SPADE-XR: XR 환경에서의 공간 데이터 권한 불일치 탐지 및 분석 프레임워크

주효중[1], 이승수[2]

*인천대학교 (학부생[1], 교수[2])

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

Hyojoong Ju[1], Seungsoo Lee[2],

*Incheon National University

(Undergraduate student[1], Professor[2])

요 약

본 연구는 확장 현실(Extended Reality, XR)환경에서의 권한 불일치가 공간 데이터 및 생체정보의 보안에 미치는 영향을 분석하였다. XR 앱은 현실 공간 데이터를 수집하는 특수 권한을 사용하며, 사용자의 위상 및 공간 정보를 추적할 수 있는 잠재적 위험을 지닌다. 본 연구에서 Manifest 파싱과 코드 분석을 결합하여 21종의 상용 XR 앱을 분석한 결과, 약 70%의 앱에서 권한 불일치가 확인되었다. 이러한 결과는 기존 Manifest 기반 검증 체계가 XR 환경의 생체 및 공간 정보 보호에 한계가 있음을 보여주며, 민감 권한 오용에 대한 정량적 탐지의 필요성을 제기한다.

I. Introduction

확장 현실(Extended Reality, XR) 기술의 대중화로, 사용자의 공간 및 생체 데이터가 대규모로 수집 및 처리되는 환경이 확산되고 있다. XR 생태계에서는 신체 추적, 공간 인식과 같은 고위험 권한이 빈번하게 사용된다. [1] 이러한 권한들은 일반 안드로이드 OS(AOSP)와 달리, 별도로 관리되며, 관련 보안 정책 또한 명확하지 않다. 기존 연구[2]는 Manifest에 선언된 권한과 실제 코드 내에서 사용되는 권한 간 불일치를 분석해왔으나 대부분 모바일 환경에 국한되어 있으며, XR 환경에 특화된 영역을 포괄하지 못한다. 본 연구는 이러한 문제 해결을 위해 XR환경에서의 권한 불일치 분석 프레임워크를 제안한다.

II. Background

Meta Horizon OS는 Android Open Source Project (AOSP)를 기반으로 개발되었지만, HAND_TRACKING, USE_SCENE, HEADSET_CAMERA(원시 카메라 스트림, 패스스루, 심도 데이터 포함) 등 일반 안드로이드 API에서는 제공되지 않는 확장 권한을 통해 신체, 공간, 센서 데이터를 수집할 수 있다. 이러한 권한들은 본질적으로 민감한 데이터를 포함하므로 유출될 경우 심각한 개인정보 침해로 이어질 수 있다. 실제로 Nair et al. [3]은 VR 기기 센서를 통해 수집된 생체 데이터만으로도 신원 식별이 가능함을 보였고, Farrukh et al. [4]은 혼합현실(MR) 환경의 의미론적 데이터를 이용해 사용자 주변 공간 정보를 추론할 수 있는 공격 벡터를 규명하였다.

III. Problem Statements

C1: 기존 권한 불일치 연구의 한계

기존의 권한 불일치 관련 연구[2]는 대부분 Android 모바일 환경을 대상으로 하며, 표준화된 권한 체계 내에서 Manifest 선언과 실제 코드 간의 불일치를 중심으로 분석해왔다. 그러나 XR 환경에서는 생체 정보뿐 아니라 영상, 심도 스캔 등의 고위험 데이터를 다루기 때문에, 기존의 모바일 중심 권한 모델만으로는 이를 포괄하기 어렵다.

이러한 XR 특화 권한에 대한 체계적 연구는 아직 미비하며, 결과적으로 실제 민감 기능이 사용되더라도 Manifest 선언이 누락되는 권한 불일치 상황이 발

