Security Status in m-Commerce

a white paper by

APP SOLID.

and

appknox

Foreword

Smartphones, social media, the Internet have started playing a more significant role in our lives today. Businesses have seen this as a vital opportunity to connect with their customers and also widen their reach. Thanks to numerous such services, people have become increasingly dependent on connected devices for entertainment, communication, financial transactions, government services, education and more.

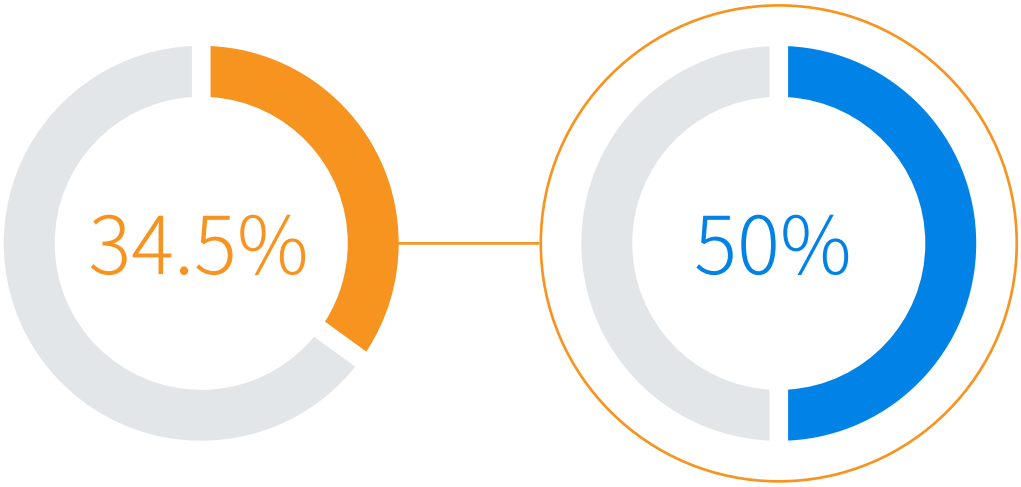
With the rapid growth of connected devices around the world, there has been tremendous exposure concerning attacks. These days hackers have become much more resourceful, and the extent of damage is way more than what can be easily imagined. Businesses of all shapes and sizes have been targets of hackers. The sad truth is that many companies do not realize when they have been hacked while many others believe they would never be attacks. This has led to a trend that encourages a reactive approach towards security.

This report takes an in-depth look at the top 50 best mobile apps in the shopping category of the app stores in the US and helps determine where they stand regarding security. The idea is to generate awareness that many popular mobile apps built are similarly plagued by security issues and vulnerabilities. We chose the shopping category because this is one of the categories with the most downloaded apps which also involve numerous financial transactions on a daily basis.

Both businesses and consumers, need to be proactive to help reach a situation where at least a necessary sanitary check is performed concerning security before launching any of these apps on the app stores. The challenges in information security have always been difficult as well as interesting. It is essential to look at it with the right perspective and try and be as proactive
as possible.

This report is an attempt to encourage a step in that direction.

As the technology gets smarter, the rapid growth of mobile commerce (m-Commerce) will continue to take over the traditional shopping experience. With this change, there are now numerous apps enabling convenient mobile shopping at your fingertips. According to **Statista, m-Commerce took 34.5%** of the total US e-Commerce sales in 2017, and its **market share is expected to be over 50%** by 2021. There is no doubt that shopping on mobile apps will become more of a common consumer behavior as time goes on.

