State of Mobile App Security

2023

ZIMPERIUM®

Mobile apps have rapidly transformed in recent years thanks to technological advancements and changing user preferences. With improved internet speeds and the global demand for instant access to data and services, mobile apps have become a dominant form of digital interaction in our work and personal lives.

As the leader in mobile security, Zimperium has unique insights into the trends and evolution of mobile app threats and protection. This State of Mobile App Security report discusses the following:

- **Key Trends:** What you must protect against
- **AppSec Standards:** Most critical violations
- **Cloud Storage:** Mistakes leading to breaches
- **Best Practices:** Prepare today for tomorrow's needs

Key Trends in Mobile App Security Threats:

Today's apps are multifunctional, combining communication, collaboration, and commerce. The fragmentation of mobile devices, cloud computing, and third-party components and services have changed how apps store, transmit, and process data. As a result, sensitive information is at risk thanks to the expansion of the attack surface and the rapid evolution of threats. Here are some key trends in the current evolution of mobile application security threats: Sophisticated Malware: Malicious apps targeting mobile devices have become increasingly sophisticated. Attackers use techniques like obfuscation, code injection, and encryption to hide malware within mobile apps. Advanced malware can bypass security measures, steal sensitive information, hijack devices, or gain unauthorized access to resources.

- **Application Vulnerabilities:** Vulnerabilities in mobile apps are a significant security concern. Attackers exploit coding errors, insecure data storage, weak authentication mechanisms, and inadequate encryption, to name a few, in order to gain unauthorized access or manipulate the app's functionality. Code scanners focus on syntax and semantics, which is a good start, but you need a mobile-focused security scanner that helps identify areas of abuse and exploitation.
- **Mobile Device Exploitation:** Mobile devices themselves can be vulnerable to security threats. Attackers may exploit device vulnerabilities, operating system weaknesses, or unpatched software to gain control over a device. This can lead to unauthorized access to data, device tampering, or the installation of malicious apps.
- **Poor Cloud Storage Configurations:** Improper cloud storage configurations in mobile apps can make them insecure. Inadequate access controls, misconfigured security settings, lack of data encryption, insecure data transfer, mismanagement of security credentials, and the failure to monitor and detect anomalies are some of the key issues. 14%Fake Mobile Apps: Fake mobile apps are a real problem that can lead to malware distribution, financial fraud, data theft, brand impersonation, user safety risks, and challenges for app store ecosystems.
- **Third-Party App Stores:** Third-party app stores pose risks to mobile app security due to their lack of stringent security screening, increased likelihood of hosting malicious or counterfeit apps, limited app review and monitoring, slower security updates, and a lack of user awareness.

42%

of mobile apps using cloud storage were vulnerable due to unsecured configurations

How Are Industry Standards and Regulations Adapting?

Regulation is evolving to adapt to the growing presence and impact of mobile apps. Here are some ways in which regulation is changing to address mobile apps:

Privacy and Data Protection: With the increasing collection and processing of personal data by mobile apps, regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States have been enacted to protect user privacy. These regulations impose requirements on how personal data is collected, used, stored, and shared by mobile apps, as well as mandate transparency and user consent.

Mobile Payment Regulations: As mobile apps increasingly facilitate financial transactions and digital payments, regulatory bodies have developed frameworks specific to mobile payments. Standards like Mobile Payments on COTS (MPoC) aim to ensure the security, integrity, and transparency of mobile payment systems, protect consumer interests, and combat fraud and money laundering.

Government Directives: Governments and regulatory bodies are emphasizing the security of mobile apps to protect users and mitigate risks. Cybersecurity measures, such as secure data storage, encryption, authentication mechanisms, and vulnerability management, will soon become mandates under directives such as the NIS2 and the FDA's Consolidated Appropriations Act, 2023 (Omnibus).

Industry Standards: The National Institute of Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP) play a crucial role in improving mobile app security. In order to enhance the security of mobile apps, NIST provides guidelines, standards, and best practices. The Mobile Top 10 and Mobile Application Security Verification Standard (MASVS) published by OWASP help mobile application developers build secure mobile apps. The OWASP compliance of mobile apps will be discussed in more detail in a later chapter.

The risks associated with mobile apps can be attributed to three key actors: developers, malicious actors, and end-users. Each of these stakeholders play a significant role in determining the susceptibility of an application to abuse and exploitation. To effectively secure mobile apps, businesses must prioritize security measures amid the development process, during publication to app stores, and while the app is in use on end-user devices. By addressing security concerns at each stage, organizations can mitigate risks and protect their apps from potential vulnerabilities and threats.

