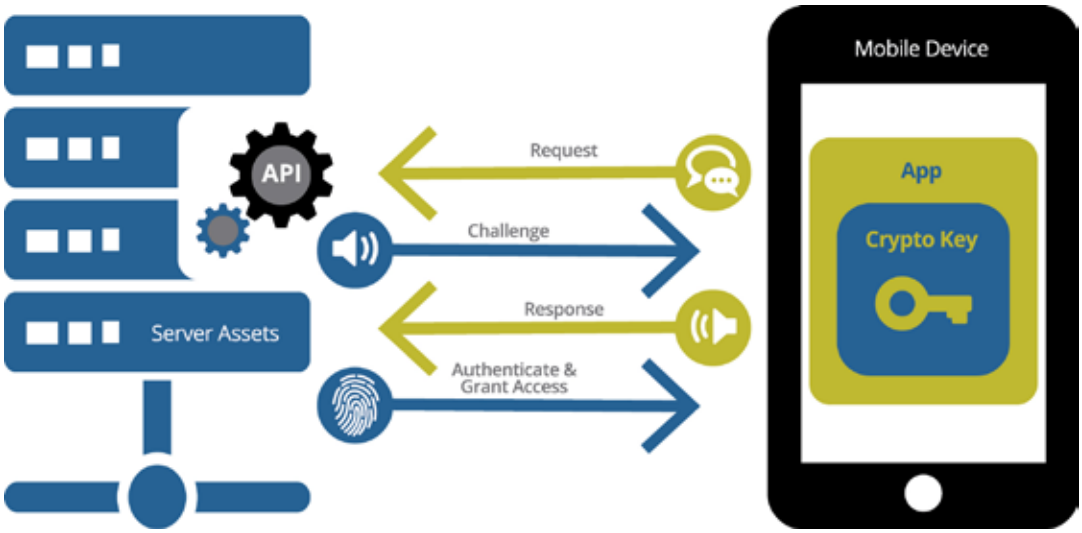
Protecting Server APIs: Safeguarding the "crown jewels" housed on back-end servers

APIs are transforming the way we develop applications and do business. Given the strategic value of APIs, adoption is growing at an unprecedented rate. This company embarked on a vision to revolutionize the way we communicate — chatting, sharing photos and videos, and it even integrated a popular payment API for peer-to-peer money exchange. They realized APIs introduced new risks / attack vectors, particularly the risks associated with client apps accessing server APIs using simple authentication based on challenge-response exchange.



Challenge: Authentication is being widely used to ensure that a client app is genuine and authorized when it tries to connect to an API server. This is typically done using a simple challenge-response exchange, which is a cryptographic operation; meaning the client contains a secret key, generally for an asymmetric cipher like RSA or ECC. The problem with this approach is that a hacker can decompile the original client app and lift the cryptographic key within it, and use the same key within a cloned version of the original app in order to pass the challenge-response test. Their cloned version of the original app may have altered functionality, and may gain access to server assets for malicious purpose.

The problem with the traditional approach is that a hacker can easily decompile the original client app and lift the cryptographic key.

Solution: In order to mitigate the key security risks associated with API usage, Arxan offered comprehensive Application Protection.

Arxan Cryptographic Key/Data Protection Secures Challenge-Response Authentication

White-box cryptography is a method for securely hiding cryptographic keys even if a hacker has full access to the software. The original key material is converted to a new representation using a trapdoor function (a one-way, non-reversible function). This new key format can only be used by the associated white-box cryptographic software, effectively hiding the key. However, this is still not enough — white-box cryptography hides the key securely, but the hacker could, still, decompile the original application and modify the app or lift out the entire white-box software package and leverage it in a separate app for nefarious objectives.

Arxan Code Protection Solution Prevents Code-Lifting and Code-Tampering Attacks

Anti-tamper techniques coupled with self-defense measures, comprised of unique patented guarding technology, can detect if the white-box software is running in the correct (unmodified) application or in a new environment, and they make decompiling the app extremely difficult. Anti-tamper techniques can respond to runtime attacks with customizable actions and notify the app owner that the app is being modified.

Results: Arxan Cryptographic Key/Data Protection has effectively hidden the secret keys used for challenge-response authentication. Given the keys are never present either in the static form or in runtime memory, hackers have not been able to gain unauthorized access to the application and the wealth of information the company manages and stores on its server. Arxan Code Protection has "hardened" the client app, making it extremely difficult for a hacker to gain access to the source code and all of the security control, lift the white-box software package and/or modify the behavior of the application at run-time.

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.**