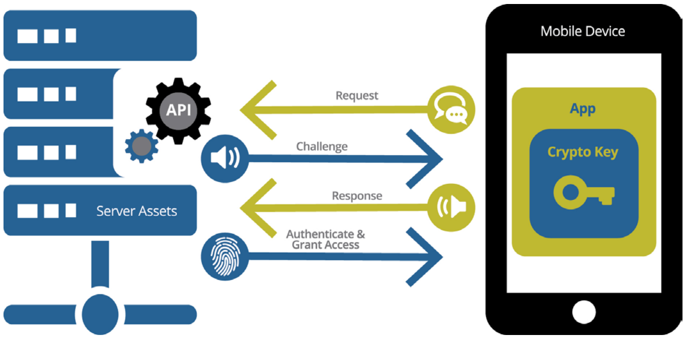
Popular Mobile Collectable Card Game (CCG) Protects Millions in Revenue with Arxan Application Protection

One of the world's leading multi-national game developers recently released a mobile online collectable card game (CCG). The mobile game featured a cutting-edge battle system and a balanced reward system for both free and paying customers. Both features were very well received and welcomed by customers, however, hackers took advantage of these features for personal gain.



Challenge:

The game developer's challenge was figuring out how to keep the cutting-edge battle system and balanced rewards in the game without allowing the features to be abused by hackers. The damage the hackers had caused already was measured in multiple millions of dollars. This lost revenue was due to excessive server costs because of the additional load hackers were creating on the game servers and in lost customers because the damage to the game experience itself.

These problems aren't unique to this mobile game, many mobile games suffer similar issues. The mobile gaming space has grown so rapidly that many developers have not had the opportunity to secure their mobile games and in turn protect their revenue.

Some common attack vectors used against mobile games:

- In-App Purchase System Circumvention – Allows purchasing without spending money
- App Repackaging and Republishing – Allows insertion of malware and loss or theft of revenue
- Network Traffic Manipulation – Allows reading and manipulation of network data for gain
- Abuse of Guest Accounts – Allows creation of many guest accounts to abuse game mechanics for gain and a vector for selling of accounts

These types of attacks directly impact the ROI of a mobile game in many aspects – server costs, service stability, lost customers, poor reviews, bad play experience just to name a few.

> The easy and timely implementation and deployment of Arxan Application Protection immediately improved the revenue position of the innovative mobile game without compromising the exciting new features.

Solution: Mobile gaming developers have largely ignored problems brought on by hacking thinking they are protected by the "built-in" security within mobile operating systems. However, in reality hackers have almost all the same tools, information and accessibility to attack a mobile game as they would on traditional platforms like PCs. In some cases, hackers have even more access on mobile platforms due to the more intimate nature of information available at the operating system level on smart devices (contact information, social media accounts, etc.).

Protecting a mobile game is a challenge. Mobile devices typically have limited resources and today's mobile games are continuously pushing the performance envelope of mobile devices. So a protection solution needs to be lightweight, effective and transparent.

Arxan's Application Protection met the game developer's requirements of being light weight, effective and transparent. The developers used Arxan Code Protection & Arxan Cryptographic Key/Data Protection to protect their title in a number of ways:

- **Obfuscation Guard:** Hide key game data from prying hackers so the data couldn't be read or modified
- **Debugger Detection Guard:** Added debugger detections to prevent automation of gameplay
- **Encryption Guard:** Encrypted game assets to prevent theft of IP
- **Checksum Guard:** Detect and report modified clients to the server
- **Arxan Cryptographic Key/Data Protection:** Used Whitebox Cryptography to hide network keys in order to prevent network traffic from being read and modified
- **Jailbreak Detection:** Used to detect and shutdown applications running on jailbroken devices that were being used with automation software to mass create game accounts

Results: The game developers were able to implement and deploy Arxan Code Protection & Arxan Cryptographic Key/Data Protection in a timely and easy to maintain fashion that immediately improved the revenue position of their innovative mobile game, while not compromising the exciting and new features. Once the hacking was dealt with, the motivation to spam account creation went away and server costs returned to expected levels as a result.

About Arxan Technologies

Arxan is the trusted global leader of Application Attack Prevention and Self-Protection products for Internet of Things (IoT), Mobile, Desktop, and other applications. We help protect our customers against financial loss, brand damage, fraud, IP theft, stolen credentials, fraudulent transactions, unauthorized access, non-compliance with regulatory and industry standards, and more. Our unique patented guarding technology **1. Defends** applications against attacks, **2. Detects** at run-time when an attack is being attempted, and **3. Deters** attacks to stop hackers, send alerts, or repair making customers' applications truly resilient. We are currently protecting applications running on more than 500 million devices across a range of industries, including: financial services, automotive (connected automobiles), healthcare (connected medical devices), digital media, gaming, high tech/independent software vendors (ISVs), and others. The company's headquarters and engineering operations are based in the United States with global offices in EMEA and APAC. **Learn more at www.arxan.com.**