OWASP Mobile Top 10 and MASVS Standards: What They Say, How they Can Help Developers Create Secure Apps

OWASP Helps Mobile App Developers

Overall, industry standards provide a valuable set of best practices and guidelines that help mobile app developers create high-quality, reliable, and secure software products that meet the needs of their target audience. Mobile app developers rely on industry standards for several reasons:

- Adhering to industry standards ensures interoperability, compatibility, and quality of software products across different platforms and devices.
- Industry standards provide a common framework that reduces the need for developers to create custom solutions, saving them time and effort.
- Following industry standards helps developers stay competitive by keeping up with the latest trends, technologies, and customer expectations.
- Industry standards also help ensure the security and privacy of mobile apps and their users by providing best practices for data protection, encryption, and authentication.
- Some industry standards are also required for specific market verticals.

Specifically, the OWASP Mobile Top 10 and MASVS help mobile application developers build secure mobile apps.

After explaining the intent and importance of each standard, the following section will show how a set of financial services, medical, and retail mobile apps fared in testing against both of them.

Key Takeaways

Here are the key takeaways from Zimperium's analysis of the OWASP and MASVS standards within health, financial, and retail apps as reviewed in the last year:

- The OWASP Mobile Top 10 and Mobile Application Security Verification Standard (MASVS) help mobile application developers build secure mobile apps.
- There are more standards violations on Android than there are on iOS.
- While violations are heavily skewed toward security risks on both platforms, it is even more pronounced on iOS.
- There are more high-severity OWASP violations on iOS than on Android.

How Does OWASP Mobile Top 10 Help?

OWASP Mobile Top 10 is a list of the top 10 security risks associated with mobile apps. The purpose of this list is to provide guidance to mobile application developers, security professionals, and end-users on the most common vulnerabilities and threats that exist in mobile apps.

By following the recommendations outlined in the OWASP Mobile Top 10, developers can create more secure mobile apps that protect sensitive user information and prevent malicious attacks. Similarly, organizations can use the list to evaluate the security of mobile apps they use or plan to deploy, and end-users can use the list to make informed decisions about the mobile apps they download and use on their devices.

How Does MASVS Help?

The OWASP MASVS is the industry standard for mobile application security. It provides a comprehensive set of security controls that can be used to assess the security of mobile apps across various platforms (e.g., Android, iOS) and deployment scenarios (e.g., consumer, enterprise). The standard covers the key components of the mobile app attack surface, including storage, cryptography, authentication and authorization, network communication, interaction with the mobile platform, code quality, and resilience against reverse engineering and tampering.

But Are Apps Really Compliant with OWASP?

To demonstrate the value of the OWASP standards, the Zimperium zLabs team analyzed the iOS and Android versions of the top 100 apps across three critical verticals. For brevity and clarity, the OWASP Top 10 is being used to demonstrate how the apps fared against the standard. The MSVS findings were in sync with this data. Only the "average number of OWASP & MSVS risks identified per app ("violations") includes the MASVS findings. Findings are as follows:

Financial Services

	iOS	Android
Average OWASP Privacy related findings %	9	10
Average OWASP Security related findings %	91	86
Average OWASP % of findings with high severity	32	8

	iOS	Android
Top OWASP & MSVS Risk Areas	Cryptography Binary Protections Network KeyChain	Cryptography Binary Protections Network Vulnerability File System Database

Medical Industry

	iOS	Android
Average OWASP Privacy related findings %	7	10
Average OWASP Security related findings %	93	85
Average OWASP % of findings with high severity	20	4

Top OWASP & MSVS Risk Areas	iOS	Android
	Cryptography Binary Protections Network KeyChain Telephony	Cryptography Binary Protections Network Vulnerability File System Database

Retail Industry

	iOS	Android
Average OWASP Privacy related findings %	15	9
Average OWASP Security related findings %	85	85
Average OWASP % of findings with high severity	13	5

Top OWASP & MSVS Risk Areas	iOS	Android
	Cryptography Binary Protections Network KeyChain Telephony	Cryptography Binary Protections Network Vulnerability File System Database

In summary, the data shows:

- There are more standards violations on Android than there are on iOS.
- While violations are heavily skewed toward security risks on both platforms, it is even more pronounced on iOS.
- Perhaps not surprisingly, retail apps had a higher percentage of privacy-related violations than the other industries.
- There are consistently more high-severity violations on iOS than on Android.
- Medical apps have noticeably more high severity findings on iOS than the other industries. The financial services industry has the same distinction on Android.
- The top risks identified include insufficient or insecure practices around cryptography, binary protection, network communications, and data storage.