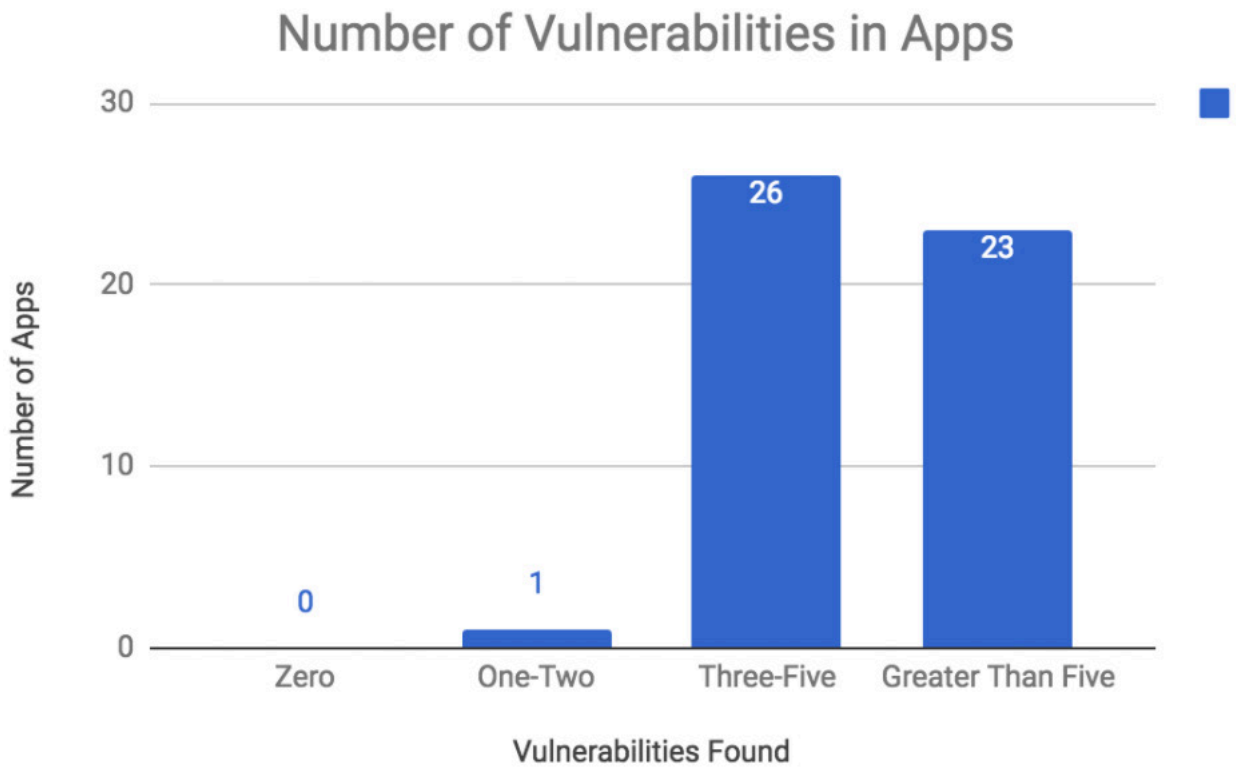


Despite the increasing number of transactions on m-Commerce, are those apps truly safe and secure? Seeing as e-Commerce has already seen **multiple security breaches** — is m-Commerce prepared for cyber attacks?

To understand the security status of mobile commerce, AppSolid and AppKnox teamed up to analyze the top 50 shopping apps on Google Play to understand the current security status in the m-Commerce landscape.

How Secure Are m-Commerce Apps?

Among the 50 apps we analyzed, there is no app that does not have security risks. In fact, 49 apps have at least three or more security vulnerabilities. Moreover, 28% of the apps have critical security issues, and 84% have three or more high level issues. Given the popularity of the apps, the results are concerning.



The 50 apps on the shopping category are measured by 34 different mobile app security categories. There are four particular security risks that many of the m-Commerce apps face in this analysis.

App Testing Methodology

Our systems use the Common Vulnerability Scoring System (CVSSv3.0) to rate vulnerabilities. CVSS is the industry standard for assessing the severity of computer system security vulnerabilities. CVSS assigns severity scores that allow you to prioritize responses and resources according to the threat.

Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of an exploit. Scores range from 0 to 10, with 10 being the most severe.

The metrics that are evaluated are as follows:

1. Attack Vector: Reflects the context by which vulnerability exploitation is possible. The value will be larger the more remotely the component can be exploited.
2. Attack Complexity: Describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.
3. Privileges Required: Describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.
4. User Interaction: Captures the requirement for a user, other than the attacker, to participate in the successful compromise of the vulnerable component.
5. Scope: States whether the vulnerability in one software component impacts resources beyond its means or privileges.
6. Confidentiality Impact: Measures impact on the confidentiality of the information resources managed by the component due to a successfully exploited vulnerability.
7. Integrity Impact: Measures impact to the integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
8. Availability Impact: Measures impact on the availability of successfully exploited vulnerability. This refers to the loss of availability of the impacted component itself.

Common Security Vulnerabilities in m-Commerce

94% of apps were affected with Unprotected Export Receivers

1. Unprotected Export Receivers

Imagine you wanted to wire money to your friend for dinner, but an unknown stranger receives your money instead? Or, you purchased a new pair of jeans with a mobile payment system, and start experiencing a small amount of money keeps leaking from your bank account for unidentified merchants? This is possible when Export Receivers are not protected properly.

Android apps export receivers, which respond to external broadcast announcements and communicate with other apps. For instance, when Receivers are not protected — hackers can modify apps' behavior as they wish, and insert data that doesn't belong to apps.

