INCHEON NATIONAL UNIVERSITY

CYBERSECURITY CONVERGENCE LAB

SPADE-XR:

A Framework for Detecting and Analyzing Spatial Data Permission Inconsistencies in XR Environments

Hyojoong Ju

Department of Computer Science & Engineering

Incheon National University

Background: What is XR?

EXTENDED REALITY

Virtual Reality

Augmented Reality

Mixed Reality

Background: What is XR?

XR

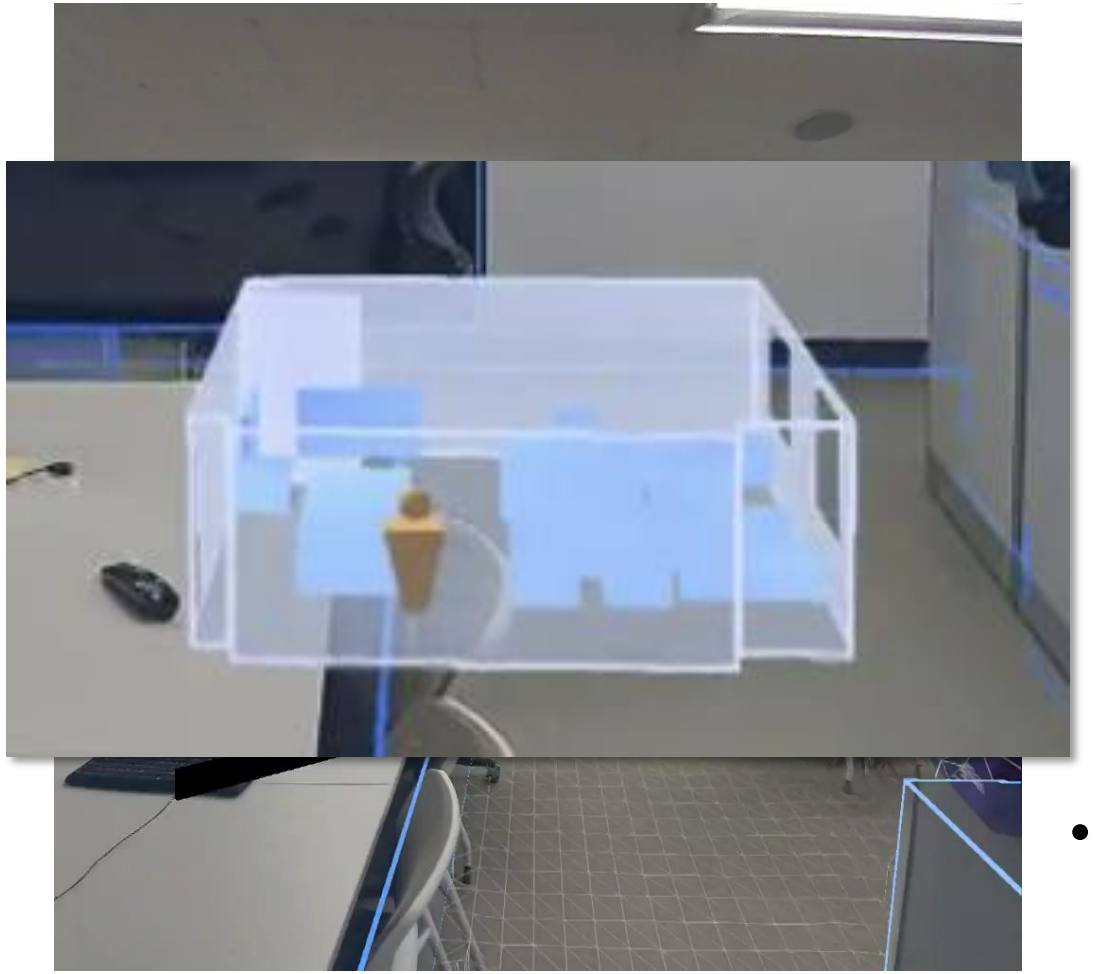
Background: XR Devices

Meta **Quest 3**

Apple **Vision Pro**

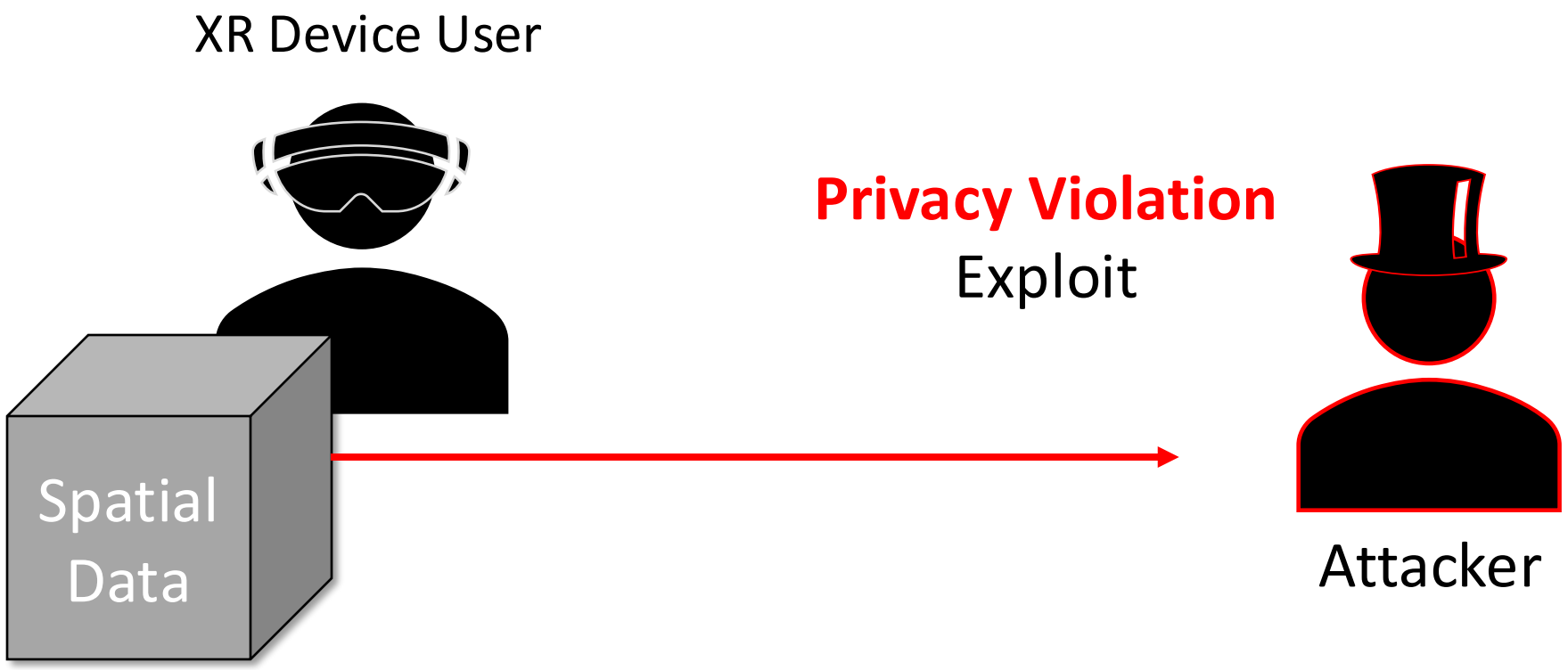
Samsung **Galaxy XR**

Background: Spatial Data

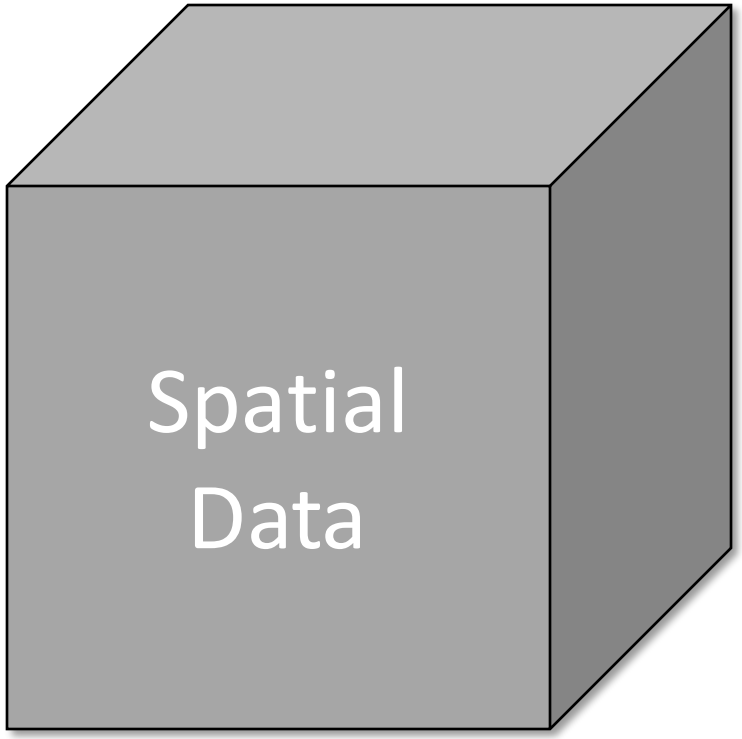


- Meta Quest 3,
  Guardian (00:10)

