approov

Mobile Security Threats in Connected Car Services: What You Need to Know

Mobile Security Threats in Connected Car Services: What You Need to Know

Key Takeaways

- **Connected Cars are Prime Targets for Cybercriminals:** The increased connectivity of vehicles and their role as data hubs make them attractive targets for cybercriminals. These threats are expanding with the complexity of connected car architectures and the high value of the data they generate.
- **Insecure Mobile Apps are a Key Attack Vector:** Mobile apps provide an entry point to the connected car ecosystem for criminals.
- **API Vulnerabilities Widen the Attack Surface:** APIs are essential in the automotive ecosystem, enabling internal system integration and external communication. However, they also introduce risks, as attackers exploit vulnerabilities to get unauthorized access or control over vehicle systems.
- **Threats to Connected Cars:** Connected car apps face multiple threat vectors, including unauthorized access, insecure data transmission, app vulnerabilities, malware, and physical security risks. These risks can compromise user safety, data privacy, and vehicle functionality.
- **Zero Trust Principles for Automotive:** Zero Trust principles address the unique vulnerabilities of connected cars by requiring continuous verification, implementing layered security measures, and adopting proactive threat monitoring.
- **Impact of Third-Party Apps and Bots:** Unauthorized apps and bot activity can overload systems, increase operational costs, and damage brand reputation. These unauthorized apps pose additional security risks and can lead to service interruptions or fraudulent activities.
- **Approov Mobile Security Solution:** Approov offers enhanced protection by ensuring only authorized apps can access vehicle APIs, preventing API abuse and unauthorized data access, and reducing operational costs.
- **Cost and Operational Efficiency Gains:** By reducing unauthorized access and enhancing system stability, solutions like Approov provide significant cost savings and operational benefits, allowing you to maintain security without a heavy resource burden.
- **Future-Proof Adaptability:** With Approov, you can adapt security policies on demand, ensuring they can respond to new threats, manage access dynamically, and continuously protect your connected car systems from evolving cyber threats.

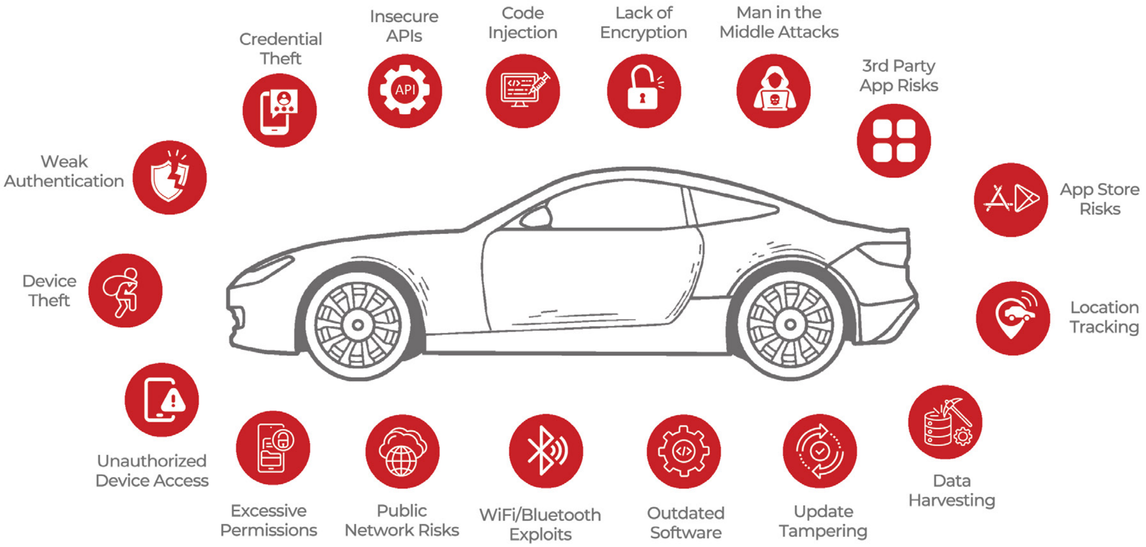
Connected Cars are Attractive for Cyber Criminals

As connected cars become mainstream, connected car architectures are becoming more and more sophisticated. Unfortunately, the automotive cyber threat opportunity is also rapidly evolving and expanding.

The automotive ecosystem extends far beyond the sensors and devices employed within vehicles. Suppliers, data brokers, API aggregators, data consumers, third-party service providers and developers of emergent applications and products all want to participate in the market.

Vehicles have become sophisticated data hubs - both creating and consuming vast quantities of valuable data. Global positioning system (GPS) location, engine, fuel-level, battery status, driver behavior, diagnostic trouble codes and service history data are all valuable information, and when combined, can deliver new insights, and this presents an opportunity for all kinds of applications focusing on fuel efficiency, vehicle performance, safety, maintenance, driver performance, local weather, environmental impact and even traffic status.

