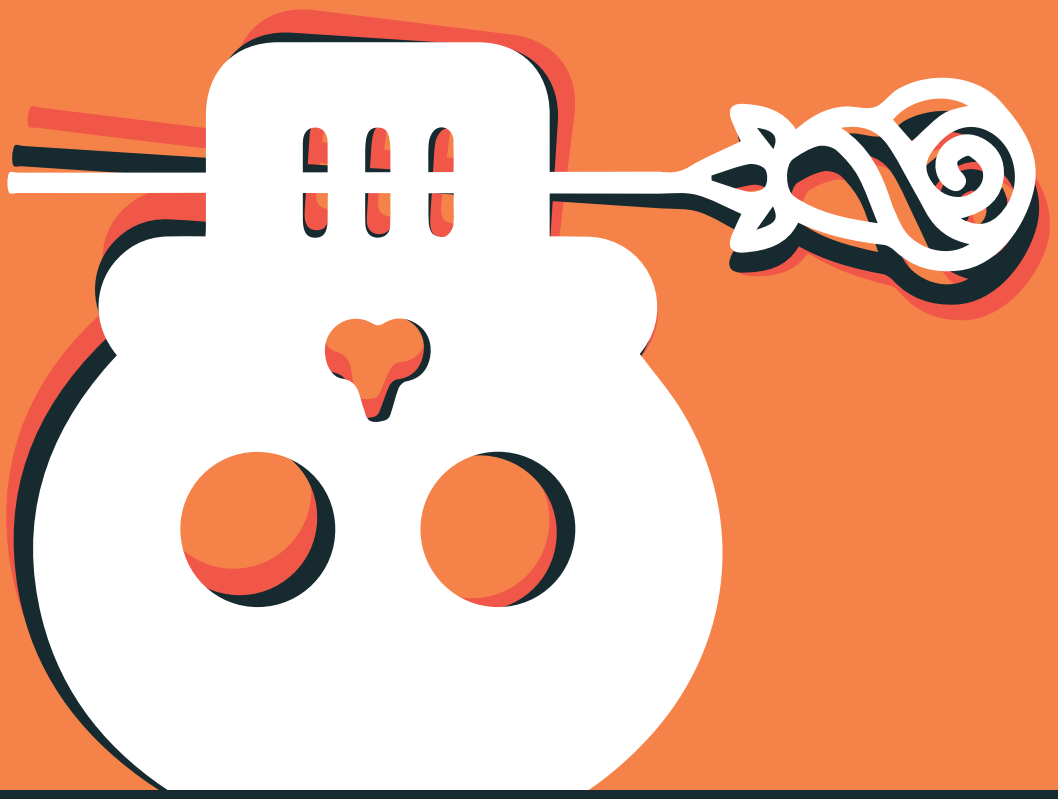
MOBILE DEVELOPERS GUIDE

MOBILE APP SECURITY

appdome

TABLE OF CONTENTS



Introduction
MOBILE APP SECURITY

Hackers are developers too. It is important to remember that when thinking about security for your Android and iOS apps. As developers themselves, hackers know exactly when, where and how to attack your apps, users and backend.

The job of legitimate and malicious hacking has exploded. Hackers, whether they are cyber criminals or legitimate pen testers, are everywhere. These professionals have tons of tools, instructions and products at their disposal, all of which makes the job of hacking apps easier than ever. These tools have amazing power to see into mobile apps, dissemble and decompile apps and sit between mobile apps and external services with ease. Finally, hackers don't have to break past security measures to accomplish attacks. They can take advantage of common coding practices in iOS and Android apps, well known vulnerabilities in iOS or Android, or the trust model of your app or the device itself.

The purpose of this Ultimate Developer Guide to Mobile App Security is to highlight the what and why developers should protect to improve the security of mobile apps, mobile businesses and users.

Top 3 Myths of **MOBILE APP SECURITY**

Building a mobile app that millions of people will use is an exhilarating experience for developers. Everyone wants your app to be all it can be, and so do you. But, the demand for more features often overrides the work needed to secure mobile apps. Failing to secure mobile apps could lead to costly and disastrous consequences, including lost data, lower ARPU, poor reviews, higher acquisition costs and churn.

