Detecting the Malicious Application using FRAppE

Yasmeen Sultana

Department of Information Science
Dayananda Sagar College of Engineering
Bengaluru, Karnataka
yasmeen734@gmail.com

Prof. B.I.Khodanpur

Department of Information Science
Dayananda Sagar College of Engineering
Bengaluru, Karnataka

Abstract- Communication technology has completely occupied all the areas of applications. Last decade has however witnessed a drastic evolution in information and communication technology due to the introduction of social media network. Business growth is further achieved via these social media. Nevertheless, increase in the usage of online social networks (OSN) such as Face book, twitter, Instagram etc has however led to the increase in privacy and security concerns. Third party applications are one of the many reasons for Facebook attractiveness. Regrettably, the users are unaware of detail that a lot of malicious Facebook applications provide on their profile. The popularity of these third party applications is such that there are almost 20 million installations per day. But cyber criminals have appreciated the popularity of third party applications and the possibility of using these apps for distributing the malware and spam. This paper proposes a method to categorize a given application as malicious or safe by using FRAppE (Facebook's Rigorous Application Evaluator), possibly one of the first tool for detecting malicious apps on the Facebook. To develop the FRAppE, the data is gathered from MyPagekeeper application, a website that provides significant information about various third party applications and their insight into their behavior.

Keywords: Online Social Networks, Malicious Facebook Apps, Spam Files, Cookies.

I. INTRODUCTION

Now-days all are familiar with online social networks (OSN) like Facebook, Twitter, etc. In social networks there are many third party applications and these applications are recognized by using online social networks. Online social networks host third party applications to improve the user experience on their platforms. In social network improving the user experience is so enhanced that it includes entertaining path which connects the people all over the world and also provide entertainment. The interesting and entertaining activities are listening music, playing games and communicating among online friends. Today all the uses of Facebook are very popular on social network. Suppose Facebook provides the application as well as developers an application program interface, an API that facilitates application integration in to Facebook to enhance user experience. In Facebook there are 500K application are available and the application installation range in every day is 20M. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear their notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Furthermore, many apps have acquired and maintain a large user base. For instance, FarmVille and City Ville apps have 26.5M and 42.8M users to date.

Malicious applications are those applications which hack personal information like e-mail id, phone -number of Facebook users. These malicious applications also provide the business for hackers by using the popularity of online social network. By using malicious applications only

hackers are getting benefited in so many ways. The malicious applications reach the huge number of Facebook users to hacking their personal information with their friends also to spread spam. There are many ways that hackers can benefit from a malicious app: (a) the app can reach large numbers of users and their friends to spread spam, (b) the app can obtain users' personal information such as email address, home town, and gender, etc. In Facebook there is many malicious applications are spreading every day.

II. LITERATURE SURVEY

. Md Sazzadur Rahman Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos [01] presents the applications that efficiently categorizes malicious applications on Facebook. By tracking a number of Facebook applications examined over the period of nine month, they proved that the malicious applications vary considerably as of the benign applications to some features. Leveraging observation, they urbanized FRAppE, a precise classifier for identifying the malicious Facebook applications.

Sanae Rosen, Zhiyun Qian, and Z. Morely Mao[02] described a system for methodically identifying privacy connected appliance behaviour in mobile system where mainly significant aspect of the appliance behavior can be arbitrated during a well defined appliance structure. This system contains two components creating an acquaintance base of the API call by privacy pertinent behavior, with this information base to create a behavior outline for requests. They have established that it can be an extremely efficient process of permitting both end users as well researcher to improve appreciates how the application behaves.

Prateek Dewan, [03] discovers a variety of study attempt to discovering the Facebook app network; analyze the malicious content on it, moreover analyzing the proceedings on the online social media in common. Then based on the review which aid in learning the hostility of malicious contents content extend on the Facebook through events. With appropriate investigate areas counting discovery of the cooperation or fake account, also Sybil nodes is in Facebook system, discovery of spam on the other social network like Twitter, trustworthiness or dependability of data of user produced content, also detection event in the online social media.

Mario Frank, Ben Dong, Adrienne Porter Felt, and Dawn Song [04] introduces a probabilistic form to extract permission request pattern as of the Android also Facebook applications. For both platforms, they found the set of pattern that fits fine to information. They establish the permission request of the small standing applications change as of the permission requests pattern of high standing applications. These indicate that the permission requests of the pattern are employed as element of the possibility metric or soft calculation of excellence of novel applications.

