Security Issues in Mobile Apps

[1] **Priti Jagwani,** [2] **Ranjan Kumar,** [3] **Gagandeep Sharma**

[1,2,3] Dept of Computer Science, Aryabhatta College
University of Delhi, New Delhi 110021, India

Abstract - With more and more people using variety of apps on their smart phones, security provided by these apps is becoming an important research consideration. The key objective of this work is to define and analyze some of the major security issues related to mobile apps. In this paper security concerns in a mobile app are highlighted. Further solutions for the same are suggested. Recent market trends and important findings of various research studies are also discussed.

Keywords - *Mobile App Security, Smart Phone Security.*

1. Introduction

In today's mobile world almost all the people are carrying one or more smart phones with them. The use of mobile computing is increasingly becoming an integral part of the framework of our daily lives. The field of mobile computing is becoming more and more prevalent throughout our daily lives. This can be seen from the increase in the number of smart phone users from 114 million to 250 million in just the one-year period between 2012 and 2013. These smart phones are loaded with various kinds of mobile apps. An app is basically a software programs which one can download and access on mobile device may it be a smart phone or tablet or any other. These apps are easy to download and often free. One can have a very versatile experience with these of playing games; getting navigational directions; and accessing books, weather, music, videos or any other information they want. These mobile applications are quickly replacing the use of web. A number of tasks can be recalled which were only done using desktop or laptop few years ago. All those tasks are possible using one or the other mobile app. They give people the ability to view a restaurant menu, plan a trip, and play a game and even conduct banking transactions from their mobile phones and tablets.

Accessing these apps can be so much easy and convenient that most of the people download them without even thinking about security issues. An app being free on internet actually costs a lot to a user in terms of the information they may gather from the device. Unfortunately, apps are the most common way through which smart phones and the data stored on them are compromised. As people increasingly download these applications and allow access to personal information, ensuring app security is becoming a matter of great urgency. In some cases this information may be misused by a service provider or a third party. Thus establishing mobile app security should be the prime concern of every mobile software developer.

2. Security Concerns

Most people don't care about privacy and security of their data while using an app. A general tendency is if an app is purchased or downloaded from a play store or a company having a good market reputation, nothing will go wrong.
According to a report [1] location is the most common element which is taken or requested by mobile apps. It is used for finding the nearest POI or a route to some place etc, but most of the time is not needed for functionality. Location information is valuable to advertisers, data brokers, and analytics frameworks to gain insight into where the app might be popular, as well as to serve targeted ads." Among other data requested, most common is device id, camera, call log, microphone, SMS and calendar. But the surprising fact is most permission is not for core functionality but for the purpose of collection of user information. To deal with these issues, developers should clearly state what information is being accessed, why the information is being accessed, and to whom the data is being sent[1]. Users are under a notion that developers must have taken care of security issues. But actually this is not the reality. Given below are the some wrong practices adopted by app developers and users which results in potential security threats:

2.1 Relying on the Security Arrangement of the App Platform

Most common practice of users in terms of security of a mobile app is to blindly rely on the security provisions made by platform or appstore itself. But in reality no app development platform is immune to security issues.

Android platform permit all the apps and allow user to choose between secure and non secure ones while apps on the Apple ios platform go through a screening process. Other app platforms also have their own security arrangements which are obviously not flaw less. So completely trusting the security arrangements built in by the app platform itself is not suggestive.

2.2 Security of Stored Data

Many apps store credential details like passwords, username etc in plain texts. This plain text can be seen and accessed by anyone having access to the phone by just connecting it to a PC. Also location information (geotagged information) can be accessed by this. With all these information in hand any unauthorized individual can make a user comprising his/her privacy and security. Its a bad but regular practice of developers to store their secret keys in app itself. These vulnerabilities can affect users even if they are not actively running the any apps.

2.3 Bypassing Security Testing

It's a general trend of app market to release an app without conducting necessary security testing. By this the app developer puts security of all its app users on stack. No app is safe from the attacks of viruses and malware. So all inlets of security breach possibilities should be tested thoroughly before release.

2.4 Using Third Party Codes

Mobile app developers generally use codes developed by other third parties. This gives hackers a chance to first provide the built in code to other developers. After the app gets released that malicious code will access all user data. Before using a third party code, an app developer should scan it properly to avoid any vulnerability towards security.

2.5 Weak or Broken Encryption

There is a need to create their own encryption algorithms by the app companies, as most widely used encryption techniques are not sufficient enough for modern security requirements of a mobile app. If an organization is interested in using already existing modern secure algorithms of cryptography, a detailed analysis, threat modeling and testing of those algorithms should be conducted. With time, encryption algorithms become obsolete and easier to crack. Sensitive user information is at risk if weak encryption has been used. Input to many apps is user's sensitive data, such as credit card numbers or personal identification information. Without good encryption, this information can be hacked. The more popular the app, the more likely it is to be hacked, too. So, good encryption is must for a secure app.