BELOW ARE THE TOP 3 MYTHS TO AVOID IN PROTECTING YOUR MOBILE APP.

MYTH #1: THE OPERATING SYSTEM IS SECURE

Android and iOS operating systems are not secure. While both will increasingly have better and more robust security features, these features are dedicated to protecting the device (not your app). It's very easy to unlock the device. Unlocking the device exposes everything about and in your app, whether or not the user is legitimately accessing your app. There are also many more tools, hacks, methods and systems that people, and hackers, use to break mobile operating systems and initiate attacks. Even without breaking the operating system, people, tools and apps can harvest data, interfere with apps, gains unauthorized access, as well as impersonate users.

MYTH #2: BACKEND SECURITY IS ENOUGH

Backend security measures, alone, are not adequate to protect your mobile business. First, many attacks, like mobile malware attacks, occur at the client level, usually from another app on the same device. Strong backend or infrastructure security measures are critical. But, mobile apps themselves include all the elements necessary to reach and connect with your backend, access users' accounts, download data and more. If these methods, URLs, keys, certificates and more are left in the clear, your backend security can be ineffective.

MYTH #3: MY APP DOESN'T HAVE SENSITIVE DATA

All apps have sensitive data. Mobile apps are where your intellectual property and brand reach your end-users. Mobile apps use all kinds of data about your network, backend, and external APIs. All apps store data about users, histories, sessions, state, and a lot more. Most mobile apps have usernames and passwords and transaction capabilities to create amazing experiences for their users.

Top Attacks on **MOBILE BUSINESSES AND USERS**

Hackers attack mobile apps for all kinds of reasons, including data theft, account take over or as part of larger attacks. Here are the top attacks on mobile apps and businesses:

1. **MOBILE FRAUD.** Mobile fraud is an attack involving the malicious or unauthorized use of mobile apps and services, including fake apps, fake users, fake accounts or fake events, misappropriated connections and more to target mobile businesses, and receive goods, services, revenue, money, attribution or rankings without paying.

2. **MOBILE MALWARE.** Mobile malware is a local, on-device exploit, compromise, or control of mobile apps by malicious mobile apps, malicious programs inside other apps, or device malware. Malware can be used to harvest data, impair or control apps, or launch distributed attacks against mobile businesses.

3. **USER LEVEL ATTACKS.** User level attacks include account takeovers, identity theft, cyber bullying and extortion. Hackers traffic in and use stolen user, business or dev credentials and stolen PII gained from mobile apps to open fake accounts, steal goods, services and money from individuals or businesses, sometimes locking valid users out of individual accounts.

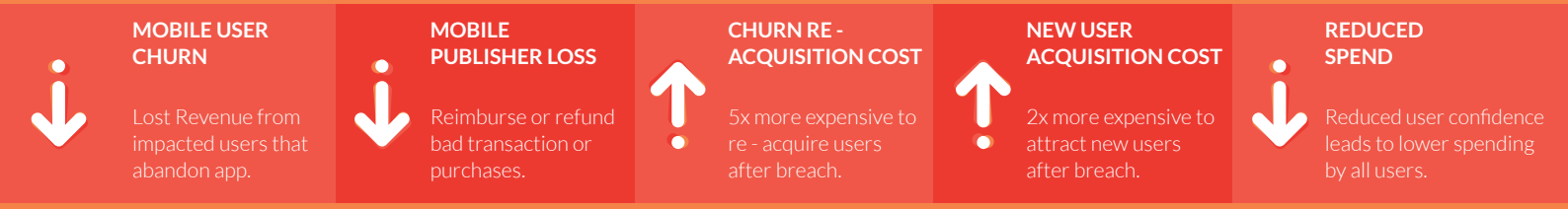
4. **MITM & BACKEND ATTACKS.** Hackers use MiTM and backend attacks to take down mobile businesses, exfiltrate data, and spy on users. DDoS, Credential Stuffing, MiTM attacks are used to gain access to backend systems or gather data in between mobile apps and their backends.

5. **DATA BREACHES.** Data breaches occur when hackers gain unauthorized access, export or steal mobile app client or mobile app backend user, business, or development data, including PII, financial, or business information.

