

# 2025. 11.

# 졸업 프로젝트 최종 발표

# Antivirus Development in Virtual Reality

VR 환경 속 백신 솔루션 개발

팀장 : 김명규

팀원 : 강민혁, 김민서, 김원태, 박준형



2025. 11. 04.

VRAY

# CONTENT

## 01 프로젝트 개요

- 프로젝트 배경 및 목적
- VR 특화 보안 솔루션의 중요성
- 목표 및 기대효과
- 일반 안드로이드 애플리케이션과의 차별점

## 02 구현 애플리케이션 소개

- 솔루션 아키텍처 설계
- 사용 기술 및 개발 환경
- 목표 및 구현 기능 도식화
- 프로젝트 진행 과정

## 03 주요 기능별 구현

- 블랙리스트 검사 (Hash 기반 방식)
- VirusTotal 연동 검사
- 정적 검사 (PE 기반 Manifest 분석)
- 동적 검사 (Background 행위 모니터링)
- 탐지 시연

## 04 향후 개선 방향 및 결론

- 프로젝트 핵심 성과 정리
- 기대효과
- 향후 발전 방향

### VR/AR/MR 시장동향 보고서 2024

#### 2021~2024년 VR/AR/MR 발전 현황



#### 2023.8 ~ 2024.4 주요 글로벌 VR/AR/MR 수혜처

|    |       |                                       |
|----|-------|---------------------------------------|
| 1위 | 교육    | 교육, 교육을 위한 솔루션과 교실의 VR 통합하여 교육 혁신     |
| 2위 | 의료    | 의료, VR 기술로 수술 훈련 및 진료 단계 부족 단계 해결 가능  |
| 3위 | 제조    | 제조, 제조시설 내 메타버스 통합하여 작업 효율성 강화        |
| 4위 | 농업    | 농업, 작업의 위험 감소 및 경험도 향상                |
| 5위 | 유희/주거 | 유희/주거, 우수한 콘텐츠 및 장난감으로 분야에 VR 메타버스 통합 |

# 프로젝트 배경 및 목적

## VR 시장 성장 및 보급 확대

### 최초의 안드로이드 XR 헤드셋, 갤럭시 XR을 소개합니다

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

이 프로젝트는



삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

### 새로운 갤럭시 XR에서 안드로이드 XR을 경험해 보세요

갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

- 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.
- 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.
- 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.
- 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

삼성 갤럭시 XR은 최초의 안드로이드 XR 헤드셋으로, 삼성은 최초의 안드로이드 XR을 선보이며, 혁신을 이끕니다.

# 프로젝트 배경 및 목적

평가하는 보안 취약점 및 위험

연구실

VR headsets can be hacked with an interception-style attack

## VR 헤드셋의 보안 취약점 발견...영화 <언셀선>식 공격 가능해지나

미국과 영국과 연구원들이 메타와 삼성의 VR 헤드셋을 해킹하여 방화벽 정보를 빼돌리고, 개인적인 정보를 유출하는 데 성공했다.

Metasploit Project 2024년 3월 19일



\*본 발표는 공개된 사용자들의 VR 헤드셋에 방화벽 정보를 빼돌리고, 개인적인 정보를 유출하는 데 성공했다고 발표 정보를 제공한 다. (현재 아직까지 검증)

# 프로젝트 배경 및 목적

## 기존 연구 동향 및 사례 분석

Submitted: 20 Apr 2023 (v1); Rejected: 23 Oct 2024 (last version: v4)

### Security and Privacy in Virtual Reality: A Literature Survey

**Alberto Sclafani** 가상현실 보안 및 개인정보 보호: 문헌 조사

Virtual reality (VR) is a multi-billion market that keeps growing, year after year. As VR is becoming pervasive in households and small businesses, it is critical to address the effects that this technology might have on the privacy and security of its users. In this paper, we explore the state-of-the-art in VR privacy and security, we categorize potential issues and threats, and we analyze causes and effects of the identified threats. Besides, we focus on the research previously conducted in the field of authentication in VR, as it stands as the most investigated area in the topic. We also provide an overview of other interesting uses of VR in the field of cybersecurity, such as the use of VR to teach cybersecurity or evaluate the usability of security solutions.

