International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

EFFECTIVE RISK MANAGEMENT FOR MOBILE APPLICATION

G Preethi,
Department of Information Technology,
Anna University Regional Campus,
Coimbatore,Tamilnadu,India.

Dr.P.Marikkannu,
Department of Information Technology,
Anna University Regional Campus,
Coimbatore,Tamilnadu,India.

Abstract : Since the mobile devices become more popular because of its advanced functionality, it is targeted by more malicious and intrusive applications. Even though there are more security measures are available for these systems, it is failed to meet the user reliance to make decisions. In android devices, the installation of any android apps seeks a user permission for avoiding the upcoming vulnerabilities. The user decision for installing certain app is considering the risk information. When these risk information is vast and more complex, it is ignored by the user, which leads the wrong installation decision. For turning the user's focus to read the risk or permission information before installing any app, the risk information is provided in a summary and more understandable format. We propose a combined technique of naïve algorithm and sentiment classification for efficiently conveying such risk information to user. By this, the good or correct decision is made by the user, which prevents the android devices from more system vulnerabilities.

Keywords: Mobile security, risk communication, smart phones, risk score.

I.INTRODUCTION

Now a days, mobile technology is growing rapidly because of its advanced functionality and portability. The use of smart phones, tablets, and other mobile devices to conduct online transactions has been rapidly grown. The mobile devices are used not only for calling and texting, but also used for video calling, emailing, online shopping, e-banking etc. Mobile devices are becoming ubiquitous, and they providing access to personal and sensitive information of the users such as phone numbers, contact lists, password, images, geolocation, and SMS messages. Crime associated with these mobile devices has increased proportionally, and many apps and business has a critical need to detect and prevent fraud related to them. The number of more innovative mobile applications are introduced in to the market day by day for providing these facilities in a consistent way. These applications are either vulnerable or safe to the mobile device. There is a need for analyzing the safeness and quality of any mobile application available in the market for preventing the user from facing the device vulnerabilities and for safeguarding the user privacy. To make their security is important challenge to developers. Mobile devices has different paradigm for install a new application comparing with desktop and laptop computers. In this paper surveying the previous techniques used for preventing the mobile risk while installing the mobile application to the mobile phone.

II. LITERATURE SURVEY

There are more techniques are reviewed for identifying the risk of the mobile application. One of the main idea to identifying or preventing the risk in the mobile application is choosing the best application or low risk apps while installing the mobile application in to mobile device. Here we have analyzing some of the related existing research work classification of the mobile risk A similar work which was the one by Adrienne Porter Felt et al.,[01], they have presented mobile application permission and user attention and behavior while install the mobile apps. They evaluate survey of the android users, in this only few percentage of users interviewed and observed the installation permission and terms and conditions. The other research person E. Chin et al.,[04] in their work have presented a general framework, user study to gain insight into the user perception and behavior of the smart phone security and installation habit. The user need not to focus the permission during installing the apps in to the mobile device, only the user focus on the reviews and rating of the mobile application. Jialiu Lin et al.,[08],in their work they have presented crowd-sourcing users' mental models crowd sourcing users' mental models for analyzing and capturing the mobile user behavior. This model capturing the user expectations of what sensitive resources mobile apps use and also report user privacy summary. Hao Peng et al.,[10],in their work they have propose probabilistic generative model for finding the risk score of the mobile application while installing the application. Any mobile app has risk score that can be monotonically decreasing with respect to the probability generated for an apps.

III. PROPOSED METHOD

The proposed summary risk rating for each app and dynamic graph of reviews and ratings for easy understanding of risk rating. The risk summary and graph can lead the user to choose a best app among all apps available in Google Play store and other sources for Android apps and also specifying the comparison risk summary of two low risk app.

Advantages

- It present the summary of permissions required for the app in more simple way so that user can ignore unsecured application.
- It provides comparison of two applications to find out which application is secure than other.

A. System Architecture

The architecture for the proposed application is explained in the Figure 1.

Figure 1: Architecture diagram for the proposed system

APK file is created and uploaded to Google play store. When the user tries to download the application, pop message is displayed as download failed. The user see a more information about the downloading or installing application in app page. So the user has to click more details to view risk information as a dynamic graph. After verification user can install the application to the mobile device.

B. Implementation

Development an Application: Using Eclipse to create a new Android Application for the mobile devices. There are three type of android application was developing such as Game application, Social Network Application and E-book Applications. Application was generated in the form of .APK File. APK (android package kit) is generated upload in play store.

