Andorid 악성 앱 분석을 위한 Unpacker 개발

지도 교수님: 양환석 교수님

요약

스마트폰 사용자 수가 증가함에 따라 스미싱, 몸캠피싱, 메신저 피싱과 같은 정보통신망을 이용한 범죄가 큰 폭으로 증가하고 있다. 이러한 범죄의 피해자는 다양한 연령층에서 발생하고 있다.
따라서 모바일 운영체제 점유율이 가장 높은 **안드로이드 운영체제를 대상으로 하는 패킹된 악성 앱 언패킹**을 수행하고 시그니처 기반 탐지 도구인 **Yara를 통해 악성 앱에 사용된 패커를 식별하는 통합 악성 앱 언패킹 시스템을 제공**하여 **악성 앱을 이용한 범죄 대응에 도움**을 줄 수 있을 것으로 기대된다.

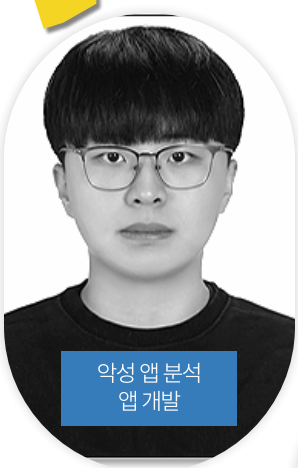
개발 목표

① 원본 Dex 파일 추출

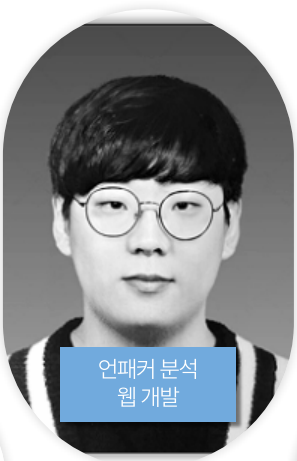
② Yara 시그니처를 응용한 패커 식별

③ 악성 앱 식별을 위한 MD5, SHA-1, SHA-256 해시 값 산출

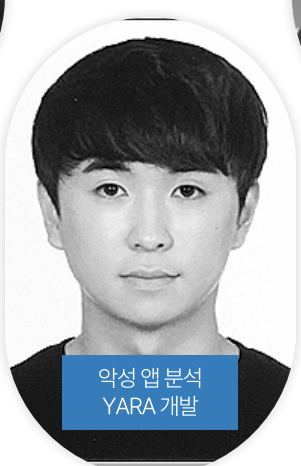
"웹 사이트에 악성 앱 파일 업로드 후, 사용된 패커 식별과 탐지된 라이브러리 및 리소스 확인 후 원본 Dex file 추출"



서동훈/총괄



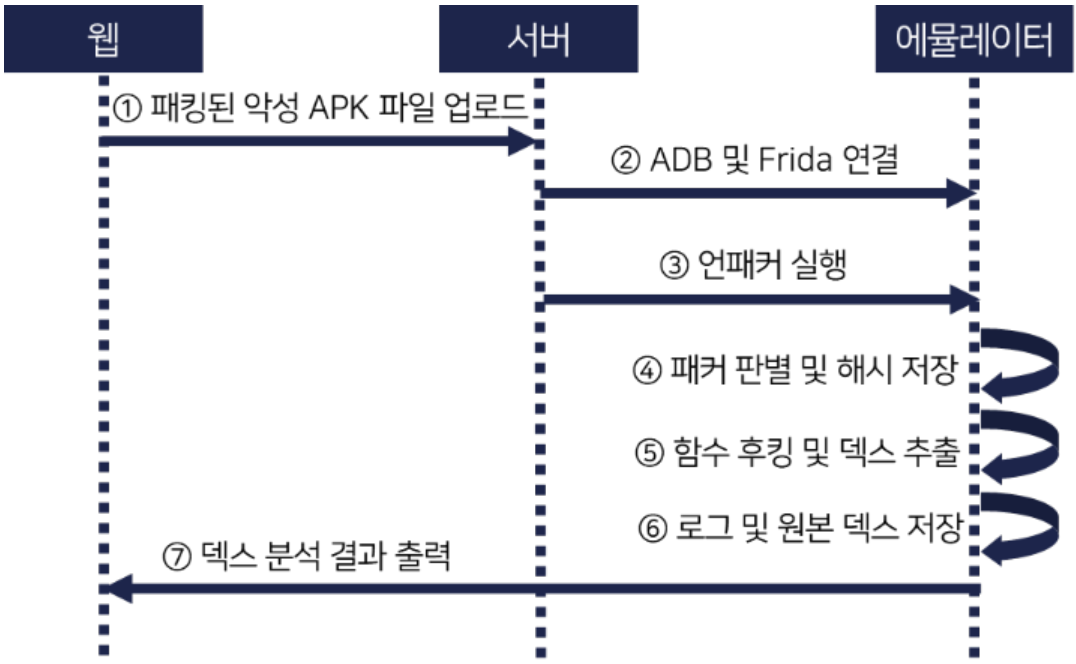
정재훈



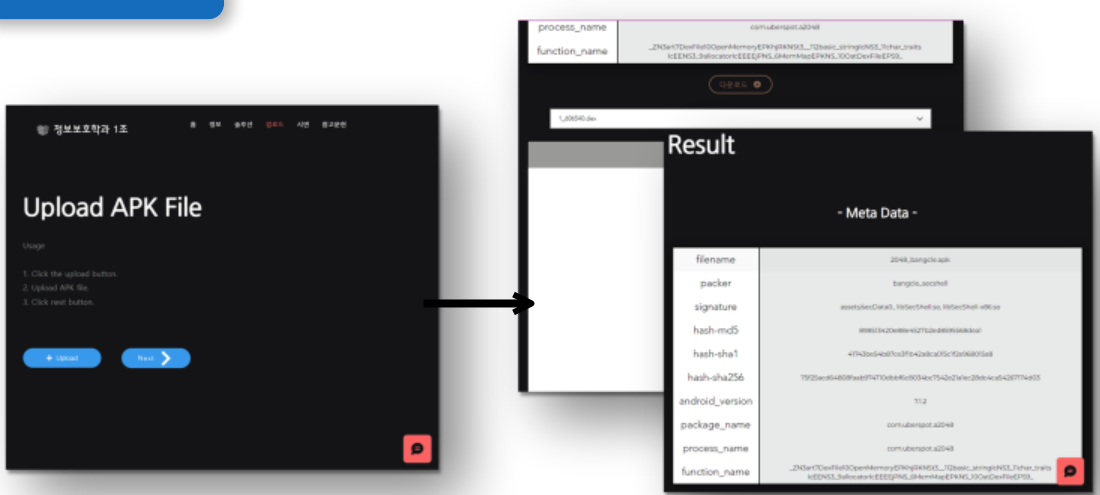
전유민

강민영

시스템 구상도



웹 페이지



〈업로드 페이지〉 〈결과 페이지〉