기존 모바일 보안 솔루션이 VR 특성을 충분히 반영하지 못하는 문제점을 설명

Submitted: 10th Dec 2023; Rejected: 1st Sep 2024 (last version: v3)

### Inception Attacks: Immersive Hijacking in Virtual Reality Systems

**Dandan Yang, Coby Yuenchen Li, Armin Shafie, Ben Y. Zhao, Helen Jiang**

현실권 공격: 가상현실 시스템에서의 몰입형 해킹

Today's virtual reality (VR) systems provide immersive interactions that seamlessly connect users with online services and one another. However, these immersive interfaces also introduce new vulnerabilities, making it easier for users to fall prey to new attacks. In this work, we introduce the inception hijacking attack, where a rogue attacker takes control of a user's interaction with their VR system, by trapping them inside a malicious app that masquerades as their VR interface. Once trapped, all other user's interactions with apps, services and other users can be recorded and modified without their knowledge. This not only allows traditional privacy attacks but also introduces new interaction attacks, where bad VR users encounter badly designed/immersive experiences during their interaction. We present an implementation of the inception hijacking attack on Meta/Quest headsets and conduct 400 app-level user studies that evaluate its efficacy and stealthiness. Finally, we discuss effectiveness and tradeoffs of various potential defenses, and propose a multifaceted defense pipeline.

VR 시스템에 특화된 새로운 공격 방식(인셉션 공격)을 통해, VR 환경에서 전통적 보안 솔루션이 무효

# VR 특화 보안 솔루션의 필요성

영양 1

VR 특화 보안 솔루션의 필요성

Meta Quest • Ray-Ban Meta • Apple Vision Pro

Meta Quest • Ray-Ban Meta • Apple Vision Pro

Meta Quest • Ray-Ban Meta • Apple Vision Pro

Meta Quest • Ray-Ban Meta • Apple Vision Pro

VR 특화 보안 솔루션의 필요성

Meta Quest • Ray-Ban Meta • Apple Vision Pro

Meta Quest • Ray-Ban Meta • Apple Vision Pro

검색 결과가 없습니다



Pixel Dungeon

# 목표 및 기대효과

## 기대 효과



VR 환경에 특화된 해션을 개발함으로써 악성코드로부터의 위협을 사전에 식별하여 안전한  
VR 생태계 구축

# 목표 및 기대효과

프로젝트 방향성



악성코드 수집 및 분석



탐지 엔진 개발



ML 고도화

# 프로젝트 진행 과정

팀원구성

## 앱 개발 팀



김민서 - UI/UX



김원태 - 백엔드



박문형 - 백엔드

## 악성코드 분석 팀



강민혁 - 악성코드 분석



김영규 - 악성코드 분석

# 사용한 기술 및 개발 환경

사용한 기술 및 개발 환경

## 앱 개발



## 개발 환경



Android  
Studio

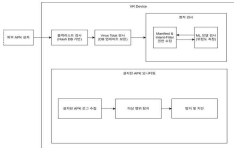
## 악성코드 분석



FRIDA

# 프로젝트 진행 과정

프로젝트 목표 및 구현 기능 도식화



# 안드로이드 애플리케이션의 특징

AndroidManifest.xml



앱의 "설계도/신분증"

- 앱 구성요소(Activities, Services, BroadcastReceivers, ContentProviders)
- 권한(카메라, 인터넷 등)
- 최소/타겟 SDK, 앱 ID, 필요 하드웨어/기능

등록 및 선언하지 않은 컴포넌트는 원칙적으로 사용할 수 없다.



# 일반 안드로이드 애플리케이션과 차별점

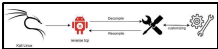
Meta Quest에만 존재

| Meta Quest                                                         | Android |
|--------------------------------------------------------------------|---------|
| <code>android.hardware.vr.headtracking</code> - 헤드 트래킹             | 해당 없음   |
| <code>com.oculus.supportedDevices</code> - 지원 헤드셋                  | 해당 없음   |
| <code>oculus.software.handtracking</code> - 핸드 트래킹                 | 해당 없음   |
| <code>com.oculus.vr.focusaware</code> - 시선 추적                      | 해당 없음   |
| <code>oculus.software.overlay_keyboard</code> - 시스템 오버레이 키보드       | 해당 없음   |
| <code>com.oculus.intent.category.VR</code> - VR 전용 인텐트 카테고리        | 해당 없음   |
| <code>com.oculus.permission.USE_SCENE</code> - 공간 행거 등 MR 공간데이터 접근 | 해당 없음   |

