Investigating Hackers on Facebook Application using FRAppE

Asha Alias[1], **Rincy Varghese**[2], **Ritu. M. Varghese**[3]
[12&3]Department of Computer Science, visvesvaraya Technological University, Belgavi, Karnataka
Email: [1]ashaalias95@gmail.com, [2]rincyvgs@gmail.com , [3]ritu_varghese@yahoo.com
[*4]**Mr. V.M. Saravana Perumal**
[4]Assistant professor, Department of Computer Science, visvesvaraya Technological University, Belgavi, Karnataka
Email: [4]saran4umohan@gmail.com

ABSTRACT-There are millions of people who install the facebook application and third party apps are always the major problem for fame and addictiveness of Facebook. Thus hackers have known the strength of the apps for spreading the unwanted things. We have found that 15% of apps are malicious. Thus for the problem we have developed our contribution ....i.e. FRAppE (Facebook Rigorous Application Evaluator).FRAppE is to focus on the investigation of malicious apps on facebook.The behavioral sense of 111k Facebook apps in 2.6 million users were used to develop FRAppE. With 99.5% accuracy FRAppE can detect malicious apps with no false positives and a low false negative rate (4.1%).We have a group of features to identify the spam app from good apps. For app testing and ranking we see FRAppE as a step towards creating an independent watchdog that warn users on Facebook before installing apps.

Keywords –Benign apps, Facebook applications, Malicious apps, MyPageKeeper

I. INTRODUCTION

One of the most popular application which comes with its own advantages and disadvantages is Facebook. Such enhancement consist of interesting and enjoyable ways of communicating among online friends and it also include interesting games and listening to music .Now a days we can see that there are 500k apps are available on Facebook ,within that 40M apps [1]are installed everyday by the Facebook users. In addition many apps get acquired and maintain a sizable user.

Unfortunately recent evidence shows that, hackers have started deploying malicious apps [7, 9] can provide a lucrative business for hackers. Hackers can benefit from a malicious app in many ways. i) The app can obtain users personal information including password, email id, gender .ii)The app can spread spam in a large number of users. Here
the problem is, there are many malicious apps spreading on Facebook every day[6].

Today, the user has very limited information about the apps at the time of installing it on Facebook. That app may be malicious. This is an open gate for the hackers to obtain the personal information from users.

To protect the Facebook users from hackers, we develop FRAppE, a suite of efficient classification technique for identifying whether an app is malicious or not. To develop FRAppE, we use data available from MyPageKeeper, is a Facebook app [36] designed for detecting the malicious posts on Facebook. That will check the Facebook profiles of 2.2 million users. FRAppE (Facebook Rigorous Application Evaluator) is a tool which is mainly focused on detecting malicious apps on Facebook. It is an effective detection approach.
Following are our key contributions.

- *FRAppE can provide 99% accuracy in detecting malicious apps.*

We build FRAppE to detect the malicious app on Facebook using on-demand and aggregation based app information. By adding aggregation based information, FRAppE can discover malware apps with 99.5% accuracy with no false positive and lower false negative(4.1%).

- *The profile of spam and good apps is different.*

The malicious app profiles are significantly different from those of benign apps. Most of the malicious app have the same name. The benign app, that provides similar functionality.

- *15% of apps on facebook are detected as malicious.*

The evidence shows that around 15% of apps on Facebook are malicious .And 100k users each by convincing them to follow the links on the posts made by these apps.

II. OVERVIEW

Apps in facebook

Third party apps developers have rights in Facebook to offer services to the user. If the user installs the Facebook application to his profile ,the user allows the application server to access the permission to a set of details that the user have provide in his Facebook profile like email address and also permission to access the some action in behalf of user such as post on the wall. By handling O Auth 2.0 token, Facebook allows this permission to any applications, this token is allocated for each user who installs the facebook.fig 2.1 show how hackers make use of the malicious apps, the malicious apps are works as follows:

- Hackers promote the user to install the apps by giving some false rewards with some keyword ―Free‖, ―Real‖, ―Hurry‖.

- After installing the app it will provide the user a new web page where the users need to give some action regarding that reward such as complete task with false promises again.
- Then it will ask for personal information from profile.
- After that the app makes malicious post on this user‘s wall.