Uploading in play store: First create a play store Application using Eclipse IDE. Then Upload our development applications into the play store. In this Scenario, please select a new Application for mobile devices. When you continue you will see more detailed information about application. Browse that information to make your choice and select an app. Android warns the user about permissions that an app requires before it is installed.

Downloading failed : The risk information was presented as a text value in the range low, medium, high, very high. With color differences to add extra emphasis ranging from blue, brown, light red, bright red. View for the app, below the average user rating, as well as above the developer (play store) description on the main view. Each permission shows the percentage of apps within that category that request that permission, and presented. Then the rare and critical permissions toward the top so that they were seen more easily.

Sentiment classification algorithm: Sentiment analysis also called as opinion mining. It is used to analysis natural language processing, text analysis and computational linguistics process to identify and retrieve subjective information. It mainly used to analyze movie, software application, customer service and social topic reviews and rating. It widely applied for whether piece of writing text or sentence is positive, negative or neutral. It analyzing the opinion of the writer mode.

Naive Bayes classifier: One of the most popular method for text categorization and classification. In simple, a naïve bayes classifier assumed that the value of a particular feature is isolated to the presence or absence of any other feature, given the class variable. Naïve bayes model is easy to implement and along with the simplicity, it is known to outclass even highly sophisticated classification method are used. It is widely used for large date set such online source and big data's.

Finding word count: Try to determine the specified text or sentence as negative or positive. After the classification, we have to count how many times positive and negative review occur in the website given by the application users. Map and reduce method is used for count the number of times the given word occur in particular site. Based on the counting result, we can determine the low risk application among the number application.

IV.ANALYSIS AND RESULTS

The result shown the step by step process of the application. Once the user install the .apk file in our mobile device, the user can see the below screen in our mobile device. If the user installing any application it redirected and show the risk application of the selected application. Based on the risk score the user install the application, best application has low risk value. The user easy to understand the risk score value through the dynamic graph.

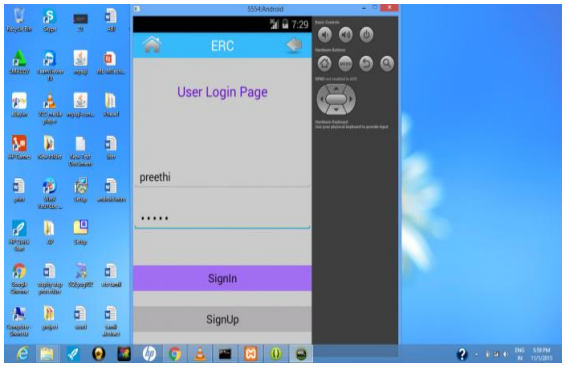

Figure 2: The login page

The figure 2 shows that the login page of the application, if the new user coming to the application they should signup and sign in to application.

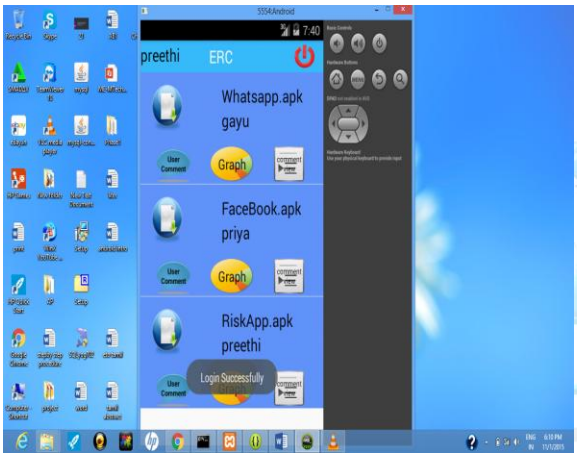

Figure 3: Application Database

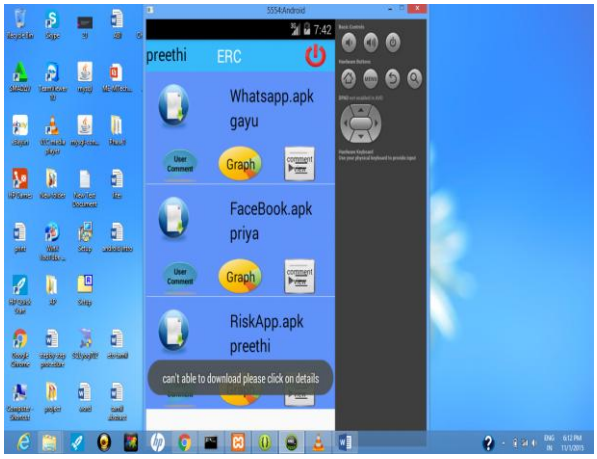

Figure 4: The risk alert to the user

The figure 3 shows the list of application in the database. If the user want to download the application he/she should analysis the risk score of the particular application is shown in the figure 4.

