Quokka

WHITEPAPER

What Is Mobile Security?

And Why Is Mobile App Security Testing Important?

What Is Mobile Security?

And Why Is Mobile App Security Testing Important?

Given the ubiquity of smartphones and tablets that promise greater functionality and convenience, it is not surprising that the mobile app market is flourishing. As of September 2022, 6.64 billion people own smartphones, constituting 83.40% of the world's population. Most businesses are now aware of the versatility and effectiveness of mobile apps when it comes to engaging with clients and increasing sales. Mobile apps are also released frequently; the Apple App Store currently has more than 1.96 million apps available for download, while the Google Play Store has about 2.87 million. Given that 88% of time spent on mobile devices is spent using apps, these mobile apps can greatly enhance the user experience.

The market for mobile apps is predicted to generate up to $935 billion in revenue by 2023 – meaning that mobile apps are pretty much indispensable. But while this is good news for those who create and publish mobile apps, security experts are concerned because this increased usage means more opportunities for hackers to exploit security vulnerabilities. Now is the time to talk about mobile application security and the need for Mobile Application Security Testing.

What Is Mobile Application Security?

Mobile application security is a technique for ensuring the software security posture of high-value mobile applications running on various operating system platforms like Windows Phone, iOS, and Android, as well as on tablets. It focuses on protecting one's digital identity from fraudulent attacks as well as preventing malicious parties from using mobile apps to launch attacks on associated users and organizations (especially with the growth of mobile economies).

Attackers looking to access accounts, carry out fraud or identity theft, steal data or trade secrets, conduct espionage, or spread malware frequently target mobile apps. Due to the increased focus on quick release cycles, teams may skip custom mobile app security testing in their SDLC processes. Some mobile app developers end up creating mobile apps with security and privacy flaws in the rush to add new features that attract users and enhance the user experience. If these apps are attacked, sensitive personally identifiable information (PII) and digital identity data are at risk.

According to the OWASP Mobile Top 10, the most prevalent security risks that affect mobile apps include inadequate cryptography, reverse engineering, obtrusive functionality, code tampering, and poor client code quality, as well as insecure data storage, authentication, communication, and authorization. Given the volatility of these risks, there is a need for custom tooling made to test mobile (Android and iOS) code. Utilizing testing tools made from and for other platforms and technologies may not suffice due to the unique technologies used in mobile. This brings us to the subject of Mobile Application Security Testing.

What Is Mobile Application Security Testing (MAST)?

Mobile Application Security Testing, or MAST, is the process of locating and examining weaknesses in mobile applications (for iOS, or Android) either during or after development. It is a type of AppSec testing that focuses on conducting testing on mobile apps to discover weaknesses and exploitable vulnerabilities in the application.

There are many MAST techniques and tools available today; however, a thorough Mobile Application Security Testing strategy will employ a combination of static analysis and dynamic analysis to evaluate risk areas holistically. The three main methods for performing Mobile Application Security Testing are as follows:

SAST: MAST solutions use static analysis to identify vulnerabilities in an application's source, binary, or bytecode.

DAST: MAST solutions use dynamic analysis to test an application while it is running.

Behavioral Testing: MAST solutions use behavioral analysis to track an app's actions while it is running in order to observe the data flows and how weaknesses identified in SAST or DAST may impact the user or developer.

Why Is Mobile App Security Testing Important?

In order to understand the importance of Mobile Application Security Testing, you must first understand the many costs associated with security breaches. Not only do security breaches result in the loss of sensitive personal data (which impacts many individuals), they also entail losses for organizations, including lost revenue and damaged reputations. In addition, organizations face financial penalties if the compromised data is governed by laws like the Global Data Privacy Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or the California Consumer Privacy Act (CCPA).

Using a comprehensive MAST solution is one of the best ways to ensure continuous monitoring and a dynamic testing strategy for addressing the highly variable landscape of mobile security threats. Automated MAST solutions test mobile apps for potential security flaws according to the platforms and frameworks on which they will likely run, as well as in relation to the anticipated user base. Developers can lower application security risks prior to the release of their apps by implementing Mobile Application Security Testing and finding and fixing weaknesses as early as possible. In addition, MAST also provides the following benefits:

- Maintaining the organization's reputation by securing applications and preventing breaches.
- Avoiding the loss of sensitive information.
- Increasing customers’ trust in the organization while safeguarding their data.
- Reducing the likelihood of both internal and external threats.
- Boosting the confidence of major investors and lenders.

Getting Started with Mobile Application Security Testing

Mobile devices have become an essential part of normal business operations due to the global shift to remote work and the rise of Bring Your Own Device (BYOD) policies. As we explained above, mobile apps are a prime target within the cybersecurity attack landscape. Any flaws in mobile apps expose users (and enterprises) to exploitation, making mobile application security more important than ever. To ensure comprehensive mobile application testing throughout the development lifecycle while also maintaining privacy, application developers and organizations must work around the clock.

As a market leader in Mobile Application Security Testing, Quokka's proactive mobile security solutions guarantee a higher level of security and privacy for mobile apps and mobile devices. Our Q-MAST platform analyzes iOS and Android apps to find security, privacy, and code quality issues without access to the source code. With our recently launched Q-Scout BYOD enterprise mobile security solution, we are disrupting and reshaping the market by offering privacy and security to device owners while still allowing access to the enterprise data that we protect. To learn more, you can watch our live demo.