6. **CYBER RANSOMING.** Cyber ransoms occur when criminals demand payment to unlock or return data, PII, assets, and/or refrain from cyber-attacks. Individuals and businesses can be targets for Cyber ransoming.

7. **MODS & FAKE APPS.** Mobile app piracy, copy-cat apps, and malicious trojans of valid apps, cause user confusion, increase the cost of customer acquisition, are used in Mobile Fraud and more. Mods and fake apps also result in loss of intellectual property, increased competitive risk, and lost innovation.

WHAT'S AT STAKE FOR YOUR MOBILE BUSINESS?



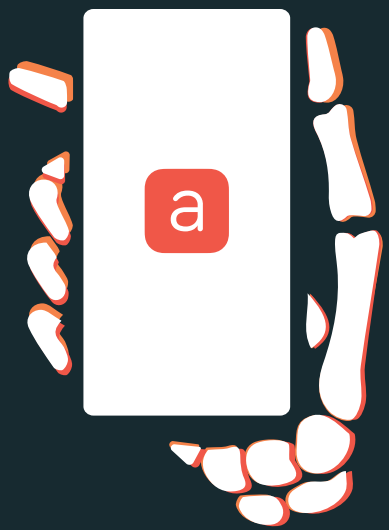
Protecting Mobile App Data
DATA AT REST ENCRYPTION

Data at rest encryption is the foundation method of any mobile security model. In app encryption is used to protect the data stored inside a mobile app or data stored by a mobile app in the application sandbox, preferences, or other areas.

What kinds of business data do mobile apps have? Mobile apps contain all the data needed to function and present your business to your users. This includes all your user data, such as passwords, account information, payment methods, and other personally identifiable information (PII) all the application text, email, and physical addresses for your business and more.

What kinds of dev data do mobile apps have? Mobile apps also contain all your development information, such as APIs, keys and secrets, backend service URLs, authentication tokens, preference and permissions data, and the certificates used for pinning and validation.

How is data stored inside a mobile app? Data inside a mobile app has three states: fixed or permanent data added by the developer, data stored or saved at rest, and data in memory or in use. All three need to be encrypted.



How does Appdome protect mobile app data?
Appdome provides a multi-layered, intelligent encryption model for all the data inside Android and iOS apps:

FILE LEVEL (SANDBOX) ENCRYPTION
Encrypts and protects files and data stored by the app without any limitation on data, file structure, or dependency on the operating system encryption.

ENCRYPTION OPTIONS
All encryption methods available with Appdome use AES 256 or FIPS 140-2 industry-standard cryptographic methods, multiple key generation options including dynamic, self-modifying encryption keys, seeded key, key management, Secure Enclaves, in-memory encryption and more.

CODE LEVEL ENCRYPTION
Encrypts all strings, secrets, preferences, constants and runtime information stored or generated by the app, including username, passwords, and other PII information, API keys, Certificates and more, removing critical loopholes hackers use to infiltrate apps.

BINARY LEVEL ENCRYPTION
Appdome's Android App Packer hides and encrypts all Java byte code of an Android app (ie: Java DEX classes). This eliminates component hijacking vulnerabilities that exist in Android apps.

Detecting OS Compromise
JAILBREAK & ROOTING PROTECTION

Mobile apps operate in zero-trust environments. As a developer, you have little (or no) control over the users' device. Any user can jailbreak or root their device. Hackers use Jailbreak and root as the quick path to exploit your app. There are plenty of tools like Frida, unc0Ver, KingoRoot, malware, and cheat engines that make jailbreak or rooting very easy. Once jailbroken or rooted, the hacker has administrative control over the device, which can make it impossible for users to use your app and more. So, it would be smart to prevent your app from running when jailbreak or rooting is present.

What does Appdome do to protect your app when the device Operating System is compromised?
Appdome provides in-app, autonomous jailbreak, and rooting protection for mobile apps. All of the intelligence needed to detect and enforce jailbreak and root conditions is added in the app itself.
If and when a jailbreak or root condition occurs, Appdome offers several methods of enforcement and notification.

