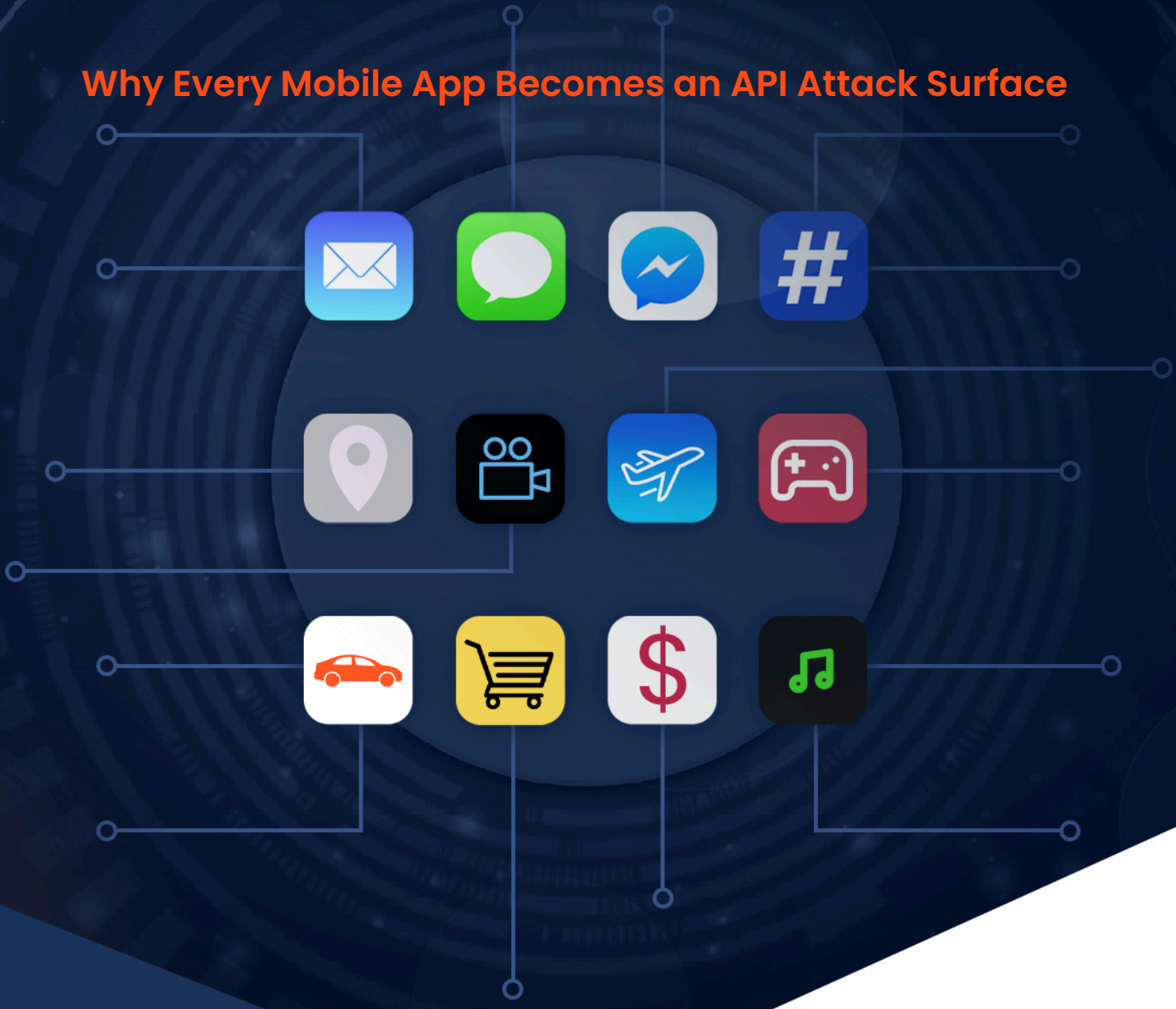
Mobile Apps: The New API Battleground

Why Every Mobile App Becomes an API Attack Surface



MAPS™

ZIMPERIUM®

Modern enterprise mobile apps rely on APIs for services, features, integrations, and secure data access. However, during mobile app development, API URLs and their calling mechanisms are embedded in the application's code, making them visible, accessible, and vulnerable to attackers. Once the app is published, attackers can reverse-engineer it and tamper with it to exploit and abuse it, thereby extracting this information.

The 2025 Zimperium Global Mobile Threat Report found that **nearly half of mobile apps still contain hardcoded secrets like API keys**, making it easier for attackers to steal and misuse them.