64% of apps were affected with App Extending WebViewClient

2. App Extending WebViewClient

If you have ever had the feeling that the mobile web browser you are using isn't quite right, but you cannot place it. It may be an insecure hacked Web Viewer.

When WebViewClients are not correctly protected in-app extensions — hackers can trick users into inputting sensitive personal information in fake or copied apps, resulting in loss of user data, damages and SSL compromising.

When an SSL communication channel is compromised, hackers can gain access to a web server, which often stores classified information. It is common for many developers to save more confidential and sensitive data on web servers rather than apps. Since most apps continuously communicate with web servers, leaving WebViewClient unsecured means exposing web servers to external threats as well.

94% of apps were affected with Unused Permissions

3. Unused Permissions

Apps need permissions from users to provide optimized services. Often one app needs multiple permissions for multifunctional purposes to increase user experiences. But, with too many permissions, it can decrease user satisfaction as well as protection. For example, a shopping app asks for permissions to access your device's camera, contacts and music? That is unneeded and dangerous to app security.

However, it is essential to think about what permissions are actually necessary. Asking for too many permissions that are not used for app operations can put users at risk. When enough security measures are not applied to apps, hackers can manipulate unused permissions to get to sensitive information. Adding security starts with minimizing ways of compromising data and user information.

70% of apps were affected with Unprotected Exported Activities

4. Unprotected Exported Activities

Hackers can use unprotected exported activities to copied or jailbroken apps and intercept and track users activities and data for other hacking attacks. That is why, on a daily basis, there are millions of copycat apps stealing user information like — usernames, password and personal information and more.

Activities are executed via authorized access. When an Activity is exported with no protection, it can be remotely launched outside of apps. This may allow hackers to gain access to sensitive information, modify the internal structure of the applications, or deceive a user into communicating with the attacked application while believing they are still interacting with the original application.

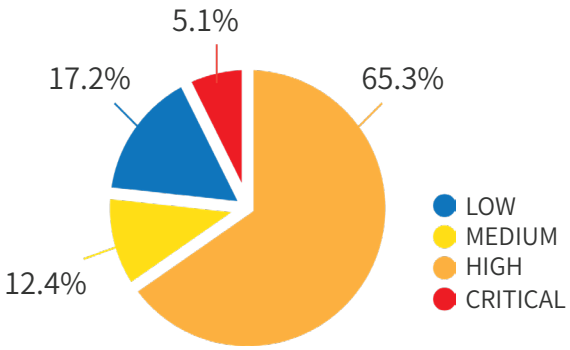
274 was the total number of vulnerabilities detected

5. Additional Findings

28% with scores of 9 or higher

84% with scores of 7 or higher

Vulnerabilities by Severity



How to Add Security Measures on m-Commerce

It is frightening to find out how widespread app security vulnerabilities are in mobile commerce. As it is directly related to sensitive information, such as credit card data, it is crucial for m-Commerce apps to add a sufficient amount of security.

Learning about security vulnerabilities is one thing, but many app developers still hesitate to add proper security measures. This is because a lot of them don’t have enough security expertise. To protect themselves from potential hacking attacks, app developers can utilize app security services, such as AppSolid and AppKnox.

Basic Measures to Secure Your Mobile App

Mobile application security can be a vast minefield. Here are few basic security measures that can be taken to help secure your business:

#1. Stay compliant with industry standards:

Ensuring your mobile app is compliant with industry standards for mobile security will help you keep secure from the latest threats and vulnerabilities. It also acts as a document to show that you have taken precautionary measures in the right direction to help secure both you and your customers. Because the mobile app threat landscape is unpredictable, at the time of a data breach, should there be any, penalties and fines imposed by the government are a little more relaxed than they would usually be. One such compliance document is The OWASP Top Ten. The OWASP Top Ten is one of the most popular and influential awareness document for web and mobile application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. OWASP keeps updating itself overtime to ensure that it covers the latest threats and vulnerabilities as well as best practices to help businesses stay on top of the security curve. PCI-DSS is also another compliance mandate for banks with cards and is administered by the Payment Card Industry Security Standards Council.

#2. Incorporate security into your development lifecycle:

They say prevention is better than cure. In the case of mobile app security, by incorporating security practices into your development lifecycle, you're not only being prepared for the inevitable but also reducing your costs drastically as compared to what you would otherwise be paying to neutralize threats that may occur at a later stage. Yes, even during development, there is a need for security experts to ensure that there are no loopholes in your app. However, there are a few great mobile app security testing tools out there that have continuous integration technology which

lets you test your app any number of times during development. This is to ensure that end-to-end basic security testing is covered before launching onto App stores.

