Risk Analysis for Web Applications

Vinita Attarde[1] Karishma Kankariya[2] Hitakshi Kotkar[3] Nisha Malvani[4]
[1,2,3,4]GES`s R. H. Sapat College of Engineering, Management Studies and Research, Nashik-5, India

Abstract— Android's important protective action against malware applications is creating a risk technique which prior to downloading an application that informs the user about the contents that application requires. Believing that user will make correct action. Such approach was inappropriate as it required much technical information. The proposed method helps the user to evaluated the risk involved while installation of application in a standard numerical and graphical format. This approach will help the user to identify the application having low risk from the same set of category and to ensure the higher security for the mobile device.

***Key words*:** Android, Malicious attack, Data mining, Vulnerable, Web based Services

I. INTRODUCTION

Android is Linux based operating system. Each android application operates as a distinct Linux user, preserving one application from accessing or changing another's private code.

Mobile phones have become vulnerable as they grant fetching of important data such as personnel messages, contacts, location etc, and providing safety for such private data is an crucial challenge. In mobile devices user install various applications that are from different developers. Because of this approach, the security of mobile devices is degrading day-by-day.

The risk information operates in independent fashion and demands too many knowledge and time to filter the important information.

Most probably the android application demands a large set of permission which are mostly similar for many applications. Such permissions are usually ignored by the user due to lack of knowledge and time to read that.

In this era, android is one of the fastest growing technology. So it is desirable for hackers to attack and grab the right to access personal data.

The system will generate numerical and graphical risk score that the user can utilize when choosing an application. It will show the risk score of the application before it gets downloaded. If the application is full of risk, user will not install it, and the purpose of security gets satisfied. If the application is malicious then the system will suggest an alternative application to the user.

II. LITERATURE SURVEY

From the various research papers to got idea about the risk involved in downloading unsecured applications. Till now there were various systems for securing the mobile systems from defective android applications such as

1) Permission Based Security Model.
2) Android Permission
3) Demystified
4) Investigating User Privacy
5) Effectiveness of Android Permissions.
6) Permission based security model

The permission based security model is used to access the various system resources. This model made the used of Self Organising Map (SOM) algorithm of Kohonen. In this model administrator and operating system used to restrict the access of resources. The main disadvantage of this system was they were not designed considering the users knowledge [1].

A. Android Permission:

While installing an application users get the chance to view the applications permissions and denied the installation if permissions are offensive. This work has performed two usability studies which were internet survey and laboratory study. The main disadvantage of this work was it didn't help to most users to make appropriate security decisions [3].

B. Android Permission Demystified:

This technology provides a tool Stowaway. This tooled was used to recognise the over-priviledged applications. It was composed of static analysis tool and permission map. The static analysis tool was used to determine what API an application calls and the Permission Based Map was used to identify the permission needed by an API call[4].

C. Investigating user privacy:

This technology studied thirteen popular ad providers.It examined which application took the advantage of undocumented permission. It also exposed sensitive data in the ad libraries that usually allows an attacker at the network to conflict the user's private data [7].

D. Effectiveness of Application Permissions:

Android Smartphone gives development platforms that provide profitable markets for third party application. This third party code creates risks for the smartphone users. These codes introduce risk. In order to prevent users from this risk, android platform presents application permissions to control access to security of users API [5].

III. EXISTING SYSTEM

A. Permission Based Model

Android important security model against malware application is a risk conveyance mechanism that warns the user regarding the permission an application needs prior to installation. It trusts that the user will make appropriate decision. This approach was ineffective in informing the user about the risk. All the android application usually requires multiple permissions. Due to the same appearance of warming, this warning loss their effectiveness as user ignore such warnings.

The main reason of failure of such approach is that the user requires lot of high-tech knowledge and time to filter the useful information.

B. Effectiveness of Android Permissions

The previous system assigned the full privileges to all the application. In this permission model, each application had a specific set of permissions on its own requirements.

The three advantages of this system were:

1) User Content
2) Defense in Depth
3) Review Triaging

1) User Content:

This security concerned users usual hesitate to accept the access of dangerous permissions.

2) Defense Of Depth:

For install-time system, the effect of a security in an application will be bound to vulnerable application privileges.

3) Review Triaging:

The application permissions declaration makes easier central review. The security analyzers usually ignore low privilege application and concentrate on application with dangerous permissions. This decrease the review time.

