Android Packing

서동훈

Contents

패킹 이란...?

패킹 (Packing)

- 배포를 하기 위해 파일의 크기를 줄이거나 보안성을 높이기 위해 실행 파일을 압축하는 기술
- 실행 파일을 압축하고 압축된 데이터를 압축 해제 코드와 합쳐 하나의 실행 파일로 만드는 기술

패킹 이란...?

패킹 (Packing)

- 배포를 하기 위해 파일의 크기를 줄이거나 보안성을 높이기 위해 실행 파일을 압축하는 기술
- 실행 파일을 압축하고 압축된 데이터를 압축 해제 코드와 합쳐 하나의 실행 파일로 만드는 기술

Android APK Structure

APK (Android application package)

- 안드로이드의 소프트웨어와 미들웨어 배포에 사용되는 패키지 파일이다.
- 확장자는 '.apk'이며, ZIP파일 기반인 JAR를 기반으로 하는 압축 파일의 한 종류이다.

Android APK Structure

AndroidManifest.xml : 애플리케이션에 대한 주요 정보(패키지 이름, 구성 요소, ...)가 포함되어 있다.

META-INF : 인증 정보가 포함된 폴더

assets : 앱 실행에 필요한 자원이 모여있는 디렉토리(주로 동영상, 일부 문서 템플릿이 포함되며 빌드 X)

res : 앱 실행에 필요한 자원이 모여있는 디렉토리로 빌드시 설치 파일에 포함되어 설치된다.

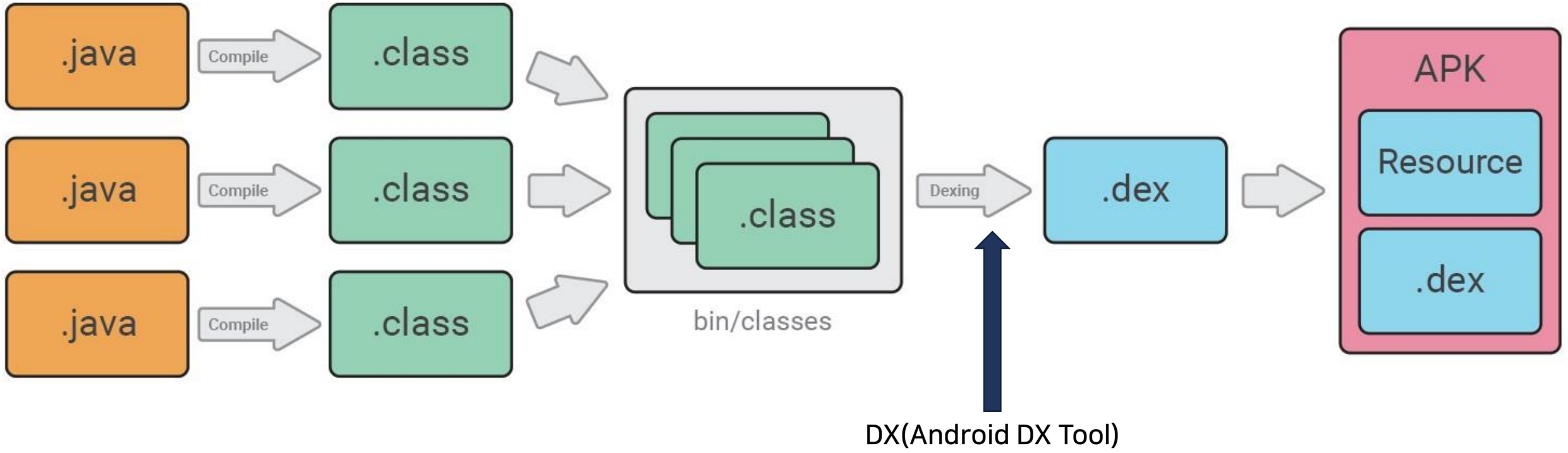
kotlin : 애플리케이션이 코틀린으로 작성된 경우만 생성되며, 코틀린과 관련된 데이터가 포함된다.

