ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

FRAPPE-For Identifying Malicious Facebook Application

C. Gowdham[1], A.Anusha[2], M.Gayathri[3]

Assistant Professor, Department of CSE, Karpaga Vinayaga College of Engineering and Technology, Chennai, India[1]

UG Students, Department of CSE, Karpaga Vinayaga College of Engineering and Technology, Chennai, India[2,3]

ABSTRACT: Many users use third-party apps that is the important reason for the popularity and addictiveness of facebook. These dayshackers have realized the potential of using apps for spreading malware and spam. Now a days the research community has eyed on identifying malicious posts and campaigns. Our key contribution is in evaluatingFRAPPE—facebook's Rigorous Application Evaluator to find the first tool focused on detecting malicious apps on social network. To evaluate FRAPPE, we use information gathered by observing the behavior of facebook apps seen across many million users on facebook. In this we identify a set of features that help us determine malicious apps from old ones. For example, we find that malicious apps frequently share names with other apps, and they typically request fewer permissions than old apps. In the next method leveraging these distinguished features, we determine that FRAPPE can detect malicious apps with their accuracy, with no false positives and a high true positive rate . At last we burst the ecosystem of harmfull facebook apps and detecting mechanisms that these apps use to propagate. Eagerly we find that many apps finalized and support each other; in our dataset. In a long method we can see FRAPPE as a step towards creating an independent active user for app assessment and ranking, so as to woundfacebook users before installing.

I.INTRODUCTION

The popular online social network is facebookwas founded by Mark Zuckerberg in 2004. Nowadays it has crossed across 750 millionactive users around the world, half of whom login to the website on daily.Nowadays there are more user on online social network. 20 million new applications are installed by its users every day. In April 2010, Facebook has launched its social network to deal with other websites. Since they launched this process, 2.5 million websites have integrated into Facebook. it provides a mobile platform used by 250 million people.facebook enable and motivate third-party applications (apps) to include the user experience on these platforms. They include interesting or entertaining ways of communicating among their online friends and interested activities such as playing games or listening to songs.

The huge volume of data is produced, and shared, the more number of users, and less number of employees. On that point which is widely used on news is heavily researched In this paper, we develop FRAPPE, which is clearly explained in figure1. A suite of efficient classification methods for detecting whether an app is malicious or not. To build FRAPPE, we use data from MyPage- Keeper, a security app in Facebook [15] that monitors the Facebook profiles of 2.2 million users. We analyze 111K apps that made 91 million posts across 9 months. The first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding harmfull apps and synchronoize the information into an effective detection.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

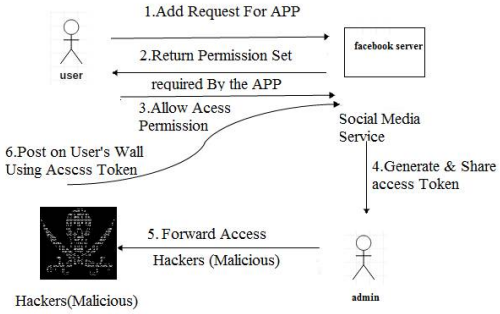

Figure 1 : FRAPPE TECHNIQUE

II.FACEBOOK TERMINOLOGY

Facebook is the biggest online social network today with many registered users who can login in daily basis. In this we discuss some standard facebook methods relevant to our work.

• Post: A post represents the common unit of information distributed on Facebook. Typical posts either contain only text (status updates), a URL with an associated text description, or a photo/album shared by a user. Many URL are used in this post.

• Wall: A Facebook user's wall is a big page where many of them, post their pages. Such messages are called wall posts. Facebook determined by the user's safety settings. Typically a user's wall is made visible to the all user's friends, and in some times to friends of friends only.

• News feed: A Facebook user's news feed page is a based on the social activity of the user's friends on Facebook. It updates the news feed of every user automatically and the content of a user's news feed depends on when it is questioned.

• Like: Like is a Facebook link that is associated with an object such as a post, a page, or an app. If a user clicks the Like link associated with an object, the object will appear in the news feed of the user's friends and thus allow information about the object to distributed across Facebook. The number of Likes (i.e., the number of users who have clicked the Like button) received by an object also represents the repeated andfamous of the particular object.

Application: Facebook allows hackers to create their own applications on facebook. Every time a user search an application's page on Facebook dynamically it loads the content of the application from a URL, called the canvas URL, pointing to the method server provided by the application's developer.
Since process of an method is dynamically loaded every time a user visits the application's page on Facebook, the application developer have control over process shown in the application page.

The Facebook platform uses OAuth 2.0 [2] for user verification, application authorization and application methods. Here, application authorization ensures that the users permit precise data (e.g., email address) and capabilities (e.g., ability to post on the user's wall) to the applications they select to add, and application methods ensures that a user allow access to the data to the correct application.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

III.THIRD PARTY APPS DATA COLLECTION PRACTICES

We gathered data from the top 200 most popular applications from each methods. By processing the list of applications, we collected the profile page URL for each application. Then, we used the software "Locoyspider" to collect and save data from the profile pages, as well as saved the number of daily active users for this applications.