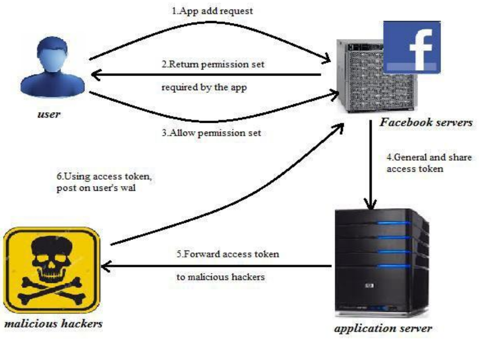

Figure 2.1 system design

MyPageKeeper.

MyPageKeeper[36] is a security app provided by facebook application. This MyPageKeeper discover the malicious posts on the the user‘s wall then apply url blacklisted as well as SVM classification technique to detect malicious apps. figure 2.2 shows the architecture design of the FRAppE.In existing system MyPageKeeper discovers only post of hackers with 97% high percentages of accuracy [28].

MyPageKeeper used Support Vector Machine (SVM) based classifier to discover whether the URL is malicious or benign. The classifier identifies the malicious post by taking some features consist of the presence of some keywords such as −click here‖ ,‖free‖, and −fast‖ and also by the resemblance of text messages and number of the likes and comments if the level of likes are lower than it is malicious. If the URL is found as malicious the all the post contains in that URL will be malicious,

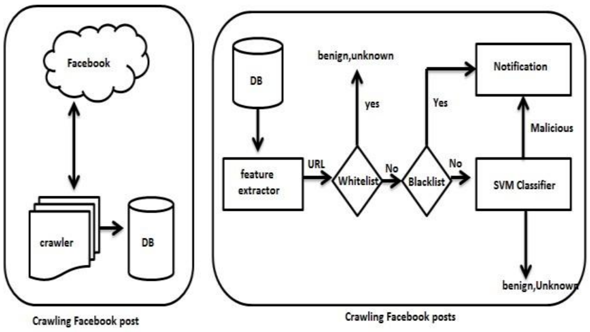

Fig 2.2 system architecture

Dataset

Over 2.2 millions install Facebook a day so Facebook apps have dataset from 2.2M Facebook user. Which has be followed by MyPageKeeper. This dataset consist of 124M posts from 2.2M walls which followed by by MyPageKeeper [13]. By investigating the faceboook, Post over 9 months from June 2013 to March 2014. This 124M post is made by 111K apps.

In the investigation we have to give some sample dataset they are by:

- Discovering malicious applications if any post has found as malicious so the application which that post has made can mark as malicious post[6].

  In several investigating we found −Death predictor‖ user also marked as malicious . this use already describes that addictiveness of facebook users. To prevent those kind of misuses, we used whitelist to classify the benign apps from URL. After whitelisted we left 6,273 malicious applications
- We also investigated about apps permission to be granted inorder to installs the application.All the application which are licensed is provided with an app_id(*httpd://www.facebook.com/apps/graph_apps?id=app_id).*By crawling all the apps this URL has been checked and detect the benign and malicious apps.

III. WIDESPREAD OF MALICIOUS APPS

The factor for identifying malicious apps and the main reason of it is that the malicious pots are posted by these apps on facebook.53% of malicious posts by MyPageKeeper was posted by malicious apps.

There are two different ways of widespread of malicious apps:-

(i) 100 thousand clicks on the URL‘s posted are got by 60% of malicious apps.

We determine the number of clicks for malicious apps on the links which are the malicious post .For the malicious apps in D-Sample dataset, we reach all bit-ly URL‘s in posts. We observe more onbit-ly UPL‘s since bit-ly offers an API[18] for receiving number of clicks is lower bound. Even bit-ly link will receive clicks from various other sources outside facebook.For this purpose for the total number of clicks received in bit-ly URL ,is an upper bound and it is done through facebook. Almost 6,273 malicious apps in D-Sample dataset, it is known that 3,805 of the apps has posted 5,700 bit-ly URL‘s in total.

We usually observe and query bit-ly for the click count in each URL.60% of malicious apps cover over 100k clicks in which 1M clicks are received by 20% each,The most eye catching was the one with 1.742,359 clicks i.e :What is the sexiest thing about you?‖.

*(ii)*There is a median of 40% malicious apps with 1000 monthly active users.

By inspecting number of users on facebook we examine the malicious apps.In order for the above study we use Monthly Active Users (MAU) provided by facebook for every app. We found that 40% of malicious application had a median MAU of atleast 1000 users, and 60% of malicious application achieved 1000 during three month observation.

