VR 환경 속 백신 솔루션 개발

Antivirus Development in Virtual Reality

팀 명	VRAV
지도교수	유승재
팀 원	김 명 규 (팀장) 강 민 혁 김 민 서 김 원 태 박 준 형

2025. 11. 4

중부대학교 미래융합공학부 정보보호학전공

목 차

1. 서론

1.1 연구 배경

메타 퀘스트(Quest) 등 최신 VR 기기는 Android 기반 Horizon OS 위에서 동작하며, 공식 스토어 외에도 개발자 모드와 사이드로딩 경로를 통해 다양한 외부 앱이 설치됩니다. 이로 인해 설치 이벤트를 기점으로 한 초기 감염, 시스템 UI 위장 (Immersive/Inception형) 및 악성 외부 도메인 연동 피싱 등 새로운 위협이 현실화되고 있습니다. VR 특성상 저지연·장시간 착용 요건으로 무거운 보안 모듈 적용이 어려워 경량·온디바이스 중심의 탐지/차단 체계가 필요합니다.

1.2 연구 필요성

- 배포 채널 다변화: 공식 스토어 비허가 외부 앱(사이드로드) 증가에 따른 설치 이벤트 기반 실시간 검증 필요.
- 플랫폼 제약: VR 프레임과 배터리에 미치는 영향을 최소화하는 경량 탐지 엔진 요구.
- 신규 위협: 가짜 홈/런처 모방, 네트워크 피싱, 권한 악용 등 VR 특화 행위에 대한 체계적 대응 부재.

1.3 연구 목적 및 주제선정 이유

본 연구는 외부 앱(비허가/사이드로드)을 핵심 범위로 하여, (1) 블랙리스트 해시 DB, (2) VirusTotal(VT) 검증, (3) 사전학습된 ML 기반 Manifest 권한/인텐트 위험도 분석, (4) 런타임 동적 모니터링(악성 외부 도메인 차단)을 결합한 4단계 검증 파이프라인을 설계·구현합니다. 설치 이벤트를 감지하여 즉시 스캔하고, 위협을 식별해 알림을 제공하며, 각 기능 화면에서 재검증이 가능하고, 모니터링은 사용자 제어(on/off)를 지원합니다.

2. 관련 연구

2.1 VR/XR 보안 위협

- Inception/Immersive Hijacking: 시스템 UI 위장 및 상호작용 탈취 위협.
- 키스트로크/제스처 추론: 착용·공유 환경에서의 민감 상호작용 유출 가능성.
- VR 보안 총설: 센서·렌더링·네트워크·소셜 영역 전반의 위협 분류 및 과제.

2.2 Android/VR 플랫폼 보안 모델

- 설치/업데이트 브로드캐스트와 패키지 가시성 제약(Android 11+): 설치 이벤트 기반 트리거 설계의 근거.
- VPNService 기반 네트워크 모니터링: 도메인 차단(피싱/악성) 및 알림 UX 연계 가능.

2.3 온디바이스 악성코드 탐지

- 권한/인텐트 특징 기반 경량 ML 탐지(예: LibreAV 계열)와 VT 결과 결합을 통한 하이브리드 탐지.
- (참고) 기존 초안에서 언급된 YARA는 본 구현에서는 사용하지 않으며, 차후 확장 옵션으로 남깁니다.

