I J C T A, 9(13) 2016, pp. 6323-6328
© International Science Press

Risk Information Analysis for Android Applications

Garima Sehgal[*] and R. Kumar[*]

ABSTRACT

The Android platform's popularity makes it attractive, because it offers more control over their devices and the apps they install. Also everyone gets the chance to post an app for download in the Market, without any review of other applications. But because of some malicious applications the users' mobile security is clearly compromised and unknowingly they accept the unwanted permission from the applications. Also the details about the permission they request for, may be a privacy threat to the users. In this paper, we determine risk scores for Android applications in order to generate another criterion that users can utilize when choosing apps. We use different techniques to generate risk scores. We introduce a framework that includes evaluating risk information.

***Keywords*:** Android, Permission, Security, Smart phone, Risk, Malicious.

I. INTRODUCTION

Smart phones are rapidly becoming dominant computing platform. The sudden growth of smart phones has lead to a revival for mobile services. Application markets such as Apple's App Store and Google's Android Market provide access to hundreds of thousands of paid and free applications. Because of the growing number of Smartphone users and the outspread use of permission systems on these platforms, it is important that we gain a better understanding of the design of Smartphone permission systems. Also people have very less technical knowledge of what exactly the permissions are requesting for because of which they install the application without knowing that it can be a malicious application. One of the distinctive and desirable feature of smart phones over traditional phones is that they are capable of running applications written by third party developers. This capability, combined with their highly peculiar nature, has caused privacy and security threats to users. In order to improve the security of mobile systems, we must understand the challenges faced by the users in installing an application in order to improve the security of mobile application. Moreover users make many decisions that affect the overall state of security of any system with which they interact. Android have become popular because it can handle the access to many resources which are sensitive. In the android application an app requests for specific permissions so that it can have access to that application. But before installing any application it requests for the permissions and expects that it will be read carefully before installing the application. Therefore it is significant strand of security to communicate about the risk of an application before it is installed. Thus in this paper, we will be providing the risk information so that best possible decision can be made out of it considering all the security measures using Android application and also warns about the permission an app requires before the it is installed. Providing risk information to user will enable them to choose the application which is less risky to mobile phone. If it is known that this application is much more risky than the other application providing similar functionalities than this will help to choose the less risky application. Also it will help in making the decision about the application way before installing that.

[*] Department of Electronics and Communication, SRM University, Chennai-603203, India, *E-mails: sehgal.garima2@gmail.com; kumar.r@ktr.srmuniv.ac.in*

II. PROPOSED SYSTEM

(A) Block Diagram of the Proposed system

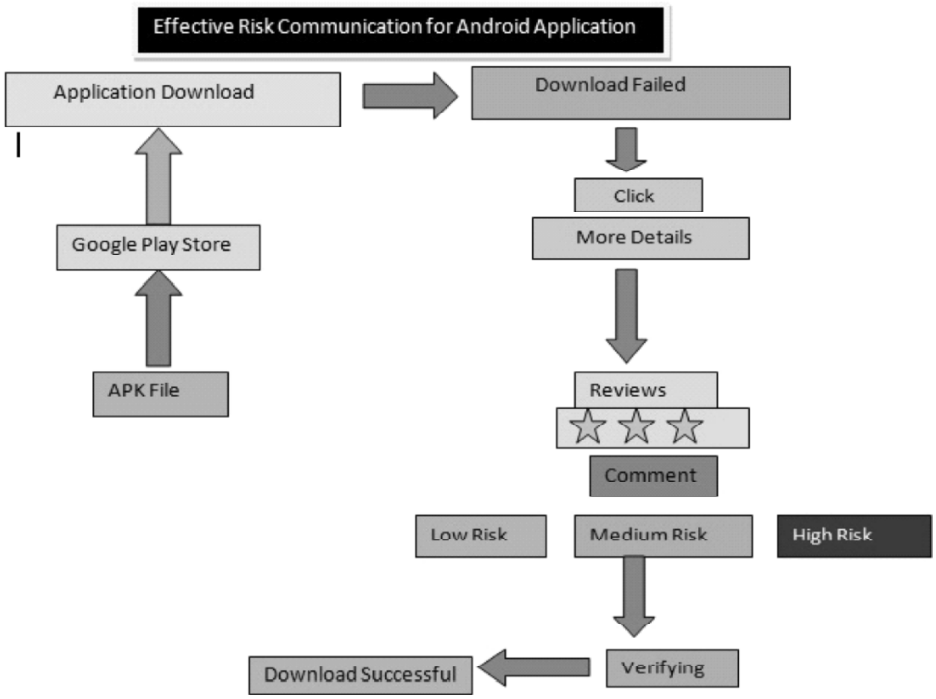

Figure 1: Block diagram of proposed system

In the Fig. 1, the APK file is uploaded to Google Play Store. When the user tries to install any application from play store, the download is failed. So user has to go to more details option where it is provided with many options such as comments, reviews. On verifying all these options user select whether to download any application or not.