One of which it became famous was −Future Teller‖ which had maximum MAU of 260,000 and median of 20,000.

a. Posting direct links to other apps.

We find 692 promoter apps in our D-Sample dataset which promoted 1,806 different apps using direct links. The activity was intense :15% of the promoters promoted atleast 5 promote apps .For example, _The App‘ was promoting 24 other apps with names _The App‘ or _La App‘.

b. Indirect app promotion:

Hackers have started using websites outside facebook to have promotion of apps. We can know the malicious apps as they contain shortened URL. If the problem from URL is identified and solved it directly points to the other website forward users to different app installation pages.

IV. PROBLEM DEFINITION

From our observations we find that malicious app are on Facebook. Our next step is to build a tool that must identify malicious content on Facebook. To develop a tool like FRAppE, we should analyze and compare the various features of malicious and benign apps. There are two divisions of features: on-demand features and aggregation based features.

On-demand features

The on-demand features comes with an application, which tells that one can obtain the on-demand feature given the application's ID. such metrics consist of name of the app, description, company, category and permissions.

Application summary

Malicious apps have incomplete application summary. In the first step, we compare malicious and benign apps with respect to application present in the application‘s summary such as app description, company name and category. Only 1.4% of malicious apps have a non empty description, whereas 93% of benign app configures their summary with a description.

***Required* permission set**

97% of malicious apps require only one permission from users. Every Facebook application requires the authorization from the user before using it. And every app requests the user to provide the set of permission at time of installation. These permissions are chosen from a pool of 64 permissions pre-defined by Facebook.

Redirect URI

Malicious app redirect user to domains with poor reputation. In an application's installation URL, the redirect URL parameter refers to the URL where the user is redirected to once she/he installs the app. We extracted the redirect URI parameter from the installation URL for apps in the D-Inst dataset and queried the trust reputation score for these URIs from WOT [8].

Aggregation-based features

Now, we analyze applications with respect to aggregation -based features. Unlike the features we considered in on - demand features. we considered so far, aggregation based features for an app cannot be obtained on-demand. Here we envision that aggregation -based features are assembled by entities that will check the posting behavior of various application across users.

App name

85% of malicious apps have an app name identical to that of at least one other malicious app. An application‘s name is fixed by the app developer at the time of the creation of that app .And every app has a unique app ID, Facebook does not impose any restrictions on app names. So it is possible to create multiple apps with the same app name.

External link to post ratio

Malicious app often post links pointing to domains outside Facebook , whereas benign apps rarely do so. Every post on facebook include an URL. These URL may be made by malicious or benign apps. We can see that 80% of benign apps do not post any external links, whereas 40% of the malicious apps have one external link on average per post. This shows that malicious apps attempt to lead users to web pages hosted outside facebook, whereas the links posted by benign apps are almost always restricted to URLs in the facebook.com domain.

V. INVESTIGATING HACKERS ON FACEBOOK

We have classified the hackers apps which is malicious and benign apps, we have 2 variants to this classifier they are FRAppE lite and FRAppE. The security apps of Facebook that is MyPageKeeper only discover the malicious post and links but not the apps. These two variants of classifier is designed to discover the malicious apps.

FRAppE lite

This lightweight version will only make use the application feature of On-Demand. On-Demand specifies with respect to the app_id and FRAppE lite crawls the application with respect to these On-Demand features.

We use SVM [15] classifier to classify the hackers and benign. The FRAppE lite will be giving the accuracy 99.0%, with low false positive (0.1%) and false negative(4.4%) accuracy is defined as the ratio of truly identified apps which benign or malicious , false positive rate is fraction of benign apps incorrectly as malicious.

FRAppE

There are 2 features used to classified the malicious apps and benign apps, this FRAppE uses the aggregation based features with the On-Demand features that it‘s lightweight version only uses the On-Demand feature. Aggregation based feature of an app which consist a cross user and cross-app view with time.

FRAppE which gives the accuracy with 99.5% and with 4.1% of false negative rate also it doesn‘t contain any false positive. We invent FRAppE which is used in Facebook and also secure from third party application of millions of users

Ways to discuss New Hackers

We used to crawl all the posts, links and apps in the user‘s wall to do so we apply FRAppE to all URLs. If any new apps has discovered it will discover the malicious URL by using different ways they are

1. Facebook used to keep checking the hackers in Facebook application then it discover and disables from the wall by using the graph which contains the malicious app list. This has done by API in Facebook (https://graph.facebook.com /appId) which returns false for a malicious app because its return false because it‘s not exist in the Facebook dataset. This process of FRAppE can be done with 87% of accuracy.

