DexGuard
GUARDSQUARE

안드로이드 앱을 위한최고의보안기술

안드로이드 앱과 SDK등은 해커들이 해킹 툴들을 사용하여 쉽게 디컴파일하고 앱 내부의 로직을 조사할 수 있습니다. 이러한 상황으로 인해 앱이 보안에 취약하게 되어 여러가지 방법으로 악용될 수가 있는데 지적 재산권을 도용하거나, 개인정보 탈취, 코드 위변조 및 앱 복제 등이 가능하게 됩니다

DexGuard 는 Java 와 **Kotlin** 를 사용한 앱이나 크로스 플랫폼인 **Unity3D** , **Cordova** , **Ionic** , **React Native** 등의 앱을 리버스 엔지니어링이나 위변조로부터 보호합니다 . **DexGuard** 는 다층의 난독화 및 암호화기술을 앱이나 SDK 에 적용하며 실시간 자체보호 메커니즘 (RASP) 을 앱에 적용하도록 합니다. 여러 단계의 보호층때문에 내부 로직을 알아내는 것이나 특정 기능을 바꾸는 것은 거의 불가능합니다.

간편한 설정, 원활한 통합

- DexGuard는 안드로이드 앱과 라이브러리를 처리하며, 최적화하고 보호하는 커맨드 라인 툴입니다.. 또한 소스코드를 공유하거나 변경없이도 앱을 보호할 수 있도록 합니다.
- DexGuard는 네이티브 Android (Java, Kotlin) 및 크로스 플랫폼 앱 (Cordova, Ionic, React Native, Unity) 에 대한 내장된 기본 지원을 제공합니다. DexGuard의 기능은 NDK 추가 모듈로 확장되어 네이티브 라이브러리를 처리하고 보호할 수 있습니다
- DexGuard는 앱 또는 SDK를 효율적이고 효과적으로 보호하는 데 도움이되는 기능을 제공합니다. 앱/SDK에 대한 보안 리포트는 앱/SDK의 출시 전에 보안을 검증하고 개선하는 데 도움이 됩니다.
- DexGuard는 Guardsquare의 실시간 해킹 모니터링 플랫폼인 ThreatCast와 원활하게 통합됩니다. ThreatCast는 앱에서 실제로 발생한 해킹 정보를 보여주고 지속적으로 변화하는 위협 환경에 맞게 보안 구성을 조정할 수 있도록 도와줍니다. ThreatCast는 무료로 Guardsquare 라이선스와 함께 제공됩니다.
- DexGuard는 ProGuard와 호환성을 가지므로 쉽게 DexGuard로 업그레이드 할 수 있습니다. ProGuard사용시 구성을 재사용할 수 있고 DexGuard를 통해 추가적으로 보호 계층을 구현할 수 있습니다.

helloworld@guardsquare.com www.guardsquare.com

GUARDSQUARE
Mobile application protection

DexGuard 는 여러가지 코드 하드닝 기술을 사용하여 앱이나 SDK 가 정적 분석에 대응하도록 합니다

식별자 난독화

DexGuard는 리소스명, 리소스 파일명, 자산(Asset) 파일명 및 리소스 XML 속성(Attribute)명 뿐만 아니라 클래스명, 필드명, 메소드명 및 네이티브 라이브러리명을 난독화합니다.

제어 흐름 난독화

DexGuard는 자동 및 수동적으로 코드를 분석하는 것을 막기 위해 소스 코드의 제어 흐름을 난독화 합니다 .

산술 난독화

DexGuard는 간단한 산술적 표현을 복잡하게 바꾸어 코드를 이해하지 못하도록 합니다.

데이터 암호화

DexGuard는 간단한 방법으로 찾아 해킹 당할 수 있는 민감한 문자열(string)을 암호화 합니다. 또한 클래스, 자산 파일, 리소스 파일 및 네이티브 라이브러리를 암호화합니다.

코드 가 상화

코드 가상화는 메소드 구현을 임의로 생성된 가상 머신을 위한 명령으로 변환시킵니다.

호출 숨김

는 서명 검증 API나 암호화하는 API 등 안드로이드에서 기본적으로 사용되며 보안에 민감한 API 를 은폐합니다.

네이티브 코드 난독화 | Requires NDK add-on

DexGuard는 네이티브 라이브러리와 앱 코드 간의 인터페이스를 포함하여 리버스 엔지니어링 및 앱 위변조로부터 네이티브 라이브러리를 보호하여 줍니다 .

안드로이드 로깅 코드 제거

DexGuard는 로깅, 디버깅 및 테스트 코드 등 중요 정보를 유출하는 코드를 제거합니다.

DexGuard 는 다양한 실시간 자체 보호 메커니즘(RASP)을 사용하여 동적 분석 및 실시간 해킹으로부터 앱이나 SDK를 보호합니다.

SSL 피닝

DexGuard는 중간에 발생될 수 있는 공격(man-in-the-middle-attack)을 방지함으로써 앱이나 SDK가 목적하는 서버에 연결될 수 있게 합니다.

인증서 확인

DexGuard는 앱이 원래의 인증서로 서명되었는 지 확인할 수 있는 기능을 제공합니다.

루팅 탐지

DexGuard 는 앱이나 SDK 가 루팅된 디바이스에서 작동하는지 루팅을 은폐하는 프레임워크에서 작동하는지를 조정할 수 있도록 합니다.

위변조 탐지

DexGuard는 앱이나 SDK가 불법적인 소스 코드 변경을 탐지할 수 있게 하며 개별 파일의 무결성을 확인할 수 있도록 합니다.

디버거 및 에뮬레이터 탐지

DexGuard 는 앱이나 SDK 가 디바이스 환경의 무결성을 검증할 수 있도록 하여 디버깅 툴 및 에뮬레이터를 사용하는 지를 탐지할 수 있도록 합니다.

후킹 탐지

DexGuard는 후킹 프레임워크들을 사용하여 앱이나 SDK 의 동작을 변경하려는 시도를 탐지하고 방지할 수 있습니다.

Guardsquare 는 모바일 앱 보안 분야의 글로벌 리더입니다. 주요 산업 분야의 전 세계 700 개 이상의 기업 고객이 Guardsquare를 사용하여 리버스 엔지니어링 및 해킹으로부터 모바일 앱을 보호합니다. 오픈 소스 **ProGuard** 기술을 기반으로 구축된 Guardsquare 소프트웨어는 앱의 개발과 정에 투명하게 통합되며 Android(DexGuard) 및 iOS(iXGuard) 앱을 여러 보호 계층을 사용하여 온 디바이스 공격과 오프 디바이스 공격 모두에 대해 보호합니다. 모바일 앱 보안 콘솔인 ThreatCast를 추가함으로써 Guardsquare 는 오늘날 시장에서 가장 완벽한 모바일 앱 보안 솔루션을 제공합니다

GUARDSQUARE
Mobile application protection

helloworld@guardsquare.com
www.guardsquare.com