Background: Spatial Data Leakage

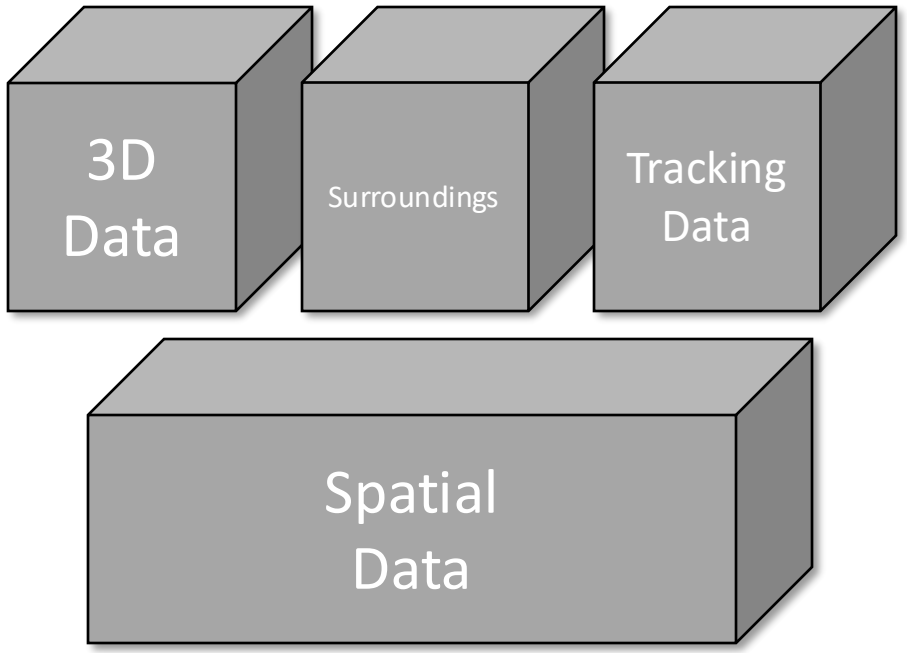


Background: Spatial Data Leakage



- XR device permissions differ from standard Android and rely on extended, XR-specific capabilities.
- Unlike simple camera access, they involve continuous 3D spatial information.
- If leaked, the exposure is not a static image but may include:
  - Interior spatial layout
  - object placement
  - user movement patterns

Background: Spatial Data Leakage



- XR device permissions differ from standard Android and rely on extended, XR-specific capabilities.
- Unlike simple camera access, they involve continuous 3D spatial information.
- If leaked, the exposure is not a static image but may include:
  - Interior spatial layout
  - object placement
  - user movement patterns

Background: Spatial Data Leakage

- Related Works
- **Nair et al.** [1]
  - Collected 120 Seconds of Tracking data from VR device sensors
  - Achieved identity recognition with about 98% accuracy
- **Farrukh et al.** [2]
  - Used semantic data from MR Environments
  - Successfully inferred the user's surrounding spatial information

[1] Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J. F., Rosenberg, L., & Song, D. (2023). Unique identification of 50,000+ virtual reality users from head & hand motion data. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 895-910).

[2] Farrukh, H., Mohamed, R., Nare, A., Bianchi, A., & Celik, Z. B. (2023). {LocIn}: Inferring semantic location from spatial maps in mixed reality. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 877-894).

Motivation

- **Challenge 1: Prior mismatch studies are not XR-Specific**
  - Focused on simpler, standardized Android mobile environments
  - XR involves **body, spatial, sensor, and semantic data**
  - Missing **Manifest** declarations may go undetected

Motivation

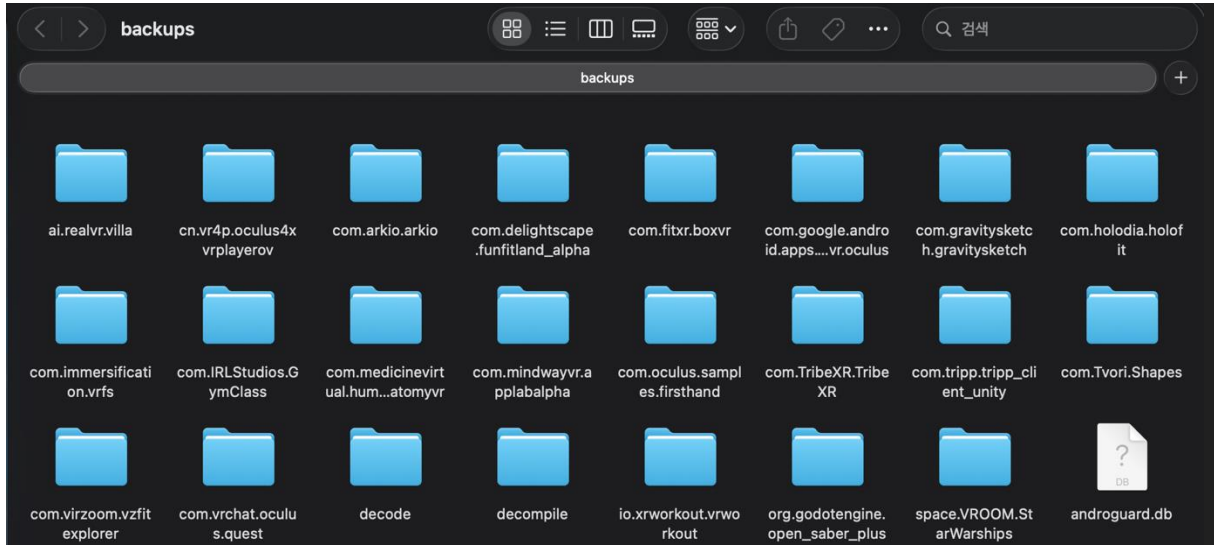
- **Challenge 2: Technical complexity of XR OS**
  - Most XR apps use Unity's IL2CPP structure
  - API calls require restoring symbols from **libil2cpp.so** and **global-metadata.dat**

