ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

Detection and blockage of malicious app in facebook

R.Vinothini, S.Vinitha, S.V.Shalini

Department Of Computer Science, Prathyusha Engineering College, Chennai, India
Department Of Computer Science, Prathyusha Engineering College, Chennai, India
Department Of Computer Science, Prathyusha Engineering College, Chennai, India

ABSTRACT: Nowadays among Online Social Networks (OSN), Facebook is the widespread one and it is used by 1.5 billion people across the world. Hackers are finding many new ways to propagate spam and malware on these platforms, which we refer to as social malware. They can easily access the personal details. Social malware cannot be identified with existing security mechanisms (e.g., URLblacklists). Facebook app called MyPageKeeper is used to protect Facebook users from social malware. FRAppE stands for Face book's Rigorous Application Evaluator, arguably the first tool focused on detecting malicious apps on Facebook. FRAppE can detect malicious apps with complete accuracy. The objective of this project is to detect malicious application and block those applications in facebook using FRAppE tool under the set of constraints. Offensive words are detected and blocked using dictionary. There is already an overview given about just finding malicious app but not on blockage of offensive words or posts. It provides only a high-level overview about threats to the Facebook graph. The main disadvantage of existing system is security is missing. In proposed system certain techniques are implemented in finding the Offensive words or any posts, and dictionary detects the words. These words will not display in public wall. Instead of that such post will be automatically migrated to blocked post list. The user can view it secretly and also a warning mail is send to user. It is safe and secure. Unnecessary information will not be added in our wall. Thus the Offensive words and posts are blocked with the help of dictionary using filters and it is not publicly posted to user wall.

I. INTRODUCTION

Hackers are involved in many spam's propagating process. In many social networks, hackers spread malware and with the help of these they can easily access the personal details of the user. Third party apps are widespread now. Hackers have started taking advantage of the Third party apps platform and developing malicious applications. There are many ways that hackers can benefit from malicious app. Those apps can reach large number of users and their friends to spread spam, the app can obtain users personal information. It does not provide safety for users in Face book. Initially existing system contains only MyPageKeeper app, which is a security app in Face book. It shows notification about the spam spreading in Face book day-to-day. In existing system, a tool named FRAppE is developed using data from the MyPageKeeper app, a security app which already existing in Face book. This tool detects the malicious app but not on the blockage of those apps. It is not that much safe and secure. The biggest disadvantage is that we face many security issues and in this we focused on only identifying malicious applications. It provides only a high level overview about the threats in the Face book, does not provide deep analysis of the system. It is the biggest drawback in the existing system.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