JAILBREAK/ROOT PROTECTION

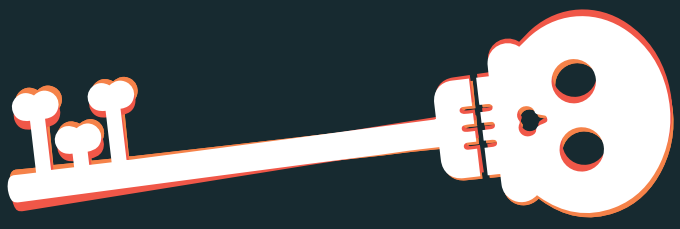
Appdome's jailbreak and rooting protection blocks mobile app use and notifies users who attempt to run your mobile app on a jailbroken or rooted device. This protection includes self-modifying jailbreak and root detection, and advanced capabilities for discovering hacking tools that rely on jailbreak and rooting, or jailbreak and root hiding programs, like Frida and others.

DETECT ANDROID ROOT OPTIONS

For Android, Appdome provides a deeper level of protection, allowing developers to prevent users from running Android apps if and when the user or another program changes Android settings that allow apps from unknown sources, allows developer options or the Android operating system has been set to allow emulators. These options are common techniques hackers use to install malware on a device, or when dynamically analyzing mobile apps to find vulnerabilities or data.

JAILBREAK AND ROOT ENFORCEMENT OPTIONS

Developers can determine the enforcement method used when a jailbreak or root condition is determined by Appdome. By default, Appdome enforces a jailbreak or rooting condition by closing the app and presenting the user with a standard notification. Alternatively, the developer can configure Appdome to pass an event to the application layer, to handle the condition inside the app itself, block certain features, invoke 2nd step authentication, and more.



Preventing Man-in-the-Middle
SECURE MOBILE COMMUNICATION

Why do hackers use fake servers and fake apps?
Mobile apps need to communicate with external services in order to function. For example, to deposit money via your mobile banking app, that app needs to connect, and data needs to travel from your app to the backed service. This connection and any information transmitted via this connection is vital to your business, critical to your users and valuable to hackers. So, it's important to ensure the connection, and any transmitted data, is protected.

What is a man-in-the-middle attack?
With unprotected connections, hackers use MiTM attacks, redirecting the user to a malicious server, presenting malicious requests to the user, or simply listening in and harvesting data on the connection. There are hundreds of techniques attackers use to compromise mobile connections and data in transit, inserting themselves between your app and the server that the app or user is attempting to connect with.

Can hackers use fake servers and fake apps?
Hackers can also impersonate the legitimate server, providing unrestricted access to your users, or impersonate the mobile client itself, i.e., connecting a malicious version of your application with the backend to execute larger exploits, DDoS attacks, and credential stuffing.

How does Appdome protect mobile connections?
Appdome uses active defense methods to avoid common MiTM methods, and detect malicious proxies and other MiTM attempts. Appdome also allows developers to validate servers and clients to ensure trusted components are using the mobile app and service.

TRUSTED SESSION – Validates authenticity of app or API sessions by preventing connections to untrusted, unknown, or malicious destinations, detecting malicious proxies, and more, without relying on the device level certificate.

SERVER AND CLIENT CERTIFICATES - In the app, secure server pinning to validate server certificate against a known trusted cert stored securely in the app. Developers can also add client certs inside the mobile app to allow backend validation and block malicious clients.

SECURE COMMUNICATION OPTIONS - Developers can specify the enforcement model for Appdome's Secure Communication by quickly and easily configuring Appdome to enforce specific Cipher Suites, TLS version, certificate roles, RSA & ECC Signatures, SHA256 Digests, URL whitelists, header secrets, and more.

Preventing Mobile Eavesdropping
MOBILE PRIVACY

Hackers don't have to break into your mobile app sandbox or reverse engineer your app to steal data from your mobile business and users. Someone at the airport can look over your users' shoulders. Hackers can also create malware that captures screenshots of your app or capture user keystrokes when people use your app.

How can you protect mobile users against mobile privacy threats?
Mobile privacy features have long been used in enterprise use cases to protect corporate data and prevent data loss. Consumer mobile app developers have now discovered that hackers use screenshots, mirroring, key logging and similar methods inside malware to steal data and user credentials. Blocking these methods can protect mobile apps from malicious code running on the same device.