III. PARAMETERS FOR PROFILING APPLICATIONS

1) Application Summary: Malicious apps typically have incomplete application summaries. First, we compare malicious and benign apps with respect to attributes present in the application's summary—app description, company name, and category.

2) Category can be selected from a predefined (by Facebook) list such as "Games," "News," etc., that matches the app functionality best. While most benign apps specify such information, very rarely malicious apps do so. For example, only 1.4% of malicious apps have a nonempty description, whereas 93% of benign applications configure their summary with a description.

3) Required Permission Set: 97% of malicious apps require only one permission from users. Every Facebook app requires authorization by a user before the user can use it.

4) Redirect URI: Malicious apps redirect users to domains with poor reputation. In an application's installation URL, the "redirect URI"

parameter refers to the URL where the user is redirected to once she installs the app.

5) Posts in App Profile: 97% of malicious apps do not have posts in their profiles. An application's profile page presents a forum for users to communicate with the app's developers (e.g., to post comments or questions about the app), or vice versa (e.g., for the app's developers to post updates about the application).

IV. METHODOLOGY

The proposed FRAPPE tool detects the malicious web applications based on the spam files and cookies generated. FRAppE detects malicious web application based on of spam file generated and gives the message to the users. Figure1 represents the general block diagram of detecting a malicious application.

The proposed model consists of three important modules that each perform specific task in the project.

These modules are

a) Admin Module
b) FRAppE Agent Module
c) FRAppE Attacker Module

A. *Admin Module*

Admin is mapping the server details and web application details. In this module in the initial stage we will maintain two servers in the each server we will maintain few applications in various servers such as Server A and Server B. In server A is having three web applications Encryption and Numerology and encoder, while server B is hosting Flames, weight on Planets and BMI calculation applications.

Admin will keep track of the hosted applications, will have access to server settings and database where the details are stored.

Admin will also be able to change password, add or remove applications or add or remove servers.

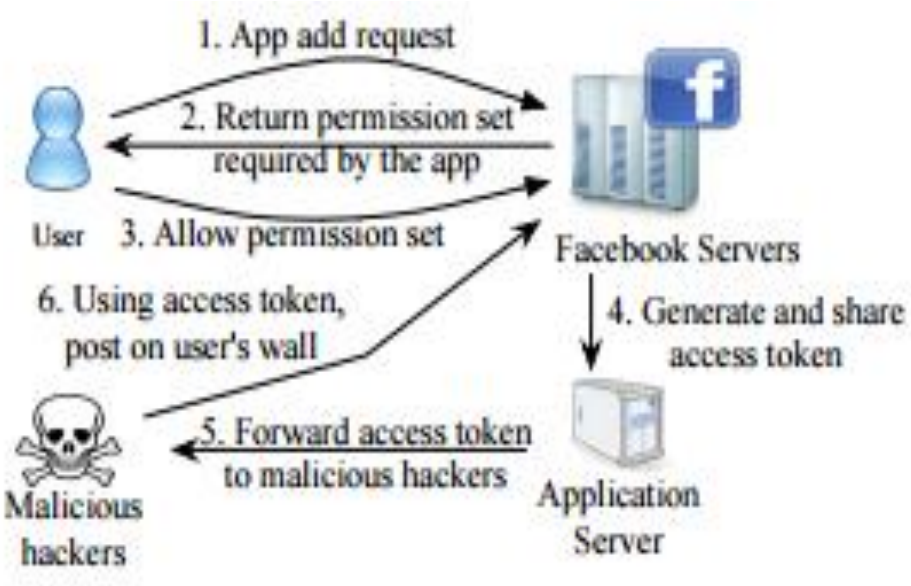

Figure 1: FRAppE Design

B. *FRAppE Agent module:*

The FRAppE agent module helps to map the IP address of the applications. It will track the IP address of server and the application accessing the user profile that is how many time it will access the application. When user accesses the application, request is handled by FRAppE Agent tool to determine to which server it belongs to.