2. In other ways we can check for similarity in the name of apps. If more number of apps seems similar with a malicious app then that apps can be taken as malicious. Otherwise some names can be given as similar but at end of that name they could give the version number that also

can take as malicious apps this is also a valid technique to find the malicious apps with FRAppE. Also we can check for the similarity in the link URL. If the posted link name is similar to the malicious URL, so easily we can identify the malicious apps.

3. At last, we are left with 157 apps that has not identified by the above technique. That apps could verified manually like check one by one and can be identified by using the similarity among this apps and can be identified more than 112 apps which is malicious using FRAppE.

VI.SOCIAL MALWARE ECOSYSTEM

By using FRAppE, we discover the harmful apps , after that we check the several ways how the social malware support each other. From our observation we find the interesting thing that malicious apps do not operate in segregation they share the same name and their work must collaboratively in encouraging each other.

- The emergent‘s of AppNets

We observed that more than 6,330 malicious apps in our dataset that emerge in collaborative promotion. In that 2.5% are promoters,58.8% are promotes, and the remaining 16.2%play both roles.

- Piggybacking

The app piggybacking is a approach in which hackers are using this. The facebook‘s API and there post are harmful post by using popular apps. There are several ways that hackers are benefited by this. The hackers make the user to share the harmful post by offering rewards. They crawl the API from Facebook by hacking the users account; they again post the harmful app in the user‘s wall. By the app in the request to post the harmful post. The Facebook could not recognize this because the app ID is already included in the appID.

In our dataset we identify the piggyback that is each app has atleast one malicious post according to myPageKeeper and we will check for the apps which is having low rates and we found that 80% apps have harmful posts to all posts rate i.e less than 0.4.

VII.CONCLUSION

Here we propose of how safeguard Facebook users from hackers. Using this paper we can understand the significant characteristics of malicious apps and how they operate. In this work we find that atleast 15 % of apps on our dataset are malicious. Malicious apps are differing from benign ones. That is most of the malicious apps have similar name. Profiling each of our observations, we designed FRAppE, a correct classifier for detecting malicious apps on Facebook. To develop FRAppE we use information gathered by observing the posting behavior of 111k Facebook apps seen across 2.2 million users on Facebook. We identify a set of features that help us to distinguish malicious apps from benign ones. And finally we explore the ecosystem of malicious Facebook apps and identify mechanism that these apps use to propagate. We will continue to investigate on hackers platform dig deep into their ecosystem to reduce the malicious app on Facebook.

ACKNOWLEDGEMENTS

This work was supported in part by grants from the Mr R Balakrishna(Principal) of Rajarajeswari College of Engineering ,Bengaluru and Dr.Usha Sakthivel (H.O.D) of Rajarajeswari College of Engineering ,Bengaluru. This work was also supported by grants from our Asst.Prof.Mr.V.M.Saravana Perumal (Project Guide) of Rajarajeswari College of Engineering, Bengaluru who helped during various stages of preparations and also provided valuable feedback for guidance

REFERENCES

[1] C. Pring, ―*100 social media statistics for 2012*,‖ 2012 [Online]. Available:http://thesocialskinny.com/100-social-media-statistics-for-2012

[2] Facebook, Palo Alto, CA, USA, ―*Facebook Opengraph API*,‖ [Online]. Available: http :/ / developers. f a cebook..com/docs/reference/api/

[3] ―*Wiki: Facebook platform*,‖ 2014 [Online]. Available: http://en wikipedia.org/wiki/Facebook_Platform

[4] ―*Whiich cartoon character are you*—*Facebook survey scam*,‖ 2012 [Online]. Available: https://appsn.face book.com/ mypagekeeper/?status= sca m _ report_fb_survey_scam_whiich_ cartoon_character_are_you_2012_03_30

[6] E. Protalinski, ―*Facebook kills app directory, wants users to search for apps*,‖ 2011 [Online]. AvaI lable: http://zd.net/MkBY9k

[7] SocialBakers, ―SocialBakers: The recipe for socIal ma arketing success,‖ [Online]. Available: http://www.socialbakers.com/

