Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1207-1210
© Research India Publications
http://www.ripublication.com

Android Application Security

Rajivkumar Mente and Asha Bagadi

Department of Computer Science, Solapur University, Solapur 413255

rajivmente@rediffmail.com, ashabagadi@gmail.com

Abstract

Smartphone have become the major part of human's life. Nowadays mobile applications are playing major role in many areas such as banking, social networking, financial apps, and entertainment and so on. For every desktop or web application an alternate mobile app is available. With just single click number of mobile apps is available from Google's play market. With this huge number of applications security is an important issue. This research article discusses about the security of the applications and the malicious apps that may affect or leak sensitive data such as International Mobile equipment Identity Number (IMEI) of device, credit or debit card information, location information and so on. As the android market is growing, security risk has increased and thus focus should be given to the security.

1. INTRODUCTION

Android is a mobile phone operating system launched by Google under the license of Apache. Due to the open source nature of android it provides flexibility to user and developer to customize basic functionality provided by android. But as day by day features provided by android has increasing, security challenges have also increased. Android operating system has been developed more secure platform but still vulnerabilities are there.

2. STRUCTURE OF ANDROID OPERATING SYSTEM

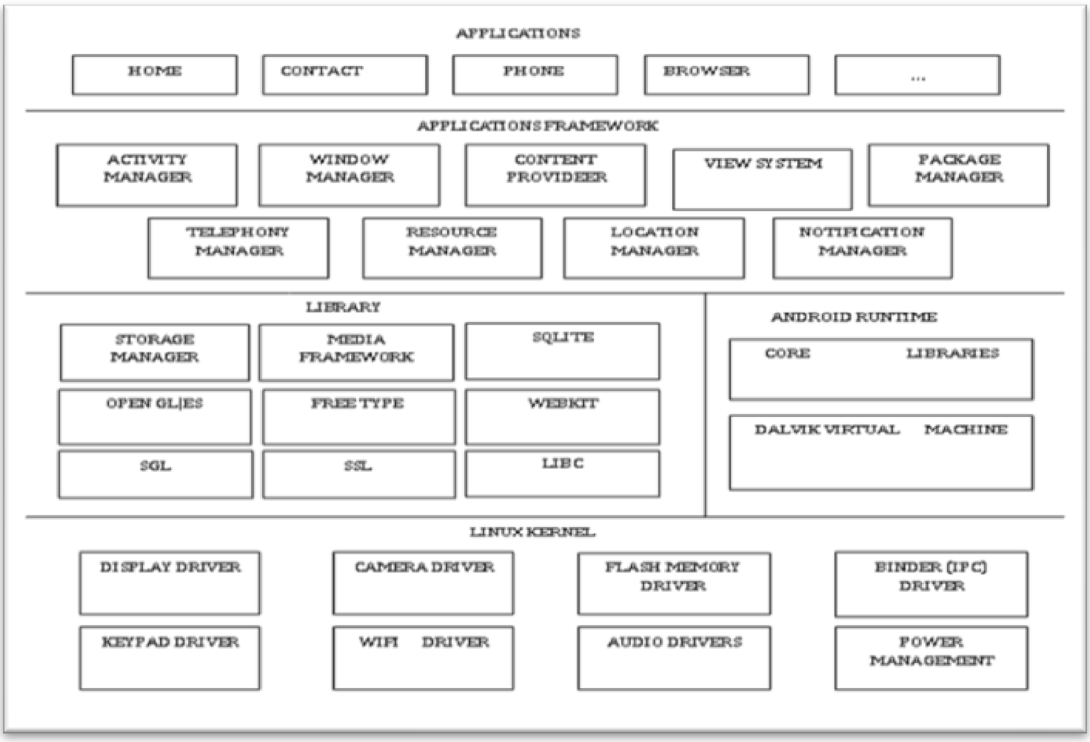

Figure 1. Structure of Android Operating System

Android is a mobile operating system and platforms for mobile application development[1]. As we go through the architecture of android it basically have following four layers

Application layer- It includes all the applications.

1. Application framework layer- This layer provides high level services for application development in the form of Java classes. Application developers are allowed to make use of these classes in their applications. These services include Activity Manager, Location Manager, Content Provider, Notification Manager, Package Manager, View System and so on.
2. Libraries- The Android system provides some C/C++ libraries. Different components of the Android system can utilize these libraries. All these libraries are accessible with the help of the application framework.
3. Android Runtime- It deals with compilation of android app under the Dalvik Virtual Machine (DVM) which produces the optimized code for mobile phones.
4. Linux Kernel- It is the last layer in the android architecture which has direct communication with hardware and which provides basic service like Inter Process Communication (IPC), security and so on.

