GUARD SQUARE

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

DexGuard

- Adds multiple, mutually reinforcing layers of protection to Android applications and SDKs. These layers are polymorphic, i.e. variable throughout the application and different in each single implementation.
- Offers extensive customization options, enabling you to adapt the applied protection to your security and performance requirements.
- Allows you to plug in proprietary algorithms for the encryption and decryption of classes, strings, resources, assets and native libraries. The use of this patent-pending feature results in a less predictable and thus stronger form of encryption.
- Combines protection techniques and optimization techniques. It improves the performance of Android applications and SDKs and reduces their size while effectively shielding them from reverse engineering attempts and hacking attacks.
- Integrates transparently in the build process: the source code of the applications and SDKs you want to protect does not need to be adapted manually.
- Supports the use of several popular security libraries (IOCipher, NetCipher, SQLCipher, Conceal, KeyCzar, SecurePreferences).
- Is fully compatible with ProGuard and with all common build tools and development environments (Gradle, Android Studio, Ant, Eclipse, Maven and custom builds).

DexGuard offers protection against static 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.

- ### Class Encryption

  DexGuard allows you to specify which classes should be encrypted in order to effectively hide critical code.

- ### Call Hiding

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

- ### Control Flow Obfuscation

  DexGuard obfuscates the control flow of the code inside the methods to confuse automated and manual code analysis by decompilers, specialized tools and determined hackers.

- ### Name Obfuscation

  DexGuard obfuscates the names of classes, fields and methods.

- ### Protection of WebView and Cordova

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

- ### String Encryption

  DexGuard allows you to determine which strings should become illegible in the code to preclude hacking through trivial searches.

- ### Removal of Android Logging Code

  DexGuard thoroughly removes logging, debugging and testing code.

- ### Native Library Encryption

  DexGuard uses advanced encryption algorithms to shield the native code from reverse engineering.

- ### Native Code Obfuscation

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

- ### Obfuscation of Native Library Names

  DexGuard consistently renames native libraries in the bytecode and in the native code.

- ### Asset Encryption

  DexGuard encrypts asset files and decrypts them on the fly.

- ### Resource Obfuscation

  DexGuard obfuscates the names of resources, resource files and resource XML attributes.

- ### Encryption of Resource Files

  DexGuard encrypts entire XML files, further raising the bar against reverse engineering, theft of intellectual property and tampering.

DexGuard provides protection against dynamic analysis and live attacks.

- ### Environment Checks

  DexGuard enables your application to check whether the device on which it is running has been rooted or is using a root cloaking framework such as Xposed or Cydia Substrate. It also gives the application the ability of detecting debugging tools and emulators.

- ### SSL Pinning

  DexGuard makes sure the protected application 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 ensures that your application reacts appropriately if a hacker has tried to modify it or is accessing it illegitimately.

DexGuard optimizes Android applications and SDKs.

- ### Code Optimization

  DexGuard improves the performance of applications and SDKs by applying optimization techniques such as method inlining, constant propagation and enumeration simplification.

- ### Resource Optimization

  DexGuard does not only optimize the code, but also the resources (constant propagation in resources and code).

- ### Removal of Unused Code

  DexGuard removes redundant classes, fields, methods and instructions, significantly reducing the size of applications and SDKs.

- ### Removal of Unused Resources

  DexGuard removes unused resources and resource files.

- ### Automatic Splitting of Dex Files

  DexGuard automatically splits Dex files that exceed the size constraints imposed by the format.

- ### Removal of Unused Native Libraries

  DexGuard removes unused (parts of) native libraries.

DexGuard can be extended with optional add-ons.

- ### 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 and arithmetic obfuscation.

- ### Whitebox Cryptography

  DexGuard offers an SDK for whitebox cryptography, to encrypt and decrypt dynamic data with a whitebox implementation of the AES algorithm.

- ### Secure Keyboard

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

- ### 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.

GUARD SQUARE

Our software protects mobile applications while making them smaller and faster. GuardSquare's open source solution ProGuard is included in SDKs by Oracle, Intel and Google. It has been downloaded tens of millions of times since its release in 2002 and has a user community of over one million developers. Building on the success of ProGuard, we now offer DexGuard, premium software for the protection of Android applications against reverse engineering and hacking. Our client base spans a broad range of industries, from telecommunication, e-commerce and financial services to gaming and new media. We have our headquarters in Leuven (Belgium) and are currently setting up offices in Asia, the Middle East and North America.

helloworld@guardsquare.com **www.guardsquare.com**