Motivation

- **Challenge 3: Limitations of Meta Horizon Store's automated review**
  - Checks mainly Manifest declarations
  - Lacks transparent checks on actual permission-API Calls
  - As a result, the review process is less trustworthy

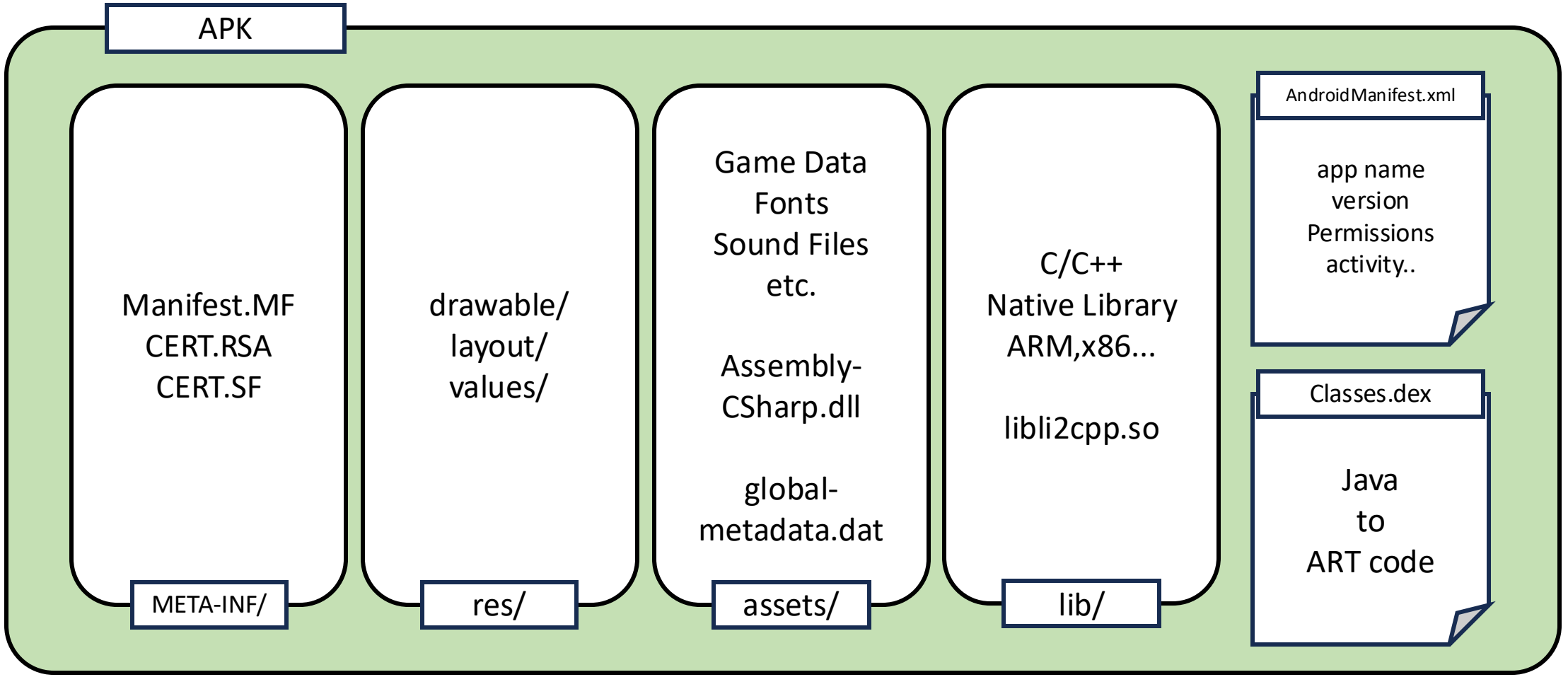
Approach

- Collected 21 Meta Quest 3 apps and prepared APK files
- Extracted declared permissions from **AndroidManifest.xml**
- Checked actual usage by mapping permissions to corresponding function calls