Why use mobile privacy to stop malware?
Mobile privacy features are used in enterprise settings where corporate data and Data Loss Prevention (DLP) are critical security use cases. Consumer mobile app makers have discovered that hackers use screenshots, mirroring and similar methods to steal data and user credentials. Blocking these methods can protect mobile apps from malicious code running on the same device too.

How Does Appdome Ensure Mobile Privacy?
Appdome puts the power to block other programs from operating on behalf of mobile apps.

KEYLOGGER PREVENTION - Autodetect approved built-in keyboards to prevent recording and exfiltration of keystrokes by malicious keyloggers.

COPY/PASTE PREVENTION - Prevent application data from being copied and pasted outside the application. Copied text will be encrypted.

PREVENT APP SCREEN RECORDING AND SCREENSHARING - Prevents mirroring, sharing, or recording the screen, notifies if a screenshot is taken, and hides the app preview thumbnails when minimized. This feature is also useful in preventing copyright theft or IP violations. For example, a video streaming service or motion picture production studio can prevent fraudsters from making bootleg copies after recording movies they watch on a mobile device.

MOBILE SCREEN DIMMING AND BLURRING - Blur app preview screen when it is minimized to prevent sensitive data from being visible outside the app.

Preventing Mobile App Fakes & Mods
APP SHIELDING

Reverse engineering or hacking an app can be used to create fake or malicious versions of the app, build and distribute cheats, and other programs that abuse the app's underlying logic. These things can result in code piracy, malicious workflows inside the app, app defacing, and more. All this can destroy your brand and the trust your users have in your app.

Why hackers create fakes and mods?
If the mobile app can be changed, hackers can use your app as a trojan for their own malicious code and use your app to attack other apps on the same device, trick users into providing account info, steal information, or launch local attacks against other apps on the same device or backend DDoS attacks.

Why hackers deface or change your app?
Hackers don't have to break into your apps to wreak havoc on your mobile users. They can change contact numbers, internal links, point users at malicious sites to change passwords, deface your app, all to cause users to delete your app, and avoid your brand.

How does Appdome Prevent Fakes & Mods?
Appdome employs dozens of methods to prevent mobile applications from being interfered with, changed, or redistributed by others. This includes changing workflows, text, icons, data fields, app resigning, and more.

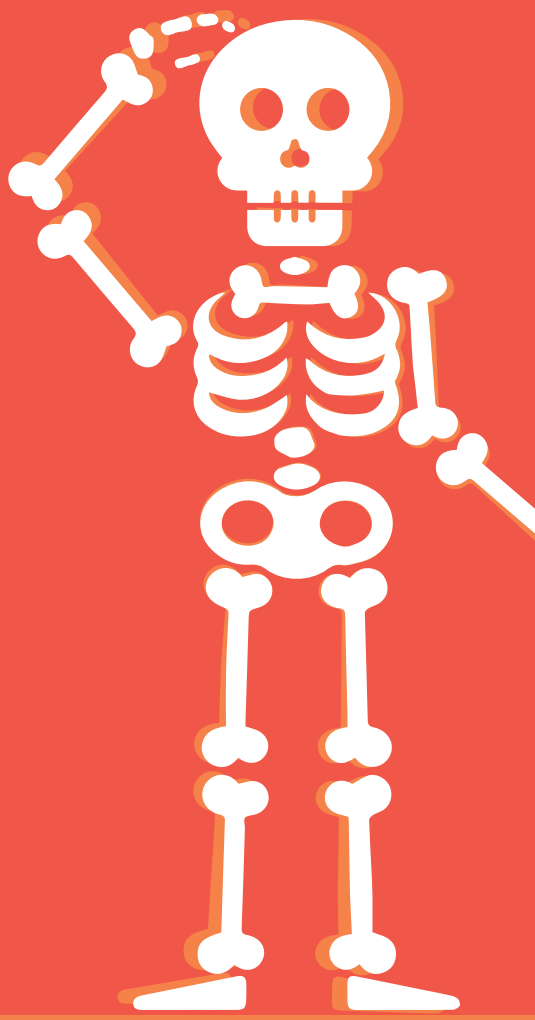
ANTI-TAMPERING - Appdome prevents mobile applications from being tampered with, changed, or redistributed by others.