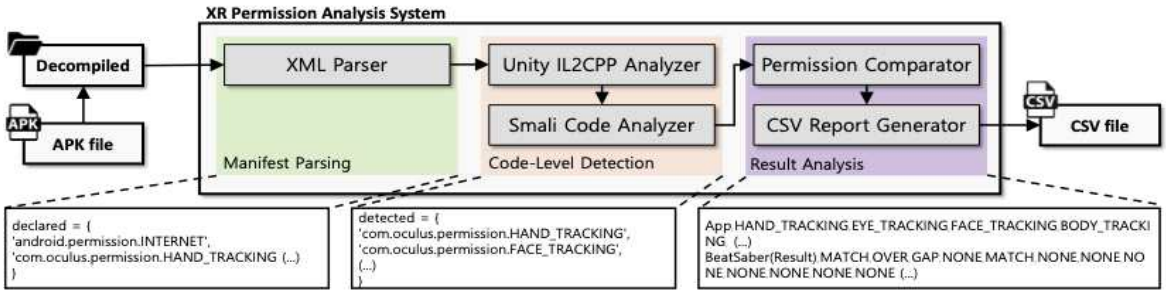

Figure 1. XR Permission Analysis System Overall Architecture

생하기 쉽다. 이는 새 공격 표면으로 이어질 수 있다.

C2: XR OS 환경의 기술적 복잡성과 추적 한계

AOSP 기반의 XR OS는 표준 안드로이드 API 외에도 3D 몰입형 환경 구현을 위한 엔진 관련 API, 사용자 움직임 추적 API, MR 경험 제공을 위한 API 등을 통합적으로 호출한다. 그러나 기존 Android용 정적 분석 도구는 이러한 엔진 레벨 호출을 완전하게 추적하기 어렵고, IL2CPP 변환된 Unity 기반 코드 구조 역시 역분석 난이도를 높인다.

이로 인해 Horizon OS 환경에서는 권한 호출 추적의 불완전성이 발생하며, 결과적으로 Manifest와 실제 코드 간의 권한 불일치가 탐지되지 않는 문제가 존재한다.

C3: 검증 체계의 한계와 공격 표면 확대

Meta는 Horizon Store를 통해 XR 앱을 배포하며, 게시 전 자동화된 심사 체계를 운영한다. 그러나 이 과정은 Manifest에 선언된 권한 검증과 패키지 서명·무결성 확인에 국한되어 있으며, 실제 코드에서 어떤 API가 호출되는지에 대한 행위 기반 검증은 수행되지 않는다.

따라서 심사를 통과한 앱이라 하더라도 실제 코드 수준에서 권한 불일치가 발생할 가능성이 있으며, 이는 민감 데이터 접근을 허용하는 새로운 공격 표면으로 이어질 수 있다.

IV. System Design

본 논문은 Meta Horizon OS 환경을 대상으로 XR 권한 분석 프레임워크를 제안한다. XR 권한 분석 프레임워크의 아키텍처는 Figure 1과 같으며, 분석은 다음의 세 단계로 진행된다: (1) Manifest에서 선언한 권한을 수집 및 정규화하고 XR 특화 12종 권한 사전에 매핑, (2) 코드 레벨에서 권한 관련 API 호출을 탐지, (3) 선언과 호출을 대조하여 불일치를 분류 및 집계한다. 이로써 XR 앱의 민감 권한 사용을 정량적으로 평가하고 잠재적 위험을 파악한다.

시스템의 입력으로는 apktool을 이용해 디컴파일된 각 앱 디렉터리를 사용하며, 분석 결과는 앱별 권한 일치 여부를 기록한 CSV 형식으로 저장된다.

4.1. Manifest Parsing

Manifest Parsing 단계에서는 디컴파일 된 APK 파일 내의 AndroidManifest.xml에서 모든 권한 선언을 추출하고, XR 특화 권한 사전과 비교하여 앱이 요청하는 기능의 민감도를 평가한다. 이 사전은 일반 Android 권한 외에 손 추적, 패스스루, 카메라 스트림 등 XR 기기에서만 제공되는 확장 권한 12종을 포함한다. 이를 통해 사용자의 명시적 동의 없이 XR 기능이 요청되거나 과도한 권한이 선언되는 사례를 식별할 수 있다.

4.2. Code-Level Detection

다음 단계에서는 앱 코드 내에서 실제 권한 관련 API가 호출되는지를 확인한다. XR 앱은 대부분 Unity 기반의 IL2CPP 구조를 사용하므로, 단순 문자열 기반 탐지는 한계가 있다. 따라서 APK 파일 내 libil2cpp.so와 global-metadata.dat 파일을 분석해 IL2CPP 구조를 복원한 뒤, 복원된 코드 내에서 XR 관련 API 키워드를 탐색한다. Java 및 Kotlin 코드의 경우, smali 파일을 정규식으로 분석하여 권한 사용 여부를 검출한다. 이를 통해 C# 스크립트가 네이티브 코드로 변환된 이후에도 실제 권한 호출을 추적할 수 있다.

