TAG

KNOW YOUR APP: THE ROLE OF ATTESTATION IN MOBILE APP SECURITY

CHRISTOPHER R. WILDER
SENIOR ANALYST, TAG

approov

KNOW YOUR APP:
THE ROLE OF ATTESTATION IN MOBILE APP SECURITY

CHRISTOPHER R. WILDER, SENIOR ANALYST, TAG

This article will focus on the importance of secure client-server communications across mobile ecosystems. We will also discuss the importance of client software attestation, approaches, and relevance to mobile application vendors. Additionally, we will provide additional context and insight into Approov's intellectual property/patent and best practices for working within its guardrails.

INTRODUCTION

Mobile application programming interfaces (API) are pivotal in enabling data and service access for mobile applications. Still, they are one of the largest targets of bad actors for security breaches. Adversaries exploit these vulnerabilities to steal critical data, disrupt services, or hijack mobile devices.

Further underscoring the urgency of this issue, API attacks dominate web application vulnerabilities, which we estimate to cost an average of $2.5 million per breach and up to $7 million for cloud-based compromises. Mobile app security is difficult because the mobile app code is available and can be reverse engineered and is potentially running in a hostile client environment, and bad actors manipulate these to mount attacks on APIs. Therefore, any mobile security solution must address the challenge of determining whether an app or the environment it runs in has been tampered with.

“In the context of client-server computing systems, it is desirable for software running in a server computing device to request that the client computing device attests that it is running an authentic version of application software. Furthermore, it might also be desirable to attest that the client is also running specific operating system platform software. The purpose of this is to determine if the client software and its execution environment may have been tampered with or altered in some way.”

Approov's patented solution (US/11163858B2) is a strong provider in this landscape by offering a client software attestation solution, authenticating the identity and genuineness of the mobile client before server access. This safeguards against potential impersonations or device compromises, thereby fortifying server-client communications.

For vendors and enterprise DevOps teams looking to bolster their mobile application security without infringing on this patent, collaborating directly with Approov is an important consideration in the early stages of the mobile application development strategy.

ATTESTING THE APP AND THE DEVICE ARE CORE OF ANY MOBILE SECURITY SOLUTION.

In 2015, Approov realized this and invented a unique secure but flexible way of doing this, which we will dig into in the rest of this paper. In traditional server-client interactions, Approov-enabled servers can determine the integrity of software applications running on client devices. By leveraging an intermediary attestation service, the server and client software can synchronize and, most importantly, secure their communications. Here is how it works. The client software creates a special code (cryptographic hash) to prove it hasn't been tampered with. It sends this code to the attestation service. The service then checks the code and decides if it's valid or not. Approov's attestation solution emphasizes thorough checks before a mobile client accesses a server. This process includes but is not limited to.

1. **Code Signing:** Confirming that the mobile application is unchanged.
2. **Detection Techniques**: Spotting devices that have been jailbroken or rooted and pinpointing if apps run in emulated settings.
3. **Device Integrity**: Checking the mobile device's operating system and key files for authenticity.

Simply put, a device is denied access to the server if it fails to meet these minimum standards. Approov's solutions are designed to be incorporated into the software development lifecycle (SDLC) to improve the overall security posture while ensuring regulatory compliance. In my experience, this approach should be considered by DevOps and vendor organizations to help streamline the CI/CD pipeline and make cybersecurity a priority.

INTEGRATING APPROOV INTO THE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

By working with Approov, DevOps and vendor organizations will see several benefits.

1. **Enhanced Security:** The system ensures heightened safety by verifying the mobile client's identity and structural integrity.
2. **Regulatory Compliance:** For organizations navigating the complexities of data protection standards, Approov aids in maintaining compliance with complicated regulations such as PCI DSS, GRPR, HIPAA, etc.
3. **Cost-efficiency:** The ease with which Approov can be integrated into existing systems negates the need for costly developments, presenting an economically viable security solution for mobile development teams.

Approov strengthens server-client interactions by validating client software for authenticity. It ensures app originality, detects compromised devices, and verifies device integrity. Organizations that adopt Approov can achieve improved security, regulatory compliance, and cost-effective integration.

Incorporating Approve into the SDLC is a good first step in deploying secure mobile applications. Approov's solutions easily incorporate into Runtime Application Self-Protection (RASP) and, when aligned with the guardrails of Approov's patent, delivers a fortified security layer throughout an application's lifecycle. Approov seamlessly integrates as a build step, verifying the mobile client device's identity and integrity before any app deployment.

UNPACKING APPROOV'S INTELLECTUAL PROPERTY AND WHY IT'S IMPORTANT.

The mobile applications ecosystem comprises diverse applications, platforms, and use cases, making it a ripe target for determined hackers. Our research indicates an average of 10 monthly active campaigns targeting mobile applications at one time, especially banking, travel, gaming, social media, and corporate mobile apps. Criminals use remote access takeover (RATs), spyware/malware, and in-app phishing campaigns to take advantage of vulnerable mobile applications. Implementing client/server attestation into the DevOps process can help; here's how.