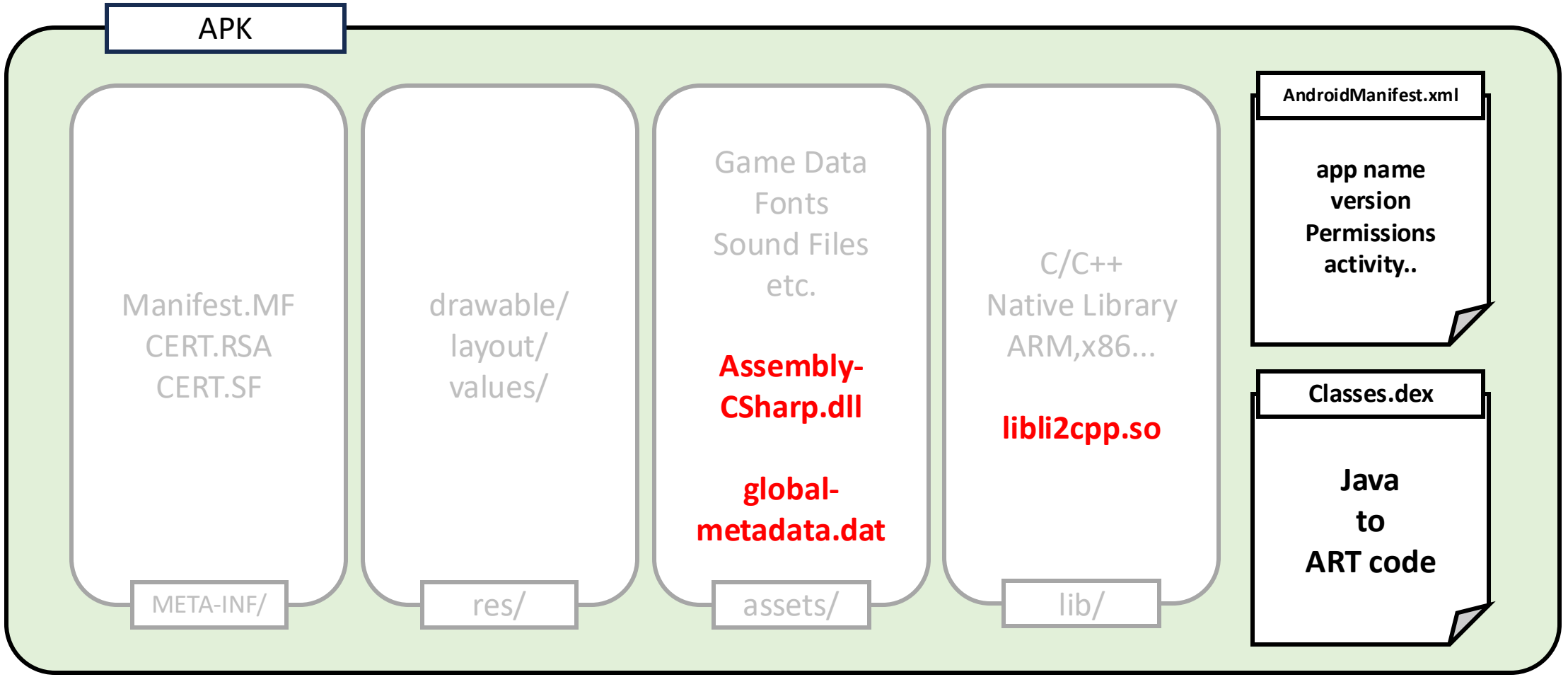



```
- out_ai.realvr.villaapks
    android.permission.INTERNET
    android.permission.WRITE_EXTERNAL_STORAGE
    android.permission.ACCESS_NETWORK_STATE
    android.permission.WAKE_LOCK
    com.android.vending.CHECK_LICENSE
    android.permission.ACCESS_WIFI_STATE
    com.android.vending.BILLING
    android.permission.RECORD_AUDIO
    android:maxSdkVersion32 android.permission.READ_EXTERNAL_STORAGE
    com.oculus.permission.FACE_TRACKING
    com.oculus.permission.EYE_TRACKING
    android.permission.READ_MEDIA_AUDIO
    114 android.permission.REQUEST_VIDEO_AUDIO_CODE
```