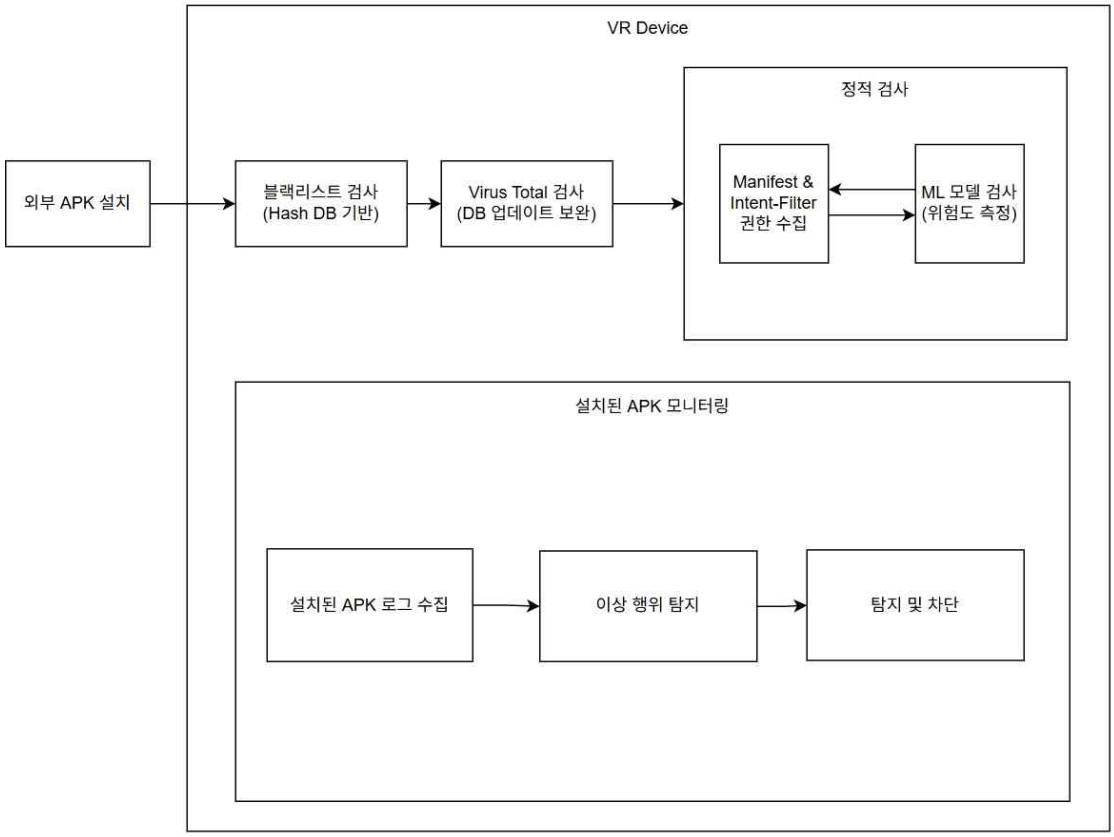
3. 프로젝트 내용

3.1 시스템 범위 및 요구사항

범위: 메타 퀘스트 계열 외부 앱(스토어 비허가/사이드로드) 중심.

- 필수 요구: (a) 설치 이벤트 실시간 감지, (b) 4단계 검증 파이프라인, (c) 위협 알림 및 재검증 UI, (d) 모니터링 on/off 사용자 제어, (e) 저지연·저전력·낮은 프레임 드랍.

3.2 아키텍처 개요



1) 이벤트/수집 계층: BroadcastReceiver로 설치/업데이트 이벤트 수신 → 스캔 트리거, FileObserver로 사이드로드 디렉터리 감시.
2) 정적 분석 계층: 해시 계산(sha256), Manifest 권한/인텐트 파싱, 패키지 메타 추출.
3) 탐지 엔진 계층: 블랙리스트 해시 매칭 → VT 샌드박스/평판照 → ML 위험도 점수화(사전학습 모델).
4) 동적 모니터링 계층: VPNService 기반 DNS/HTTP(S) 도메인 필터링(피싱/악성), 허용/차단 목록 관리.
5) 대응/UX 계층: 설치 차단 제안, 격리/삭제 워크플로우(정책 범위 내), VR 친화 HUD 알림 및 상세 화면 재검증.
6) 설정/정책: 모니터링 on/off, 주기 스캔 간격, VT 질의 모드(프라이버시/트래픽 고려) 등 사용자 선택 제공.

3.3 4단계 검증 파이프라인(현재 구현 기준)

단계	기능	입력	기법/모델	결과/조치
1	블랙리스트 해시 DB	APK/AAB 해시(sha256)	로컬 해시 DB 매칭	일치 시 고위험 경고·격리/설치 차단 제안
2	VirusTotal 기반 검사	sha256 또는 VT 지원 메타	VT 평판/탐지 결과	다수 엔진 탐지 시 "의심/악성" 플래그
3	ML 위험도 분석	Manifest 권한·인텐트, 메타	사전학습 경량 모델(TFLite/GBDT)	위험도 점수→임계값 초과 시 경고
4	동적 모니터링	실행 중 네트워크 요청	VPNService DNS/HTTP(S) 도메인 필터링	악성/피싱 도메인 차단·알림

3.4 데이터셋·모델

- 데이터: AndroZoo, CIC-AndMal, AMD 등 공개 APK 데이터셋 + 자체 수집(사이드로드 표본).
- 특징: 권한/인텐트, 패키지 메타, 간단한 API/문자열 통계(경량).
- 모델: 경량 트리(GBDT/LightGBM) 또는 소형 DNN(TFLite) — 온디바이스 추론 최적화(양자화/프루닝).
- 라벨링: VT 다수결/시간 분할(개념 드리프트 고려)로 Train/Val/Test 분리.