The API Security Starting Point

According to the May 2024 Gartner® Market Guide for API Protection, the typical API breach can leak at least **10 times** more data than an average security breach. But organizations typically begin their API security journey with traditional solutions that focus on discovery, configuring them correctly, enforcing access control, monitoring traffic for malicious usage, and applying rate limiting. Most of these solutions, including firewalls, gateways, and proxies, operate at the enterprise perimeter, inspecting and controlling traffic as it enters or exits the environment.

These security measures are essential but not enough for mobile APIs because mobile apps operate in untrusted environments.

Where Traditional Security Breaks Down

While traditional API security plays a vital role at the perimeter, real-world mobile environments introduce complexities that these tools were never designed to handle. Several mobile-specific nuances and challenges undermine their effectiveness, making it difficult to secure mobile app APIs.

1 in 3 android apps
leak sensitive data

more than half of iOS apps
leak sensitive data

Here are the key challenges:

APIs Are Exposed Inside the App

- Attackers can reverse-engineer an app to extract API endpoints, tokens, and logic, enabling offline abuse that backend tools cannot trace to its true origin. The GMTR found that **about 1 in 3 Android apps and more than half of iOS apps leak sensitive data**, giving attackers easy paths to map APIs and harvest tokens.

Client-Side Tampering Happens Before Traffic Leaves the Device

- Tools like Frida or Xposed let attackers intercept and modify API calls directly inside the app, long before they reach the backend. The GMTR found that **1 in 400 Android devices is rooted and 1 in 2,500 iOS devices is jailbroken**, giving attackers complete control of the environment.

No Device or App Integrity Awareness

- Traditional tools can't tell if traffic is coming from a genuine app on a trusted device or from a repackaged clone on an emulator. The GMTR found that **3 out of every 1,000 mobile devices are already compromised**, and **1 in 5 Android devices encounters malware in the wild**, underscoring how often attackers operate from unsafe environments.

SSL Pinning Blocks Visibility

- Mobile apps often use SSL pinning to prevent man-in-the-middle attacks. But pinning also prevents API gateways and WAAPs from inspecting encrypted traffic. And despite its use, the GMTR found that **nearly 1 in 3 Android finance apps and about 1 in 5 iOS travel apps remain vulnerable to man-in-the-middle attacks**, leaving sensitive data and API traffic exposed.

Schema Validation Can't Catch Business Logic Abuse

- Even well-formed requests can be malicious. Traditional tools often overlook context-specific abuse, such as price manipulation, promotional stacking, or unauthorized access.

To close these gaps, organizations need protection that starts at the mobile app itself.

What Can Go Wrong

Mobile apps don't just consume APIs—they expose them. Yet, most security strategies stop at the perimeter, leaving the client-side unprotected. Without visibility into the app and device making the call, attackers can do the following:

1. **Map and manipulate API behavior by modifying app code**
   By tampering with the app or hooking into runtime functions, attackers can replay, alter, or craft API calls that bypass the app's intended flow.

2. **Extract secrets and tokens by reverse engineering the app**
   Attackers decompile the app to steal API keys, auth tokens, and signing logic, then reuse them from emulators or automated tools to bypass security.

3. **Exploit device-level controls to simulate real usage**
   Running the app on rooted devices or emulators allows attackers to spoof identity, location, and device identifiers, thereby automating transactions and evading traditional network-level defenses.

Securing APIs from the Inside Out

The way to stop these attacks is to make the app itself part of the defense. Protecting APIs can't be done at the perimeter alone; it has to start with the mobile app calling them. Hardening the client side and proving the integrity of every request shuts down the abuse paths attackers rely on.
Here are two essential strategies to assist in achieving that:

API Hardening

Sensitive endpoints, tokens, and business logic must be shielded inside the app so attackers cannot extract or manipulate them. Code obfuscation, secure storage of keys, and runtime defenses make it harder for attackers to reverse engineer or tamper with the API interaction.

App Attestation

Every API call should prove it comes from a genuine, untampered app running in a trusted environment. App attestation enables servers to verify the authenticity of requests, ensuring they originate from a genuine app, not a repackaged one, emulator, or compromised device.

Conclusion: Why Client-Side API Protection Matters

Securing APIs at the perimeter is crucial, but it only addresses part of the issue. As attackers increasingly target mobile apps to steal secrets, manipulate API behavior, and automate fraud, protecting the client side becomes vital. By combining server-side defenses with in-app protections, organizations can close security gaps, lower exposure, and develop a truly resilient API security strategy that begins at the source.

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank. Learn more at www.zimperium.com and connect on LinkedIn and X (@Zimperium).

ZIMPERIUM®

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

© 2025 Zimperium, Inc. All rights reserved.