International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 1, January-2016

FRAppE Detecting Malicious Facebook Applications

Rohini Lokare[1], Khushi Kumari[2], Urvashi Yadav[3], Suhasini Borge[4], Prof. D. V. Shinkar[5]

[1,2,3,4,5]Information Technology Department, JSPM's Bhivarabi Sawant Institute of Technology and Research, (Affiliated to Savitribai Phule Pune University) Pune, India

ABSTRACT

Nowadays use of social networking site like Facebook, Twitter, Google+ for communication and maintaining relationship among various user is increased due to its popularity on network. Each user that uses the social networking sites are making profiles and uploading their private information. These social networks users are not aware of numerous security risk included in this networks like privacy, identity stealing and erotic harassment and so on. The third party apps on social sites have main role to make the site more attractive and incredible. The hackers are using these third party apps to get the private information and get unlawful access to their accounts. As we aware that not most but least of the applications on sites are malicious. As research goes on the research community has focused on detecting malicious wall-posts and campaigns. In this paper, we are going to find that applications are malicious or not? In earlier system, It is important to note that My Page-Keeper that is our base data, cannot detect malicious apps; it only detects malicious posts on Facebook. Though malicious apps comprises the bunch of malicious posts. In contrast, FRAppE Lite and FRAppE are designed to detect malicious apps. Therefore the FRAppE or FRAppE Lite that is being developed is more controlling than My Page-Keeper To develop FRAppE, we use information collected by observing the posting behaviour of basic Facebook apps that are running on it. So, First we try to find out the features of malicious apps and another characteristics of malicious apps that are harmful to users.

Keywords: Facebook Apps, Malicious Apps, Profiling Apps, Online Social Network.

1. INTRODUCTION

Online social networks (OSN) enable and encourage third party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of collaborating 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 . 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 .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 ,and (c) the app can "re-produce" by making other malicious apps popular. Despite the above worrisome trends, today, a user has very limited information at the time of installing an app on Facebook. In other words, the problem is: given an app's uniqueness number (the unique identifier assigned to the app by Facebook), can we detect if the app is malicious? Currently, there is no commercial service, publicly-available information, or research-based tool to advise a user about the risks of an app. Malicious apps are widespread and they easily spread, as a diseased user endangers the safety of all its friends. Most research related to spam and malware on Facebook has focused on detecting malicious post sand socials pam crusades. In this work, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from My Page Keeper, a security app in Facebook thatmonitorstheFacebookprofilesof2.2million users.

Our work makes the following key contributions:

• **Malicious and benign app pro files significantly differ**: We systematically profile apps and show that malicious app profiles are significantly different than those of benign apps. A striking comment is the "laziness" of hackers; many

malicious apps have the same name, as 8% of unique names of malicious apps are each used by more than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) those that can be obtained on-demand given an application's identifier (e.g., the permissions required by the app and the columns in the application's profile page), and (b) others that require a cross-user view to aggregate information across time and across apps (e.g., the posting behavior of the app and the similarity of its name to other apps).

• **The appearance of App Nets: apps collude at massive scale.** We conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used to promote malicious apps. The most stimulating result is that apps collude and collaborate at a massive scale. Apps promote other apps via posts that point to the "promoted" apps.

• **Malicious hackers mimic applications**. We were surprised to find popular good apps, such as 'FarmVille' and 'Facebook for iPhone', posting malicious posts. On further investigation, we found a lax authentication rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

• **FRAppE can detect malicious apps with 99% accuracy**. We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps either using only landscapes that can be obtained on-demand or using both on-demand and aggregation based app information. FRAppE Lite, which only uses information available on-demand, can identify malicious apps with 99.0% accuracy, with low false positives (0.1%) and false negatives(4.4%). By adding aggregation-based information, FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and lower false negatives (4.1%).

2. BACKGROUND

In this section, we discuss how applications work on Facebook, provide an overview of My Page Keeper (our primary data source), and summary the datasets that we use in this paper

▪ FACEBOOK APPS

Facebook enables third-party developers to offer services to its users by means of Facebook applications. Unlike typical desktop and smart phone applications, connection of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a worker adds a Facebook application to her profile, the user grants the application server: (a) authorisation to access a subset of the information listed on the user's Facebook profile (e.g. the user's email address), and (b) permission to perform certain actions on behalf of the user (e.g., the ability to post on the user's wall). Facebook grants these permissions to any application by handing an O Auth 2.0 [4] token to the application server for each user who installs the application. Thereafter, the application can access the data and perform the explicitly-permitted actions on behalf of the user. Fig. 1 depicts the steps involved in the installation and process of a Facebook application.

