approov
mobile security

SOLUTION BRIEF

Five Critical Threats to Mobile Games and Five Vital Security Measures

Key Approov Benefits

Block Illegal App Copies

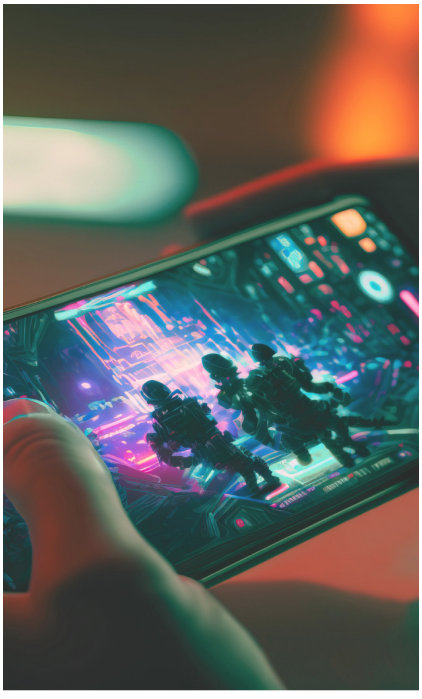
Detect and Defend Against Cheating Tools and Emulators

Detect Rooted, Jailbroken and Modified Devices

Protect Against Runtime Attacks on the Game

Stop Man-in-the-Middle Attacks

Prevent Exploitation of Secrets



Today, Gaming Means Mobile Gaming

With the rise in popularity, mobile games have become lucrative targets for hackers, making security a paramount concern for both developers and players.

This solution brief identifies the key security threats that mobile games face and explores effective strategies to safeguard these games, ensuring a secure and enjoyable gaming experience for users.

What Are the Threats to Mobile Games?

From a hackers perspective, mobile games can be directly attacked for gamers personal data or they can provide useful information which can be used in other types of attacks. There are many risks, instead of a long list, lets just look at some of the worst things that can happen.

1. Personal Data Theft and Abuse

Mobile games often provide in-game currency and wallets and collect large amounts of personal and sensitive data. This makes them a prime target for hackers seeking to steal game assets or personally identifiable information (PII).

Hackers can gain access to credit card details, bank account numbers, or other financial information stored within the game or on your device if compromised. This can lead to unauthorized purchases, fraudulent transactions, and even identity theft.

Personal information can also be leaked if game developers don't properly protect the databases and code repositories they use. Researchers discovered recently that Tap Busters: Bounty Hunters leaked data through unprotected access to Firebase, Google's development and database platform. The uncovered dataset contained user ids, usernames, timestamps, and private messages. This wealth of data could be used for targeted phishing attacks, stalking, or other malicious activities.

Leaked usernames, passwords, and email addresses associated with a users game account can be used to gain access to other online accounts, potentially exposing the users digital identity. If hackers access users accounts, they can interfere with progress in the game, manipulate virtual currency, and even personalized items. Leaked contact information can lead to an influx of spam emails, unwanted in-game messages, and even unwanted phone calls.

2. Illicit Copies of Games

Cloned or repackaged games pose a security threat because they enable hackers to exploit popular titles for financial gains. The clones may also contain malware or other malicious code that can access personal data such as login credentials and financial information. Developers should, of course, implement robust code protection to protect games from code alterations or injection attacks.

Deceptive in-game offers or messages posing as legitimate game features can trick players into revealing sensitive financial information. This can lead to financial losses as well as compromise your online security.

Modified and cloned games are tempting for their potential advantages like unlimited resources or altered gameplay, but they come with a wide range of risks that players should be aware of before diving in. Here's a breakdown of the potential dangers:

- Malware: Modified games can be injected with malware designed to steal your personal information, financial data, or even hijack your device for nefarious purposes. Downloading from untrusted sources dramatically increases the risk of encountering such infected versions.
- Privacy breaches: Modified games might collect your data without your consent or knowledge, potentially tracking your activity, online habits, and even location. This information could be sold to third parties or used for malicious purposes.
- Account compromise: Cloned games may be used to trick players into logging in with their existing accounts, exposing their login credentials and potentially leading to account takeover and loss of in-game progress or purchases.
- Unfair advantage: Modified games often grant unfair advantages like unlimited resources, god mode, or wall hacks, ruining the competitive balance and frustrating legitimate players. This can create a toxic environment and drive away players who value fair play.
- Bugs and crashes: Modifications can introduce unintended bugs and crashes, disrupting gameplay and potentially corrupting save files, leading to lost progress and frustration.

