Applying OWASP's Mobile App Security Guidance With Confidence

2022

ZIMPERIUM®

The Open Web Application Security Project® (OWASP) works to improve software security through its community-led, open-source software projects. The organization hosts local and global conferences, and it has hundreds of chapters and tens of thousands of members around the world. Zimperium is an honorable benefactor of one of the organization's flagship projects, the OWASP Mobile Application Security (MAS) project.

The project developed the MASVS (Mobile Application Security Verification Standard) that contains practical guidance for security teams and application architects, developers, and testers. The standard defines the qualities of a secure mobile app, providing a security model and specific requirements that need to be addressed. The project also delivered the OWASP MASTG (Mobile Application Security Testing Guide), which includes recommendations and testing procedures to verify that MASVS requirements are being addressed, as well as a handy dandy checklist bringing everything together.

The MASVS offers coverage of several different areas:

- Data Storage and Privacy (MASVS-STORAGE)
- Cryptography (MASVS-CRYPTO)
- Authentication and Authorization (MASVS-AUTH)
- Network Communication (MASVS-NETWORK)
- Interaction with the Mobile Platform (MASVS-PLATFORM)
- Code Quality and Exploit Mitigation (MASVS-CODE)
- Anti-Tampering and Anti-Reversing (MASVS-RESILIENCE)

How Zimperium Helps Developers Meet OWASP MASVS

Mobile application risks start in development and persist throughout the app's entire lifecycle, including when running on an end-user's device. Zimperium's Mobile Application Protection Suite (MAPS) enables teams to establish robust security across this lifecycle.

The MAPS platform consists of four security solutions, and it features a centralized dashboard that enables teams to view threat trajectory data, so they can more intelligently create, manage and enact critical response policies. MAPS is the only unified mobile security suite that combines centralized visibility with comprehensive in-app protection, helping organizations to meet OWASP's mobile app security requirements.

Data Storage and Privacy

Today, mobile apps are used to access and process a range of sensitive data, including enterprise credentials, payment card details, and personally identifiable information (PII). In order to establish cohesive mobile security, it is essential to establish strong safeguards around these assets.

However, data on today's mobile devices is subject to an array of risks. For example, if an app incorrectly uses APIs of a mobile OS, such as one used for local storage or inter-process communication (IPC), sensitive data may be exposed or leaked to other apps running on the same device. In these scenarios, it is also possible that data can be leaked to cloud storage, backups, or the keyboard cache. Further, mobile devices are more prone to theft and loss, which means it is more likely devices, and the data they hold, will be exposed.

For all these reasons, it is vital that mobile app developers take precautions in how they store user data. For example, teams can ensure they use appropriate key storage APIs and leverage available hardware-backed security features.

This can be easier said than done in the mobile arena. One primary problem is due to the proliferation of device variations, particularly with Android devices. For example, hardware-backed secure storage is not available on all Android devices, and even when present is rendered unsafe when the device is compromised. Further, many users are running outdated versions of Android. If an app developer wants to make their app available on an out-of-date device, they would have to build their app using an older version of Android's API, which may lack important security features. Given this, teams sometimes have to make the tough choice of whether to accept compromised security or exclude a portion of their potential user base.

Another issue stems from the use of cloud storage. The reality is that app developers rely heavily on the cloud infrastructures of various service providers. Cloud Native apps are quickly becoming the norm. All too often, the access to cloud storage repositories is poorly configured within the app allowing unauthorized access and theft to sensitive data. In fact, analysis from zLabs, Zimperium's advanced research team, found that 14% of the iOS and Android apps that use cloud storage had insecure configurations and were vulnerable to a number of significant issues that left sensitive data exposed.

zScan, Zimperium's mobile app security testing (MAST) solution, not only helps application teams prevent insecure storage but also helps mitigate privacy, security, and compliance risks across the entire application. zScan can be integrated with an organization's CI/CD process and scan an app each time it gets built. If any security issues are found, zScan will highlight them and provide recommendations to resolve the issue.

Cryptography

Cryptography represents an integral capability for securing data stored and transmitted on a mobile device. However, if proper standards and best practices aren't employed, the risks associated with data loss can be significant. To maximize the data security, mobile app developers need to use proven cryptographic libraries, effectively configure cryptographic primitives, and employ a solid random number generator. Further, cryptographic keys must be effectively secured at all times, even when the device is compromised.

