International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

SECURED ANALYSIS OF ANDROID APPLICATIONS USING PERMISSION ACCESSING SYSTEM

PRASHANTH SUDARSHAN.C P[1], RAMADEVI.M[2], SHARON.M[3],DR.SWAMINATHAN.B[4]

[1]*Student, Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Tamil Nadu, India.*
[2]*Student, Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Tamil Nadu, India.*
[3]*Student, Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Tamil Nadu, India.*
[4]*Professor, Dept. of Computer Science and Engineering, Rajalakshmi Engineering College, Tamil Nadu, India.*

Abstract – *In today's world, there is a huge rise in malware infections and spam campaigns to which more smartphone users are being affected. Hence there is a need to identify and prevent such attacks. So, in the proposed system the methodology we applied is to help us identify the ad libraries embedded in the applications, triggering web links, malware, spam Play Store itself has a filtering mechanism to identify malicious applications, we deploy an application separately in the smartphone that analyses and checks if the application is to be installed or not, as the preliminary process of filtering. This dynamic application is trained with a large set of access permissions such as camera, call logs, external SD card, location, etc. which helps us to identify applications which demand unwanted permission.*

Key Words *:* **Categorization, Permission Checking, Malicious links, Redirect URL, Misbehaving apps.**

1. INTRODUCTION

Android is one of the most widely used operating system. It is an open source software that helps us to create our own applications very easily due to which most people prefer to use this operating system. However many malware infections easily attack android OS due to its openness of allowing all applications to be installed without in-depth verification for the presence of malware and provenance of applications. Due to its open nature there is a high chance of existence of malware leading to damage of personal data. The malware which are targeted towards desktops are gaining their targets towards smart phones hence there is need to restrain such attacks from causing trouble to mobile phones and desktop users. Hence researchers have spent significant effort in analyzing malicious applications and the important factor to be considered is the redirection of legitimate applications which may lead users to websites hosting malicious content. This may occur either by web links which are embedded directly in the applications or occur via the landing pages of the advertisements through ad networks. The suitable solution found for analyzing how the malicious content propagates consists of 3 main components the triggering web-links, presence of malicious content and source of malware. Due to the existence of many different complex problem we need different techniques and approach to deal with different malwares and UI which would be better understood via app or web interface. Hence we have developed a framework that identifies all the web links reachable from the application that has a presence of malware. We dynamically analyse applications by exercising their UI automatically and visiting and recording any web links that are triggered. We have monitored many applications gathering around millions of URL links which are then analyzed using URL blacklists and anti-virus systems are being for identify malicious websites and applications that are downloadable from these websites.

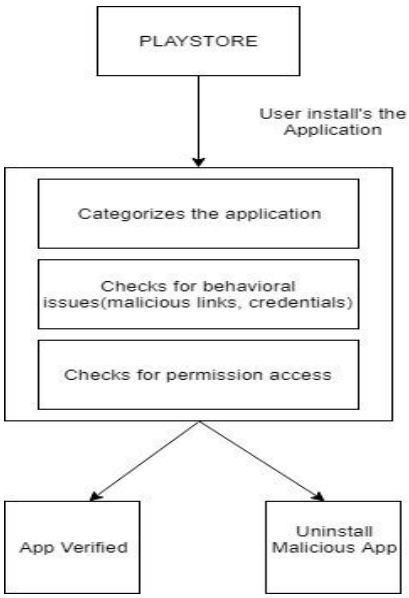
1.1 Existing Systems

Mobile users are increasingly becoming targets of malware infections and scams due to the increase in smart phone models. Mostly android users are more greatly affected due to the open nature of the android eco system and it is freely available to customize according to the developer's needs. This in-turn makes it easier for hackers or people who want to cause harm to develop harmful viruses, threats, Trojans, etc. easily. These type of harmful software's are found after they cause damage to the user but it should also prevent it from occurring. Hence there is a need to curb such attacks.

Disadvantages :

- Malicious application are installed via a link
- Applications ask permissions to access unnecessary information like contacts, gallery, video.
- Redirect the browser into another website or webpage
- Malicious websites or links are blocked only after visiting the webpage and there is no prevention mechanism.
- These applications does not prevent installation of applications from external sources other than play store.

1.2 FRAMEWORK:



2. MODULE DESCRIPTION

Categorization:

In this module, all the mobile applications will be categorized based on their type of permissions required. We install many android apps, in which some apps may gather unwanted data's from our mobile. For example in OLA application, location alone is enough but it asks permission for the access of camera and storage which is unnecessary. Similarly, most of the applications were accessing unnecessary data which we need to deny them.

Malicious and URL detection:

Malicious links and URL's are blocked for the user. If the user doesn't need to go on a specific website, that website is compared with the proposed data set and it's blocked. Once that particular URL is blocked the user cannot visit that website. Also, the URL's which redirect to other pages are also blocked.

Permission optimization:

After categorizing the app based on their type and detecting the malicious and unwanted URL links, the server asks for the user's permission and then install the app. If the user finds that the particular app is malicious then the user can deny the unnecessary application or uninstall it. This module checks the application's permission and suggests the user whether to install or uninstall the application.

2.1 IMPLEMENTATION

Initially, the user will download the application from the play store then the proposed app installed in the mobile phone will categorize the application based on their type of permissions required, then it checks for the malicious links and URL's. If any URL causes harm to the user then it can be blocked. Then the application asks for the user's permission to access the service's, if the app is found to be misbehaving or malicious then the user is prompted with a notification whether to uninstall this app or not. So the proposed app in the mobile phone will be helping the user to seek out whether or not the applications in our mobile phone are safe and it'll block all the unwanted application that requests unnecessary permission access like contacts, gallery and so on. Also, it'll help the user to avoid unwanted websites by blocking the redirecting URL through the proposed application.

3. CONCLUSIONS

In order to restraint the malware attacks and scams it is necessary to understand the provenance of such attacks and eliminate them. Our proposed system helps us to detect malicious links, behavior attack, access permission and block all the unwanted application. Which makes it much easier for the end-user to install a legitimate application.

REFERENCES

[1] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna, "The dark alleys of madison avenue: Understanding malicious advertisements," in Proceedings of the 2014 Conference on Internet Measurement Conference. ACM, 2014, pp. 373–380.

[2] J. Buhler, "Efficient large-scale sequence comparison by localitysensitive hashing," vol. 17, no. 5, pp. 419–428, 2001.

[3] V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, and R. Riley, "Are these ads safe: Detecting hidden attacks through the mobile app-web interfaces," 2016.

[4] W. Zhou, Y. Zhou, M. Grace, X. Jiang, and S. Zou, "Fast, scalable detection of piggybacked mobile applications," in Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013, pp. 185–196.

[5] V. Rastogi, Y. Chen, and W. Enck, "AppsPlayground: Automatic Security Analysis of Smartphone Applications," in Proceedings of ACM CODASPY, 2013.

[6] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, "Knowing your enemy: understanding and detecting malicious web advertising," in Proceedings of the 2012 ACM conference on Computer and Communications Security. ACM, 2012, pp. 674–686.

[7] A. Z. Broder, "On the resemblance and containment of documents," in Compression and Complexity of Sequences 1997. Proceedings, Jun 1997, pp. 21–29.