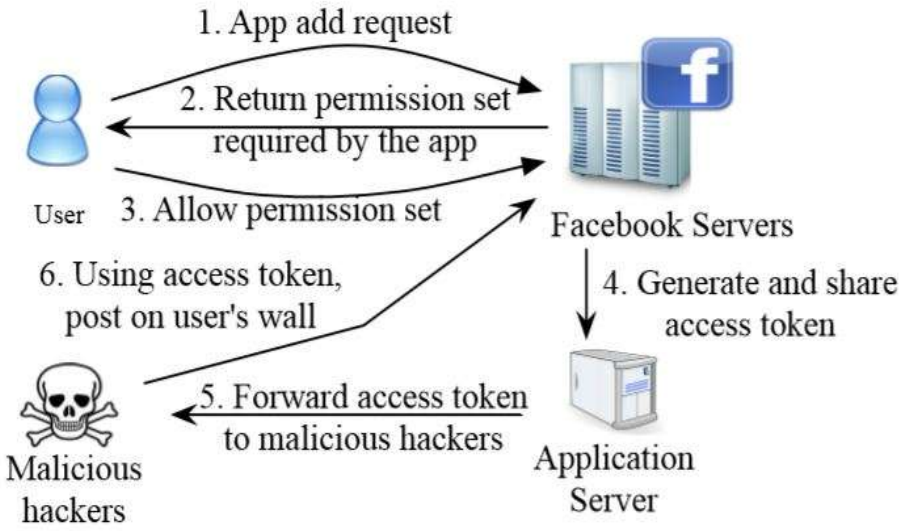

Fig 1: Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims' walls.

Operation of malicious applications: Malicious Facebook applications typically operate as follows.

• Step 1: Hackers prove users to install the app, usually with some fake promise (e.g., free iPads).

• Step 2: Once a user installs the app, it redirects the user to a web page where the user is requested to achieve tasks, such as completing a survey, again with the lure of fake rewards.

• Step 3: The app thereafter accesses personal information (e.g., birth date) from the user's profile, which the hackers can hypothetically use to profit.

• Step 4: The app makes malicious posts on behalf of the user to lure the user's friends to install the same app .
This way the cycle continues with the app or colluding apps reaching more and more users. Private information or surveys can be "sold" to third parties to eventually profit the hackers.

- **MYPAGEKEEPER**

My Page Keeper is a Facebook app designed for sensing malicious posts on Facebook. Once a Facebook user installs My Page Keeper, it periodically crawls posts from the user's wall and news feed. My PageKeeper then applies URL blacklists as well as custom classification techniques to identify malicious posts. The key thing to note here is that My PageKeeper identifies social malware at the granularity of discrete posts, without grouping together posts made by any given application. In other words, for every post that it crawls from the wall or news feed of a promised user, My Page Keeper's determination of whether to flag that post does not take into version the application accountable for the post. Indeed, a large fraction of posts (37%) monitored by My PageKeeper are not posted by any application; many posts are made manually by a user or posted via a social plug-in (e.g., by a user clicking 'Like' or 'Share' on an external website). Even among malicious posts identified by My PageKeeper, 27% do not have an associated claim. My PageKeeper's classification primarily relies on a Support Vector Machine (SVM) based classifier that evaluates every URL by combining information obtained from all posts containing that URL. Examples of features used in My PageKeeper's classifier include a) the presence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts comprising the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like' sand comments). Once a URL is identified as malicious, My PageKeeper symbols all posts containing the URL as malicious.

- **OUR DATASET**

  - The D-Sample dataset: Finding malicious applications. To identify malicious Facebook claims in our dataset, we start with a simple heuristic: if any post made by an application was flagged as malicious by My Page Keeper, we mark the application as malicious, we find this to be an effective technique for identifying malicious apps.
  - The D-Sample dataset: Including benevolent applications. To select an equal number of benign apps from the initial D-Total dataset, we use two criteria: (a) none of their posts were identified as malicious by My PageKeeper, and (b) they are "vetted" by Social Bakers, which monitors the "social marketing success" of apps.
  - The D-Summary dataset: Apps with app summary. We amass app summaries through the Facebook Open graph API, which is made available by Facebook at a URL facebook has a unique identifier for each application. An app summary includes several pieces of information such as application name, description, company name, profile link, and monthly active users. If any application has been removed from Facebook, the query results in an error.
  - The D-Profile Feed: Posts on the app profile. Users can make posts on the profile page of an app, which we can call the profile feed of the app. We collect these posts using the Open graph API from Facebook. The API returns posts appearing on the application's page, with several characteristics for each post, such as message, link, and create time

- Coverage: While the emphasis of our study is to highlight the differences between malicious and benign apps and to develop a sound methodology to detect malicious apps, we cannot aim to detect all malicious apps contemporary on Facebook. This is because My PageKeeper has a limited view of Facebook data—the view provided by its subscribed users—and therefore it cannot see all the malicious apps present on Facebook.
- Data privacy: In possession with Facebook's policy and IRB requirements, data collected by My PageKeeper is kept private, since it crawls posts from the walls and news feeds of users who have explicitly given it permission to do so at the time of My PageKeeper connection. In addition, we also use data obtained via Facebook's open graph API, which is publicly accessible to anyone.