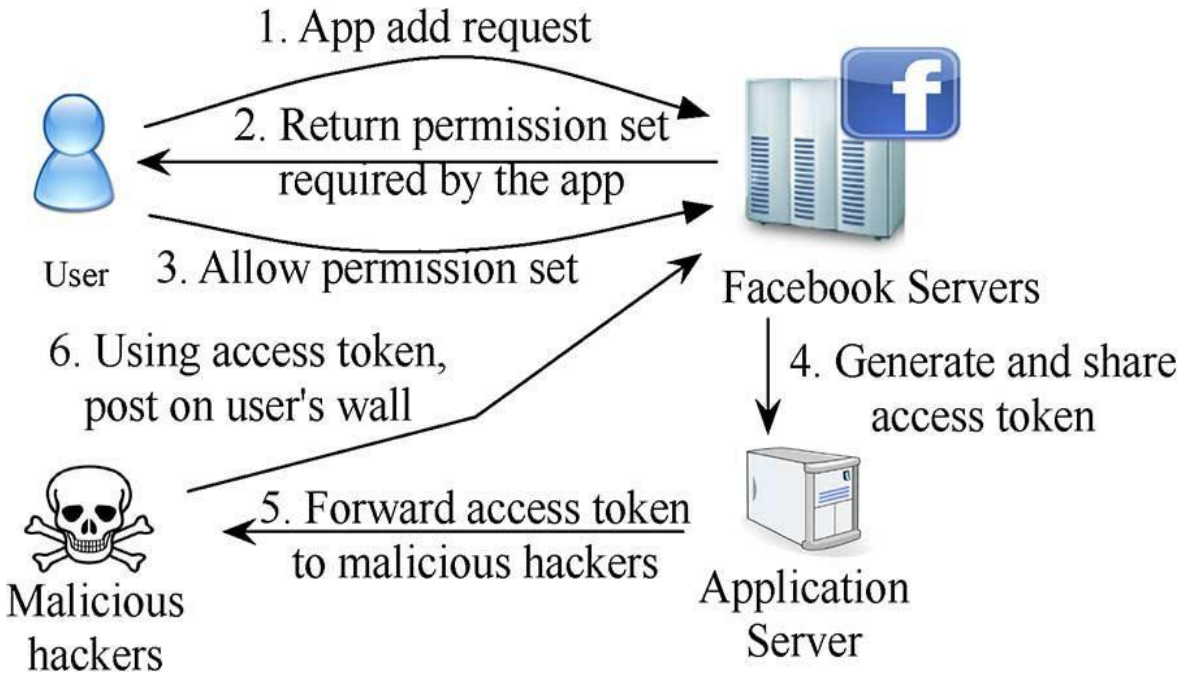

Fig 1 System architecture for Existing system

II. PROPOSED SYSTEM

These problems are overcomes in the proposed system. In the proposed system using the FRAppE tool, we detect and block the malicious applications in the Face book. When user is trying to post the offensive words or posts to the user's Face book wall, those words or posts are detected using the dictionary and it gets filtered. When we found any installation of the malicious app, user wall gives a warning notification that the app found is malicious, whether to install it or not. Offensive words or posts which are not related are detected and blocked using the FRAppE tool. These words or posts will not display in the public wall. Instead of that such post will be migrated to the blocked post list. User can view those things secretly and also a warning mail is send to the user. It is safe and secure. Unnecessary information will not be added in our wall.

FRAppE, a tool stands for Face book's Rigorous Application Evaluator which is helpful in monitoring the entire system. In Authentication and Authorization module, the user will register the data and login into the pages to view their profile to see all the contacts, the user will do all the works here. They can easily access the data from the database. If any malicious app is found in the profile, it will be detected using FRAppE in warn malicious app module and after detecting it will send the warning notification message. If there is any post of offensive words or posts in the user wall, those offensive words will be detected and blocked using the dictionary and these overall details will be stored in the database. The next work to be done by the database is to send a warning mail to the user. The blocked words will be send to the private wall and it can be viewed in blocked post list by the user alone.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