C. *FRAppE attacker module:*

FRAppE attacker module will keep the track of all the applications. it keeps count of number of cookies and spam files. It maintains a table with application name, application id and the count of spam files and cookies and it will also check whether any application is misbehaved or not based on threshold value of the spam files and cookies.. If any application has misbehaved FRAppE tool will detect that application it will give the message to end user to come out of the application and then blocks the application if required.

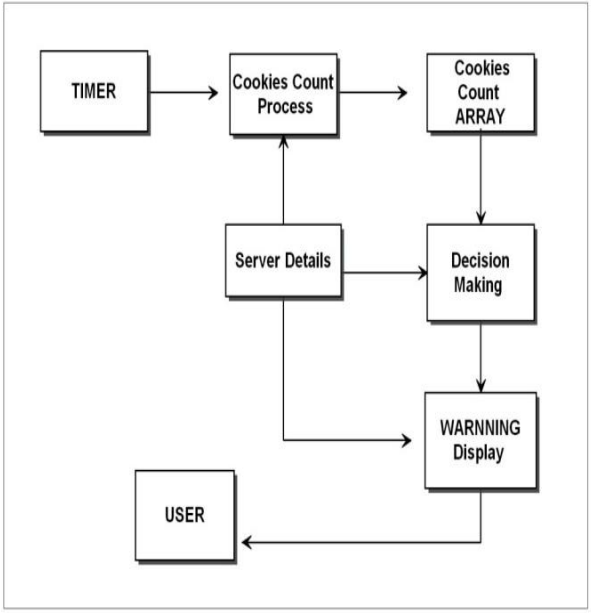

Figure 2 : FRAppE Architecture

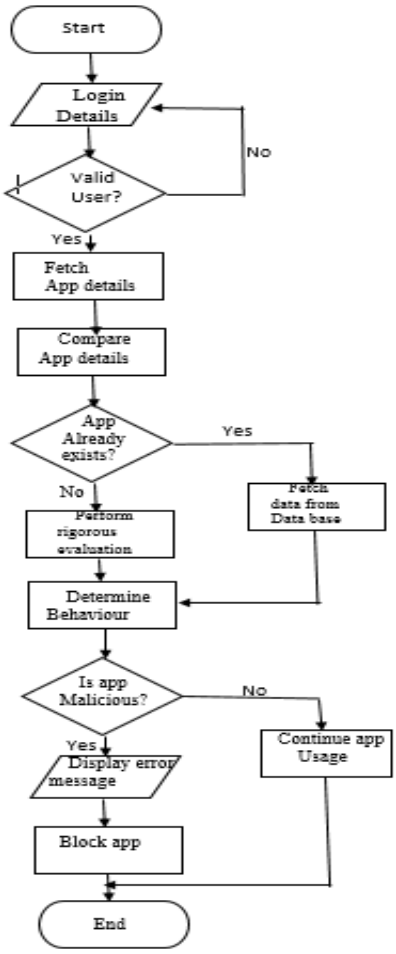

Figure 3: Flow chart

V. RESULTS

The experimental results have been discussed in this section. Mainly we have three modules like Admin Module, FRAppE agent and FRAppE attacker. FRAppE Agent will track all applications, server ID, server IP Address and number of access. Similarly FRAppE attacker module will track application Id, Application Name, number of cookies and spam file creation. Figure 5 represents the snap shot of web application for detecting malicious application. Figure 6 depicts the activation of numerology server. Figure 7 tracking the FRAppE Agent and Figure 8 represents the identification of malicious applications.

