CriticalBlue's Approov Chosen by Nimses to Protect Their Next Generation Social Media Platform

Approov deployment stops fake account creation and keeps spam away from genuine users

SAN JOSE, CALIFORNIA, USA, October 31, 2017 /EINPresswire.com/ -- CriticalBlue, provider of the award winning Approov mobile API protection solution, today announced the successful deployment of Approov within the Nimses social media platform. Fast growing mobile businesses are an attractive target for bad actors who will attack the rich APIs between mobile apps and enterprises' backends to attempt exploits such as scraping of competitive data, fake account onboarding, fraud, DDoS and account takeover. Time and again, basic encryption and embedded secrets in mobile apps have proven to be insufficient barriers against these automated scripts and hackers.

> The simplicity of Approov's integration meant that we went from initial contact with CriticalBlue to a deployed solution in only 8 days."
>
> *Andrii Sirchenko, CMO, Nimses*

According to Gartner Inc., "API security provides a secure communication channel in order to prevent malicious usage, as well as anti-automation protection against scripted attacks (for example, using bots)."*** The level of protection of their APIs will determine the resilience of an enterprise's mobile business against external disruption, in particular automated attacks. Approov is able to reliably identify and reject the 10-15% of traffic on mobile APIs which CriticalBlue customers typically report as not coming from genuine and untampered mobile apps. The solution adopts a positive approach by identifying good traffic via a cloud based software authentication service. Unlike existing approaches the security is not dependent on static secrets embedded inside the app but instead uses a dynamic measurement of the app environment at runtime to guarantee its presence and integrity. Coupled with a simple integration and deployment approach, Approov delivers a new level of protection with negligible development or operational overhead.

Nimses and Approov

Nimses is a worldwide system which records and saves the time of a human being's life. After the

user registers an account with Nimses, each minute of the person's life turns into a single Nim, a unique and indestructible unit of digital currency. The total number of Nims produced and gained by one person is accumulated into their individual account balance, called the Nimb. One can manage their personal Nimb through the free, location-based Nimses App.

"When the Nimses platform launched, the growth of new users was very rapid, exactly as we hoped. However, this soon attracted automated attacks against our API which threatened to pollute our environment and negatively impact our users' experience," commented Andrii Sirchenko, CMO, Nimses. "We wanted a solution that could ensure that we only processed traffic coming from genuine app instances and Approov delivers that. Additionally, the simplicity of integration meant that we went from initial contact with CriticalBlue to a deployed solution in only 8 days."

Software Authentication for Mobile API Protection

Protecting server digital assets while preserving a frictionless user experience is of vital importance in mobile business. From the server's perspective, knowing which customer is sending the traffic is important but it can only get the complete picture if it is also known what software is sending the traffic. Approov authenticates that the traffic is coming from the untampered mobile app through the encrypted transmission of short lifetime JWT tokens signed by a secret known only to the backend server and the Approov cloud service. Reverse engineering the mobile app, tampering with it, scripting API traffic generation or employing a man-in-the-middle attack will all result in failed authentication and blocked communication. Recent releases have added detection of rooted/jailbroken devices, use of emulators and the installation of root frameworks.

"We are seeing increasing instances of automated fake account onboarding in high growth mobile businesses such as Nimses," stated David Stewart, CEO, CriticalBlue. "An abundance of fake accounts can have a huge impact on an emerging business due to reduced revenue, damage to brand reputation and increase in cloud costs. We are delighted that Nimses acted quickly and decisively and we strongly recommend that businesses with strong mobile channels do likewise."

*** Gartner, "API Security is a Fundamental Enabler of Digital Business", 12 May 2016, ID: G00303186

Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Approov

Approov is a cloud service which verifies the authenticity of a mobile app instance and securely communicates the verdict to your backend server using industry standard JWTs. This establishes positive trust between your server and app with no impact on user experience. Approov consists of three elements:

- A library to be included in your mobile app
- An app authentication cloud service
- A token check function for your server

For more technical information, pricing details, or to sign up for a free trial, visit https://approov.io

About CriticalBlue

CriticalBlue safeguards revenue generation and security of its customers' businesses. Patented binary level dynamic analysis technology underpins the delivery of the Approov mobile API protection solution.

For more, visit https://criticalblue.com or @critblue

David Stewart
CriticalBlue
+447967728249
email us here