(B) Advantages of Proposed System

The attack of malicious applications is reduced in the system. Increase the performance for Android system with maximum accuracy. The usage of these mobile devices poses new privacy and security threats. The mobile devices contain contact lists, email messages, passwords, and access to files which are stored locally and in the cloud. This can be accessed by the unauthorized users causing risk to user. Also these devices have many which can have access to physical lives. The GPS can tell exactly where you are, the microphone can record audio, and the camera can record images. Additionally, mobile devices have link to email messages and also some password are saved which can directly affect your account. There are some applications which require the access to videos and personal images which are private. This access means that any application (or app) that is allowed to run on the devices potentially has the ability to tap into certain aspects of the information. Mobile devices use different parameters to install any application. For computers most of the applications are from known vendors but for mobile devices user can download any application from many unknown vendors, with each application proving same functionality. Hence different approach requires different ways to deal with the risks provided by the applications. And in this system users are provided with the risk information in the form of reviews which can be stars or any other symbol or comments such as low risk, medium risk, high risk, which enables them to take best decision while installing any application even though having no technical knowledge about what the permissions are actually requesting for.

III. IMPLEMENTATION

Android is a Linux based operating system for mobile devices such as smart phones, tablets. Android's User Interface is based on direct manipulation, using touch gestures like swiping, tapping and also virtual keyboard is provided for text input. Android Application Package (APK) is the package file format used by the Android operating system for installation of mobile applications from Google play store. To make an APK file a program for Android is first compiled and then packaged into one file. APK files are type of archive files, especially in zip format packages with .apk as file extension name. When you download any application from Google play store it means you are installing an APK file on your device. You can also install an APK file directly to the device from a desktop computer using a communication program such as Android Software Development which is a process by which new applications are created for the Android Operating System. But by default ability to install any application directly from desktop is blocked because of the security reasons.

(A) XAMPP Software

XAMPP is free and open source cross platform web server developed by Apache friends consisting of Apache HTTP server, MySQL database. XAMPP stands for Cross-Platform (X), Apache (A), MySQL (M), PHP(P), Perl(P). It is used for developing local web servers for testing purposes. It is versatile as it work compatibly with Linux, Mac, Windows. XAMPP is basically designed to allow the website designers and programmers to test their work without having any access to internet. It can also serve web pages on World Wide Web. Once XAMPP is installed it becomes easy to use Localhost as Remote host by connecting it to FTP client.