3.5 구현 세부 및 정책 준수

- 설치 감지: ACTION_PACKAGE_ADDED/REPLACED 브로드캐스트 기반 트리거.
- 패키지 가시성: Android 11+에서 queries 선언 최소화, 필요한 대상만 명시.
- 네트워크 차단: VPNService로 로컬 DNS 프록시·도메인 블록리스트 적용, 허용/차단 목록 UI 제공.
- 프라이버시: VT 질의 시 해시(sha256) 우선, 원본 APK 전송 금지. 통계는 익명화/옵트인.
- 성능: 스캔/모니터링의 프레임 드랍률·배터리 영향 목표치를 사전 정의 및 측정.

3.6 평가 계획

- 정확도: 단계별/전체 앙상블 TPR, FPR, AUC.
- 성능: 설치-결정 지연, 프레임 드랍률(±%), 배터리 소모(%) 및 발열.
- 시나리오: 신규 설치 즉시 스캔, 재검증 UI, 모니터링 on/off 토글, 악성 도메인 접속 차단 알림.
- 비교군: (a) 해시/VT 단독, (b) ML 단독, (c) 제안 4단계 하이브리드(본 연구).

4. 결론

본 연구는 외부 앱(사이드로드) 중심의 VR 보안 공백을 해소하기 위해, 해시·VT·ML·동적 모니터링을 결합한 4단계 경량 파이프라인을 제안·구현합니다. 설치 이벤트 기반 즉시 탐지, 재검증 가능한 UX, 사용자 제어 가능한 모니터링을 통해 실사용 환경에서 높은 실효성과 낮은 성능 저하를 동시에 달성하는 것을 목표로 합니다.

4.1 결론 및 기대효과

- 외부 앱 설치 단계에서의 초기 감염 차단 및 사용자 경고 강화.
- VT·ML·동적 모니터링 결합으로 알려진/미확인 위협 모두에 대한 대응력 향상.
- 온디바이스 경량 설계로 VR 사용성(프레임/배터리) 저하 최소화.

4.2 향후 계획

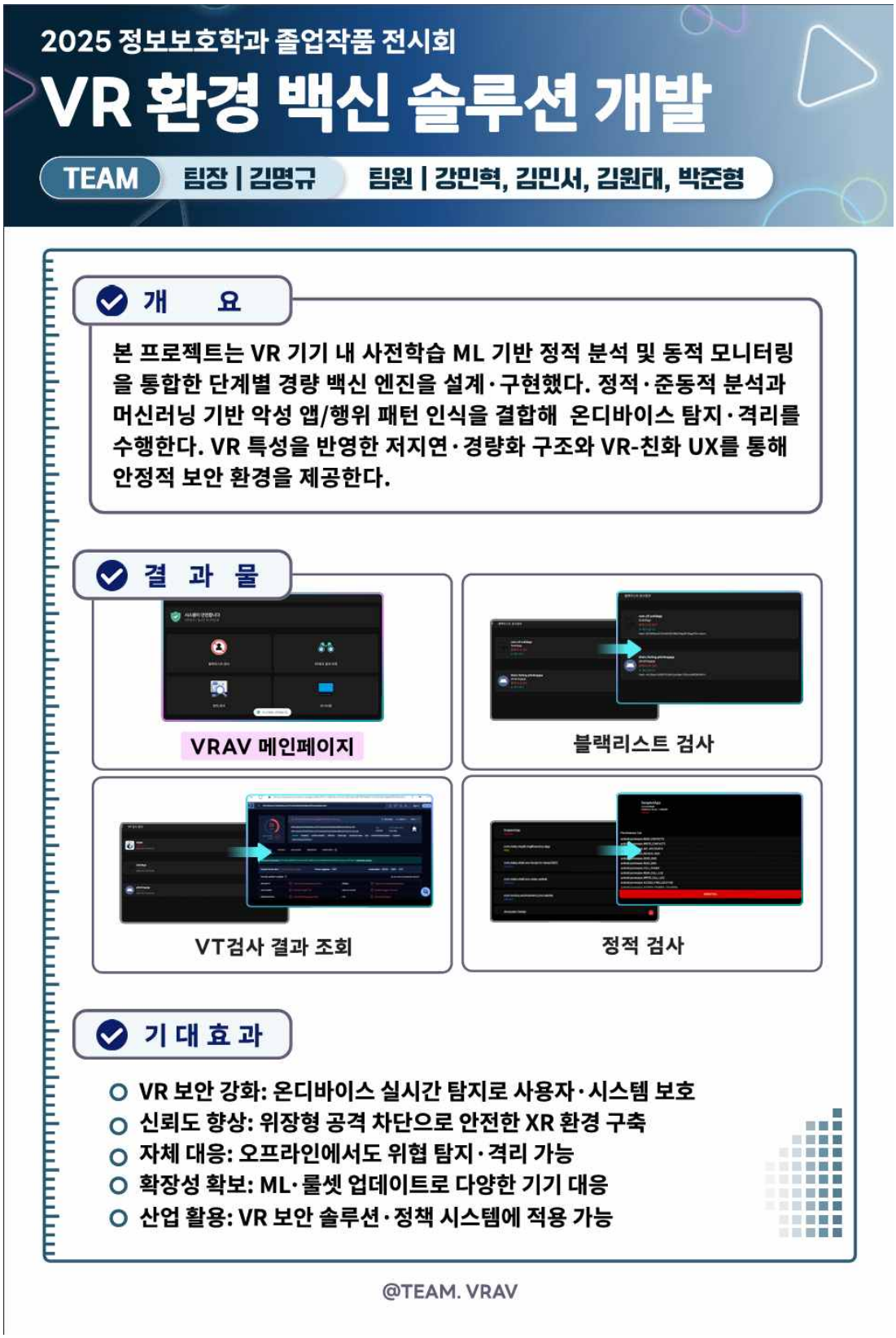
- 비공개 악성 도메인/신종 페이로드에 대한 탐지 공백을 줄이기 위한 인텔 동기화 전략 필요.
- (옵션) YARA 등 규칙 기반 탐지를 추후 도입해 정적 탐지 커버리지 확대 검토.
- 모델 개념 드리프트 대응: 주기적 재학습·온디바이스 적응학습 검토.