3. In App Purchase Fraud

In-app purchase bypassing is a serious threat as it leads to lost revenue. It also harms the integrity of the game and may reduce player engagement. As an example, fraudsters can create a guest account, then use a stolen card to level-up/buy digital goods or load the game virtual currency on the account, they then sell the account online. The buyer links the account to their social media account in order to use it.

For gaming app developers, the financial costs of in-app purchase fraud are potentially massive. As well as chargebacks which arise from the use of stolen cards, the app also loses the value from the customer who paid out to the fraudster instead of the app.

Hackers can also easily bypass in-app purchases by using an emulator for a game and creating a patch. Just as concerning, emulators and other tools like debuggers may also enable hackers to create copycat games and even transform games into malware-carrying trojans.

To ensure the security of an in-app purchase system, developers should use security measures such as server-side validation, encryption, app attestation and anti-tampering to detect any modifications to code or data.

4. Cheating

The use of emulators to cheat in games, particularly mobile games, is a complex issue. Emulators can enable players to access mobile games on their PCs or laptops, offering a more comfortable and potentially powerful platform with better hardware and no battery issues. This can benefit players with older or weaker mobile devices, allowing them to experience the game in a better way. Some emulators also allow for macro creation and automation of repetitive tasks, which might eliminate some more tedious aspects of games. This can save players time and effort, but of course, raises concerns about fairness.

There are serious downsides of course:

- Cheating : Emulators can provide significant advantages in competitive games, especially when combined with keyboard and mouse controls or automated scripts. This can create an uneven playing field for mobile players using touch controls, leading to frustration and potentially driving them away from the game. Some emulator software specifically facilitates cheating by offering pre-built scripts or hacks that grant unfair advantages like wallhacks, aimbots, or infinite resources. This undermines the integrity of competitive gameplay and disrupts the balance for legitimate players.
- Security vulnerabilities in the tools themselves: Downloading and using third-party emulators can introduce security risks, especially when downloaded from untrusted sources. These emulators might contain malware or spyware that can steal personal information or compromise your device.
- Violation of terms of service: Many mobile game developers explicitly prohibit the use of emulators in their terms of service. Using them can result in account suspension or bans, depending on the developer's enforcement policies. But this all depends on being able to tell if an emulator is being used.

Cheating in mobile games, while seemingly harmless to some, presents a significant problem with far-reaching consequences for players, developers, and the entire gaming ecosystem. For legitimate users, the game becomes frustrating, unfair and potentially toxic. Cheating can drive away legitimate players, which translates to lost revenue for developers. As player interest dwindles, the game's overall value depreciates, impacting future investments and development plans and reducing the value of the brand.

Developers are constantly evolving their efforts to combat cheating, employing techniques like server-side checks, anti-cheat software, and machine learning algorithms. However, the battle against cheaters is an ongoing one.

5. Stealing and Abusing Secrets from Mobile Games

We mentioned theft and abuse of personal data but one of the worst scenarios is the theft of secrets such as API Keys that can be reused by hackers to target backend services directly. Mobile apps are notorious for storing the keys in ways that can be easily accessed. Hackers systematically acquire keys and secrets and use them to access backend systems. Recent high-profile cases are due to secrets exposed in public repositories such as github. Even if keys and secrets cannot be easily reverse engineered from the mobile app code, hackers can get another opportunity to grab secrets at runtime by manipulating the app, the environment and/or the communication channel(s).

The Tap Busters: Bounty Hunters leak which we mentioned previously also exposed some sensitive secrets including API keys which were hardcoded in the application's client side.

Similarly a leak from the widely used Escalators game exposed some critical API Keys including the Firebase URL and its key. Also included were Google and Apple in-app payment API keys. While the API keys were obfuscated, the research team found instructions to deobfuscate the data online. These keys, coupled with access to the game's source code, could enable attackers to make in-game purchases without developers' permission. That could lead to financial losses for the company and fraud.