3. Solutions

It is clear from the discussion in the above section that mobile apps are vulnerable for security. For this malicious apps designed to steal a user's data as well as lazy coding tendencies are responsible. Developers write apps that access everything because it's easier than writing more specific code and it also paves the way for any future enhancements that might actually need it. [2]

The better solution is for developers to build security and privacy into the apps from square one. Developers should be aware of the potential implications of how their apps access data and interact with other apps, and design them to be secure by default[2]. So in order to maintain the security of user data, application developers must follow security practices as illustrated below:

3.1 Thinking about Security at Very Early Stages

Most loopholes in the security of an app can be prevented if security is taken care of, right from the early stages. Security risks will definitely rise at later levels of development with a magnificent volume if they are ignored at earlier levels. [4,5] Incorporating security at initial stages will definitely save time, money and effort.

3.2 At the Design Stage

If an app is being designed for a particular company, company's privacy policy is needed to be considered. Further at the design stage, privacy complications of various operating systems must be taken care of for the security compliance of the app. Security issues arising during this phase are the ones that are the most difficult to spot and resolve. The best way to minimize the risk factor here would be to create a list of all the potential traps, well in advance, also planning your course of action to avoid each of them[4]. This is followed by performing a detailed security design review, which is usually handled by a security expert, authorized to carry out this particular check.

3.3 At Development Stage

Development stage is very vital from the point of view of security incorporation in app. There can be various third party tools to find and correct security flaws[5]. But some of these tools may not be able to detect very complicated security vulnerabilities.

3.4 Testing Stage

After development, an app is required to be tested thoroughly, before launching it in the market. Before security testing all the test cases should be ready and their proper analysis should be done. A testing professional can build a systematic road map of testing. At the time of deploying the app, it is advisable for testing team to closely monitor the app to ensure complete security.

For complete security solutions it is necessary to provide developers with mandatory security training[4,5]. By this they will understand and follow the best practices for developing quality apps. In general, app developers should ideally have a grasp on the basic terminology, security processes and the knowledge of implementing appropriate strategies to effectively tackle issues relating to app security.

4. Discussions

With mobile becoming an indispensable part of common man's life; use of various mobile apps is also increasing expeditiously. According to the report [3], ratio of downloading free apps vs paid ones is 1:11. By 2017 revenue from mobile apps are expected to reach $70 billion. Till 2014 Android was dominating mobile market by capturing 85% market. [3] also reveals the figures of security analysis of apps. They showed that most of the apps can be hacked very easily. Figures showed that 80% of free Android apps and 75%of free ios apps have been hacked. Data is showing a darker picture of paid apps. The numbers of paid apps that can be hacked are 97% and 87% for Android and ios. The above study reveals that day by day these figures are getting worsened. Numbers of apps that can be hacked were less in 2012 and 2013 as compared to 2014. Most of the apps which are the target of hackers belong to financial and health care/ medical domain then comes retail sector.

According to a study report by HP, 97% of the apps access aleast one private information stored on the mobile. Most of the applications use weak encryption; also many others don't implement security correctly while sending the user data over the connection. Above studies show that security risks are increasing at an alarming rate. As most of the mobile attacks are not difficult to execute.

5. Conclusion

Mobile has become an indispensable part of today's life. Mobile apps are providing users with convenience on their finger tips but this convenience has come with increased security risks. This article showed that mobile app security is still in its infancy. Many procedures resulting in security threats, also practices to tackle them are highlighted.

References

[1] http://www.scmagazine.com/mobile-app-study-reveals-privacy-concerns/article/371312/

[2] http://www.pcworld.com/article/2068824/study-finds-most-mobile-apps-put-your-security-and-privacy-at-risk.html

[3] https://www.arxan.com/resources/state-of-security-in-the-app-economy/

[4] http://www.kony.com/resources/blog/eight-security-issues-prepare-mobile-app-development

[5] http://www.informationweek.com/mobile/mobile-applications/mobile-app-development-5-worst-security-dangers/d/d-id/1204488

[6] Butler, M., "Android: Changing the Mobile Landscape," Pervasive Computing, IEEE , vol.10, no.1, pp.4,7,Jan.-March2011 doi: 10.1109/MPRV.2011.1

[7] Miller, C., "Mobile Attacks and Defense," Security & Privacy, IEEE , vol.9, no.4, pp.68,70, July-Aug. 2011

[8] http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-1057ENW.pdf