#3. Use automated mobile app security testing:

The mobile app security landscape changes very frequently. New threats arise each day. When there are new parameters of security put up, there is always someone looking for a way around them. Due to the constantly evolving nature of threats, it is essential that routine testing cycles be carried out to ensure your app's security is up to date with the latest threats. Using an automated system helps eliminate the need for manual eorts and additional resources that could prove to be time consuming and expensive. Apart from being great at helping you get routine assessments done with lesser eorts, automated mobile app security testing also has the added perk of helping you beat the competition with faster time to market.

#4. Get regular manual assessments done:

Although automation helps reduce the eorts for security testing substantially, nothing beats the human mind. Manual application security testing helps attain a deeper level of testing for your app that can only be bypassed by human intelligence. Combine manual assessments with an automated evaluation to get maximum security coverage for your mobile banking apps. With that being said, it is essential to receive manual testing done only by security researchers who have vast experience with testing mobile applications. There are many components of mobile app testing which are similar to web testing but there are also a lot of other components that are entirely different and need dedicated mobile app security expertise.

#5. Strategize with mobile app security experts:

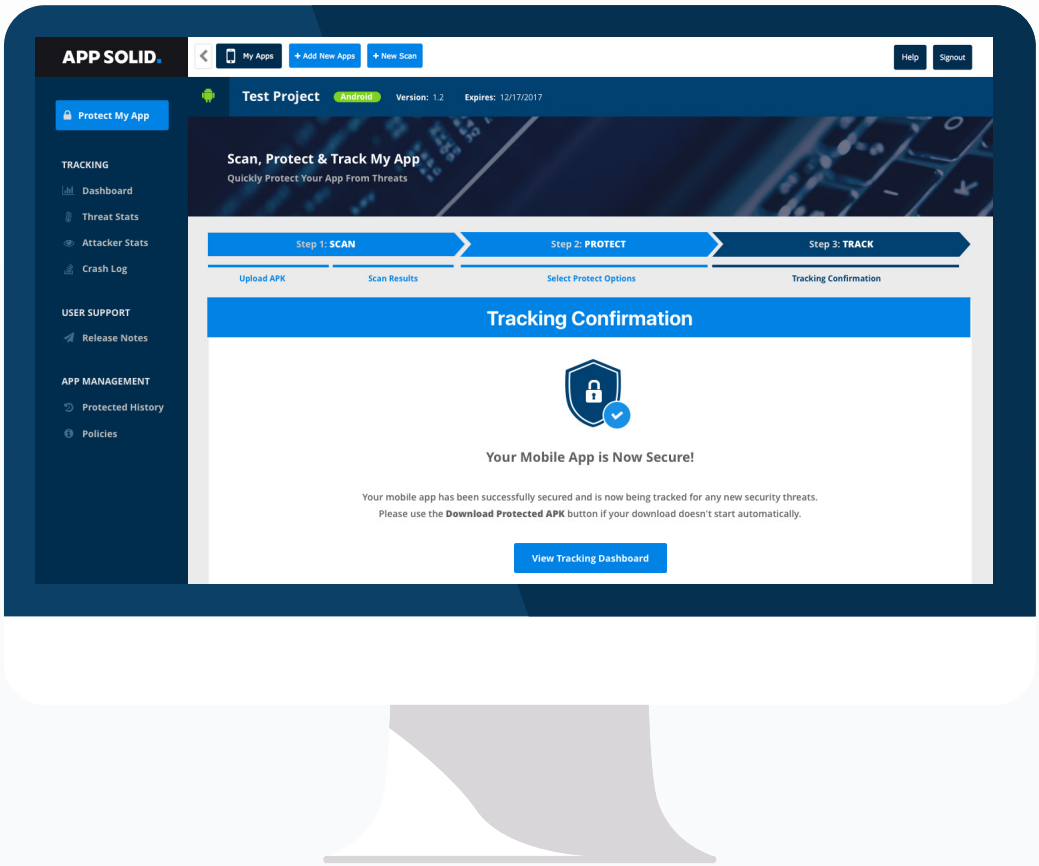
Mobile app security is a very niche space. There may be many security experts out there who claim to know all about security. The truth, however, is that cybersecurity, in general, is a vast area of unexplored territory. Ensure you speak with experts specifically in the field of mobile app security testing to ensure that your mobile banking apps are completely secured. Get the mobile app security experts to give you a complete and comprehensive plan for incorporating security into your business strategy. It helps to get a security plan right from development to production and even during maintenance.