A Word About Why Mobile Game Security is Lacking Today

Some of the reasons that games are not well protected today :

- There is a perceived tradeoff between a great customer experience and applying advanced security techniques. Developers want to prioritize feature velocity and DevOps teams want to avoid anything that has the risk of interfering with customer experience or game performance.
- Cost of implementation and management of security solutions can spiral out of control, especially if developers invest time and resources in ad hoc approaches to security. This can take away from resources that could be used to improve the game or create new content.
- Some security solutions need constant attention to be effective and need skilled tuning to avoid false positives. Security resources are scarce, making the administration of such complex security solutions a challenge for small

organizations.

With a careful selection of the approach and the security solutions to be deployed, these concerns can be directly addressed and mitigated. Security solutions should always be evaluated along the following lines:

- How easy is it to deploy?
- What is the management overhead of continuous operation? How easy is the solution to keep up to date?
- Is the vendor ready and committed to deliver regular updates as the threat landscape changes?
- What are the risks of false-positives interfering with legitimate users?
- Can policy changes be made easily without code changes or version updates?
- In the event of a breach, or accounts or secrets being compromised, can immediate action be taken to block access for compromised users, or rotate secrets, while preserving customer experience for unaffected users?
- What are the latency and performance impacts of the security solution?

By prioritizing security without compromising usability, developers can create mobile games that are both safe and enjoyable, ultimately earning user trust and fostering long-term engagement.

With these requirements in mind, here are the five ways you can secure your mobile game.

Five Ways To Protect your Mobile Games

1. Anti-tampering

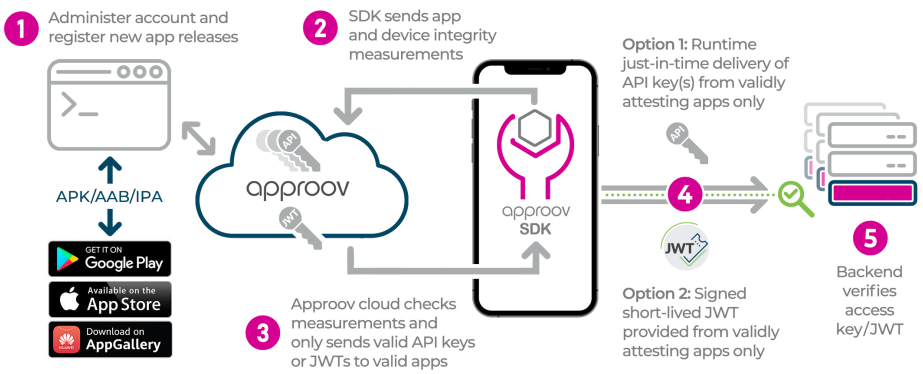
Anti-tampering can detect any unauthorized code modifications on the client device, by using integrity checking, root detection, and emulator detection. Once it detects malicious activity, it activates a response, such as denying access or shutting down the app entirely.

Here are a few examples of how anti-tampering can protect mobile games:

- Anti-tampering can prevent cheating by detecting hackers trying to modify code to give themselves an unfair advantage in the game.
- Anti-tampering protects in-app purchases by preventing hackers from bypassing the in-app purchase system.
- Anti-tampering can protect user data like saved games and game progress by preventing hackers from accessing such data.

2. App Attestation to Defend Against Repackaged Apps

App attestation makes it harder for hackers to clone app code. It detects whether an app has been modified or repackaged, and once detected, the app can take appropriate action, such as shutting down or alerting the user. This may also prevent the distribution of the cloned app.



3. Runtime Application Self Protection (RASP)

Protection against static attacks alone is not enough to fully protect your gaming app. You need to combine code protection with runtime protection for real-time monitoring, automatic blocking of malicious requests, and app-specific protection.

Runtime protection provided by a Runtime Application Self-Protection (RASP) solution can monitor the device's memory for known cheating tools or detect when a user is running a game in an emulator. It can also block malicious code and shut down the app to prevent vulnerabilities from being exploited.

4. Protect the Communications Channel to the APIs

The APIs and the communications channel between app and APIs must also be protected.

Mobile apps are particularly prone to MitM attacks even if TLS is used to encrypt traffic between the app and backend servers. If an attacker has access to a mobile device they can use a MitM tool, such as 'mitmproxy' to intercept traffic. There are many such tools available. Attackers can manipulate traffic to and from the backend to steal data or keys. This is a popular and rapidly growing mechanism, as it is effective even if the user has implemented two-factor authentication (2FA).

Certificate pinning is a solution which is recommended, by the OWASP MASVS guidelines, in order to protect the channel. Also, anti tampering and client integrity checks can prevent attacks on the device.