Zimperium's zKeyBox protects confidential data by securing cryptographic keys. The solution employs white-box cryptography to ensure keys cannot be discovered, extracted, or manipulated. zKeyBox keeps keys secure at all times, including when they're at rest, in transit, and in use. By leveraging zKeyBox, teams can ensure their apps comply with OWASP's cryptography requirements.

Authentication and Authorization

In most mobile app architectures, users log in to a remote service. In these instances, much of the authentication and authorization logic typically happens at the endpoint. However, there are also some implementation challenges on the mobile app side. Mobile apps often store long-term session tokens on the device that are unlocked with user-to-device authentication features, such as fingerprint scanning. (These authentication features are usually based on OWASP MSTG specifications.) While these authentication mechanisms can enable fast logins and an improved user experience, they can also introduce a great deal of complexity and security concerns.

Many mobile app architectures now also incorporate authorization frameworks like OAuth2. These frameworks often either delegate authentication processes to a separate service or to a third-party authentication provider. With OAuth2, teams can outsource client-side authentication logic to other apps on the same device. To achieve maximum security in their implementations, development and testing teams must be clear on the pros and cons of these different frameworks.

Often, these frameworks operate on the assumption that the underlying mobile device can always be trusted, which is only sometimes the case. The risk posture of the mobile device is dynamic as it's driven by end-user behavior. So without this real-time visibility into the device's risk posture, user access and data remain prone to attacks.

Organizations should use white-box cryptography to transform and obscure cryptographic algorithms so that keys never appear in the clear and the execution logic is untraceable. Zimperium's zKeyBox leverages white-box cryptography to protect keys and secrets within your mobile application. Your keys cannot be extracted—even if the device itself has been compromised.

In addition, Zimperium's zDefend enables mobile apps to detect and protect themselves proactively against runtime threats and attacks on the device. With this runtime application self-protection (RASP) capability, mobile apps can assess device risk posture in real-time and dynamically prevent access or disable high-risk functionality to minimize fraud and theft attempts on end-user devices proactively.

Network Communication

Mobile device users often access a range of networks, including free Wi-Fi networks at a café, library, airport, or number of other locations. This leaves users, their data and their devices exposed to a broad range of network-based attacks. To guard against these threats, it is imperative that application teams establish mechanisms that safeguard the confidentiality and integrity of information transmitted between the mobile app and remote service endpoints. Toward that end, it's imperative for teams to employ the TLS protocol to implement an encrypted channel for network communication.

zScan identifies privacy, security, and compliance risks in the development process—before mobile apps are released to the public. zScan performs a static and dynamic analysis of code, identifies risks, and provides a prioritized list of findings. The solution can uncover a range of risks, including insecure API calls and sensitive data exposure.

With zDefend, organizations can enable their application to detect compromised and unsafe networks and proactively protect itself by taking actions on the end user's device. The solution provides continuous monitoring and protection and delivers effective threat modeling capabilities. With zDefend, teams can prevent high-risk transactions from occurring in untrusted network environments.

Interaction With the Mobile Platform

The architectures of mobile OSs vary substantially from traditional desktop architectures. For example, compared to desktops, all mobile OSs implement app permission systems that regulate access to specific APIs. They also offer a range of inter-process communication (IPC) capabilities that enable different apps to exchange signals and data. These OS-specific features can present both advantages and specific risks. For example, if an app doesn't use an IPC API correctly, sensitive data may be exposed to other apps running on the device, including malware and compromised apps.

MAPS delivers comprehensive capabilities for addressing risks that are unique to mobile devices and apps. With zScan, teams can spot and detect problematic API calls and risky permissions that may be introduced during the development lifecycle. Additionally, zDefend enables teams to establish real-time protections against malware and zero-day exploits that typically abuse these threat vectors. With these capabilities, teams can safeguard data that may otherwise be exposed by malware attacks and compromised apps running on the same device.

Code Quality and Exploit Mitigation

Mobile app development teams are focused on getting features and functionality delivered quickly and often use a wide variety of programming languages and third-party (open-source or proprietary) code. Given the varying sources of code and limited visibility into their risk, it's easy for code quality to drop. Where code is messy and complex, it's easier for hackers to find vulnerabilities, execute attacks and hide their tracks.

