DexGuard

GUARDSQUARE

State-of-the-art protection for Android apps

DexGuard is Guardsquare's state-of-the-art mobile security software. It has been specifically developed to protect Android applications and SDKs from reverse engineering and hacking.

DexGuard protects your applications and SDKs against static analysis using multiple code hardening techniques.

Name obfuscation

DexGuard obfuscates the names of classes, fields, methods and native libraries, as well as the names of resources, resource files, asset files and resource XML attributes.

Control flow obfuscation

DexGuard obfuscates the control flow of the code inside the methods to hinder automated and manual code analysis.

Arithmetic obfuscation

DexGuard transforms simple arithmetic and logical expressions into difficult to analyze code. This enables you to hide common expressions, such as simple loop increments, and to protect proprietary formulas.

Call hiding

DexGuard adds reflection to access-sensitive APIs, such as the standard Android APIs for signature validation or cryptographic operations.

Code packing

DexGuard can efficiently encrypt all combined bytecode as an additional layer of protection.

Encryption

DexGuard encrypts sensitive strings to prevent hacking attempts through trivial searches. It also encrypts classes, asset files, resource files and native libraries.

Native code obfuscation

DexGuard obfuscates JNI function names in native libraries and in the Dalvik bytecode.

Removal of Android logging code

Logging code can provide information about the structure and execution flow of the applications and SDKs. DexGuard removes logging, debugging and testing code to thwart any attempt at exploiting this information.

Protection of WebView and Cordova

DexGuard encrypts the contents of WebView and Cordova/Phonegap applications (html, css, js, etc.).

helloworld@guardsquare.com www.guardsquare.com

DexGuard shields your applications and SDKs against dynamic analysis and live attacks using various runtime self-protection mechanisms.

SSL pinning

DexGuard makes sure the protected application or SDK is connecting to the intended servers, preventing man-in-the-middle attacks.

Certificate checks

DexGuard gives your application the ability to make sure it has been signed with the original certificate.

Tamper detection

DexGuard enables your application or SDK to detect illegitimate code modifications and to verify the integrity of individual files.

Root detection

DexGuard enables your application or SDK to control whether it is running on a rooted device or a device using a root cloaking framework.

Debugger and emulator checks

DexGuard enables your application or SDK to verify the integrity of its environment, detecting the use of debugging tools and emulators.

Hook detection

DexGuard enables your application or SDK to detect and prevent attempts by hooking frameworks to modify its behavior.

Multiple, mutually reinforcing layers

Code hardening and runtime protection are complementary security strategies. Name obfuscation, string encryption, reflection, asset encryption, resource encryption and native library encryption prevent hackers from gaining insight into the source code of your application. Tamper detection and environment checks shield the application while it is running. Class encryption provides a final layer of protection: it makes sure the runtime protection libraries are not modified or removed and completely hides the decryption and reflection code.

helloworld@guardsquare.com www.guardsquare.com

GUARDSQUARE
Mobile application protection

DexGuard performs optimizations that can significantly reduce the size and improve the performance of your application or SDK.

DexGuard reduces the size of your application by shrinking your code and resources. It performs various optimizations to reduce the size of resource configurations and optimize the Dex file structure. DexGuard's optimizations provide an additional layer of security by removing logging code, debugging and testing code that can leak sensitive information.

Seamless integration

- DexGuard enables you to fully protect your application in-house. It doesn't require you to share your source code.
- DexGuard integrates transparently into the build process and requires no changes to your source code. It comes with plugins for all common build tools and development environments (Gradle, Android Studio, Ant, Eclipse, Maven and custom builds). DexGuard can also post-process APK files.
- DexGuard is backward compatible with ProGuard. This enables you to upgrade easily.
- DexGuard comes with a plugin for Android Studio, supporting syntax highlighting, autocompletion and highlighting of potentially suboptimal or erroneous configuration. DexGuard automatically generates configurations for library projects that will be successively obfuscated.
- Extensive customization options, including customizable encryption algorithms, enable you to adapt the applied layers of protection to your security and performance requirements.
- DexGuard backports Java 8 functionality, providing universal support across all versions of Android.
- DexGuard automatically creates Instant Apps from traditional installed app projects, without requiring project restructuring or manual code refactoring.

Optional add-ons for extra protection

NDK

DexGuard NDK

DexGuard's plugin for the Android NDK (Native Development Kit) can harden your native libraries at an advanced level. It provides string encryption, arithmetic obfuscation and control flow obfuscation. The NDK add-on is compatible with ndk-build and CMake.

This add-on is used to build the native libraries in C/C++ code and harden them during the build process. The add-on applies string encryption and code obfuscation at the SO binary level.

Secure Keyboard

DexGuard offers an SDK with a keyboard implementation that is hardened against keylogging and other forms of snooping.

When a user enters confidential data using a keyboard, there is a risk that this data is intercepted by malicious software. This SDK ensures that the keyboard is secure and that the entered information is transferred to the intended recipient.

Device Fingerprinting

DexGuard's device fingerprinting SDK can determine the identity of devices, for instance as a parameter to assess the risk of sensitive transactions.

A device fingerprint is a unique identifier for a remote computing device, such as a smartphone. It can be used to determine the risk associated with certain transactions. A log-in attempt from a device that is not usually used by a particular user can be recognized as suspicious and blocked or subjected to additional authentication checks.