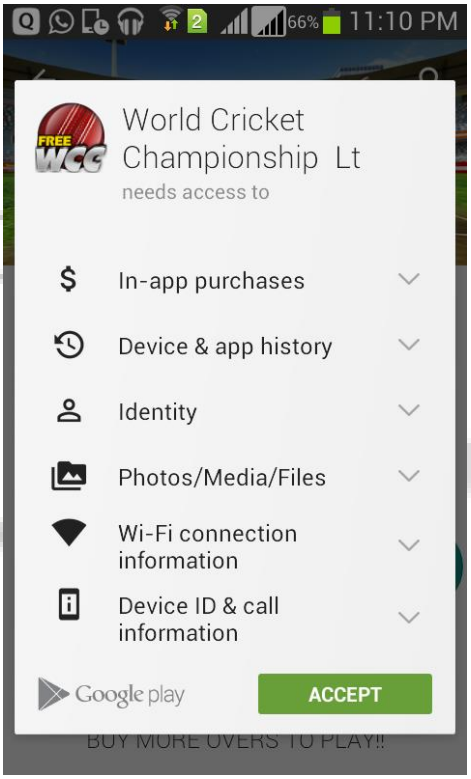

Fig. 1: Existing System

IV. PROPOSED SYSTEM

The main purpose of the proposed system is to improve the existing security mechanism. In this approach, we are identifying the critical permission that have personal impact factors, if the application requires critical permission that are not present in the similar categories of application then the application is labelled as risky. We are thus proposing the idea of risk score function. This function will be used to allocate every application a numerical score, which demonstrate how risky the application is. This approach provide a easy way to evaluate the risk in installing the application and compare it with the same category of application.

In this approach we have used Bayesian approach for risk calculation. Here we have introduced a framework that contains rarity-based signals and probability models

Fig. 2: Proposed System

V. CONCLUSION

We had done a detailed study of the existing system from that study we conclude that the previous system are not efficient. Thus we have developed an application for mobile phones security.

The risk analysis for web based application will be generating a numerical risk score for easy evaluation of the application present at the google play store. The application will use naive Bayesian algorithm for generation the risk score for the users interested application.

REFERENCES

[1] D.Barrera., H.G.Kayacik, P.C.Van Oorschot and A. Somayaji, "A methodology for empirical analysis of permission based security model and its applications to android" Proc. 17th ACM Conf. Computer and comm. Security, pp.73-84, 2010.

[2] A.P.Felt, E.Ha, S.Egelman, A.haney, E.chin and D.wagner, "Android Permission User Attension, Comprehension, and Behavior", Proc. Eighth symp usable privacy and security article 3,2012.

[3] By G.Portokalidis, P.Homburg, K.Anagnostakis, and H.Bos,"Paranoid Android:Versatile Protection For Smartphone", Proc.26th Ann. Conf. computer security application, PP.347-356, 2010.

[4] By.Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, Dawid Wagner, "Android Permissions Demystified".

[5] A.P.Felt, K.Greenwood, and D.Wagner, "Effectiveness of Application Permission", Proc.Second USENIX Conf. Web application Development, 2011.

[6] Y.Song, A.Kocz, and C.L.Giles, "Better Naïve Bayes Classification for High-precision spam Detection," Software Practice and Experience, vol.39,no.11,pp.1003-1024,2009.

[7] R.Stevens,C.Gibler,J.Crussell,J.Erickson, and H.Chen, "Investigating user privacy in Android Ad Libraries,"Proc.IEEE Mobile Security Technologies(MoST'12),2012.

[8] D.W.Stewart and I.M.Martin, "Intended and Unintended Consequences of warning Messages:A Review and Synthesis of Empirical

Research,"J.Public Policy & Marketing,vol.13,no.1,pp.1-19,1994.

[9] H.Peng, C.Gates, B.Sarma, N.Li, Y.Qi, R.Potharaju, C.NitaRotaru, and I.Molloy, "Using Probabilistic Generative Models for Ranking Risks of Android Apps," Proc.Conf.Computer and Comm Security,(CCS'12),pp.241-252,2012.

[10] P.G.Kelley, S.Consolvo, L.F.Cranor, J.Junk, N.sadeh, and D.Wetherall, "A Conundrum of permissions : Installing Application on an Android Smartphone," Proc.Workshop Usable Security (USEC'12), Feb.2012 .

[11] Google Bouncer.http://goo.gl/QnC6G 2014 .