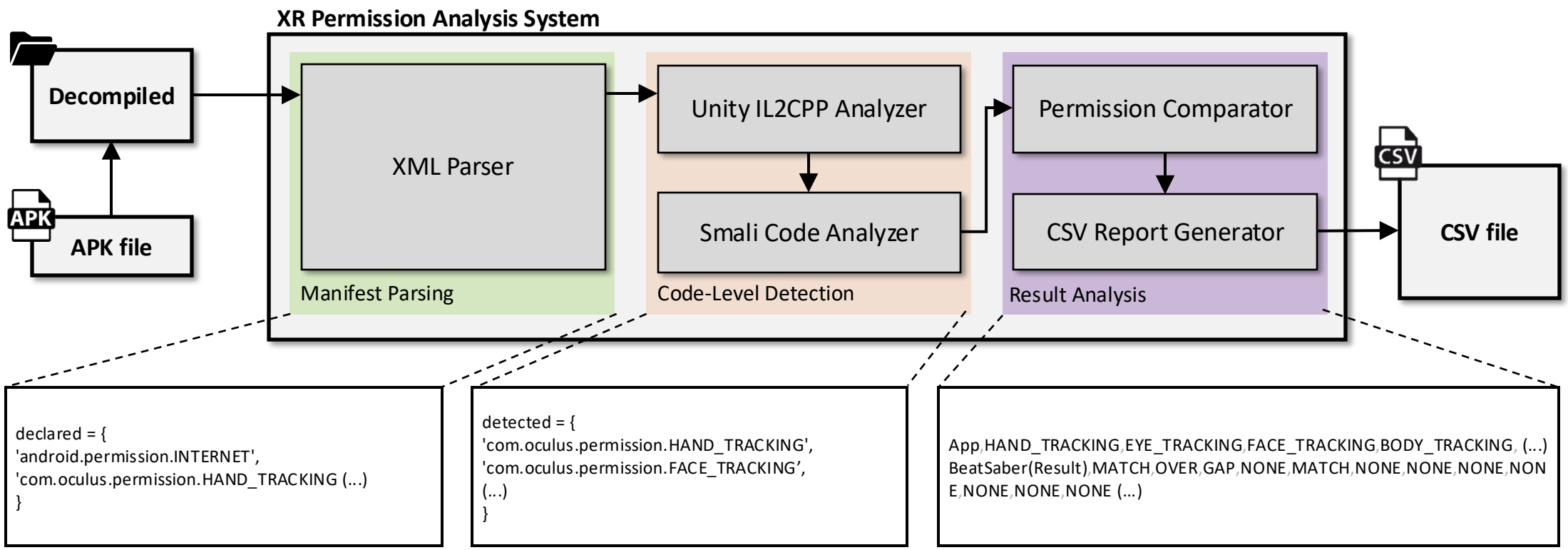
Approach: APK File Architecture



Approach: APK File Architecture

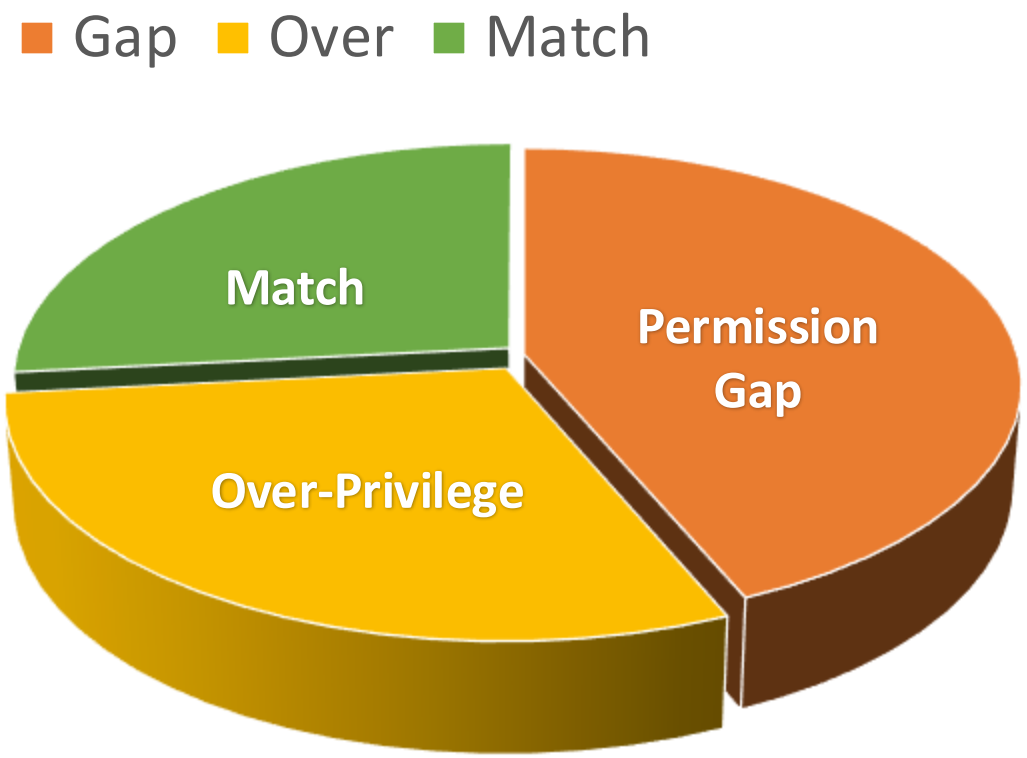


Approach: SPADE-XR System Design



Evaluation

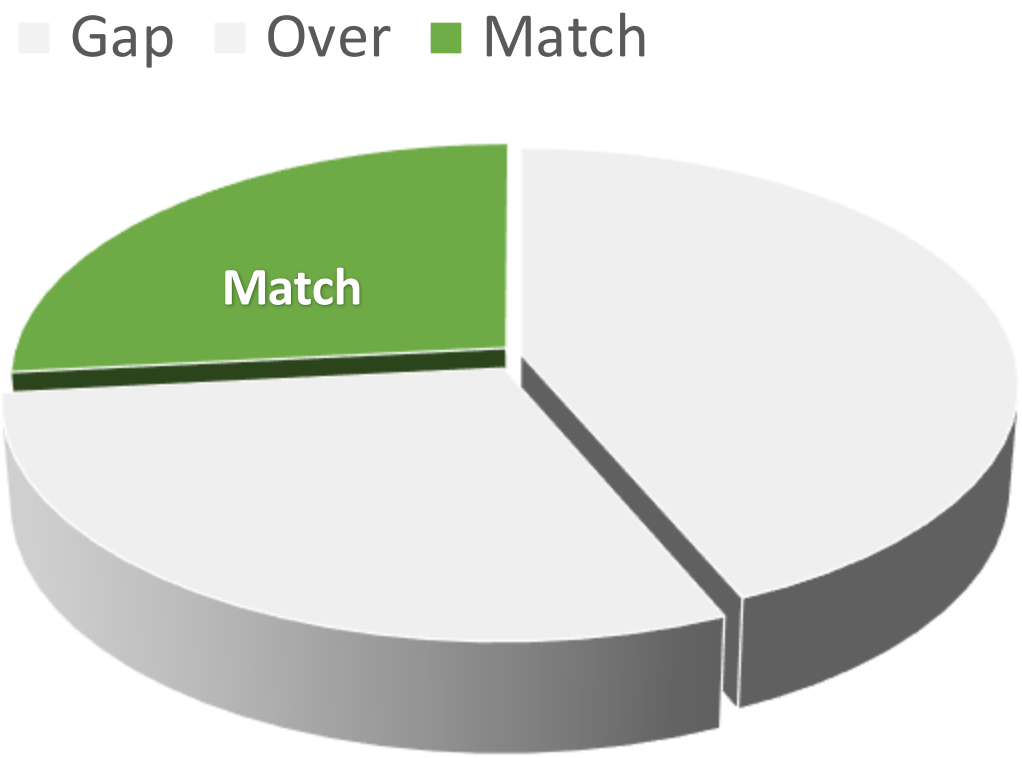
- **Evaluation(21 Apps total)**
- Permission match only **25.37%**
- Permission Gap(Undeclared calls): **41.47%**