4.3. Result Analysis

마지막 단계에서는 Manifest와 코드 분석 결과를 비교하여 권한 일치 여부를 분류한다. 선언된 권한이 실제로 호출된 경우는 Match, 선언되지 않았으나 호출된 경우는 Gap, 선언만 되어 있고 사용되지 않은 경우는 Over로 구분한다.

분류 결과는 자동으로 CSV 파일로 정리되며, 앱 단위 및 권한 단위로 통계적 비교가 가능하다. 이를

통해 XR 앱의 권한 불일치 현황을 정량적으로 파악하고, 정책적 보안 개선에 활용할 수 있다.

V. Evaluation

5.1. Experimental Environment

Horizon Store의 MR기반 무료 앱 상위 19종과, SideQuest 배포 비공식 앱 2종, 총 21개의 앱을 대상으로 실험을 수행하였다. 모든 실험은 Ubuntu 22.04 환경에서 수행되었으며, Quest 3 기기에서 추출한 APK를 apktool로 디컴파일 후 Python 기반 스캐너를 통해 Manifest 파싱, IL2CPP 복원 및 정규식 기반 문자열 탐지를 자동화하여 선언된 권한과 실제 호출된 권한 비교를 수행하였다. 분석 대상 권한은 12종의 XR 특화 권한으로 구성, 각 권한 대응 메서드 호출 여부를 비교하였다.

5.2. Analysis Evaluation

평가 결과는 Figure 2와 같다. 전체 21개의 애플리케이션 중 41.47%의 앱에서 Permission gap이 있었으며, 28.39%의 앱에서는 Over privilege가 존재하였다. 권한 일치 비율은 25.37%밖에 되지 않았다. 특히 USE_ANCHOR_API, USE_SCENE, HAND_TRACKING 등의 권한에서 높은 불일치 비율을 보였다. 원시 패스스루 데이터 및 심도 정보를 제공하는 고위험 권한인 HEADSET_CAMERA의 경우, 선언되지 않은 비율이 높았으나, 83.33%의 앱에서 불일치가 감지되었다.

VI. Conclusion

본 연구는 XR 환경에서 선언 기반 검증의 한계를 보이고, Manifest 파싱, IL2CPP 복원, 정규식 기반 탐지를 결합한 정적 스캐너를 제안하였다. 분석 결과, 선언되지 않은 권한 호출이 다수 확인되었으며 이는 공간 및 생체 데이터 등 민감정보 유출 가능성을 시사한다. 본 연구에서 구축한 스캐너를 기반으로 향후 권한별 위험도 가중치를 적용한 Risk Score 산출 모델을 개발하고 정적 분석에 동적 행위 분석을 병행하여 실제 실행 단계의 API 호출 및 페이로드 수준에서 위험을 평가할 수 있는 통합 검증 체계로 확장할 예정이다.

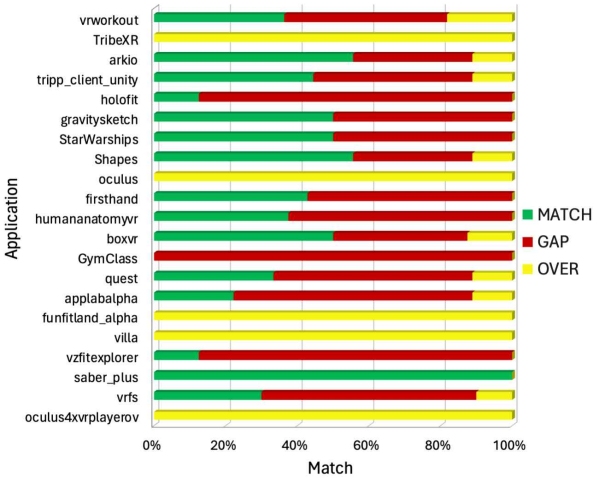

Figure 2. Permission Gap Ratio

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2025-16069415).

[참고문헌]

[1] Cai, K., Zhang, J., Li, Y., Wang, Z., Chen, X., Li, T., & Tian, Y. (2025). From Perception to Protection: A Developer-Centered Study of Security and Privacy Threats in Extended Reality (XR). arXiv preprint arXiv:2509.06368.

[2] 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).

[3] 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).

[4] 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).