- **Mobile Application Stores:** Ensures only genuine and uncompromised apps get listed, bolstering user trust and increasing revenue for paid apps.
- **Mobile Device Management (MDM):** Client attestation ensures devices under management have not been tampered with, adding an extra layer of security for enterprises.
- **Mobile Payment Systems:** Reduces fraud by ensuring genuine and uncompromised payment apps and securing transactions and sensitive financial data. Further, this approach helps to reduce account takeover (ATO) and man-in-the-middle (MitM) attacks which are some of the most prolific attack techniques used by attackers.
- **Malware Mitigation Solutions for Mobile Applications:** Incorporating client attestation can add another layer of protection, verifying apps before scanning and providing a dual layer of security.
- **Enterprise Applications:** Approov can verify the integrity of enterprise apps in real-time, safeguarding sensitive corporate data and intellectual property.
- **IoT/OT Device Management:** Enhances the security posture of IoT devices by ensuring only authenticated applications can interact with the device ecosystem. This is an emerging market, but these devices control critical infrastructure systems and must be protected.
- **Custom ROMs and Operating Systems:** read only memory (ROM) and real time operating systems (RTOS) developers can utilize client server attestation to ensure their distributions remain unaltered and uncompromised after installation. These systems make-up most of the edge, robotics, and remote devices.
- **Mobile VPN:** Assures users that their VPN app is genuine and has not been tampered with, thereby securing their online activities.
- **Mobile Game Development:** Protects against cheating and game modifications, ensuring fair play and safeguarding in-game purchases.

Leveraging Approov's intellectual property provides an effective way to improve mobile application security. Server attestation fortifies mobile platforms: application stores can ensure app authenticity, carriers can validate pre-installed apps, and game developers can guard against unauthorized changes. Furthermore, enhanced device security checks benefit sectors like Mobile Device Management and IoT/OT. In short, by adopting Approov's IP, entities strengthen their own security measures and enrich the broader mobile ecosystem's trustworthiness.

WORKING WITH APPROOV TO DEPLOY SECURE MOBILE APPLICATIONS

For mobile application developers, the oversight or inadvertent breach of patent rights can lead to significant legal and financial ramifications. Further, as open-source software is used by development teams, in a recent study by ReversingLabs, over 50% use software in their SDLC, making the risk of patent infringement even more daunting. Awareness of these patent risks can no longer be an afterthought. Ignoring these risks can impact on a company's reputation and pose severe legal challenges, potentially leading to substantial financial losses.

To circumvent these pitfalls, proactive measures are crucial. Mobile application developers should take on a forward-thinking approach rather than reactively handling infringements, ensuring they have well-versed IP rights for their adopted methods and tools. DevOps and application developers must understand what functionality they include in their applications, including knowledge of their own rights and an understanding of IP risks to reduce the risk of patent infringements.

Lastly, when companies inadvertently purchase software that violates another entity's patent rights, they expose themselves to a myriad of potential liabilities. This includes substantial financial penalties resulting from infringement lawsuits and potential reputational damage that can erode trust among clients, partners, and stakeholders. Further, the company might face injunctions that halt the use or sale of the infringing software, leading to operational disruptions and lost revenue. Furthermore, rectifying such infringements often necessitates time-consuming software rebuilds, replacement, and the elimination of application functionality. Due diligence before software acquisition is essential to prevent these significant risks and ensure sustainable business operations.

WRAPPING IT UP

The drive to quickly create new, revenue-generating mobile services is causing enterprises and vendor development teams to focus on speed-to-market rather than doing due diligence to avoid costly mistakes. The risk of IP infringement is real, especially with many tech enterprises leveraging open-source software and third-party consultants. Inadvertent breaches can lead to significant legal complications and financial costs. For mobile application developers wanting to "do the work," Approov is a compelling partner for building and deploying more secure applications and services. Approov's patented solutions focus on ensuring that mobile applications communicate in the most secure manner possible. It acts as a shield, verifying app authenticity before granting access to servers.

Furthermore, as development teams increasingly rely on various software components, the risk of unknowingly infringing on a patent grows. By working alongside Approov, businesses can receive guidance to stay within the confines of their IP while receiving the benefits of enhanced mobile security. It's a dual advantage: improving security measures and ensuring adherence to IP guidelines. In essence, Approov is a reliable ally for firms wanting to both safeguard their operations and respect the intellectual property landscape.

TAG'S TAKE

Approov's client software attestation technology offers a unique advantage when fortifying mobile app security. We believe it's pivotal for developers and enterprises to stay current on emerging technologies and patents to navigate the challenging IP landscape effectively and avoid inadvertent infringements. DevOps organizations should invest upfront to understand and periodically audit the source and methods of their mobile solutions, especially if using open source code.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Christopher R. Wilder

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc.." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: Approov commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.