- Over-privilege(Declared but unused): **28.39%**



Evaluation

- **Evaluation(21 Apps total)**
- Permission match only **25.37%**
- Permission Gap(Undeclared calls): **41.47%**
- Over-privilege(Declared but unused): **28.39%**

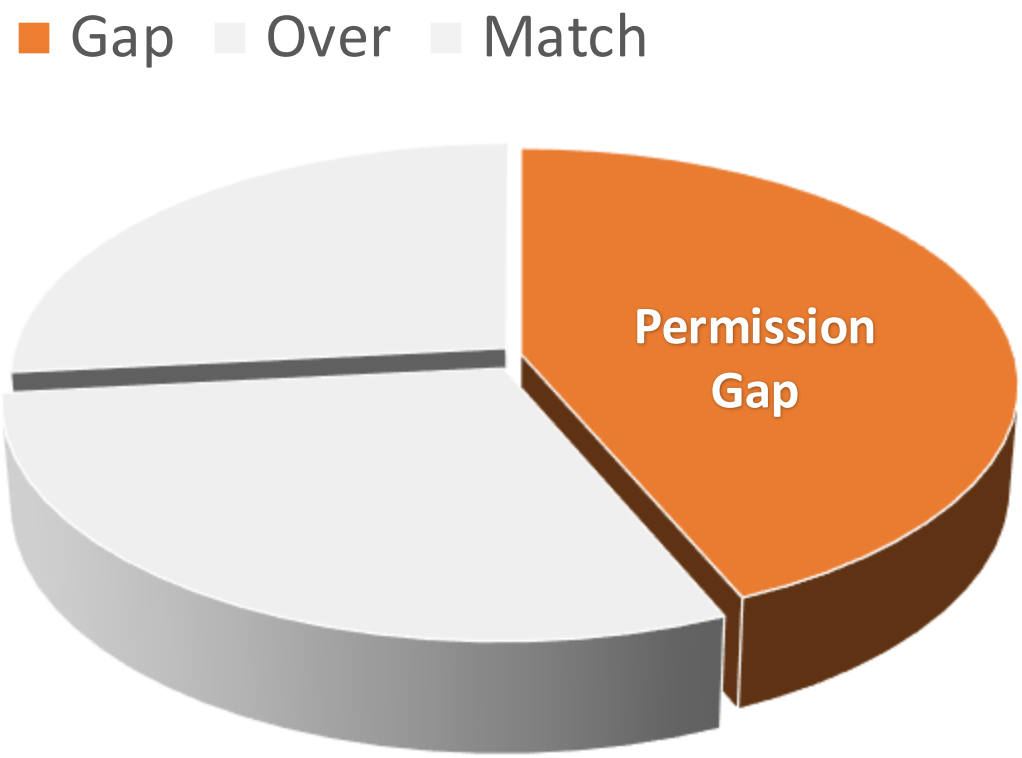
- This demonstrates that real threats can go undetected.



