SOLUTION BRIEF - Quokka MAST with Approov RASP

Mobile Apps Leak Secrets and Their APIs Are Exposed

Mobile apps are now a critical element of B2B and B2C businesses worldwide.

However apps can be analyzed, understood, cloned or copied, and the environments they run in can be hacked, rooted, instrumented and manipulated to interfere with the operation of an app. Hackers can intercept or manipulate financial transactions, steal credentials to use in ransomware attacks, target APIs with fake apps and bots, or simply aim to stop the operation of the service.

Current Security Approaches Don't Work

Current security approaches are insufficient and don't integrate well with the devops pipeline, leaving gaps which attackers can exploit.

Until now the complexity and expense of implementing comprehensive end-to-end security for apps and APIs has been seen as prohibitive for many organizations.

The Solution - Deploy MAST and RASP Together

Using Quokka and Approov together provides a cost-effective way to protect against the rapid rise in mobile threats.

Using both solutions provides a dynamic and continuous feedback loop between testing before deployment and zero trust validation at runtime. In this way applications are protected throughout the lifecycle.

- Scan your app using Quokka to quickly identify vulnerabilities, prioritize remediation efforts and inject security into the development process. Upload your app binary to the Quokka service or scan your app directly from an app store. You will immediately see detailed findings and guid-

ance on how to address the most urgent issues. The Quokka solution categorizes risks as critical, high, medium or low and you can tune the risk criteria for your particular industry and use-case.

- Use runtime app and API security from Approov to add Zero Trust protections against runtime attacks and gain continuous visibility to new threats. Approov checks the authenticity of the app and the device at runtime and validates every API request. Approov also shows in real time what device, app and man-in-the-middle attacks are happening and gives you the actionable intelligence that you're going to need to feed back to previous stages in the SDLC.

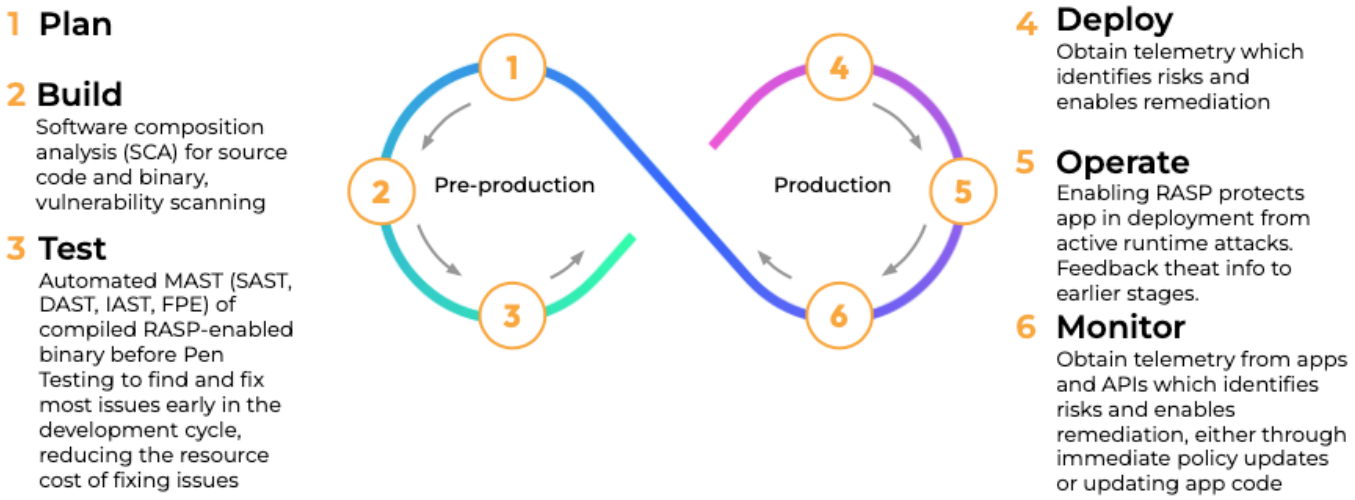
Example Use Case - Using Quokka and Approov to Eliminate API Keys and Secrets

One high category issue your first Quokka scan will uncover is that you have API keys or secrets in your code. Numerous studies have found secrets exposed in widely deployed apps in both Apple and Android app stores. Even if your own code is clean, often libraries used in app code expose secrets.

One thing you can do immediately with the Approov solution is you can get those API keys out of your code. Because of the unique way Approov acquires attestation information about the device and the application, API keys can be delivered just in time to the application but only when the device and app are verified as genuine and unmodified.

Using Quokka to perform that first scan and and Approov to remove any exposed API keys is a simple first step which has immediate benefits and will radically improve your security profile: this is an "easy win" as far as security is concerned.

Complete Protection for Mobile Apps and APIs Throughout the SDLC



Key Quokka Capabilities

Quokka Q-mast delivers defense-grade mobile app scanning capabilities including comprehensive app analysis including static (SAST), dynamic (DAST), interactive (IAST), and forced-path execution app analysis. Quokka leverages extensive threat research to identify zero-day vulnerabilities and deliver unsurpassed insights. Q-mast enables security and development teams to proactively mitigate issues early in development, saving costs and minimizing exposure to zero-day attacks.

- **Automated scanning in minutes**

  Scans apps in minutes without requiring source code, even for the latest OS versions.
- **Cloud-based platform**

  Avoids putting a strain on hardware or bandwidth.
- **Vulnerability reporting**

  Can generate and analyze SBOMs to report vulnerabilities to specific library versions.
- **Enforcement of security standards**

  Validates against security and privacy standards such as NIAP, NIST, and MASVS.
- **Malicious behavior profiling**

  Profiles malicious behavior, including app collusion.
- **Evaluates cryptographic implementations**

  Evaluates cryptographic implementations to ensure they provide robust protections.

Key Approov Capabilities

Approov RASP provides defense against runtime threats, validating each API request after checking the app has not been modified and scanning the runtime environment for hooking tools and dozens of other potential threats. Approov also provides dynamic protection and delivery of API keys and secrets at runtime so that secrets never appear in your code and can be rotated immediately when needed.

- **Runtime app attestation and authentication**

  Patented and unique approach protects against fake and modified apps.
- **Comprehensive device protection at runtime**

  Detects any runtime tampering including jailbroken/rooted devices and providing confidence that the client environment is always secure.
- **API abuse protection**

  Blocks any bots and fake and cloned apps from accessing APIs.
- **Dynamic API Key and secrets protection**

  Runtime delivery of secrets to apps only when validated, immediate rotation when needed.
- **Protection from Man-in-the-Middle attacks**

  Dynamic certificate pinning for channel protection and service continuity.
- **Cross platform support for iOS, Android, non-GMS and Harmony OS**

  Seamless operation, independent of client platform.
- **Real-time analytics for control and compliance**

  Reporting on current and emerging threats.
- **Easy integration and operation**

  Fast deployment, ease-of-operation and no false positives to manage.

Contact Approov for a free technical consultation - our security experts will provide a free Quokka app security assessment and show you how to protect your revenue and business data by using Quokka and deploying Approov Mobile Security.