5. Get Secrets out of your App Code

Hardcoding sensitive data into the client side of a mobile app is unsafe, as in most cases, it can be easily accessed through reverse engineering. The API keys used to authenticate and authorize access to backend services from mobile apps must be protected from being stolen and abused. Developers need to get secrets out of their code, and manage cryptographic keys securely and handle key rotation appropriately for ongoing security.

> **We saw an immediate 99.9% reduction of malicious access to our backend resources once Approov was implemented. Approov's ability to provide unlimited and unthrottled protection is unlike native or any other mobile apps solutions.**
>
> - Kevin Kim, COO at Genopets

Approov Provides Easy, Fast, Effective Protection for Mobile Games

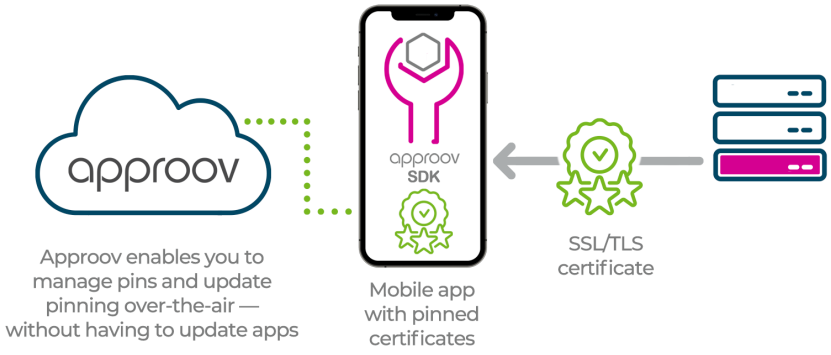
Approov provides mobile game developers and studios an easy way to stay ahead of mobile cheaters, hacks, and player emulator platforms. With Approov in place, you preserve fair play, secure private data, and protect company revenue streams. Approov mobile runtime application self-protection (RASP) protects your games with minimal impact to game development and no impact on game performance.

- Approov is 100% accurate and never creates poor user experience caused by security false positives. Over-the-air updates mean secrets and policies can be updated immediately without needing to update code and deploy a new version of your game.
- Approov is simple to deploy and operate, providing immediate protection without the burden of complex security measures or excessive management overhead. Approov integrates easily into your DevOps pipeline for a streamlined workflow.

- As your user base expands, Approov ensures a seamless customer experience. It maintains optimal game performance, never obstructs legitimate users, and effortlessly scales to accommodate millions of users.

With Approov in Place You Can:

- Block Illegal App Copies: Approov app attestation blocks everything except your genuine and untampered mobile app, running in a safe environment, from accessing your backend API's, so you can eliminate the threat of cloned and copied apps once and for all.
- Detect and Defend Against Cheating Tools and Emulators: Approov detects and defends against popular cheat engines and cheating apps, making sure your game works as intended.
- Detect Rooted, Jailbroken and Modified Devices: Approov protects iOS, WatchOS, Android and HarmonyOS by detecting rooted or jailbroken devices as well as the presence of GameGuardian, Cycript, Cydia, Xposed, Frida, Magisk, Zygisk and others. You decide what is acceptable with a high level of granularity via over the air policy updates.
- Protect Against Runtime Attacks on the Game: Dynamic instrumentation tools can tweak mobile games at runtime. Approov RASP attests the actual executing code, providing robust and continuous protection against any runtime tampering.
- Stop Man-in-the-Middle Attacks: Approov Dynamic Certificate Pinning protects from mobile Man-in-the-Middle attacks and makes it easy to manage and rotate certificates over-the-air.



- Prevent Exploitation of Secrets: Game developers need to get API keys and secrets out of app packages. Approov keeps API keys and certificates securely in the cloud, delivering them "just-in-time" only when app and device integrity checks are passed. You can rotate them easily and immediately via over-the-air updates. It also works for any third party APIs you use.

Conclusion: Now is the Time to Secure Mobile Games

The cybersecurity risks presented by the growth of mobile games are real and the consequences of lack of security are serious. Fortunately, game developers no longer need to decide between customer experience and security: there are cost-effective security solutions which provide effective protection and are easy to deploy and manage.

Discover how Approov's security solutions elevate Mobile Gaming and Gambling experiences.

Contact us for a free technical consultation - our security experts will show you how to protect your revenue and business data by deploying Approov Mobile Security
https://approov.io/info/contact