# 프로젝트 진행 과정

가상의 공격 시나리오 설정





기본 android 기반 reverse tcp

- 정상적인 앱으로 위장
- 앱 실행 시 tcp port 오픈
- 공격자 서버와 통신

포유리스 악재 관련 복제 단계

usb 문제



Customizing reverse tcp

- 정상적인 앱으로 위장
- 앱 실행 시 tcp port 오픈
- adb port(5555) 오픈
- 공격자 서버와 통신

## 프로젝트 진행 과정

악성 APK 설치 시 위험 시나리오 도출



사용자 키보드 이벤트를 수집을 통한 정보 유출



사용자 화면 노출을 통한 정보 유출

## 주요기능별 구현

**▶ 품목 리스트 검사 - 설치 시 검사와 수통 검사**

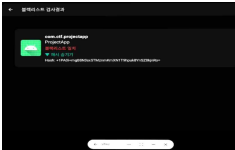
| Page | Page |
|------|------|
| 1    | 1    |
| 2    | 2    |
| 3    | 3    |
| 4    | 4    |
| 5    | 5    |
| 6    | 6    |
| 7    | 7    |
| 8    | 8    |
| 9    | 9    |
| 10   | 10   |
| 11   | 11   |
| 12   | 12   |
| 13   | 13   |
| 14   | 14   |
| 15   | 15   |
| 16   | 16   |
| 17   | 17   |
| 18   | 18   |
| 19   | 19   |
| 20   | 20   |
| 21   | 21   |
| 22   | 22   |
| 23   | 23   |
| 24   | 24   |
| 25   | 25   |
| 26   | 26   |
| 27   | 27   |
| 28   | 28   |
| 29   | 29   |
| 30   | 30   |
| 31   | 31   |
| 32   | 32   |
| 33   | 33   |
| 34   | 34   |
| 35   | 35   |
| 36   | 36   |
| 37   | 37   |
| 38   | 38   |
| 39   | 39   |
| 40   | 40   |
| 41   | 41   |
| 42   | 42   |
| 43   | 43   |
| 44   | 44   |
| 45   | 45   |
| 46   | 46   |
| 47   | 47   |
| 48   | 48   |
| 49   | 49   |
| 50   | 50   |
| 51   | 51   |
| 52   | 52   |
| 53   | 53   |
| 54   | 54   |
| 55   | 55   |
| 56   | 56   |
| 57   | 57   |
| 58   | 58   |
| 59   | 59   |
| 60   | 60   |
| 61   | 61   |
| 62   | 62   |
| 63   | 63   |
| 64   | 64   |
| 65   | 65   |
| 66   | 66   |
| 67   | 67   |
| 68   | 68   |
| 69   | 69   |
| 70   | 70   |
| 71   | 71   |
| 72   | 72   |
| 73   | 73   |
| 74   | 74   |
| 75   | 75   |
| 76   | 76   |
| 77   | 77   |
| 78   | 78   |
| 79   | 79   |
| 80   | 80   |
| 81   | 81   |
| 82   | 82   |
| 83   | 83   |
| 84   | 84   |
| 85   | 85   |
| 86   | 86   |
| 87   | 87   |
| 88   | 88   |
| 89   | 89   |
| 90   | 90   |
| 91   | 91   |
| 92   | 92   |
| 93   | 93   |
| 94   | 94   |
| 95   | 95   |
| 96   | 96   |
| 97   | 97   |
| 98   | 98   |
| 99   | 99   |
| 100  | 100  |

