DATASHEET

appdome
SECURITY SUITE

COMPLETE MOBILE APPLICATION PROTECTION - NO CODING REQUIRED

Appdome's Mobile Security Suite is a comprehensive, best practice mobile security feature set that can be added to any Android or iOS app by anyone in minutes. Mobile developers and non-developers alike can add sophisticated runtime application self-protection (RASP) features like anti-tampering, anti-debugging, code obfuscation and more, to apps quickly and easily. This prevents malicious threats to mobile users, apps and data. Every feature in Appdome's Mobile Security Suite is applied directly to the app binary - no source code or coding required. The key features of Appdome Security Suite are as follows:

MOBILE DATA LOSS PREVENTION

Data at Rest Encryption

Protects mobile app data with dynamic AES 256-CTR (industry standard cryptographic protocols), without any dependencies on data structure, databases or file structures. Developer options allow users to exclude certain file types, files, folders or media files from being encrypted. Discrete blocks of data are encrypted and placed in a self-contained and segregated environment to isolate mobile app data from other resources. This makes it impossible for non-secure apps on the same device or different devices to decrypt and open this encrypted data.

Data Loss Prevention

Appdome offers two data loss prevention features. Copy and paste protection prevents data leakage via mobile apps by prohibiting users from copying and pasting mobile app data outside the app. Disable Screenshots prevents application screen captures (i.e., users from taking screen shots) of what is displaying on an app and also prevents the operating system from taking automatic screenshots.

OPERATING SYSTEM INTEGRITY

Jailbreak and Root Protection

Detects if a device has been jailbroken (iOS) or rooted (Android). If the device has been jailbroken or rooted, Fused apps can be configured to shut down or "exit." Developer options also allow users to create in-app workflows for this event.

Detect Unknown Sources

Detects if a mobile device has been set to allow app install from "unknown sources." If the setting has been enabled, Fused apps can be configured to shut down or "exit." Developer options also allow users to create in app workflows for this event.

MOBILE DATA PRIVACY

In-App Pin Code

Adds a simple or complex pin code to Android or iOS apps (including TouchID and face recognition).

Mobile Permission Control™

Disables certain features in apps that you fuse, so that the apps will be more secure. For example, prevent app screen sharing, blur the application screen, disallow access by the app to camera, microphone, location (GPS), local contacts and local calendar and allow in-app calls and messages only.

COMPLIANCE

FIPS 140-2 Cryptographic Modules (available upon request)

Adds FIPS 140-2 certified versions of the commercially available encryption libraries to be implemented to apps. You may choose to have Appdome use FIPS 140-2 certified cryptographic modules for data at rest encryption and network connections.

App Expiration

Sets conditions under which the fused app will no longer function such as a time bound condition.

SECURE COMMUNICATION

Trusted Session Inspections

Protects against malicious proxies and Man-in-the-Middle (MITM) attacks. Detects if a session is intercepted by an unauthorized or unknown party and redirected to a server or proxy. By keeping track of SSL sessions and validating the CA authenticity as it is being sent, it delivers malicious proxy detection whether the proxy is internal or external to the mobile device. It can also prohibit state sessions to prevent authorized session reuse and SessionID reclaiming.

SSL Certificate Validation

Verifies certificates and Certificate Authorities (CAs) to ensure that apps are only communicating with trusted sites with valid and authentic certificates. The Appdome administrator can manually add known trusted certificates to a whitelist. Appdome ensures that all communication with external sources is conducted over secure or encrypted transport protocols such as SSL and TLS.

Manual Whitelisting

To limit app access to just a handful of known sites, you can manually enter the sites that you want the app to communicate with. When that is done, all other sites will be blocked.

Hostname Verification

Some apps don't verify hostnames in their certificate pinning schemes. This exposes the app to possible MiTM attacks. Appdome verifies hostnames for all CAs to protect our customers' apps against MiTM attacks.

TOTALCODE™ OBFUSCATION

Appdome's proprietary binary based obfuscation method obfuscates the entire app binary, including the framework and non-native filesystems, without source code or developer implementation. Appdome protects the entire app, including apps built in Cordova, React Native, Xamarin and other modern frameworks. Advanced features include Flow Relocation to obfuscate control flows and business logic across the binary, without the need to code or expose source code. Strip debug symbols removes source code file names, line numbers, and variable names.

ONESHIELD™ APP SHIELDING

Anti Debugging-Tampering-Reversing

Appdome's comprehensive app shielding prevents others from debugging, tampering with or reverse engineering your apps. With Appdome, even the most sophisticated hacker cannot understand how your apps work. Your app will be shielded from changes and modifications by others. Additionally, key logical elements and resources such as methods, protocols and assets will be encrypted to make reverse engineering impossible.

Encrypt Strings and Resources

Encrypt all the apps' constants, strings and run-time information, removing critical loopholes hackers use to infiltrate apps.

Encrypt In-App User Preferences

Encrypt preferences such as username, email, contact information and other PII data that are otherwise stored in the clear inside an app, ensuring user and resource privacy inside of the app.

Checksum Validation

Appdome performs checksum validation to calculate a unique hash or fingerprint of binary data and assets and validates them at runtime. This prevents changes to your app, its resources, code, configuration and more.

Obfuscate Fused Services

Appdome's proprietary binary based obfuscation method obfuscates Appdome-fused services added to the app. This protects service implementations against hacking and reverse engineering.

App Integrity and Structure Scan

Check your app's composition, data structure, data elements, and communication paths to validate the integrity and authenticity of the app. It also detects elements within the app which could be used as attack vectors such as unknown or malicious URLs.

ABOUT APPDOME

Appdome is the industry's first cloud hub for mobile integration. Appdome's patented* technology enables the rapid integration of multiple third-party functions to apps, shortening the deployment cycle and connecting mobile apps to other services on demand. This codeless service operates as a mobile integration workflow in the cloud and allows users to perform integration projects on the final application package. No source code or development expertise is required. Likewise, no modifications to an app or an SDK are required to complete integration projects on Appdome. The solution is used by the world's leading financial, healthcare and e-commerce companies to support productivity, compliance, and security for consumers and employees. For more information, visit www.appdome.com.

*Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.