Vehicle data will not be anonymized because if it were, its value would dramatically decrease. Unfortunately this rich source of personalized data will also motivate cybercriminals and bad actors and this will attract coordinated, large-scale cyberattacks against connected vehicles.



APIs Expand the Attack Surface

APIs are a key element of the automotive data ecosystem. They are widely deployed to connect a vehicle's various internal systems and are used for external activation of these systems from mobile apps. They are also accessed by third-party services which provide emergency assistance and energy management. Car makers depend heavily on APIs to provide updates to vehicle software. In every connected car architecture, there are cloud-based APIs for communication between services, cloud-to-vehicle APIs and mobile-to-vehicle APIs.

However, APIs have vulnerabilities and attackers are quick to exploit them. The combination of APIs and mobile apps is particularly problematic since anyone – including attackers – can freely install an application and reverse engineer and study it for weaknesses. There have already been cases where hackers have acquired account credentials and exploited them to execute remote attacks on vehicle APIs.

API aggregators such as Smartcar have built a business model which provides a single API to app developers, hiding the complexity of accessing individual car maker's systems, accelerating the development of scores of apps which access vehicle data.

Understanding the Threat Landscape for Connected Cars

Key security threats to connected cars specifically related to their associated mobile apps and third-party apps:

- **Unauthorized Access to Vehicle Controls:**
  - **Weak Authentication:** Insufficient authentication mechanisms in the app can allow attackers to gain unauthorized access to vehicle controls, enabling them to start the engine, lock/unlock doors, or even drive the car.
  - **Credential Theft:** Phishing attacks or malware on the user's mobile device can steal login credentials, granting unauthorized access to the connected car.
- **Insecure Data Transmission:**
  - **Lack of Encryption:** Data transmitted between the app and the vehicle might not be properly encrypted, allowing attackers to intercept sensitive information such as location data, driving habits, and personal details.
  - **Man-in-the-Middle (MitM) Attacks:** Attackers can intercept and alter communication between the app and the vehicle if the connection is not properly secured.
- **App Vulnerabilities:**
  - **Insecure APIs:** Vulnerabilities in the APIs used by the app to communicate with the vehicle can be exploited to gain unauthorized access or control.
  - **Code Injection:** If the app is not properly secured, attackers might inject malicious code to manipulate the app's behavior and gain control over vehicle functions.
- **Malware and Malicious Apps:**
  - **Third-Party App Risks:** Third-party apps with access to the connected car's functions can introduce vulnerabilities if they are not properly vetted or secured. Malicious apps can exploit these vulnerabilities to control or monitor the vehicle.
  - **App Store Risks:** Users might download malicious apps from unofficial app stores, leading to compromised devices and, subsequently, the connected car system.
- **Privacy Invasion:**
  - **Data Harvesting:** Apps (both official and third-party) might collect more data than necessary, leading to potential privacy breaches. This data can be misused if not properly protected.
  - **Location Tracking:** Continuous tracking of the vehicle's location by the app can pose significant privacy risks if this information is accessed by unauthorized parties.
- **Insecure Software Updates:**
  - **Update Tampering:** If the app or vehicle firmware updates are not securely transmitted, attackers can intercept and alter these updates to introduce malicious code.
  - **Outdated Software:** Failure to update the app or vehicle software promptly can leave the system vulnerable to known exploits.
- **Network Security Issues:**
  - **Wi-Fi and Bluetooth Exploits:** Many connected car apps use wireless technologies to communicate with the vehicle. If these connections are not secure,

attackers can exploit them to gain access.

- **Public Network Risks:** Using the app over public or unsecured Wi-Fi networks can expose the communication to interception and manipulation.

- **Physical Security of the Mobile Device:**
  - **Device Theft:** If the mobile device used to control the car is lost or stolen, an unauthorized person could gain access to the vehicle.
  - **Unauthorized Device Access:** If the mobile device is not secured with strong passwords or biometric authentication, it can be easily accessed by others.
- **Insufficient App Permissions Management:**
  - **Excessive Permissions:** Apps that request more permissions than necessary can become security risks. For instance, a third-party app with extensive access permissions could misuse its privileges to compromise the connected car system.

To address these threats, it is critical for developers to enforce strict security protocols, including end-to-end encryption, robust authentication methods, regular security audits, and secure update mechanisms. Users should also be educated on best practices, such as downloading apps only from trusted sources, keeping their devices secure, and regularly updating both their apps and vehicle firmware.