Evaluation

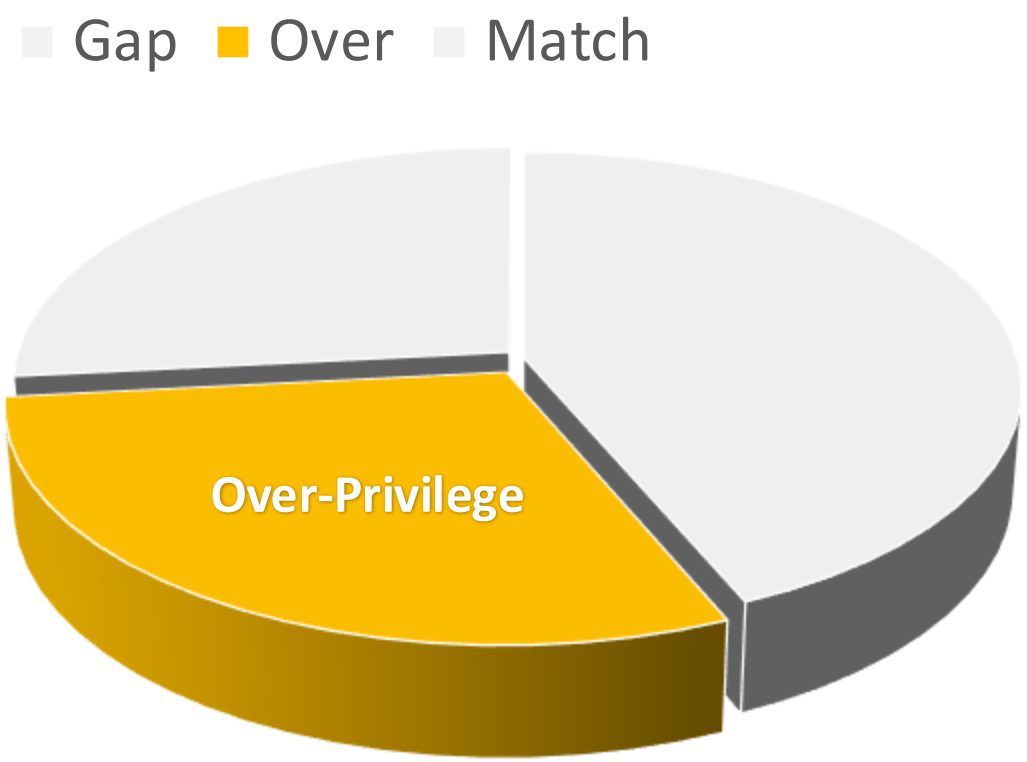
- **Evaluation(21 Apps total)**
- Permission match only **25.37%**
- Permission Gap(Undeclared calls): **41.47%**
- Over-privilege(Declared but unused): **28.39%**

- Possible intentional hiding
- or, engine-level automatic invocation.



Evaluation

- **Evaluation(21 Apps total)**
- Permission match only **25.37%**
- Permission Gap(Undeclared calls): **41.47%**
- Over-privilege(Declared but unused): **28.39%**
- Requests excessively broad user permissions
- May pre-authorize wide access, enabling malicious behavior in future updates



Benefit

- **Quantify** spatial data leakage risk in XR applications and propose **risk profiling**
- **Detail API lists** corresponding to XR-related permissions from a S&P perspective
- Visualize, in quantitative form, whether permissions are **properly used** and **disclosed to users**

Competition

- **Guo et al.**[1] – Analyzed ~500 XR apps via static methods, but focused on general Android permissions, **lacking XR-specific policy analysis.**
- XR app platforms show uncertain code-permission mapping; propose a framework to supplement existing store review policies

[1] Guo, H., Dai, H. N., Luo, X., Zheng, Z., Xu, G., & He, F. (2024, April). An empirical study on oculus virtual reality applications: Security and privacy perspectives. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (pp. 1-13).

Conclusion and Future Work

- Develop a **risk-score model** using weighted risk levels per permission
- Combine eBPF-based **dynamic analysis** to detect and evaluate risks during actual execution

Thank you for Listening

Q&A