This analysis clearly demonstrates the importance of evaluating mobile apps against standards like OWASP and MASVS. Zimperium highly recommends developers build this into their development process.

Top OWASP Risk Areas

1 Cryptography Requirements

These findings indicate the mobile app's cryptographic mechanisms were not **designed or implemented securely**. As a result, sensitive data and communications may not be well protected from unauthorized access or modification.

2 Resilience Requirements

The findings indicate a lack of binary protections that may expose the application and its owner to various technical and business risks if the underlying application is insecure or exposes sensitive intellectual property. Without binary protection, an adversary can quickly analyze, reverse-engineer, and modify a mobile app.

3 Network Communication & Requirements

These findings indicate that mobile app developers **have not built secure network communication** into their apps. Therefore, sensitive user data may not be adequately protected from network-based attacks.

4 Data Storage & Privacy Requirements

Data storage and privacy requirements in mobile apps are important for protecting user data from unauthorized access or misuse. These findings indicate violations that can result in serious implications, such as data breaches, compliance violations, loss of user trust, and negative media attention. Therefore, it's important for app developers to follow these requirements to protect user data and avoid legal and reputational damages.

Mobile Apps and Insecure Cloud Storage: A Dangerous Mix

Key Takeaways

Here are the key takeaways associated with unsecured cloud storage:

- **2%** of all iOS and **10%** of all Android mobile apps accessed insecure cloud instances.
- **30%** of the inspected unsecured cloud storage instances expose potentially sensitive information, such as passwords, encryption keys, and personally identifiable information.

We use mobile apps. A lot of mobile apps. During 2022, mobile device users downloaded 255 billion apps.[1] In addition, the digital transformation driving enterprise cloud usage continues to create explosive growth. Between 2015 and 2022, the percentage of corporate data stored in the cloud doubled, moving from 30% to 60%.[2]

There are three primary types of cloud storage in use. These include object storage, file storage, and block storage. File storage is the best choice for organizing data in a hierarchical folder and file format. Object storage is designed to handle unstructured data, while block storage stores data in the form of blocks, making it an efficient choice for enterprise applications that utilize databases.

As an example, Google Cloud is a general-purpose cloud storage service that can be used to store any type of data. On the other hand, Google Firebase is a cloud storage service that is specifically designed for mobile and web applications, providing features such as real-time data synchronization, offline access, and user authentication.

All of this cloud infrastructure is highly attractive for mobile app developers. As organizations increasingly rely on cloud environments, mobile app developers are following suit by leveraging cloud infrastructure to the greatest extent practical. One way developers accomplish this is by utilizing cloud-based storage. This approach offers several advantages, but also exposes potential security risks.

The team at Zimperium does extensive research into the apps that are being downloaded from the major app stores. In fact, the team has analyzed thousands of mobile apps over the course of 2022. As part of the extensive investigation and monitoring of these apps, Zimperium analyzes the cloud storage instances that these apps access. The team then specifically looks at which instances have read permissions without requiring any authentication. Across the entire database of inventoried mobile apps, 2% of all iOS and 10% of all Android mobile apps accessed insecure cloud instances.

1 Statista, "Mobile app usage - Statistics & Facts," L. Ceci, Nov 17, 2022, URL: https://www.statista.com/topics/1002/mobile-app-usage/#topicOverview
2 Statista, "Cloud storage of corporate data in organizations worldwide 2015-2022," Lionel Sujay Vailshery, Mar 28, 2022, URL: https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

Here's a breakdown of the type of cloud storage instances being accessed that don't require authentication to access:

- **40%** are Google Firebase instances
- **25%** are Google Cloud Platform instances
- **23%** are Amazon S3 instances
- **11%** are Microsoft Azure Cloud Storage instances

It is important to note that this problem is not the fault of the cloud providers. Google, Microsoft, and AWS all offer options for employing authentication on their storage instances. In fact, AWS has even made authentication part of the default configuration for S3 instances. The problem is that development teams aren't configuring their cloud instances properly to leverage these protections.