III. ARCHITECTURE DIAGRAM

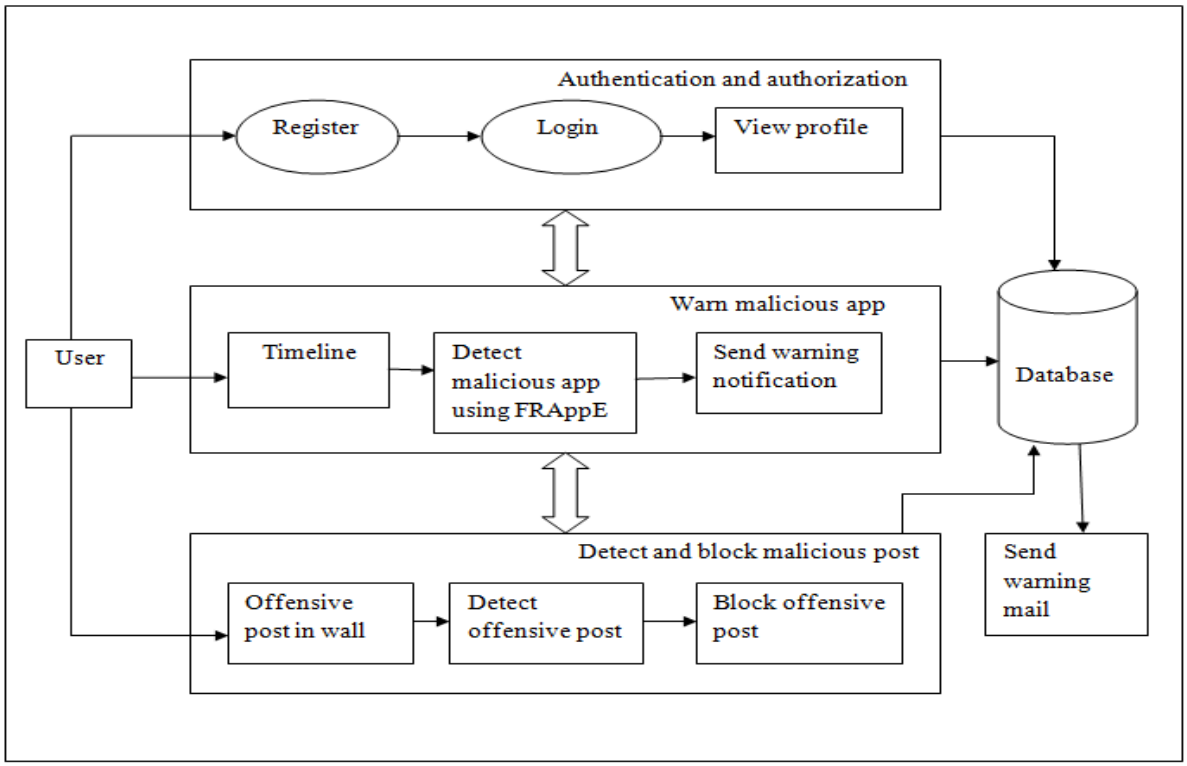

Fig 2 System Architecture for proposed system

IV.AUTHENTICATION & AUTHORIZATION

In this module first user has to register then only the person can access the database. After the Registration, the user can login into the site. The authorization and authentication process facilities the system to protect it and besides it protects the whole mechanism from unauthorized usage. The registration involves in getting the details of the users who wants to use this application and then user can view their profile.

V. WARN MALICIOUS APP

When user trying to post or suggest malicious apps or links, the FRAppE detects the apps or links which is malicious. There are two variants in malicious app classifier FRAppE Lite and FRAppE. A FRAppE Lite is a light weight version that makes use of only the applications features available on demand. E.g. When given a specific app ID, FRAppE Lite crawls the on- demand features for that application and evaluates the application based on those features in real time. FRAppE is another variant that makes use of both on-demand and aggregation based features. When a malicious app is found in the face book wall, it will give us a warning message whether to continue to install the app or deny the message.

VI. DETECT & BLOCK OFFENSIVE WORDS

When the user trying to post Offensive post with the help of dictionary, then it detects the words. This post will not display in public wall. Instead of that such post will be automatically migrated to blocked post list. The user can not display the result in user Face book wall. The user can view the blocked post list anytime if they are interested secretly in the blocked post list.

VII.SEND WARNING MAIL

After the detection and blockage of offensive words or posts, they will be sent to the blocked post list, the user will receive a warning message or the notification regarding the blocked posts. The notification will be send to user mail.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

If the user has a wish to open the mail, he/she can switch into the mail and know what is there in the blocked content. They will not be displayed in the public wall.

VIII. CONCLUSION

Applications present convenient means for hackers to spread malicious content on Face book. However, little is understood about the characteristics of malicious apps and how they operate. A large corpus of malicious Face book apps observed over a 9-month period, we showed 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, and they typically request fewer permissions than benign apps. Leveraging our observations, we used a tool named FRAppE, an accurate classifier for detecting malicious Face book applications and blocked those apps. Most interestingly, we highlighted the emergence of app-nets—large groups of tightly connected applications that promote each other. We will continue to dig deeper into system of malicious apps on Face book, and we hope that Face book will benefit from our recommendations for reducing the menace of hackers on their platform.

IX. FUTURE ENHANCEMENT

Since we undergone the concept is all about posting and detecting applications on the Wall and the project has been designed keeping in mind the future scopes. A lot of tools can be used to shape many things in the future, thus this project will give rise to many future modifications focusing in all t he directions. The near future scope of this project is to block the images with offensive form of text and messages from the user wall.

REFERENCES

[1] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in Proc. ACSAC, vol -1, pp. 1–9, Dec 2010
[2] H. Gao et al., "Detecting and characterizing social spam campaigns," in Proc. IMC, vol- 3, pp. 35–47, Nov 2010.
[3] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. NDSS*, 2012.
[4] A. Le, A.Markopoulou, and M. Faloutsos, "PhishDef: URL names say it all," in *Proc. IEEE INFOCOM*, vol-1, pp. 191–195,2011.
[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in *Proc. IEEESymp. Security Privacy*, pp. 447–462, 2011.
[6] A. Makridakis *et al.*, "Understanding the behavior of malicious applications in social networks," *IEEE Netw.*, vol. 24, no. 5, pp. 14–19, Sep.–Oct. 2010.
[7] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in Proc. USENIX Security, vol -1, p. 32, Sep 2012
[8] Md S. Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michal's Faloutsos "FRAppE: Detecting Malicious Facebook Applications "vol-2, issue 3, Apr 2015
[9]C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *Trans. Intel. Syst. Technol.*, vol. 2, no. 3, 2011, Art. no. 27.