Now list out the method "Go to App" URLs to generate the verifying methods dialog ("Request for Permission") which lists all the information that the app ask their users, or to be redirected to the app's external page. In our dataset, we only recognize those applications which would pop-up the security verified dialog box after clicking the button of "Go to App".

From these authentication dialog box, we select the types of information in each app desires to access from users. Merging all the information (i.e., types of information requests) with the number of daily active users for each application, we can count repeated process a specific type of information is executed to an app within a month.
Among those 1800 applications is popular, there were 1305 applications displaying authentication dialogs box when they requested data access from users. From the user perspective, there were 12 categories of information/behavior requested by the authentication dialogs. In these list of methods of their requests, we first compiled a list of applications that require it. We summed up the number of daily active users for each application on the list to get the more number of users who were asked for the information. We treat this more number as the total times that such user information is requested per month. The malicious application detection using FRAPPE is explained clearly in figure2.

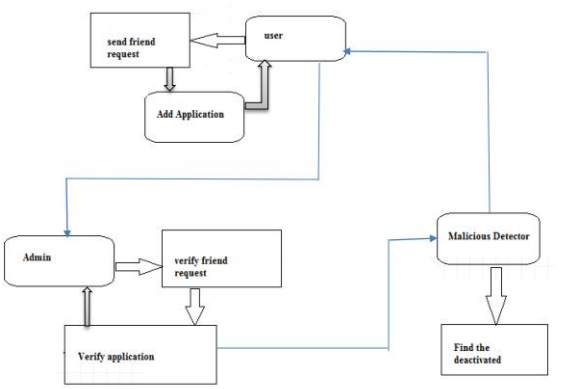

Figure 2: Malicious application detection

a. HOW TO STAY AWAY FROM MALICIOUS AND ROGUE

Don't click on any untrusted links on your Friends' posts. Obviously messages like the following aren't posted by your friends' but rogue facebook apps. If you have already added any application that you don't trust, then **remove it immediately**.
If you see these kind of virus links on any of your friends' profile then **alert** her about the problem and ask her to delete or remove that post and the rogue application immediately. You can explain her about this page so that she can knew that complication may occur . simple to acces and get fresh friends using the online social networking platforms like facebook to make sure that your personal information is not to be entered in that process.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV.COPY RIGHT AND FAIR USE

A healthy copyright system must equalize the need to provide strong economic process growth through exclusive rights with the need to protect and save important public interests like free speech and expression. Fair use is pillar to that balance.
It is major role toprevent copyright from the creativity it is expressed to foster, and from imposing other difficulty that would prohibit rather than promote the creation and spread of knowledge and learning.
The Fair Use Project (FUP) was established in 2006 to provide legal support to a range of projects designed to clarify, and extend their boundaries of fair use in order to make creative freedom and protect important public rights. It is the famous organization in country commitedspecifically to give free and extensive legal representation to authors, filmmakers, artists, musicians
The other content creators who face unmerited copyright claims, or other improper restrictions on their expressive passion. The FUP has litigated important cases across the country, and in the Supreme Court of the United States, and worked with the mark of filmmakers and other list developer to secure the unimpeded release of their work.

V.A TECHNIQUE FOR COMPUTER DETECTION

The described method assumes that a wordwhich cannot be search in a dictionary has at least one error, which might be a fault, missing or extra letter in a single transposition. The unidentified input word is compared to the dictionary again, identifying each time to see if the words match--assuming one of these errors occurred.

During a test run on garbled text, identifications were made for over 95 percent to correct these error types. As nowadays computers-are used in process variety of lexical processing tasks, the problem of error detection and correction becomes more critic. They will cause the employment of manual detection and correction procedures.

The fault detection method described below was developed to cope with the error problem in a coordinate indexing and retrieval system, although it is believed to be printed for other applications where the material to be entered is key pressed or produced on a Flexible writer or other similar device, or where material is sent over electrical Circuits and is subject to transmission error.

Information Control between Users and Third-Parties:

In addition to they provide the limit information access among users, Face book also provides mechanisms to restrict information process between users and third-party apps, even though these mechanisms are found to be some problem systematic process later in our study. To limit third-party apps' information access, Face book primarily relies on the OAuth 2.0 protocol is used for hacker's verification and authorization.

In the classic method client-server verification model, the client can serve as a protected resource on the server by verifying with the server using the resource owner's credentials. OAuth 2.0 adds an verified layer and split the role of the client (hackers application) from resource owner (Face book user).

Verification before downloading Apps from the OAuth 2.0 protocol, when a user wants to add an application to her Face book profile, the application is required to questioned the user for her permission to access, for example, basic data and/or other shared data on Face book includes a representative example of the user interface associated with this security authentication dialogue.

In the sample authentication method, the first category "access my basic data" represents the default data that will be generated by the app, which includes user's basic information such as name, profile picture, sex, network, applicant ID, list of friends, and any other information the user has shared with everyone.

