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, mobile data encryption and more, to apps quickly and easily. This prevents malicious threats to mobile users, apps and data and protects the app against all OWASP Mobile top 10 risks. 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:

TOTALDATA™ ENCRYPTION

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. 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 an non-authorized user to decrypt and open this encrypted data.

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.

Encryption Control (Requires Appdome-DEV)

Customers who require a greater level of control over their mobile data encryption implementations can use encryption control. This allows them to seed the encryption keys, enable data in use (in memory) encryption and others.

FIPS 140-2 Cryptographic Modules

Use FIPS 140-2 certified cryptographic modules for data at rest encryption and network connections.

MOBILE PRIVACY

Keylogging Prevention

Prevents the use of a non-trusted keyboard in the app. Default setting is to only use the OS built-in keyboard.

Copy/Paste Prevention

Prevents app data from being copied and pasted outside of the app. Copy/Paste is available between Appdome-built Apps.

Prevent App Screen Sharing

Prevents taking screenshots, mirroring and sharing the app's screen and hides the preview thumbnail when minimized.

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, Developer Options, Emulators and Banned Devices

Specifically for Android devices, an Appdome-built app can detects if a mobile device has been set to allow app install from "unknown sources" or has enabled "developer options". Additionally, Appdome-Fused apps can be prevented from running on an "Emulator" or on a "Banned Device". If these settings has been enabled, Fused apps can be configured to shut down or "exit."

SECURE COMMUNICATION

Trusted Session

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.

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.

Session Control (Requires Appdome-DEV)

Customers who require a greater level of control over their secure communication implementations can use session control. This allows them to pin a trusted CA to the app and the webserver. Session control can also enforce cipher suites, TLS version, strong RSA and ECC signatures, SHA256 digest and certificate roles. It can also make real IP address visible to the app and pin a static client certificate to the Appdome-Fused app to authenticate client connections on the MicroVPN gateway.

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.

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.

Prevent Running on Simulators

Protects the app by restricting app install and execution to physical mobile devices only.

Obfuscate Built Services

Appdome's proprietary binary based obfuscation method obfuscates Appdome-built 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.

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.

DEV-EVENTS™

Mobile app developers can code their mobile apps with the ability to take specific actions based on events that happen in the app or on the device. Effectively, they are giving their mobile apps the operational intelligence to act independently (i.e., without the need for an external policy service) when security events happen.

DEV-Events are available for all the security categories listed in this document.

Learn more about the Appdome Security Suite at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

ABOUT APPDOME

Appdome is the industry's first no-code mobile integration platform. Appdome's patented*, Fusion technology and its AI-Digital Developer™, known as AMI, powers a self-service platform that allows anyone to complete the integration of thousands of mobile services, standards, vendors, SDKs and APIs in security, authentication, access, mobility, mobile threat, analytics and more, adding these services to any mobile app instantly. Leading financial, healthcare, government and e-commerce providers use Appdome to deliver rich mobile experiences, eliminating development complexity and accelerating mobile app lifecycles. 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.