Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 1, January -2016

Detection of Malicious App. Through FRappE Classifier

Prof.Nilesh Deshmukh[1], Shahbaz Naveed[2], MD Sufiyan[3], Mohsin Farooqui[4], Pathan Mujtaba[5]

[1,2,3,4,5]*Pad. Dr. D.Y. Patil Institute of Engineering & Technology*

Abstract *— In Online Social Networking (OSN), With 20 million installs a day, third-party apps are a major reason for the popularity and addictiveness of Facebook (OSN). Unfortunately, hackers have realized the potential of using apps for spreading malware and spam which are harmful to facebook users. The problem is already significant, as we find that at least 13% of apps in our dataset are malicious. So far, the research community has focused on detecting malicious posts and campaigns.In this project, we ask the question to the facebook user that, given a Facebook application, can you determine whether that application is malicious? Of course that user couldn't identify that. So, our key contribution is in developing "FRAppE—Facebook's Rigorous Application Evaluator", arguably the first tool focused on 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. First, we identify a set of features that help us distinguish between malicious apps and benign apps. For example, we find that malicious apps often share names with other apps, and they typically request few permissions than benign apps. Second, leveraging these distinguishing features, we show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a low false negative rate (4.1%). Finally, we explore the ecosystem of malicious Facebook apps and identify mechanisms that these apps use to propagate. Interestingly, we find that many apps collude and support each other; in our dataset, we find 1,584 apps enabling the viral propagation of 3,723 other apps through their posts. Long-term, we see FRAppE as a step towards creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.*

Keywords:- Online social networks, Spam, Malicious Campaigns, Security and Protection : Access controls, Verification.

I. INTRODUCTION

Online social networks (OSN) enable and encourage third party applications to enhance the user experience on these platforms like FACEBOOK. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app integration into the Facebook user-experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a large user base. We have observed that , FarmVille and CityVille apps have 26.5M and 42.8M users to date. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users.

A. FRAppE Lite: FRAppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FRAppE Lite crawls the on-demand features for that application and evaluates the application based on these features in real time. We envision that FRAppE Lite can be incorporated, for example, into a browser extension that can evaluate any Facebook application at the time when a user is considering installing it to her profile. All of these features can be collected on demand at the time of classification and do not require prior knowledge about the app being evaluated. We use the Support Vector Machine (SVM) classifier for classifying malicious apps. SVM is widely used for binary classification in security and other disciplines.

We use accuracy, false positive (FP) rate, and true positive (TP) rate as the three metrics to measure the classifier's performance. Accuracy is defined as the ratio of correctly identified apps (i.e., a benign/malicious app is appropriately identified as benign/malicious) to the total number of apps. False positive rate is the fraction of benign apps incorrectly classified as malicious, and true positive rate is the fraction of benign and malicious apps correctly classified (i.e., as benign and malicious, respectively).

II. LITERATURE REVIEW

1) Detecting and Characterizing Social Spam Campaigns

Authors: Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao.

Description:

In this paper, authors presented an initial study to quantify and characterize spam campaigns launched using accounts on online social networks. They studied a large anonymized dataset of asynchronous "wall" messages between Facebook users. We analyze all wall messages received by roughly 3.5 million Facebook users (more than 187 million messages in all), and use a set of automated techniques to detect and characterize coordinated spam campaigns. System detected roughly 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that more than 70% of all malicious wall posts advertise phishing sites.

They study the characteristics of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts created solely for the purpose of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post activity in the early morning hours, when normal users are asleep.

2) **Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals**

Authors: Pern Hui Chia, Yusuke Yamamoto, N. Asokan

Description:

Third-party applications (apps) drive the attractiveness of web and mobile application platforms. Many of these platforms adopt a decentralized control strategy, relying on explicit user consent for granting permissions that the apps request. Users have to rely primarily on community ratings as the signals to identify the potentially harmful and inappropriate apps even though community ratings typically reflect opinions about perceived functionality or performance rather than about risks. With the arrival of HTML5 web apps, such user-consent permission systems will become more widespread. We study the effectiveness of user-consent permission systems through a large scale data collection of Facebook apps, Chrome extensions and Android apps. The analysis confirms that the current forms of community ratings used in app markets today are not reliable indicators of privacy risks of an app. We find some evidence indicating attempts to mislead or entice users into granting permissions: free applications and applications with mature content request more permissions than is typical; "lookalike" applications which have names similar to popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

3) **LIBSVM: A Library for Support Vector Machines.**

Authors: Chih-Chung Chang and Chih-Jen Lin

Description:

LIBSVM is a library for Support Vector Machines (SVMs). Authors have been actively developing this package since the year 2000. The goal is to help users to easily apply SVM to their applications. LIBSVM has gained wide popularity in machine learning and many other areas. In this, authors presented all implementation details of LIBSVM. Issues such as solving SVM optimization problems, theoretical convergence, multi-class classification, probability estimates, and parameter selection are discussed in detail. Support Vector Machines (SVMs) are a popular machine learning method for classification, regression, and other learning tasks. LIBSVM is currently one of the most widely used SVM software.

4) **Social Applications: Exploring A More Secure Framework**

Authors: Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek

Description:

Online social network sites, such as MySpace, Facebook and others have grown rapidly, with hundreds of millions of active users. A new feature on many sites is social applications applications and services written by third party developers that provide additional functionality linked to a user's profile. However, current application platforms put users at risk by permitting the disclosure of large amounts of personal information to these applications and their developers. This paper formally abstracts and defines the current access control model applied to these applications, and builds on it to create a more secure framework. We do so in the interest of preserving as much of the current architecture as possible, while seeking to provide a practical balance between security and privacy needs of the users, and the needs of the applications to access users' information. We present a user study of our interface design for setting a user-to-application policy. Our results indicate that the model and interface work for users who are more concerned with their privacy, but we still need to explore alternate means of creating policies for those who are less concerned.