5. 참고 자료

⑴ Inception Attacks: Immersive Hijacking in Virtual Reality Systems, 2024
⑵ Keystroke inference in shared VR environments, USENIX Security
34 Security and Privacy in Virtual Reality — Literature Survey,
2024
⑶ Security and privacy in virtual reality: literature survey/review(2022-2024)
⑷ Meta Quest 개발 문서(Quest = Android 기반 Horizon OS, Unity/네이티브 개발 개요)
⑸ Android Broadcasts(설치/업데이트 브로드캐스트), FileObserver API.
⑹ Android 11+ Package Visibility 가이드
⑺ IntelliAV: Effective On-Device Android Malware Detector.
⑻ DL-Droid: Deep learning-based Android malware detection using real devices.
⑼ LibreAV(ML 기반 오픈소스 안드로이드 안티-멀웨어) 저장소/문서.
⑽ YARA / YARA-X 문서 및 공개 룰셋 저장소.
⑾ ReversingLabs YARA rules.
⑿ AndroZoo(대규모 APK 데이터셋) 및 최신 레트로스펙티브 논문.
⒀ CIC-AndMal2017/2020 데이터셋.
⒁ AMD(2017) 데이터셋 및 파생 연구. [R16] Android
⒂ malware detection 벤치마킹/개념 드리프트 논문

6. 별첨

6.1 소개 자료


2025 정보보호학과 졸업작품 전시회
VR 환경 백신 솔루션 개발
TEAM
팀장 | 김명규
팀원 | 강민혁, 김민서, 김원대, 박준형
개 요
본 프로젝트는 VR 기기 내 사전학습 ML 기반 정적 분석 및 동적 모니터링을 통합한 단계별 경량 백신 엔진을 설계·구현했다. 정적·준동적 분석과 머신러닝 기반 악성 앱/행위 패턴 인식을 결합해 온디바이스 탐지·격리를 수행한다. VR 특성을 반영한 저지연·경량화 구조와 VR-친화 UX를 통해 안정적 보안 환경을 제공한다.
결 과 물
VRAV 메인페이지
블랙리스트 검사
VT검사 결과 조회
정적 검사
기 대 효 과
VR 보안 강화: 온디바이스 실시간 탐지로 사용자·시스템 보호
신뢰도 향상: 위장형 공격 차단으로 안전한 XR 환경 구축
자체 대응: 오프라인에서도 위협 탐지·격리 가능
확장성 확보: ML·룰셋 업데이트로 다양한 기기 대응
산업 활용: VR 보안 솔루션·정책 시스템에 적용 가능
@TEAM. VRAV

6.2 프로젝트 소개

시연 영상 링크

6.3 팀 소개