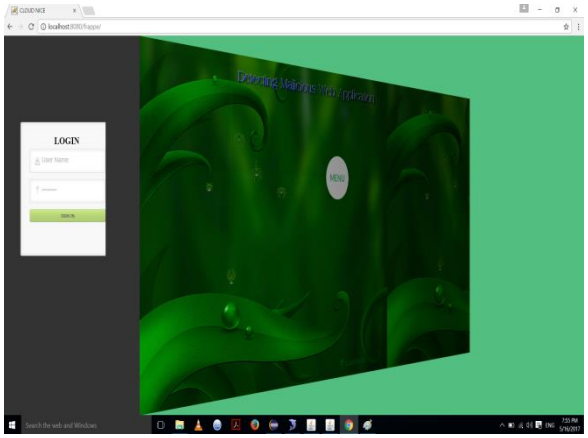

Fig 4: Admin Module

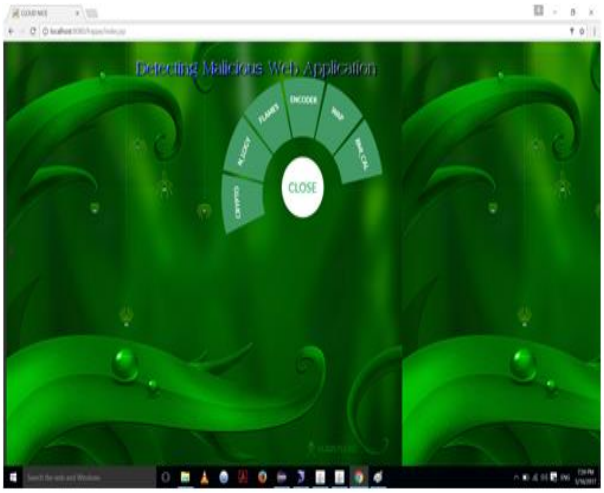

Fig 5: Main Menu

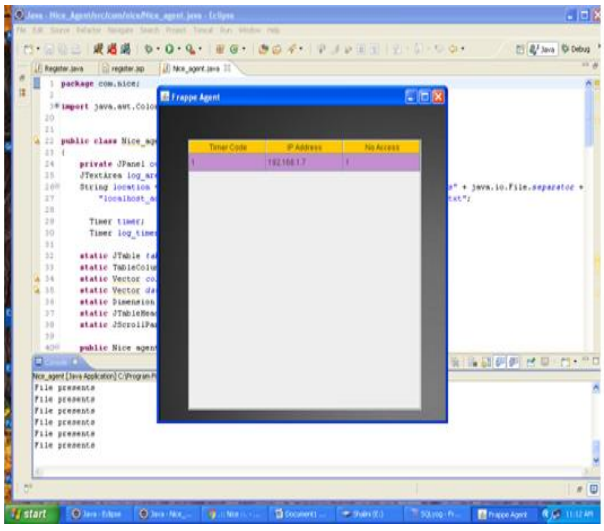

Fig 6: Agent Module

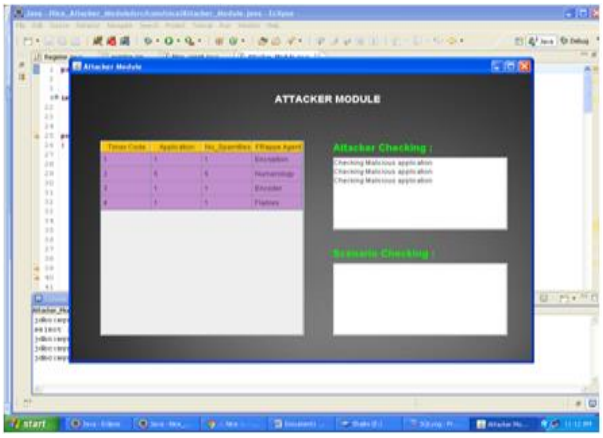

Fig 7: Attacker Module

Fig 8: Third Party Application

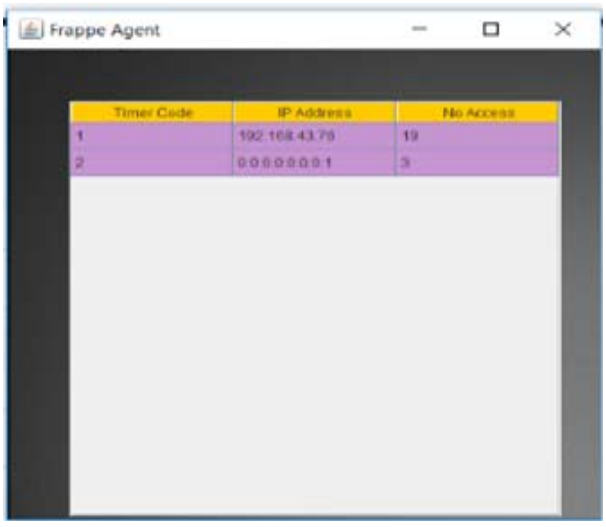

Fig 9: Agent Module Tracking

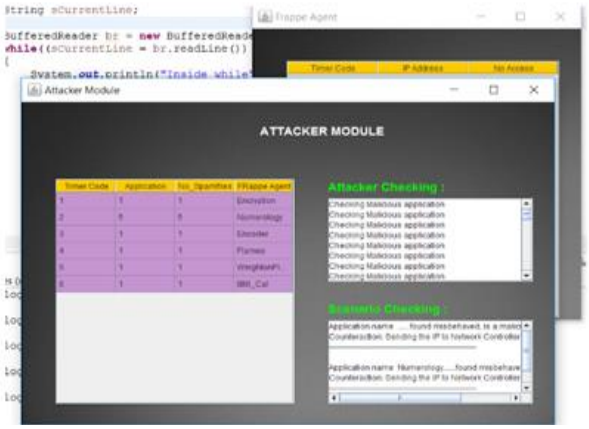

Fig 10: Malicious Application Detected

VI. Conclusion

Evaluation of large variety of Facebook apps observed over time, it is seen that malicious third party apps pose a constant threat to privacy and security and that malicious apps differ significantly from benign apps with respect to several features. For example, malicious apps are much more likely to share names with other apps, or connected to app-nets etc.

Based on these observations FRAppE has been developed, as classifier for detecting malicious Facebook applications.

The model that has been developed now, works fine with sample applications, but it needs to be tested with real applications.

VII. REFERENCES

[1] R.Vinothini, S.Vinitha, S.V.Shalini, “Detection and blockage of malicious app in facebook”, International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue 3, 2016.

[2] Rosen, Sanae, Zhiyun Qian, and Z. Morely Mao, "Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users", In Proceedings of the third ACM conference on Data and application security and privacy, pp. 221-232, 2013.

[3] Prateek Dewan, “A Survey on Identification and Analysis of Poor Quality Content on Facebook”, Comprehensive Examination Survey Report, Vol. 1, No. 1, 2014.

[4] Frank, Mario, Ben Dong, Adrienne Porter Felt, and Dawn Song, “Mining permission request patterns from android and facebook applications", In Data Mining (ICDM), 12th International Conference on IEEE, pp. 870-875, 2012.

[5] Egele, Manuel, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna, "Compa: Detecting compromised accounts on social networks", In NDSS, 2013.