lib : 라이브러리 파일이 저장되어 있는 디렉토리

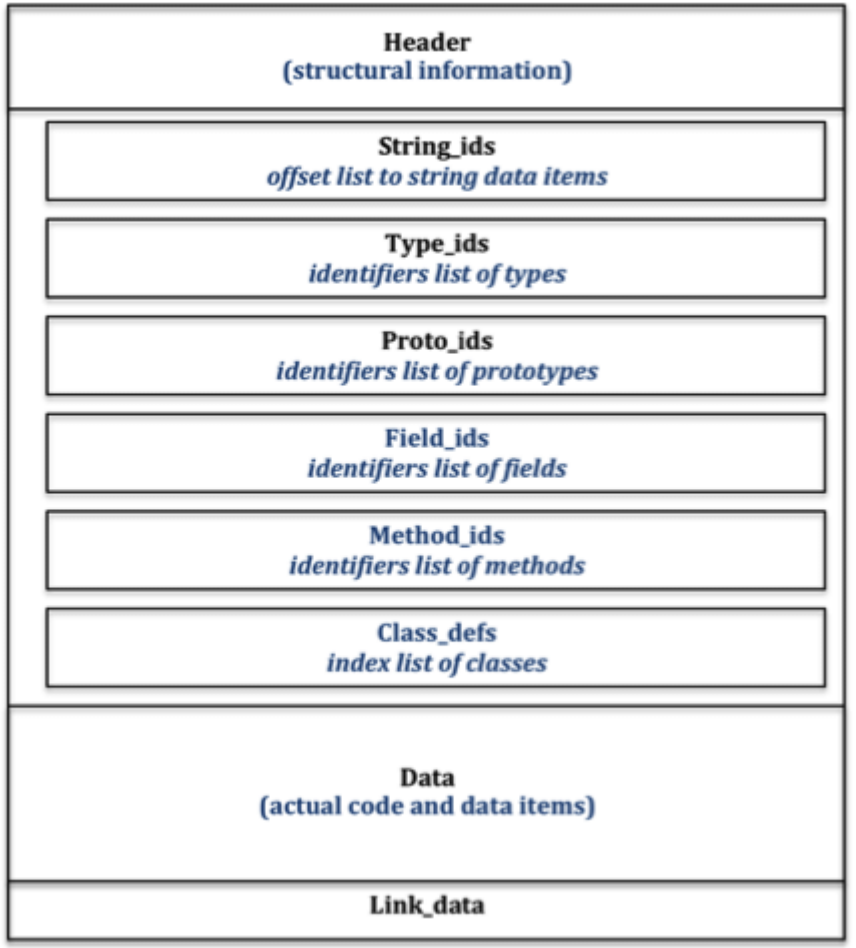
resources.arsc : 컴파일된 리소스가 포함된다.

