ZIMPERIUM

Protecting Connected Car Apps and Services with Zimperium

Safeguarding The Future of Connected Vehicles

Automotive innovation is increasingly driven by mobile apps and in-vehicle services. From unlocking cars with a phone to activating emergency services and maintenance, mobile apps are integral to modern driving experiences. But as convenience increases, so does risk. Threat actors now target automotive apps to gain unauthorized access, tamper with critical features, and exfiltrate sensitive data.

THE STATS

- By 2030, **96%** of new vehicles worldwide are expected to be shipped as connected cars.
- **56%** of drivers have connected their vehicle to a mobility application.
- **61%** of connected services subscribers want more features in their subscription

Challenge

- **Digital Key Security:** Digital car keys must be protected against reverse engineering and abuse to prevent theft.
- **Subscription Feature Protection:** Apps enabling subscription-based features must ensure client-side code and APIs are hardened to prevent spoofing or abuse.
- **Unified Security Posture:** OEMs must standardize protections and gain consistent threat visibility across all mobile apps, including those developed by third parties.

How Zimperium Secures Connected Cars

Zimperium's Mobile Application Protection Suite (MAPS) platform helps automotive vendors embed app shielding, white-box cryptography, and runtime protections directly into their apps.

Use Case 1 - Secure Digital Car Keys

- **The Challenge**: Mobile apps for car keys, remote access, and self-parking create new attack surfaces. Compromise risks unauthorized vehicle access/operation.
- **The Solution**: Code Obfuscation & Protection; Anti-Tampering & Integrity Checks; Secure Key Management; Runtime Threat Detection
- **The Outcome**: Ensures digital car keys cannot be hijacked, remote parking remains safe, and trust in connected mobility grows.

Use Case 2 - Protect In-Vehicle Subscription Services

- **The Challenge:** Apps delivering emergency assistance, diagnostics, and infotainment must be secure and prevent abuse.
- **The Solution:** Obfuscation to prevent reverse engineering; Runtime Protection against tampering; Secure API & Key Protection; Built-in Regulatory Compliance
- **The Outcome:** Keeps critical in-vehicle services safe, compliant, and trustworthy—preserving driver safety and regulatory standing.

Use Case 3 - Unified Security Across All Mobile Apps

- **The Challenge:** The global automotive ecosystem's mobile apps lack consistent security, centralized oversight, and risk visibility, leading to production incidents.
- **The Solution:** Comprehensive AppSec Platform; Application Vetting; Runtime Threat Visibility.
- **The Outcome**: A unified security framework that protects all mobile apps—regardless of who built them—while enabling consistent security practices, reducing operational risk, and improving threat response across the enterprise.

Real-World Case Study: Securing Apps, IP & Customer Trust

Challenge:

A global automaker aimed to protect its mobile apps and IP while improving app security and resilience. They lacked consistent protection across apps, had limited visibility into runtime threats, and needed to respond faster to incidents affecting trust and compliance.

Outcomes Achieved with Zimperium:

- **Security Streamlined**: 100% of mobile apps hardened and monitored. CI/CD pipelines integrated with Zimperium's app's security
- **Build Tamper-Resistant Apps**: Apply protection against tampering, repackaging, emulators, and unsafe networks during development.
- **Respond Faster** - Automated, on-device responses streamline workflows, significantly reducing threat resolution time.
- **Enhanced Security with Shift-Left Testing**: Automating binary testing during development leads to fewer penetration test findings late in the cycle and builds stakeholder confidence from the start.

Ready to secure your connected car mobile apps and services?

Request a Demo or email **info@zimperium.com**

ZIMPERIUM®

Learn more at: Zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244