[6] Abu-Nimeh, Saeed, Thomas Chen and Omar Alzubi, “Malicious and spam posts in online social networks”, Computer, Vol. 44, No. 9, pp. 23-28, 2011.

[7] Gilbert, Peter, Byung-Gon Chun, Landon P. Cox, and Jaeyeon Jung, “Vision: automated security validation of mobile apps at app markets”, In Proceedings of the second international workshop on Mobile cloud computing and services, pp. 21-26, 2011

[8] Lande Ashutosh, Patil Akshay, Bondre Pankaj, Akshata Phawde, “ Detecting Malicious Apps on OSN Facebook Walls”, International Journal of Advance Engineering and Research Development Volume 3, Issue 1, January -2016

[9] Rahman, Md Sazzadur, “Detecting Social Malware and its Ecosystem in Online Social Networks”, University of California, Riverside, 2012.

[10] C. Gowdham, A.Anusha, M.Gayathri, “FRAPPE-For Identifying Malicious Facebook Application”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 4, 2016.

[11] Rahman, M. S., Huang, T. K., Madhyastha, H. V., & Faloutsos, M, “FRAppE: detecting malicious facebook applications”, In Proceedings of the 8th international conference on Emerging networking experiments and technologies, pp. 313-324, 2012.

[12] Urvashi Yadav, Khushi Kumari, Rohini Lokare, Suhasini Borge, D.V. Shinkar, “FRAppE: Identifying Malicious Facebook Application”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, 2016.

[13] Ritu Kumari, Utkarsha Mamidwar, Sanjoli Kapoor, Kritika Sharma, “FRAPPE: Making Facebook More Secure”, International Journal of Computer Science Trends and Technology (IJCST), Vol. 3, Issue 6, 2015.

[14] T. Griffiths and M. Steyvers. Finding scientific topics. Proceedings of the National Academy of Sciences of the United States of America,101(Suppl 1):5228–5235, 2004.

[15] P. Guttorp. An introduction to the theory of point processes (D. j.daley and d. vere-jones). SIAM Review, 32(1):175–176, 1990.