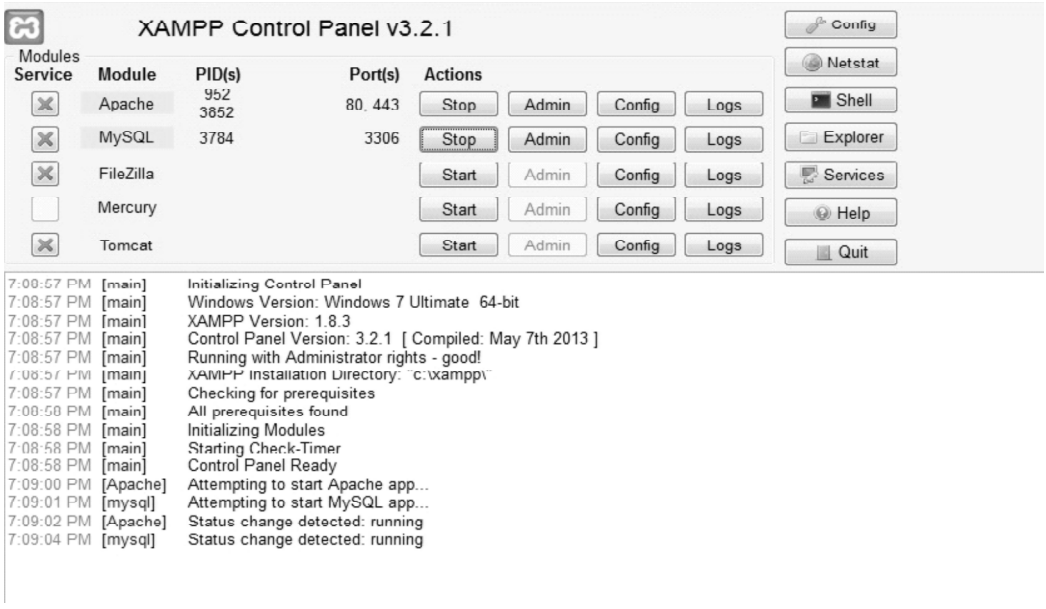

Figure 2: XAMPP Software

(B) phpMyAdmin

phpMyAdmin is free open source tool which is written in PHP to administer MySQL with the use of web browser. It performs various tasks like creating modifying or deleting databases, tables, fields or rows and also manages permissions. Localhost is a host name. It is used to access the network services that are running on the host with the help of loopback network interfaces. Local loopback is used for testing software during development. It helps in administering multiple servers and creating PDF graphics of database layout.

