iXGuard

GUARDSQUARE

Cutting-edge protection for your iOS apps

iOS applications and SDKs are not immune to reverse engineering. Hackers can use easily available tools to disassemble and inspect your iOS applications and SDKs to gain insight into their inner workings. This leaves apps vulnerable to various forms of abuse, including intellectual property theft, cloning, credential harvesting, API key extraction and code tampering.

iXGuard has been designed to protect your iOS applications and SDKs against reverse engineering and hacking. It hardens their code using a variety of obfuscation and encryption techniques. The applied layers of protection make it virtually impossible to gain insight into their internal logic.

Secure development made easy

- iXGuard processes your project as a whole, including libraries and extensions. This enables stronger and more extensive hardening.
- iXGuard does not require any changes to the source code of your applications or SDKs.
- iXGuard has no impact on your development process. It functions as a stand-alone solution that processes your compiled applications.
- iXGuard is easy to configure. It can be set up to protect entire applications or specific functions with a single configuration file.

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

Name obfuscation

iXGuard obfuscates identifiers in both Swift and Objective-C code to hide semantic information from reverse engineers. Most common reflection constructs are supported out-of-the-box.

String encryption

iXGuard encrypts sensitive strings in your applications and SDKs using a random algorithm and a new key for each single string. This prevents API endpoints, tokens etc. from leaking.

Control flow obfuscation

iXGuard hides the original function logic to better shield your applications and SDKs against automated and manual code analysis.

Arithmetic obfuscation

iXGuard transforms arithmetic statements into more complex but equivalent alternatives to conceal the original computation. The transformations yield different outcomes in every single build.

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

Jailbreak and debugger detection

iXGuard enables your application to monitor the integrity of the environment in which it is running. It lets you determine how the application should react when a potentially harmful environment is detected.

Repackaging detection

iXGuard makes sure your application has not been repackaged by a third party by performing signature-based checks and by comparing additional fields of the binary with the observed state at compile time.

Hook detection

iXGuard enables your application to detect and prevent attempts by hooking frameworks (i.e. Frida or Cydia Substrate) to modify its behavior.

Requirements

- Xcode version 8.3.3 to 10.2
- Bitcode-enabled archive build

U.S. Toll-Free Phone: 888-690-2424
International Phone: +1-952-933-1223
info@entrust.com
entrust.com

GUARDSQUARE
Mobile application protection

ENTRUST