3. PROBLEM DEFINITION

Social Malwares are out of control on social networks, Cyber Attacks jumps 81 percent on social networks. 83 millions of accounts are fake and duplicate. Therefore discovering the malicious apps on OSNs is become a major issue. So we are implementing the system to detect malicious applications on social networks.

4. PROPOSED SYSTEM

In this work, we develop FRAppE, a suite of effectual classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from My PageKeeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyze 111K apps that made 91 million posts over nine months. This is arguably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and empathetic malicious apps, and synthesizes this information into an effective detection approach.

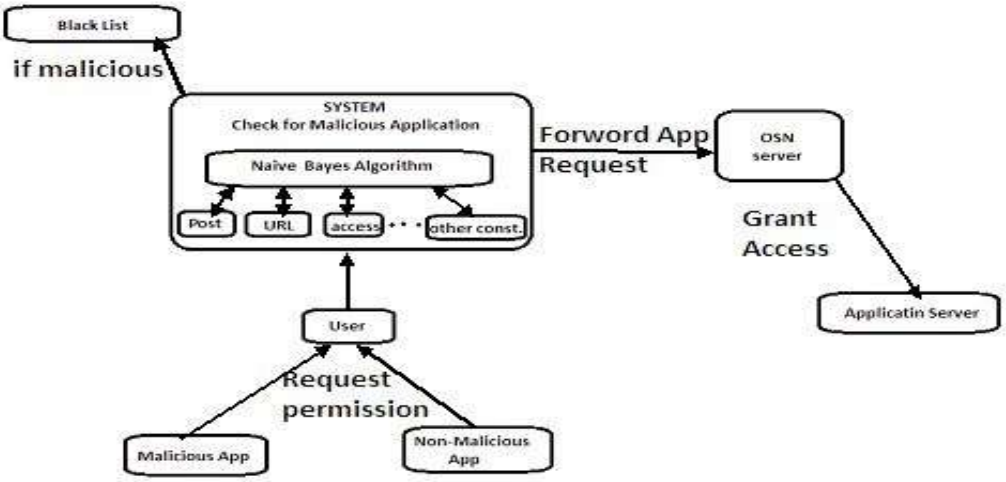

Fig 2: Architecture diagram

The architectural design elaborate about what the actual system is. As shown in diagram Our system will detect weather the submission is malicious or not By using naïve bayes classifier algorithm .As shown in fig App is popped to user and user gives request to server to use this app but before this request is going to proceed we will check whether the application is malicious or not by applying constraints on app (constraints such as is that app have suspicious redirecting url?, app post contents, app close functions etc.). otherwise it will pass that app request to server. Then server gives authorization to user to access that app.

CONCLUSION AND FUTURE SCOPE

Applications present a convenient means for hackers to spread malicious happy on Facebook. However, little is tacit about the characteristics of malicious apps and how they operate. In this work, using a large body of malicious Facebook apps observed over a nine month dated, we exhibited 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 explanations, we developed FRAppE, an correct classifier for detecting malicious Facebook applications. Most interestingly, we painted the emergence of App Nets— large groups of tightly connected applications that promote each other. We will continue to dig deeper into this system of malicious apps on Facebook, and we optimism that Facebook will benefit from our endorsements for reducing the menace of hackers on their podium.

REFERENCES

[1] Facebook Open graph API. http://developers. facebook.com/docs/reference/api/.
[2] My PageKeeper. https://www.facebook.com/ apps/application.php?id=167087893342260.
[3] Profile stalker: rogue Facebook application. https://apps.facebook.com/mypagekeeper/ ?status=scam_report_fb_survey_scam_ pr0file_viewer_2012_4_4.
[4] Which cartoon character are you - rogue Facebook application. https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30

[5] P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? a large scale study on application permissions and risk signals. In WWW, 2012.
[6] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 2012.
[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In IMC, 2010.
[8] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos. Efficient and Scalable Socware Detection in Online Social Networks. In USENIX Security, 2012.