[8] ―*Selenium*—*Web browser automation*,‖ [Online]. Ava ilable:http://seleniumhq.org/

[9] ―bit.lyAPI,‖2012[Online].Available: http://code.g oogle.com/p/bitlyapi/wiki/ApiDocumentation

[10] Facebook, Palo Alto, CA, USA, ―*Permissions r e f e r ence*,‖ [Online].Available: https://developers. facebook.com/docs/authentication/ permissions/

[11] Facebook, Palo Alto, CA, USA, —*Facebook develope ers*,‖ [Online].Available: https://developers.facebook . com/docs/appsonfacebook/tutorial/

[12] –*Web-of-Trust,*‖ [Online]. Available: http://www.mywt.com/

[13] F. J. Damerau, –*A technique for computer detection and correction of spelling errors*,‖ *Commun. ACM*, vol. 7, no. 3, pp. 171–176,Mar. 1964.

[14] C.-C. Chang and C.-J. Lin, –*LIBSVM: A library for support vector machines,*‖ *Trans. Intell. Syst. Technol.*, vol. 2, no. 3, 2011, Art. no. 27.

[15] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, –*Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs,*‖ in *Proc. KDD*, 2009, pp. 1245–1254.

[16] A. Le, A.Markopoulou, and M. Faloutsos, –*PhishDef: URL names say it all*,‖ in *Proc. IEEE INFOCOM*, 2011, pp. 191–195.

[17] C. Wueest, –*Fast-flux Facebook application scams*,‖ 2014 [Online].Available:http://www.symantec.com/ connect/blogs/fast-fluxfacebook- application-scams

[18] –*Longest path problem,*‖ 2014 [Online]. Available: http://en.wikipedia. org/wiki/Longest_path_problem

[19] –*App piggybacking example,*‖ [Online]. Available: https://apps:Facebook.Com/mypagekeeper/?status=scam _report_fb_survey_scam_Converse_shoes_2012 _05_17_boQ

[20] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, *Design and evaluation of a real-time URL spam filtering service*,‖ in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 447–462.

[21] S. Lee and J. Kim, –*WarningBird: Detecting suspicious URLs in Twitter stream*,‖ in *Proc. NDSS*, 2012.

[22] C. Yang, R. Harkreader, and G. Gu, –*Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers*,‖ in *Proc. RAID*, 2011, pp. 318–337.

[23] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almida, –*Detectin spammers on Twitter*,‖ in *Proc. CEAS*, 2010, pp. 1–9.

[24] G. Stringhini, C. Kruegel, and G. Vigna, –*Detecting spammers on social networks*,‖ in *Proc. ACSAC*, 2010, p.1–p 9.

[25] K. Lee, J. Caverlee, and S.Webb, –*Uncovering social spammers: Social honeypots + machine learning*,‖ in *Proc. SIGIR*, 2010, pp. 435–442.

[26] S.Yardi, D.Romero, G.Schoenebeck,and D.Boyd, ―*Detecting spamin a twitter network*,‖*First Monday*, vol. 15,no.1,2010[Online]

[27] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek, –*Social Applications;Explorin a more secure frame work*,‖ in *Proc. SOUPS*, 2009,Art. no. 2.

[28] N. Wang, H. Xu, and J. Grossklags, –*Third-party apps on Facebook:Privacy and the illusion of control* ,‖ in *Proc. CHIMIT*, 2011, Art. no.4

[29] 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.

[30] J. King, A. Lampinen, and A. Smolen, ―*Privacy: Is there an app for that?,*‖ in *Proc. SOUPS*, 2011, Art. no. 12.

[31] M. Gjoka, M. Sirivianos, A. Markopoulou, and X. yang , –Poking *Facebook: Characterization of OSN applications*,‖ in *Proc. 1st WOSN*, 2008, pp. 31–36.

[32] T. Stein, E. Chen, and K. Mangla, –*Facebook immune system*,‖ in *Proc. 4th Workshop Social Netw. Syst.*, 2011, Art. no. 8.

[33] L. Parfeni, ―*Facebook softens its app spam controls, Introduces better tools for developers*,‖ 2011 [Online]. Available: http://bit.ly/LLmZpM

[34] ―*Norton Safe Web*,‖ [Online]. Available: http ://www .facebook.com/ apps/application.php?id= 310877173418