ANTI-DEBUGGING - Appdome's anti-debugging methods protect the app from debugging attempts.

PREVENT SIMULATORS - Attackers routinely use emulators as a part of static and dynamic code analysis. This feature protects the app by restricting execution to physical mobile devices only.

CHECKSUM VALIDATION - Appdome adds checksums throughout the app to ensure the binary file integrity. Any change in a mobile app, malicious modifications, will cause the checksum to fail and the application to stop functioning.

APP STRUCTURE & INTEGRITY SCAN - Performs a structure scan of the app for checking app integrity.



Block Mobile App Reverse Engineering
CODE OBFUSCATION

Code obfuscation prevents reverse engineering techniques that rely on static analysis tools like IDA, Hopper, and more. Without code obfuscation, hackers can inspect and discover how your app works, and sensitive processes, systems, control flows, and file names can be easily found by attackers. That information can be used stand-alone or in combination with other exploits to create attacks against your mobile app, users, and businesses.

Biggest challenges with obfuscation?
There are four top challenges when obfuscating mobile app code. First, obfuscation is a one-way process and, so, developers have to be careful what they obfuscate or else they run the risk of breaking their app. Obfuscate the wrong process or component and your app cannot function. Second, obfuscation typically requires the developer to use symbols to tell machines where to begin and end obfuscation in native source code. This takes time and effort and has to be updated every time the app is released. Third, non-native code and third-party components, such as SDKs, cannot be obfuscated by developers. Fourth, obfuscation can interfere with crash reporting and adds file size to the bundle, that may cause the app to go over guidelines required by the App Store and Google Play.

How does Appdome Prevent Reverse Engineering?
Appdome is the only solution on the market that obfuscates mobile app code without source code or developers needing to tell a system where to begin and end the obfuscation method.

BINARY CODE OBFUSCATION - Appdome's code obfuscation operates at the binary level. This means that the obfuscation scrambles the entire code base, including native code, non-native components, 3rd party SDKs, frameworks, and more inside the app. With Appdome, there is no need to limit the obfuscation methods or worry that the app will crash as a result of obfuscation methods.

FLOW RELOCATION - Relocate and obfuscate mobile app code and control flows to block static analysis tools. With this feature enabled, hackers cannot tell how the app works.

NON-NATIVE CODE OBFUSCATION - Obfuscate non-native mobile application code such as Cordova JS, React Native JS, and Xamarin DLL. With this feature enabled, hackers don't have access to your non-native code.

STRIP DEBUG LOGS - Remove symbols and debug information in the mobile application's executable.

CONCLUSION

Best Practice Mobile Security FINAL RECOMMENDATIONS

Choosing how to secure your app requires careful consideration of your app's purpose, your users' expectations, and any industry or regulatory requirements imposed on your mobile business. No matter what, developers are advised to avoid the myths and take proactive steps to add security methods inside the client mobile apps.

There is no silver bullet when it comes to mobile app security features. Proper mobile app security requires a layered defense. Multiple features should be combined, creating a self defending model, to protect mobile apps, including the users and businesses that rely on mobile apps.

To operationalize security in your development pipeline, look for solutions that offer comprehensive protection, speed of implementation, ease of maintenance, and security innovation. These considerations are critical to prevent breaches, backend attacks, or malicious code from stealing data in your app, on the user's device, or on your backend. Adding security features like encryption, obfuscation, shielding, OS integrity, and Secure Communications is just the first step. Doing so, can be time-consuming and complex. But, with Appdome, securing mobile apps is easy.

For more information on using Appdome to secure your mobile apps, write to securemyapp@appdome.com or get started today at fusion.appdome.com.

SECURE MOBILE APPS FOR GOOD WITH APPDOME!

SECURE MOBILE APPS FAST!
fusion.appdome.com

appdome

3 Twin Dolphin Drive Suite 375
Redwood City, CA 94065
+1.650.567.6100
+1.844.360.FUSE (3873)
info@appdome.com
www.appdome.com