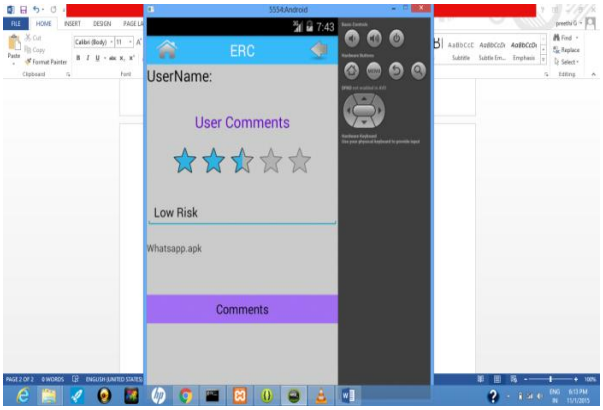

Figure 5: User reviews and comments page

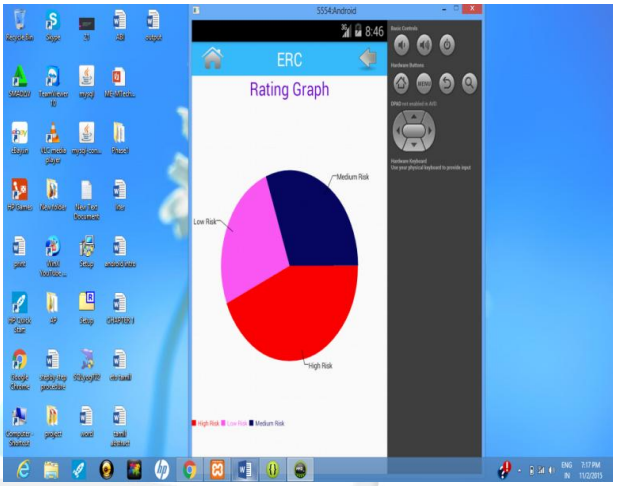

Figure 6: The outcome of the dynamic graph.

User specifying the comments and reviews of the application is show in figure 5 based on the multiple user reviews and comments plotting the dynamic graph to specifying the risk score of the application showed in figure 6.

V. CONCLUSION

Thus the various classification of the mobile apps are used to classifying the mobile apps effectively. The result obtained from these techniques lead the user to choose the safe apps while installing the apps for the mobile devices. The naïve bayes classifier and sentimental classification techniques are used to improve security of the mobile apps. The result, dynamic chart improving the security concerns of the malicious apps in easy to understand the risk of apps such low, high, medium. It is user friendly and easy to understand since the result shows the required apps is offline or online and payable or not payable.

VI.REFERENCES

[1] 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, 2012.

[2] Christopher S. Gates, Ninghui Li, Hao Peng, Bhaskar Sharma, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru and Ian Molloy, ``Generating Summary Risk Scores For Mobile Applications", IEEE Transactions on dependable and secure computing (Volume :11, Issue: 03), May-June 2014.

[3] Hengshu Zhu, Enhong Chen, Hui Xiong, Huanhuan Cao, and Jilei Tian, ``Mobile App Classification with Enriched Contextual Information", IEEE Transactions on mobile computing (Volume:13, Issue: 07), 7 July 2014.

[4] 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), pp. 1-16, 2012.

[5] M.L. Finucane, A. Alhakami, P. Slovic, and S.M. Johnson, "The Affect Heuristic in Judgments of Risks and Benefits," J. Behavioral Decision Making, vol. 13, no. 1, pp. 1-17, 2000.

[6] 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.

[7] T. H.J. Kim, P. Gupta, J. Han, E. Owusu, J. Hong, A. Perrig, and D. Gao, "OTO: Online Trust Oracle for User-Centric Trust Establishment," Proc. ACM Conf. Computer and Comm. Security, pp. 391-403, 2012.

[8] 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.

[9] R.D. Luce, Response Times: Their Role in Inferring Elementary Mental Organization. Oxford Univ. Press, 1986.

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

[11] 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.

[12] XF. Xie, M. Wang, R. Zhang, J. Li, and QY. Yu, "The Role of Emotions in Risk Communication," Risk Analysis, vol. 31, no. 3, pp. 450-465, 2011.