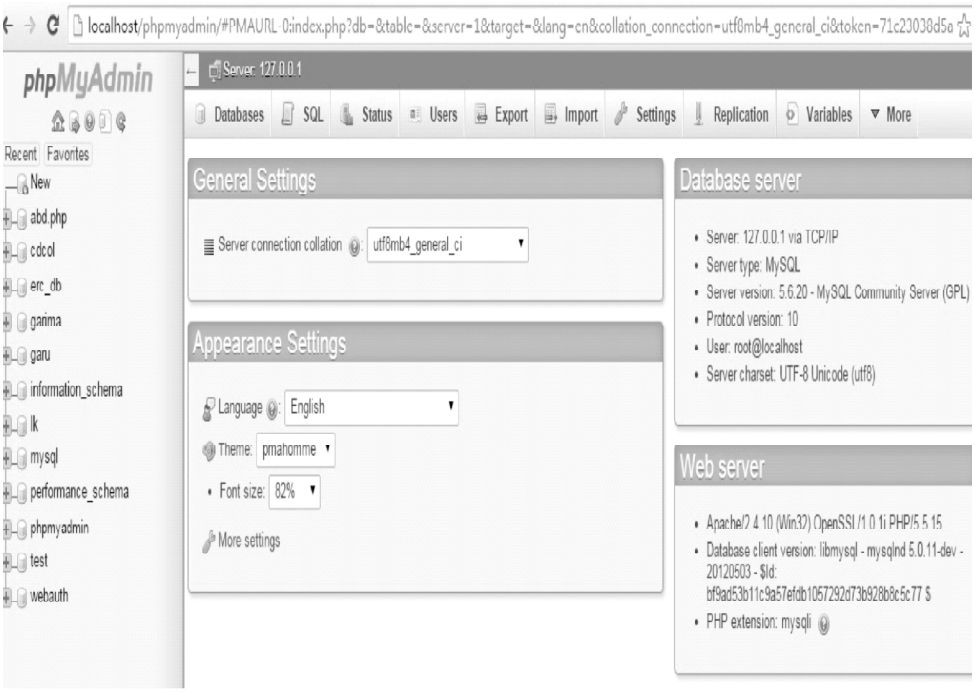

Figure 3: phpMyAdmin

IV. RESULTS AND DISCUSSIONS

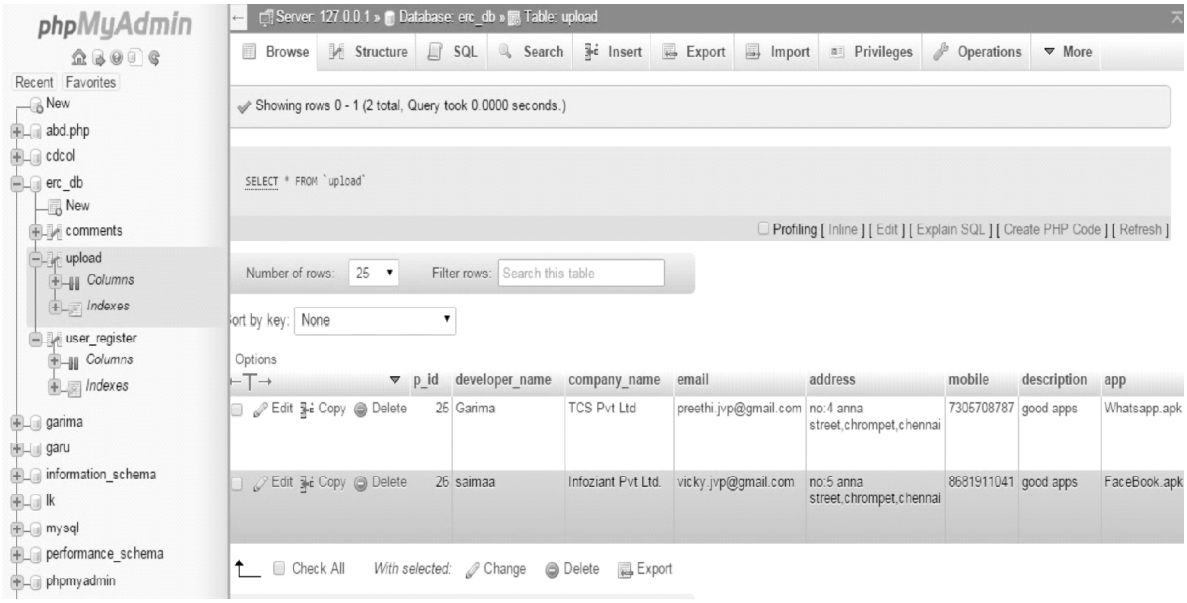

Figure 4: Output of Database

Fig 4 shows the output of APK file uploaded in Google play store. It is uploaded with the developer name, company name, email, address, mobile, description and app. If you want to edit or delete any APK file you can use Edit or Delete option.

Fig.5. shows the Login page with the Username, Password, Sign in and Sign up. New User have to first sign up with username , password, mobile number and email. After it has been sign up, user can sign in with the credentials they have created to login.

