Summary of Key Security Threats to Connected Car Mobile Apps

Threat 1: Unauthorized Third-Party Apps

Third-party vendors replicate official connected car mobile app functionalities and promote these apps directly to consumers. Although some of these apps are legitimately adding value, their proliferation poses risks:

- **Monetary Costs:** Third-party apps can place excessive load on cloud systems by not adhering to careful coding practices and access policies, leading to excessive consumption of cloud resources and increased costs.
- **Operational Distractions:** Unauthorized access of APIs can trigger alerts and alarms, causing additional, time-consuming work for DevOps teams.
- **Reputation Damage:** Lack of quality and poor performance of app copies can provide a degraded user experience, and this can have a negative impact on the overall reputation of the car brand.

Approov's Mitigation:

Approov Mobile Security ensures only authorized apps can access backend APIs by validating the legitimacy of the requests through continuous deep inspection - you decide which apps are authorized. This prevents unauthorized third-party apps from abusing API keys, thereby reducing cloud costs, minimizing operational distractions, and protecting the brand's reputation.

Threat 2: Direct API Access by Hackers and Hobbyists

Information is available via APIs which can be useful for genuine users (eg charging status for home automation software) or nefarious purposes (eg tracking apps). Tools and guidance are readily available to help enthusiasts create custom integrations, which leads to:

- **High Load on Systems:** These users often generate significant load by continuously polling APIs for vehicle data.
- **Evasion of Security Measures:** Communities quickly adapt and circumvent any blocks which are put in place, creating an ongoing struggle between hackers and security teams.
- **Theft of API Keys and API Abuse:** Any vulnerabilities in published APIs are swiftly published and exploited by hackers.

Approov's Mitigation:

Approov's advanced API protection can restrict access to only verified, legitimate apps, ensuring unauthorized code can never exploit the API. This reduces the system load and prevents continuous security evasion, leading to stable and cost-effective cloud operations. Approov also allows any API keys to be rotated immediately whenever there is an issue, without need for app updates.

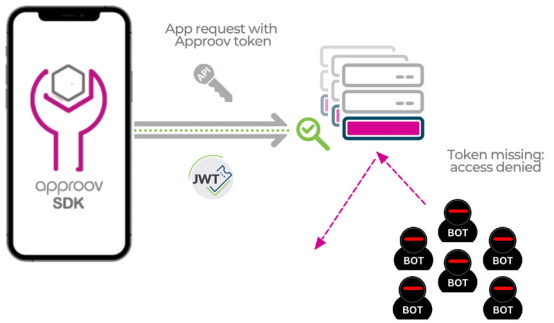
Threat 3: Bots

In some markets, social media functionalities are integrated into the connected car app in order to encourage engagement and promotion. Unfortunately bots can exploit this by:

- **Generating Fake Content:** Bots create fake posts and likes, undermining the integrity of the community.
- **Monetary Fraud:** Bots automate the process of earning virtual credits via fraudulent activities, which are then used to purchase real products, leading to real financial losses.
- **Denial of Service Attacks:** Bots can put a strain on backend systems by repeating requests to the point where service is interrupted.

Approov's Mitigation:

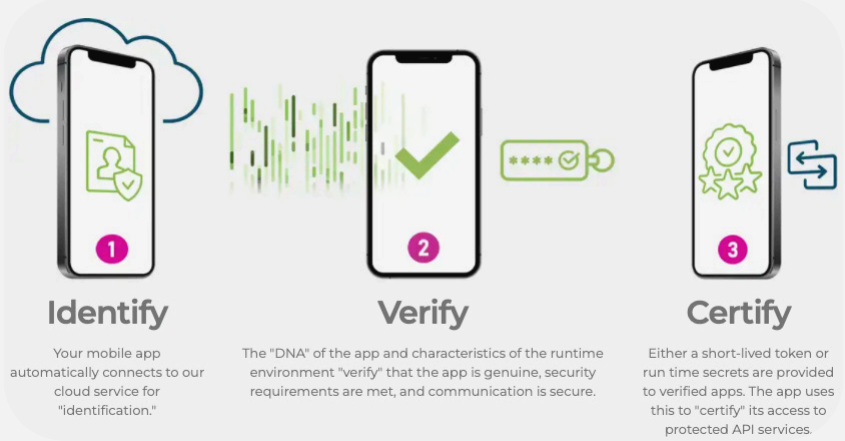
Approov ensures that only genuine users can interact with the app by validating each request's authenticity. This prevents bots from creating fake accounts, generating content, and earning credits fraudulently. The result is a secure, trustworthy community and a significant reduction in financial losses.



Overall Benefits of Approov Mobile Security:

1. **Monetary Savings:** By preventing unauthorized access and reducing unnecessary cloud usage, Approov helps cut down on operational costs.
2. **Enhanced Security:** Continuous inspection and validation ensure that only legitimate requests are processed, enhancing overall security.
3. **Reputation Protection:** By ensuring a seamless and secure user experience, Approov helps maintain and protect the brand's reputation.
4. **Operational Efficiency:** Reducing false alarms and unauthorized activities allows the DevOps team to focus on real issues, improving operational efficiency. Certificates and secrets can be rotated immediately when there are issues, preserving service continuity.
5. **Adaptability:** With Approov you can update what apps have access to your APIs and turn this access on or off anytime. Security policies, certificates and keys can also be updated at any time without requiring your users to update their mobile apps. Finally, updates are also made over the air to be able to combat the latest threats as well as recently discovered zero day vulnerabilities.

By addressing these pain points with Approov Mobile Security, businesses can mitigate significant risks, reduce costs, protect their reputation, and ensure stable and secure cloud operations.



Only your own mobile apps — running in safe environments and communicating over secured connections — can use your APIs and backend resources. Botnets, malicious scripts, tampered and fake apps are blocked.

Get expert advice on safeguarding your mobile apps from API abuse, tampering, and reverse engineering.

Contact us today: https://approov.io/info/contact