A Small Number of Insecure Instances Present a Big Threat

Out of all the apps accessing unprotected cloud storage instances, 60% are accessing a very small percentage of instances, roughly 1%. The research team suspects that this small percentage of unprotected instances is offered by service providers or featured within specific software development kits (SDKs). This underscores how even a small number of unprotected instances or improperly configured apps can introduce a lot of exposure.

The Threat: Approximately 30% of Insecure Instances Expose Sensitive Data

For legal reasons, Zimperium doesn't inspect the contents of exposed Google Firebase instances, so the research team has no way of knowing how many of those instances may expose sensitive data. Of the remaining insecure cloud storage instances inspected, the team found roughly 30% expose potentially sensitive information, such as passwords, encryption keys, and personally identifiable information.

Too often, developers are unaware of the risk posed by these unprotected storage instances.

Consequently, any time these exposed cloud instances are deployed, there's always the risk of developers unwittingly starting to use them to store sensitive assets. Put another way, just because 70% of instances don't hold sensitive data today, doesn't mean they won't tomorrow.

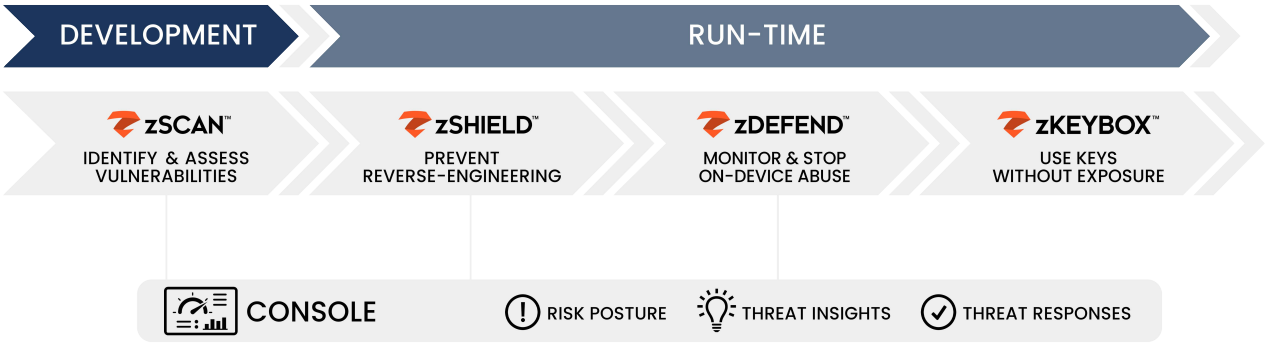
Cybersecurity in software development is not always about a lack of awareness. Developers often give priority to releasing their products, placing security as a secondary concern, or not considering it at all. As a result, if the development team fails to evaluate and address the risk of overlooking security, both the organization and the application's users may be exposed to vulnerabilities, potentially leading to a breach that could go undetected until the damage is already done.

Tackling Mobile Threats & Preparing for Future Risks

Although traditional mobile app security practices and solutions have made significant progress in protecting apps, they have been unable to keep up with the evolving threat landscape. A majority of solutions are built for web and retrofitted for mobile, are free or open source with little support, and provide little to no visibility and protection once they are published. In the face of increasing speed to market pressures, enterprises and mobile-powered businesses find it difficult to adopt practical mobile app security solutions.

Zimperium provides an alternative approach with a single, integrated platform that provides protection from mobile app development through runtime.

Zimperium's Mobile Application Protection Suite (MAPS) helps enterprises build safe and secure mobile apps resistant to attacks. It is the only unified platform that combines comprehensive in-app protection with centralized threat visibility. The platform provides app shielding, key protection, app scanning, and runtime protection capabilities. In addition, a threat management dashboard provides real-time threat visibility and the ability to respond to emerging threats instantly without an app update. MAPS consists of four products:



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.

To learn more about how Zimperium can protect your organization and customers from mobile app threats, contact us for a demo.

About Zimperium

Zimperium enables companies to realize the full potential of mobile-powered business by activating a Mobile-First Security Strategy. Built for the demands of mobile business, Zimperium's Mobile-First Security Platform ™ delivers unmatched security across both applications and devices. Only Zimperium delivers autonomous mobile security that dynamically adapts to changing environments so companies can capitalize on the new world of mobile-powered opportunities, securely. For more information, visit

www.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