DATASHEET

appdome

TOTALCode™ Obfuscation

DOING MORE WITH LESS TO PROTECT APPS AND SERVICES

Appdome's TOTALCode Obfuscation changes the traditional obfuscation paradigms and ushers in new options to obfuscate binaries and post-production apps. TOTALCode makes obfuscation applicable to any app, without accessing its source code. There is no need to attempt code obfuscation in source code or waste time in lengthy trial and error scenarios just to get to a "semi" obfuscation outcome.

Appdome's TOTALCode Obfuscation provides a complete binary based obfuscation, agnostic to build system, tools and source code languages. There is no optimization to code, no change to app logic required, and no impact to the operation, performance or functionality. An entire app can be obfuscated, with no development effort, and just with a click of a button.

THE BASICS OF CODE OBFUSCATION

Code obfuscation is a must in order to protect a mobile app's internal logic, intellectual property, frameworks, language, and structure. It makes the "reading" of an app's binary/compiled code difficult and impractical.

The goal of code obfuscation is to confuse and frustrate hackers while they try to uncover how an app works. Before Appdome, the only way to integrate code obfuscation was by compiling/adding/coding the obfuscation technique into an app's source code.

THE CHALLENGE OF OBFUSCATION IN SOURCE CODE

Obfuscation of source code in a mobile app isn't easy on developers. Developers have to decide what needs to be obfuscated, modify code to "comply" with obfuscation techniques, and be limited in choosing programming languages, frameworks and build environments.

Obfuscating an entire app's source code always comes with additional and significant performance impact.

More importantly, there are parts of an app that cannot be obfuscated in the source code. For example, strings and secrets that point to external services, third-party SDK vendors and language dependent constructs. These elements remain non-obfuscated or in the clear form, and provide hackers with just enough data to reverse engineer an app.

In addition, it requires major proficiency to obfuscate code without integration help from a third-party. A developer thinks he has obfuscated the source code but an experienced hacker will "see right through it".

ob·fus·cate
(IPA: ['äbfəˌskāt]):
From latin "Obfuscare" meaning darkened. Making unintelligible/ dark; contrary to popular belief, this is not the combination of "obscure" and "complicate", though the interpretation is quite understandable.

WHAT IS TOTALCODE OBFUSCATION?

Appdome's TOTALCode Obfuscation obfuscates the entire app binary, protects workflows, business logic, secrets, strings and data constructs throughout the binary, without exposing the source code.

By selecting the ONEShield option at the Appdome platform, users can apply TOTALCode Obfuscation to an entire app – protecting the implementation, code, framework, structure, logic, strings and secrets contained in the app. No other obfuscation method in the market comes even close to achieving this outcome – without accessing the source code.

BENEFITS OF TOTALCODE OBFUSCATION:

- ✓ **Eliminates obfuscation tradeoffs**
  Developers don’t need to make tradeoffs between securing their app, build environments and selection of services.
- ✓ **No performance and functionality impact**
  Binary obfuscation, unlike source code obfuscation, works seamlessly within the app, with no impact to performance, usability and functionality.
- ✓ **Obfuscate third-party service implementations (SDKs)**
  TOTALCode Obfuscation protects third-party integration such as services, SDKs and APIs into an app.
- ✓ **Obfuscate strings and secrets in the app**
  The Achilles heel of all other obfuscation methods is strings and secrets contained in an app. As long as they are in clear text, obfuscation is always reversible. TOTALCode Obfuscation operates at the binary level, delivering obfuscation strength to strings and secrets.

Appdome’s TOTALCode Obfuscation enables choice driven and complete app protection, without requiring access to the source code. Now, anyone can obfuscate apps with a click of a button.

HOW APPDOME’S TOTALCODE OBFUSCATION WORKS WITH IOS AND ANDROID APPLICATIONS:

	iOS	Android
Binary Code Obfuscation	Appdome scrambles the code parts. So, when an attacker tries to load an iOS application into a reversing tool (IDA/Hopper), the internal referencing code-to-code or data-to-code will either show up as irrelevant or give an error message. No “map” of the .ipa will be visible using these tools.	Appdome encrypts dynamic shared libraries (which contains native code stored inside an application’s package (APK)). So, when an attacker tries to load an Android application into a reversing tool (IDA/Hopper), the attacker will not be able to analyze the dynamic libraries even if they are extracted directly from the APK or device. No “map” of the .apk will be visible using these tools.
Flow Relocation	Appdome relocates parts of the code to a separate binary location. This makes it extremely difficult to read an application’s logic or structure as referenced locations do not exist within the obfuscated executable binary.	Appdome replaces function calls (a.k.a. invocations) with obfuscated calls. This makes it extremely difficult to read an application’s logic or structure because the obfuscated calls "cover the tracks" of an application’s logic and structure.
Non-native Code Obfuscation	Appdome extends the reach of obfuscation to non-native code (i.e. Cordova, React Native, Xamarin, etc.) in apps. As the files are obfuscated, it makes it impossible for malicious agent to extract the files for reverse-engineering.	Appdome extends the reach of obfuscation to non-native code (i.e. Cordova, React Native, Xamarin, etc.) in apps. That means malicious agent that extract files to perform reverse-engineering can no longer do so as the files are now obfuscated.
Strip Debug Information	Appdome eliminates all information such as debug symbols, which is not required for the application to function. This means that attackers cannot search for obvious application pointers such as "password" to figure out how an application does password validation. Appdome eliminates this information during the Fusion process.	Appdome eliminates all information such as debug symbols, which is not required for the application to function. In addition, on Android, DEX files (compiled Java/Kotlin code) usually comes with extra information to aid developers in identifying the purpose of certain parts of the code. Appdome eliminates this information during the Fusion process.

To learn more about Appdome’s TOTALCode Obfuscation, visit www.appdome.com, open a free Appdome account and start fusing!

ABOUT APPDOME

Appdome is the industry’s first cloud hub for mobile integration. Appdome enables the rapid integration of multiple third-party functions to apps, shortening the deployment cycle and connecting mobile apps to other services on demand. The codeless service operates as a mobile integration workflow in the cloud and allows users to perform integr ation projects on the final application package. No source code or de velopment expertise is required. Likewise, no modifications to an app or an SDK are required to complete integ ration projects on Appdome. The solution is currently used b y the world’s leading financial, healthcare and e-commerce companies to support productivity, compliance, and security for consumers and employees. Appdome was rated a Cool Vendor in Mobile Security by Gartner in 2015. For more information, visit www.appdome.com.