Some Recent Security Issues

1. In 2024, a researcher demonstrated the ability to remotely control cars by exploiting vulnerabilities in the Sirius XM app, which is commonly used in vehicles from brands like Nissan, Honda, and Toyota. The hack only required the vehicle's VIN (Vehicle Identification Number) to gain access to app code and control functions like starting, stopping, locking, and unlocking the vehicle remotely.
2. API attacks account for 12% of automotive hacking cases, according to Upstream
3. Hackers often exploit weaknesses in the APIs that allow integration and communication between vehicles and apps.
4. The increasing adoption of connected car technology has raised concerns about cybersecurity risks. It's projected that 100% of new cars sold will be connected by 2026, potentially increasing the relevance of car hacking threats
5. In 2015, researchers Charlie Miller and Chris Valasek demonstrated the ability to remotely control a Land Rover's infotainment system, climate control, and speed from 10 miles away. While this incident is older, it highlights the ongoing evolution of connected car vulnerabilities.
6. A new insurance product called "Cyber for Auto" was recently introduced by Munich RE to cover drivers against cyberattacks, ransomware, and identity theft related to connected cars. This development indicates a growing awareness of the potential risks associated with connected car technologies and mobile apps.

Security in Connected Car Apps

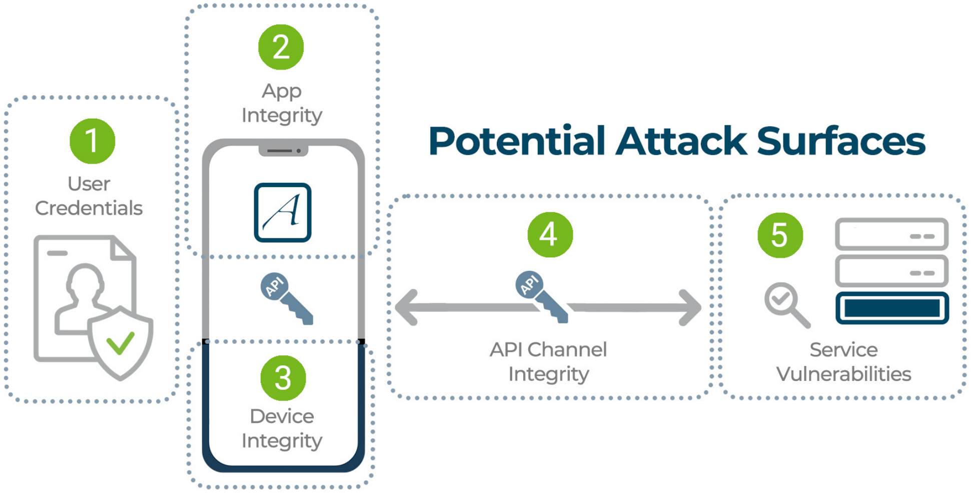
Every connected car has a corresponding mobile app. This mobile app will communicate to the car via bluetooth or ultra-wideband, and to back-end APIs via the internet using Wifi or cellular networks. The mobile app will run on a device which is owned by the consumer. It's important that the mobile app does not become an entry point for hackers to back-end systems or to the car itself.

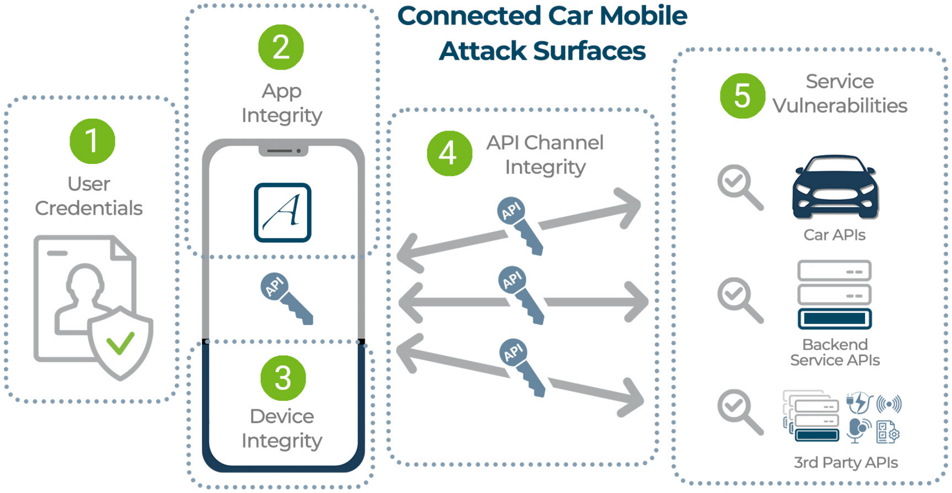
Attack Surfaces in Mobile Apps and Why This Matters for Connected Cars

There are two fundamental security challenges with mobile apps: The first is that they can be reverse engineered, even if an obfuscation tool has been used. The second is that they run in a client environment which is open to hackers and is neither owned or controlled by the app owner. Unless steps are taken, 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. Also, because the device is open to abuse, hackers can intercept communications, even if channels are encrypted.