Zimperium helps organizations address code quality and mitigate exploits with several solutions, Zimperium zScan can help developers identify risks in their app binaries. zScan's static and dynamic analysis identifies the specific risks an attacker could exploit, including in first-party code, third-party built applications, and any third-party components. With zScan, teams can identify privacy, security, and compliance risks before apps are released to the public. Zimperium's zShield offers advanced obfuscation and anti-tampering capabilities that enable teams to harden and protect apps at all times. With zKeyBox, teams can establish strong security around cryptographic keys, without being saddled by the challenges of internally sourced or hardware-based protection approaches. zKeyBox ensures keys are obscured, concealed, and never shown in plaintext, even if an attacker gains control of the execution environment.

Anti-Tampering and Anti-Reverse Engineering

Today, it is easy for malicious actors to download a mobile app from an app store, reverse engineer it, find exploitable errors and vulnerabilities, and perform malicious activities, including code injection, piracy, and more. For example, criminals can reconfigure and repackage an app to use in a phishing campaign designed to steal a victim's credentials.

To counter the threats of code compromise, teams must employ mobile app obfuscation, which makes it difficult and time-consuming for potential attackers to determine how the code works. Teams also need to establish robust app shielding capabilities so that, if an attacker bypasses the obfuscation techniques employed, they can't tamper with or bypass business logic to gain access to sensitive data or start to modify the code.

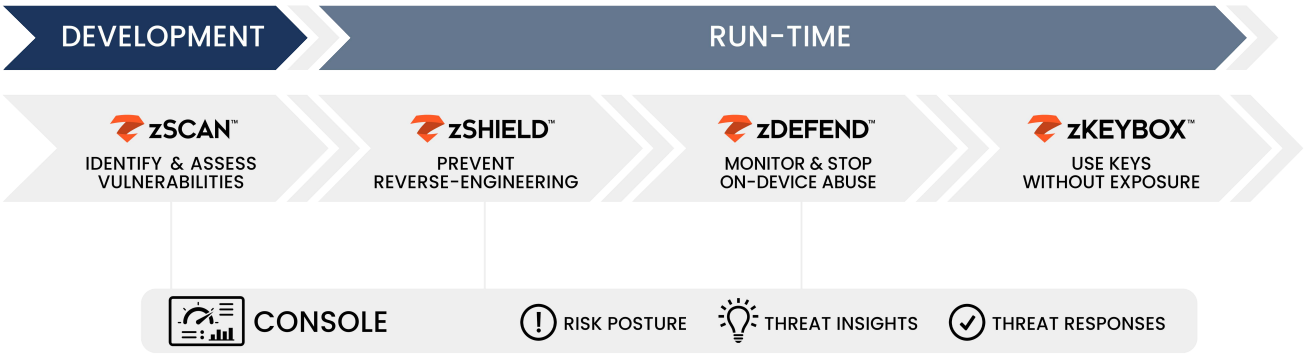
With zShield, teams can harden and protect their apps. The solution offers advanced code obfuscation and anti-tampering functionality. With these capabilities, zShield can protect the source code, intellectual property, and data within the application.

On top of zShield, once the advanced code obfuscation forces the attacker to move from static analysis to dynamic analysis, you'll want to have zDefend embedded into the app. zDefend not only provides real-time telemetry of the risks affecting your app, it also provides advanced machine learning-based detection of the threats affecting the device and its environment. zDefend does not rely on signatures and can detect root/jailbreak evasion and bypass tools, malware and trojans, active tampering, such as ssl pinning bypass, and app hooking. Furthermore, zDefend's detection logic can be updated over the air without the need to re-publish your app, which provides continuous protection against emerging attacks.

Why Zimperium MAPS

Zimperium's Mobile Application Protection Suite (MAPS) helps enterprises build safe and secure mobile apps resistant to attacks. It is the only unified solution that combines comprehensive app protection with centralized threat visibility.

MAPS comprises four capabilities, each of which address a specific enterprise need as shown below.



Solutions	Value Proposition
zSCAN™	Helps organizations continuously discover and fix compliance, privacy, and security issues prior to being published.
zSHIELD™	Protects the source code, intellectual property (IP), and data from potential attacks like reverse engineering and code tampering.
zDEFEND™	Provides threat visibility and on-device ML-based run-time protection against device, network, phishing, and malware attacks.
zKEYBOX™	Protect your keys so they cannot be discovered, extracted, or manipulated.