Commerce in general is a security-sensitive area with numerous monetary transactions. The advanced mobile technology enables more and easier commerce activities, but this also means bigger security threats. Personal and financial information as well as confidential business details and others can all be targets.

Adding sufficient security measures on mobile commerce apps is not as difficult as a lot of people think when you can utilize solutions like AppSolid and AppKnox. It is too late if you try to fix the damages after hacking attacks. Preventing such possibilities in advance is the the best way to fight against security threats.

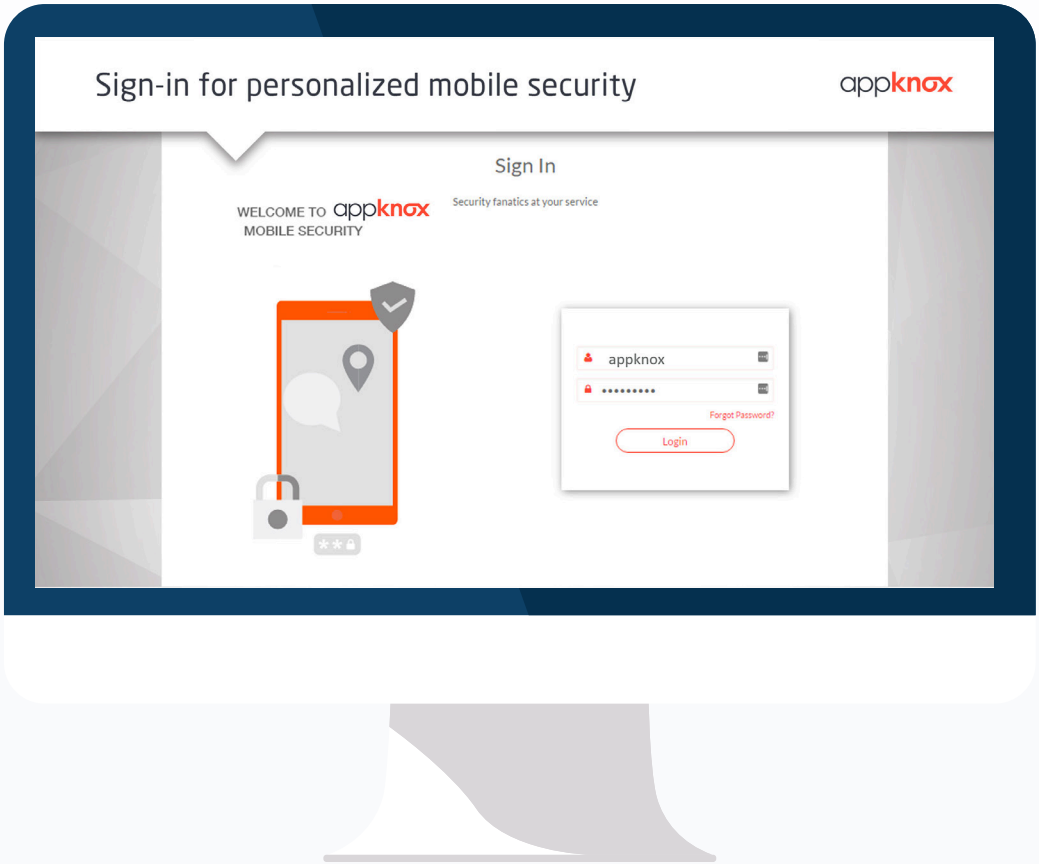
APP SOLID.

AppSolid is a cloud-based mobile app security solution that provides advanced level of security. In addition to various security features like encryption, obfuscation, and Runtime Application Self Protection (RASP), AppSolid also offers scanning for security vulnerabilities and monitoring of real-time security status. It's easy to use as AppSolid is applied after apps are fully compiled. Simply upload a compiled app file, and you'll be able to learn existing security vulnerabilities within seconds. Then, you can add advanced security and download a secured app file. After the app goes live, and you can track the security status in real time on the AppSolid Dashboard. If any suspicious attempts are detected, you can easily terminate them on a device level with a single click of Kill-Switch.



appknox

Appknox is a cloud-based security product that detects threats and vulnerabilities in mobile apps with a detailed reporting document that provides suggestions to fix them. Apart from using state of the art technology for mobile security automation, Appknox also uses industry renowned security researchers to perform manual assessments on apps to ensure total mobile security.



Secure Your App With AppSolid & AppKnox

a white paper by

APP SOLID.

https://appsolid.net

and

appknox

www.appknox.com

help@appsolid.net

info@appknox.com