Linux kernel provides uid for each process, pre-emptive multitasking, etc. Each application has its own uid and it runs in its own virtual machine. In addition to this android also provide permission mechanism and Application and signing mechanism for security purposes.

3. ANDROID SECURITY MODEL

Android has a predefined set of permissions. This permission must be specified by the application in the manifest file of the application it request for. At the time of installation of the application all the permissions are displayed to the user. If user allows all the permission then the application installed successfully otherwise it is rejected completely. But in this case user do not have any choice to approve selected permission. There are near about 134 system defined permissions and developer can also create their own user defined permissions.

Javed Parvez et al proposed an enhanced Android Security Framework (AFS) which applies Advanced Encryption Standards (AES) algorithm to all the files stored in media and if any malicious app that want to modify the file found to be vulnerable then it will restrict access to the file [7]. Malware detection can be done using 3 techniques as

1. Signature Matching
2. Heuristics
3. Hashes

A new security enhancement in the package installer system is proposed by Aparana Bhonde et al in which it is suggested that Android system should be able to identify the malware before the application that is being installed. When an application gets installed Package Manager should be able to detect the vulnerability along with the authenticity of the android application. For this purpose a provision is suggested in android operating system structure[8].

4. REVERSE ENGINEERING

Basically reverse engineering is the process of getting source code from the apk file. Reverse engineering can be done using tools such as apktool, 7zip, dex2jar, jd-gui. Taranjeet et al and William et al found that most of the apps source code was analysed using static and dynamic analysis which shown that apps used to leak data such as current location of the user via email or SMS[2, 3]. From that reverse engineering of apps it was concluded that a strong security testing mechanism is needed for testing the security of the apps [4]. According to Jae-Kyung Park et al most of the apps uses the permission that were even not required by the application and most of the apps uses the permissions for accessing network services and access other sensitive data and is one of the reasons for security problems[5]. Reverse engineering also found many security flaws in the source code of the application.

5. SSL/TLS (SECURED SOCKET LAYER/TRANSPORT LAYER SECURITY)

Most of the android application needs to communicate with the server. For example login process, get data from server. This communication can undergo the Man In The Middle (MITM) attacks and may leak the sensitive data. Even though SSL and its successor TLS are secure attacker can win against them. Sascha Fahl et al have developed a tool MalloDroid that uses static code analysis to detect apps that potential uses SSL/TLS inadequately and incorrectly hence may be vulnerable to MITM attacks[6].

6. CONCLUSIONS

From the above it is concluded that even though android provides good security but still, vulnerabilities and security problems arrive because of security flaws and improper development of the applications. For this reason a proper security mechanism is needed to avoid the security risks and identify the malicious apps for the security of the sensitive data.

REFERENCES

[1] Manvindar Singh Chauhan, Kulvinder Singh, “Security Risk Associated with Android Applications”, Department of CSE, DIET Rishikesh, Uttarakhand, India

[2] Taranjeet Kaur Chawla, Aditi Kajala, 4, April 2014, 1204-1268, “Transfiguring of an Android App Using Reverse Engineering”, International Journal of Computer Science and Mobile Computing Vol. 3 Jssue.

[3] Enck, William et al., 2011, "A Study of Android Application Securit y", USENIX security symposium.

[4] QBRST, July 2014, “Mobile Application Security”, Best Practices to Optimize Security.

[5] Jae-Kyung Park* and Sang-Yong Choi, “Studying Security Weaknesses of Android System”, International Journal of Security and Its Applications, 9(3).

[6] Sascha Fahl, 2015, 7-12, Marian Harbach et al “Why Eye and Mellory Love Android : “An Analysis Of Android SSl (In) Security”.

[7] Javed Parvez , Muneer Ahmad Dar, 8, April 2014, “Ä Novel Stratergy to Enhance the Android Security Framework”. InterNational Journal of Computer Applications (0975-8887) Volume 91-No.

[8] Aparana Bhonde, 9, September 2014, Madhumita Chatterjee “Security Solution for Android Application Assessment” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3 Issue.