classes.dex : Dalvik이 인식하도록 자바로 짜여진 코드를 컴파일하여 바이트 코드로 변환한 소스 파일

Android APK Structure

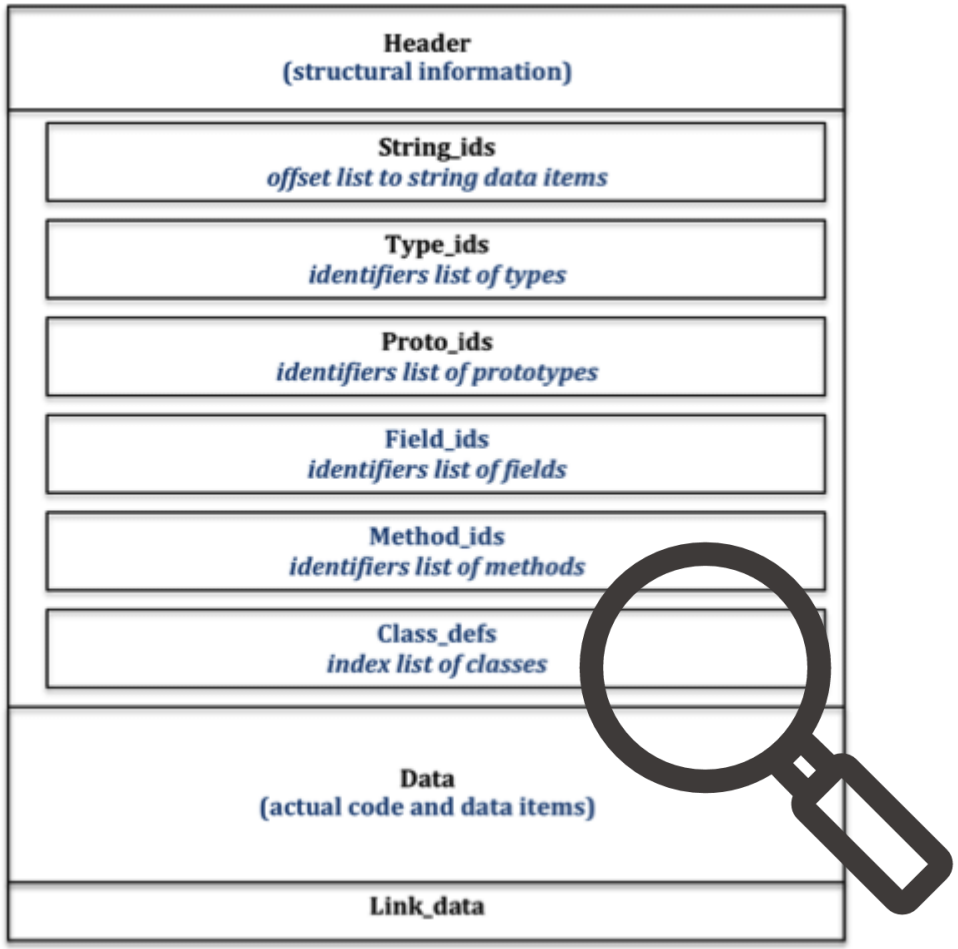


패킹이 필요한 이유



Dex file structure

패킹이 필요한 이유



Dex file structure

- Dex 구조는 이미 공개되어 있다.
- 바이트코드로 구성되어 있어 역공학에 취약

패킹이 필요한 이유

ProGuard

- Android에서 제공하는 무료 도구
- Java 코드를 압축, 최적화 및 난독화의 기능을 가짐

패킹이 필요한 이유

ProGuard

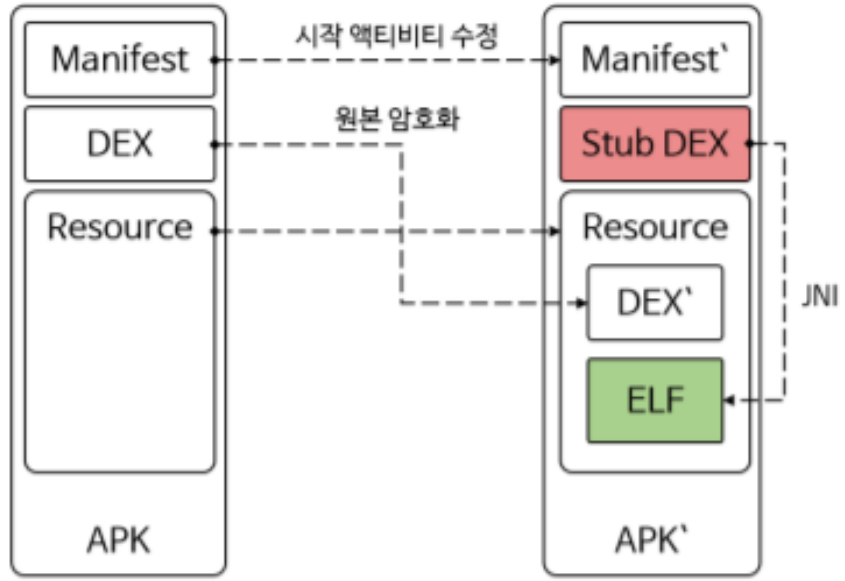
- Android에서 제공하는 무료 도구
- Java 코드를 압축, 최적화 및 난독화의 기능을 가짐

Semantics-Aware Machine Learning for Function Recognition in Binary Code

이와 같은 머신러닝을 통한 우회 기법들이 등장하여 우회가 가능해짐

안드로이드에서 패킹이란...?

- 원본 덱스를 암호화하여 리소스에 포함한 후 원본 덱스 자리에는 복호화를 수행할 스텁 덱스를 넣어 원본 덱스를 지키는 것
- 구현에 따라 원본 덱스의 위치는 바뀐다.
- 스텁 덱스도 결국은 바이트 코드이기 때문에 역공학에 취약
- 이를 보완하기 위해 JNI를 사용하여 네이티브 단계에서 진행
- 런타임 보호 기법 실행 -> 원본 덱스 복호화 -> 복호화된 덱스를 통해 클래스 로더 생성 -> 스텁 클래스 로더를 원본 클래스 로더로 치환 -> 원본 클래스 정보를 불러온 후 기존의 흐름대로 진행



기본적인 패킹앱 구조

Ref. 패킹된 안드로이드 어플리케이션의 안전한 실행을 위한 실행 환경 무결성 검증 기법

상용화된 패커 종류

Packer	Packer Protection Techniques							
	Code Obfuscation	Dynamic Code Loading	Dynamic Code Modification	Debugger Detection	Append shared Libraries	Additional Class insertion	DVM Support	ART Support
APKProtect	✔	✔	✔	✔	✔	✔	✔	✗
Ali	✔	✔	✔	✔	✔	✔	✔	✗
Baidu	✔	✔	✔	✔	✔	✔	✔	✔
Bangle	✔	✔	✗	✔	✔	✔	✔	✔
Ijiami	✔	✔	✗	✔	✔	✔	✔	✔
HoseDex2jar	✔	✔	✗	✔	✗	✗	✔	✗
Pangxie	✔	✗	✗	✗	✗	✔	✔	✗

Ref. Android Code Protection via Obfuscation Techniques:Past, Present and Future Directions

Q & A