This is why mobile connected car apps are a target for hackers.

Attackers do not target only one attack surface. They will often seek useful information from one and then use that to target another in a systematic way using automated tools.





Attack surfaces in detail:

1. **User Credentials:** The authentication and authorization of the user is critical, before access to a connected car app is granted. Frameworks such as OpenID Connect, and OAuth2 can be used and 2FA and biometrics provide a further level of protection. Some of the worst documented hacks so far have been where a user email or a VIN number have been all that was required to access car software. User credentials are often stolen and traded on the dark web and credential stuffing attacks are used to cycle through stolen ids until one works. Man-in-the-middle attacks on comms channels can steal credentials even when multi-factor authentication (MFA) and encrypted traffic are used. Even with the best authentication, additional mechanisms are needed.
2. **App Integrity:** At run-time any API should seek to establish the validity of what is making the request to the API server. Is it really coming from a genuine instance of your mobile app, or is it a script or a bot. There are secure ways for an app to attest its identity.

3. **Device Integrity:** Hackers install tools on the device to interfere with the running app. Continuous assessment of the device environment is needed.
4. **Channel Integrity:** In connected cars the communications channels can be multiple. If we focus on the app there will be a connection to the car itself (V2D) and to the cloud (for APIs). Since hackers have access to the device, they can carry out MitM attacks unless these are blocked.
5. **Service Integrity:**

    - **Car APIs:** Accessing the car APIs is the most dangerous scenario, fake apps and scripts can scale up attempts to find vulnerabilities, and MitM attacks on the channel are the method used by attackers to steal secrets used to access APIs.
    - **Back-end APIs:** Hackers can access back end data using stolen identities and API keys, again using automated tools.

(You can find more detail on each attack surface here)

Applying the principles of Zero Trust to Connected Cars

Zero Trust is a key concept in modern security.

However, initial approaches to automotive cybersecurity have typically relied on perimeter-based static defenses, assuming that potential threats can be stopped at the network boundaries with authentication and authorization.

This is dangerous, since there is no perimeter as such with connected cars and given the dynamic nature of threats and the growing interconnectivity of connected vehicles, a new methodology is needed to address the automotive industry's rapidly evolving threat landscape.

This is where zero trust, a security concept that assumes no implicit trust, regardless of whether the connection is external or internal, is highly relevant. In the automotive industry, zero trust architecture is a great model to address the inherent vulnerabilities and complexities arising from many interconnected systems, remote access, and integrating third-party APIs and services. The key principles of zero trust are:

- **Never trust, always verify:** Every access request to every system or API must be verified
- **Defense-in-depth:** Multiple levels of security are needed - e.g. do not depend on code obfuscation alone, add app attestation to strong user authentication, check for MitM attacks, etc.
- **Continuous Security must be runtime and not static:** One criticism of car security is it is static in nature - continuous monitoring and checking is needed
- **Assume breach:** Another key principle of ZT is assuming that hackers will be successful so preparing for this is key to keep the service running. It must be possible to manage and rotate API keys, certificates as well as block suspect devices and users immediately when issues arise.

Other Threats for Connected Car Apps

The worst scenario is for hackers to gain access to the car's controls and functions but there are other ways hackers can target connected car apps. Here are three serious threats which are top of mind for security teams.

Threat Number 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.

Threat Number 2: Direct API Access by Hackers and Hobbyists

Information is available via APIs which can be useful for genuine users (e.g. charging status for home automation software) or nefarious purposes (e.g. 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 undisciplined access and 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.

Threat Number 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 and Connected Car Security

Approov Mobile Security ensures only authorized apps can access car and 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. Apporov protects car and service APIs while reducing cloud costs, minimizing operational distractions, and protecting the brand's reputation.

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.

In summary, deploying Approov protects connected car apps and their APIs and provides the following benefits:

- **Enhanced Security:** Zero trust approach provides continuous inspection and validation to ensure that only legitimate requests are processed, enhancing overall security. Without needing to deploy a large security team.
- **Monetary Savings:** By preventing unauthorized access and reducing unnecessary cloud usage, Approov helps cut down on operational costs.

- **Reputation Protection:** By ensuring a seamless and secure user experience, Approov helps maintain and protect the brand's reputation.
- **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.
- **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 operations.

References

Cybersecurity Best Practices for the Safety of Modern Vehicles by U.S. department of Transportation, National Highway Traffic Safety Administration