[illegible]

|    | id  | name |
|----|-----|------|
| 1  | 101 | 101  |
| 2  | 102 | 102  |
| 3  | 103 | 103  |
| 4  | 104 | 104  |
| 5  | 105 | 105  |
| 6  | 106 | 106  |
| 7  | 107 | 107  |
| 8  | 108 | 108  |
| 9  | 109 | 109  |
| 10 | 110 | 110  |
| 11 | 111 | 111  |
| 12 | 112 | 112  |
| 13 | 113 | 113  |
| 14 | 114 | 114  |
| 15 | 115 | 115  |
| 16 | 116 | 116  |
| 17 | 117 | 117  |
| 18 | 118 | 118  |
| 19 | 119 | 119  |
| 20 | 120 | 120  |
| 21 | 121 | 121  |
| 22 | 122 | 122  |
| 23 | 123 | 123  |
| 24 | 124 | 124  |
| 25 | 125 | 125  |
| 26 | 126 | 126  |
| 27 | 127 | 127  |
| 28 | 128 | 128  |
| 29 | 129 | 129  |
| 30 | 130 | 130  |
| 31 | 131 | 131  |
| 32 | 132 | 132  |
| 33 | 133 | 133  |
| 34 | 134 | 134  |
| 35 | 135 | 135  |
| 36 | 136 | 136  |
| 37 | 137 | 137  |
| 38 | 138 | 138  |
| 39 | 139 | 139  |
| 40 | 140 | 140  |
| 41 | 141 | 141  |
| 42 | 142 | 142  |
| 43 | 143 | 143  |
| 44 | 144 | 144  |
| 45 | 145 | 145  |
| 46 | 146 | 146  |
| 47 | 147 | 147  |
| 48 | 148 | 148  |
| 49 | 149 | 149  |
| 50 | 150 | 150  |

# 주요 기능별 구현

블랙리스트 검사 - 설치시 검사 & 수동 검사



# 주요 기능별 구현

Virus Total 검사 - 설치시 검사



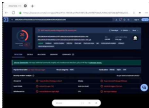
새로운 앱이 설치된 후 알림



새로 설치된 앱들의 VirusTotal 검사결과 조회 창

# 주요 기능별 구현

Virus Total 검사 - 설치시 검사



| 업 이름       | 결과         | 결과 링크                                                                 | 스캔시간           |
|------------|------------|-----------------------------------------------------------------------|----------------|
| SampleAPP  | Benign     | <a href="https://www.virustotal.com/">https://www.virustotal.com/</a> | 년 - 월 - 일 - 시간 |
| SampleAPP2 | Suspicious | ..                                                                    | ..             |
| SampleAPP3 | Malicious  | ..                                                                    | ..             |
| SampleAPP4 | Unknown    | ..                                                                    | ..             |

업 클릭 시 검사결과 페이지로 리다이렉트

알림 클릭 시 검사결과 페이지로 리다이렉트

# 주요 기능별 구현

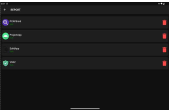
정책 검사 - 설치 시 검사 & 수동 검사

- 일반적인 안드로이드 애플리케이션과 VR 전용 애플리케이션의 차이점 적용
- AndroidManifest & Intent-Filter 기반 AI 검사
- 학습된 AI는 설치된 apk의 AndroidManifest 와 Intent-Filter를 검사하여 위험도 측정

| SCORE              | 악성 유무 |
|--------------------|-------|
| score < 0.5        | 안전    |
| 0.5 ≤ score < 0.75 | 위협    |
| 0.75 ≤ score       | 악성    |

# 주요 기능 별 구현

정책 검사 - 설치 시 검사 & 수동 검사



결과페이지

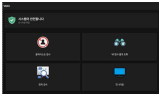


결과 리포트

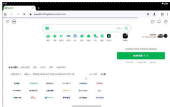
# 주요 기능별 구현

## 동적 검사 - background 실행

- 지속적으로 설치된 apk의 악성행위 모니터링
- 의심되는 외부 도메인(피싱 사이트 등)으로 정보 전송 시 알림 및 차단



모니터링 적용 상태



정상 접근가능

# 주요 기능별 구현

## 동적 검사 - background 실행

- 지속적으로 설치된 apk의 악성행위 모니터링
- 의심되는 외부 도메인(피싱 사이트 등)으로 정보 전송 시 알림 및 차단



실시간 모니터링 상태



접근 불가

# 향후 개선 방향 및 결론

프로젝트 핵심 성과 정리



VR 환경에 대한 위험 시나리오 수립



악성코드 수집 및 분석



ML 기반 탐지 솔루션 개발



모델 고도화



악성 도메인 수집 및 차단 강화

© 2020. 11.04

국립중앙도서관

## Antivirus Development in Virtual Reality

# Thank You

Team VRAY

김영규, 장민혁, 김민서, 김원태, 박준형