_up` and `blinds_down` into `meeting_room` after analysis showed lighting conditions indistinguishable
- Imputed furniture-related columns with 0 (absence = furniture doesn't exist) while dropping other columns with NaN values

Spatial Seer: Unity Model Pipeline

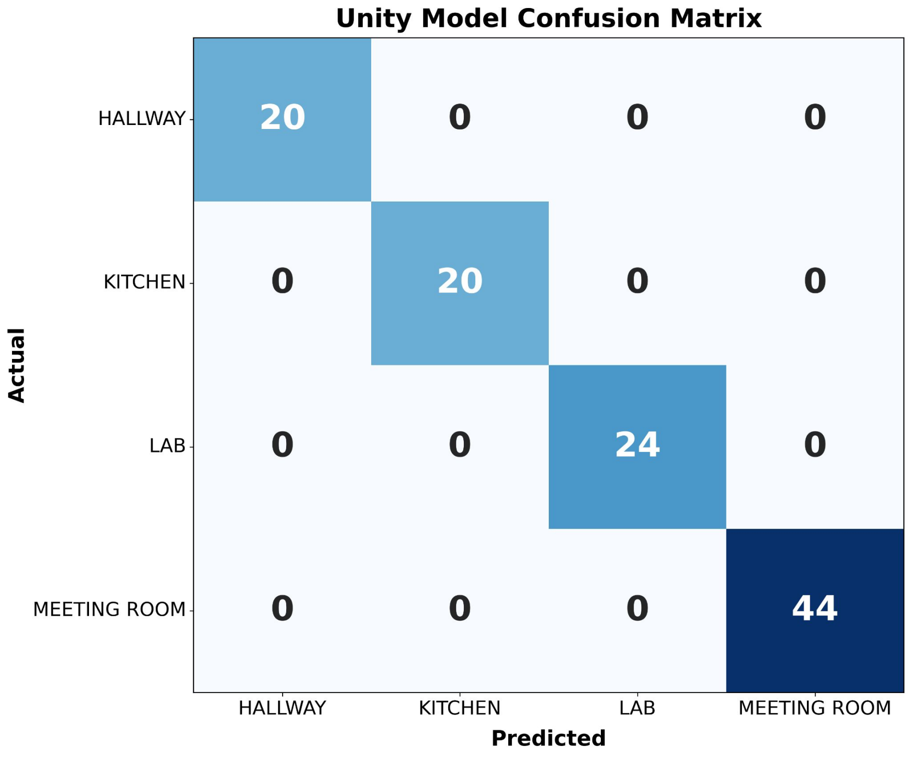
Feature Selection:

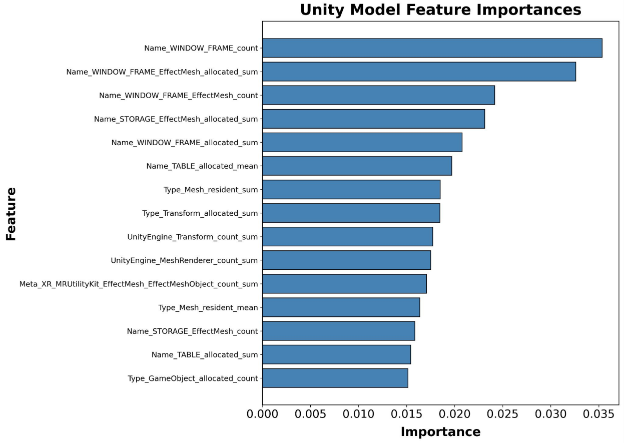
- Compared features between rooms to find discriminating features
- Analyzed blinds_up vs blinds_down distributions and confirmed overlapping ranges (lighting not distinguishable)

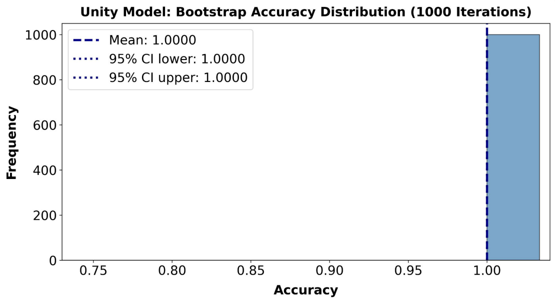
Model Training & Evaluation:

- Trained Random Forest classifier (100 trees)
- 5-Fold Stratified Cross-Validation for performance estimation
- Bootstrap validation (1000 iterations) for confidence intervals
- Achieved ~100% accuracy with 95% CI from bootstrap

Spatial Seer: Perfetto Random Forest Model







Spatial Seer: Exploiting Telemetry to Expose XR User Environment

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

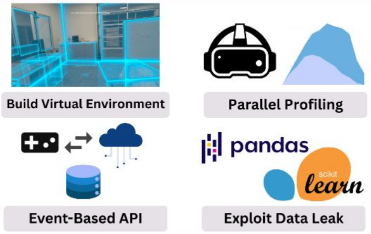
VIRGINIA TECH
COLLEGE OF ENGINEERING COMPUTER SCIENCE VIRGINIA TECH
Commonwealth Cyber Initiative
BURGS

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 **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

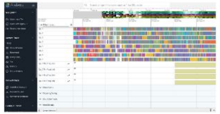
System-Wide Profiling

Perfetto

Traces: time-series telemetry data

↓

Aggregated time series into summary statistics per scan

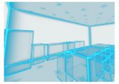


Application-Based Profiling

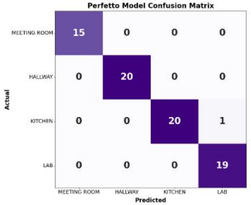
Unity

Unity Profiler: tabled performance data

Unity Memory Profiler: snapshots containing memory usage counters

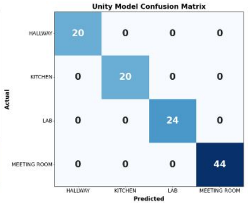


Results



Random Forest Model (300 trees, 30 features)

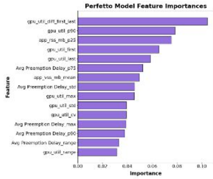
5-Fold Cross-Validation Accuracy:
98.67% ± 2.67%

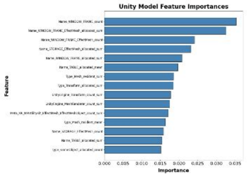


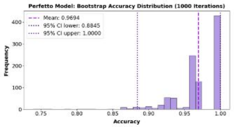
Random Forest Model (100 trees, 194 features)

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

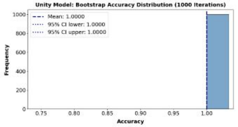
Analysis & Validation







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



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

Conclusions

We have high test accuracy for system-wide profiling (<98.7%) and application-based profiling (<100%). 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.

Questions

1. We have high accuracy for our models, but how would you advise us to prepare about questions for potential data leakage? What other questions do you think we might be asked for our presentation?
2. Any feedback for our poster and/or our abstract?