III. SURVEY OF PROPOSED SYSTEM

Currently, malicious apps often do not include a category, company, or description in their app summary. To detect the malicious facebook applications which may affects to user's private information on his/her profile. As we see user did not get much information about application expect name of that application while installing as a result no security available on facebook.

Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications which can provide a lucrative business for hackers, given by the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app. To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day.

IV. MATHEMATICAL MODEL

Let S is the Whole System Consists:

S = {U, P, Req, A, APP}.

1. U is the set of number of user on the facebook.

   U={u1,u2,……..un}.

2. P is the set of number of permission set for user .

   P={p1,p2,……pn}.

3. Req is set of number of add app request from user to server.

   Req={a1,a2,……an}.

4. A is the set of number of set of access tokens of user.

5. APP is the set of number of facebook benign application available on facebooks application server.

   APP = {ap1,ap2,……apn}.

Step 1: At first user sends request to facebook server for adding an application to his profile like some game app etc.

Step 2: When request comes to facebook server from client it returns the one set which contains the permissions required to app which he want to install on his profile , permissions like , Application wants to access user information from profile like name, date of birth etc. and this token are send to application server.

Step 3: In this step user allow the access the information from his profile to that particular app, Here user doesn't aware that whether that app is benign or malicious so, here our FRAppE comes in picture. FRAppE checks whether that app is malicious or benign by applying some classifications such as FRAppE Lite and FRAppE.

FRAppE Lite: This is the initial level detection or classifier i.e. FRAppE Lite checks the application ID no, name and location of application and verifies with the available benign application in the application server.

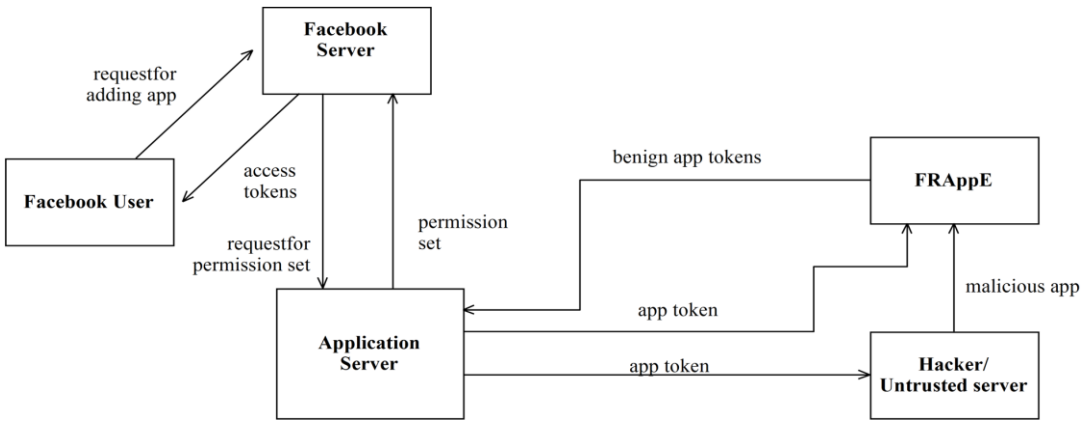
FRAppE: This is actual step of detecting the malicious apps in the facebook. If an application is found malicious then that application will be blocked for all the users so, that in future users don't get request from that application to add.

Step 4: In this step, the FRAppE allows only the benign apps to add on user's wall.

Output: Detecting malicious apps and providing access to only benign apps to user.

.

V. SYSTEM ARCHITECTURE



.

VI. METHODOLOGIES OF PROBLEM SOLVING

1) Detecting malicious apps:-
   In this module we are analyzing the different characteristics of malicious and benign apps,
2) Identifying New Malicious Apps:
   We next train FRAppE's classifier on the entire D-Sample dataset i.e. for which we have all the features and the ground truth classification and use this classifier to identify new malicious apps.
3) Background on App Cross Promotion:-
   Cross promotion among apps, which is forbidden as per Facebook's platform policy, happens in two different ways. The promoting app can post a link that points directly to another app, or it can post a link those points to a redirection URL, which points dynamically to any one of a set of apps.
4) App Collaboration:-
   Next, we attempt to identify the major hacker groups involved in malicious app collusion. For this, we consider different variants of the "Campaign graph" as follows.
5) Hosting Domains:-
   We investigate the hosting domain that enables redirection Web sites. First, we find that most of the links in the posts are shortened URLs, and 80% of them use the bitly shortening service.

VII. CONCLUSION AND FUTURE WORK

An application presents a convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In this project, using a large corpus of malicious Facebook apps observed over a nine 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 few permissions than benign apps. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of AppNets large groups of tightly connected applications that promote each other.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

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.facebook.com/docs/reference/api/
[3] "Wiki: Facebook platform," 2014 [Online]. Available: http://en. wikipedia.org/wiki/Facebook_Platform
[4] "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report- _fb_survey_scam_pr0file_viewer_2012_4_4
[5] "Whiich cartoon character are you—Facebook survey scam," 2012 [Online]. Available: https://apps.facebook.com/ mypagekeeper/?status=scam_report_fb_survey_scam_whiich_ cartoon_character_are_you_2012_03_30
[6] G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/ 27/pink-facebook-survey-scam/
[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/ index.htm
[8] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI
[9] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5
[10] 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*, 2012, p. 32.
[11] H. Gao *et al.*, "Detecting and characterizing social spam campaigns," in *Proc. IMC*, 2010, pp. 35–47.
[12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. NDSS*, 2012.