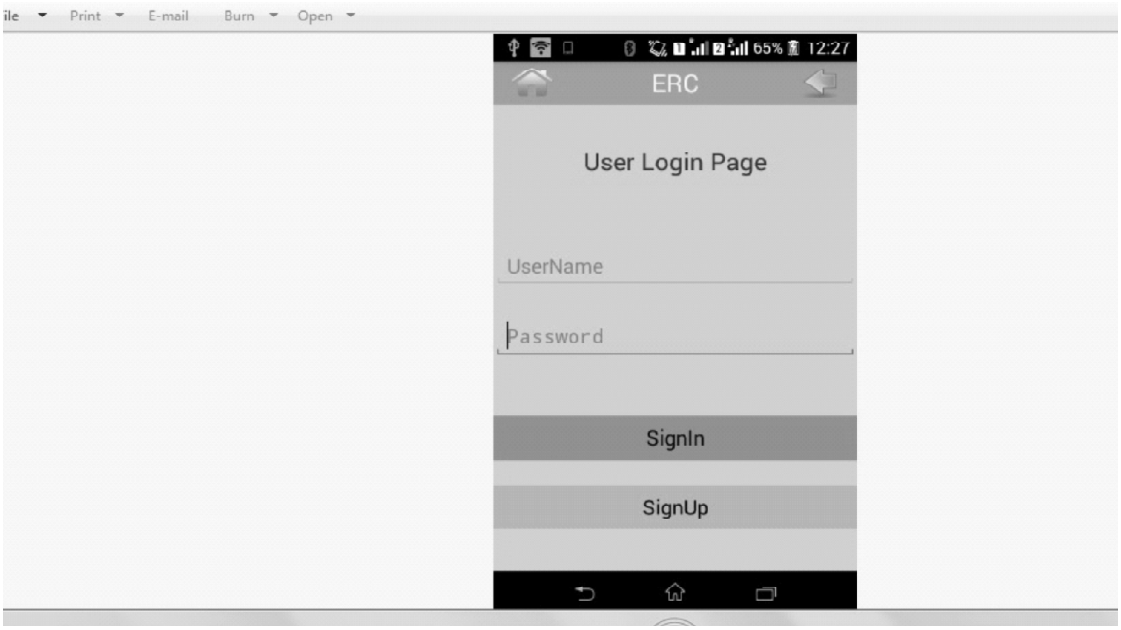

Figure 5: Login Page

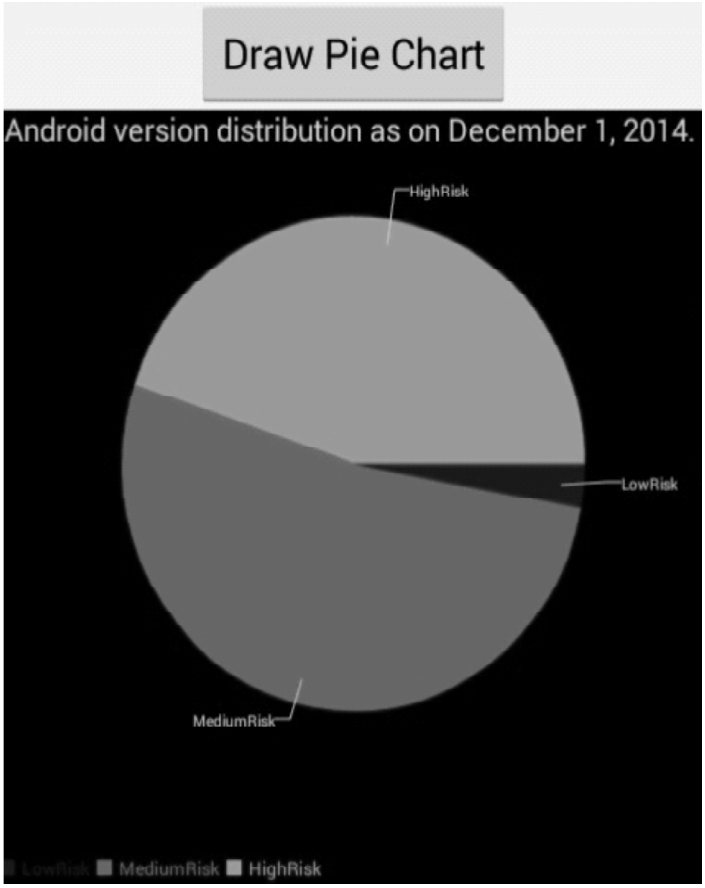

Figure 6: Pie Chart

Fig. 6. shows the Pie Diagram providing the risk information. In the above figure blue depicts for low risk, Green depicts high risk and purple depicts medium risk. Based on these analysis user can choose the application which can be less risky providing same functionalities.

V. CONCLUSION

In this paper, login page is created using XAMPP software and phpMyAdmin and risk information is provided in the form of pie chart mentioning low risk, medium risk or high risk which will help in choosing the application having no security threat. The aim of this project is to introduce a framework that includes probabilistic models for evaluating risk scores. And to introduce idea of risk score functions to improve risk communication for Android applications.

ACKNOWLEDGMENT

This work was supported by SRM University, Chennai, India.

REFERENCES

[1] E. Chin, A.P. Felt, V. Sekar, and D. Wagner, "Measuring User Confidence in Smartphone Security and Privacy," Proc. Eighth Symp. Usable Privacy and Security, (SOUPS '12), article 1, 2012.

[2] A.P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," Proc. Eighth Symp. Usable Privacy and Security, article 3, 2012.

[3] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A Study of Android Application Security," Proc. 20th USENIX Conf. Security, (SEC '11), pp. 21-21, 2011.

[4] P.G. Kelley, L.F. Cranor, and N. Sadeh, "Privacy as Part of the App Decision-Making Process," Proc. Conf. Human Factors in Computing Systems (CHI '13), pp. 3393-3402, 2013.

[5] H. Peng, C.S. Gates, B.P. Sarma, N. Li, Y. Qi, R. Potharaju, C. NitaRotaru, and I. Molloy, "Using Probabilistic Generative Models for Ranking Risks of Android Apps," Proc. ACM Conf. Computer and Comm. Security, pp. 241-252, 2012.

[6] A.P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android Permissions Demystified," Proc. 18th ACM Conf. Computer and Comm. Security, pp. 627-638, 2011.

[7] D. Barrera, H.G. Kayacik, P.C. van Oorschot, and A. Somayaji, "A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 73-84, 2010.

[8] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are Privacy Concerns a Turn-Off?: Engagement and Privacy in Social Networks," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-13, 2012.

[9] W. Van Wassenhove, K. Dressel, A. Perazzini, and G. Ru, "A Comparative Study of Stakeholder Risk Perception and Risk Communication in Europe: A Bovine Spongiform Encephalopathy Case Study," J. Risk Research, vol. 15, no. 6, pp. 565-582, 2012

[10] J. Lin, S. Amini, J.I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing," Proc. ACM Conf. Ubiquitous Computing (UbiComp '12), pp. 501-510, 2012.

[11] P.G. Kelley, S. Consolvo, L.F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone," Proc. Workshop Usable Security (USEC '12), Feb. 2012.

[12] M. Gondan, C. Gotze, and M.W. Greenlee, "Redundancy Gains in € Simple Responses and Go/no-Go Tasks," Attention, Perception, & Psychophysics, vol. 72, no. 6, pp. 1692-1709, 2010.

[13] L.F. Cranor, P. Guduru, and M. Arjula, "User Interfaces for Privacy Agents," ACM Trans. Computer-Human Interaction (TOCHI '06), vol. 13, no. 2, pp. 135-178, 2006.

[14] M. Nauman, S. Khan, and X. Zhang, "Apex: Extending Android Permission Model and Enforcement with User-Defined Runtime Constraints," Proc. Fifth ACM Symp. Information, Computer and Comm. Security, pp. 328-332, 2010.