If the app developer implements a need for information beyond these basic categories, she will need to ask the license from the user. In addition to the category of "basic information".

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The apps could request extended license to generate various data (e.g., contact data, photos, videos and friends data', etc.) or to act on behalf of the user (e.g., to post on users profile, and send sms to users).

VI.DETECTING MALICIOUS APPS

The various characteristics of harmfull appsand benign apps, we next use these features to develop powerful classification method to identify malicious Facebook applications. We present two variants of our malicious app classifier—FRAPPE Lite and FRAPPE.

A. FRAPPE Lite

FRAPPE Lite is a less weight version that makes use of onlythe application features available on demand. Given a specific app ID, FRAPPE Lite tells the on-demand features for that applicationand evaluates the application based on these features in real time features.

We envision that FRAPPE Lite can be incorporated, for example, into a browser extension can develop the Facebook application at the time. when a user is considering installing it to her profile. The lists of features used as input to FRAPPE Lite and the source of each feature. All of these features can be together on demand at the time of allocation and do not require prior knowledge about the app being evaluated.

We use the Support Vector Machine (SVM) [27] classifier for arranging malicious apps. SVM is widely used for binary classification in security and other disciplines [28], [29].We use the D-Complete dataset for training and testing the classifier. As the D-Complete dataset consists of 487 malicious apps and 2255 benign apps.

FRAPPE

Next, we consider FRAPPE—a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features. that FRAPPE uses in addition to those used in FRAPPE Lite. Since the aggregation- based features for an app require a cross-user and cross-app view over time, in contrast to FRAPPE Lite.

We envision that FRAPPE can be used by Facebook or by third-party security applications that protect a large population of users.Here, we again conduct a 5-fold cross validation with the D-Complete dataset for various ratios of benign to malicious apps.

In this case, we find that, with a ratio of 7:1 in benign to malicious apps, FRAPPE's additional features improve the accuracyto 99.5% (true positive rate 95.1% and true negative rate100%), as compared to 99.0% with FRAPPE Lite. The true positive rate raise from 95.6% to 95.9%, and we do not have a single false positive.

Identifying New Malicious Apps

We next identify FRAPPE's classifier on the entire D-Sample dataset (for which we have all the features and the ground truth classification) and use this classifier to search new malicious apps. To do so, we apply FRAPPE to all the apps in our D-Total dataset that are not in the D-Sample dataset; for these apps, we lack information as to whether they are harmfull app or benign. There are 98 609 apps that we test in this experiment, 8144 apps were flagged as malicious by FRAPPE.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Validation:

The true datafor the application flagged as malicious, we apply a host of complementary techniques to classify FRAPPE's allocation. We next describe these validation methods; as, we were able to validate 98.5% of the apps flagged by FRAPPE.

Deleted From Facebook Graph:

Facebook itself maintain its platform for malicious activities, and it disables and deletes from the Facebook graph malicious apps that it identifies. If the Facebook application interface (https://graph.facebook.com/appID) returns false for a particular app ID, this indicates that the app no longer trying to exists on Facebook; we consider this to be indicative of blacklisting by Facebook. This technique validates 81% of the malicious apps identified by FRAPPE.

Note that Facebook's measures for identifying harmfullapps are however not sufficient; of the 1464 malicious apps identified by FRAPPE (that were validated by other methods) but are still active on Facebook, 35% have been active on Facebook since over 4 months with 10% dating back to over 8 months.

App Name Similarity

If an application's name relates that of multiple malicious apps in the D-Sampledataset, that app too is likely to be some part of the same campaignand therefore malicious. On the other hand, we found severalmalicious apps using history of numbers in their name (e.g.,"Profile Watchers v4.32," "How long have you spent loggedin? v8"). Therefore, in addition, if an app name contains ahistory of number at the end and the rest of its name is identicalto multiple known malicious apps that similarly use histroy numbers, this too is indicative of the app likely being malicious.

Posted Link Similarity:

If a URL send a app matches the URL pale by a previously known malicious app, then these apps are likely part of the same harmful apps, thus validating the former as malicious.

VII.CONCLUSION

Function present available means for hackers to spread malicious content on Facebook. However, little is clear about the aspect of harmfull apps andthey access. In this paper, using a large corpus of malicious Facebook apps seen over a 9-month period, we showed that malicious apps varies from benign apps with respect to several features.

For reference, malicious apps are fair to share names with other apps, and they typically request the fewer permissions than begin apps.

Leveraging our observations, we developed FRAPPE, an accurate classifier for detecting malicious Facebook applications. Attractively we highlighted the emergence of app-nets—large groups of tightly connected applications that increases level to each other. We will continue to dig deeper into this ecosystem of malicious apps on Facebook, and we belive that Facebook will use from our recommendations for reducing the menace of hackers on their platform.

REFERENCES

[1] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online].
[2] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos,"Efficient and scalable socware detection in online social networks,"inProc. USENIX Security, 2012, p. 32.
[3] "WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation," [Online]. Available:
[4] F. J. Damerau, "A technique for computer detection and correction ofspelling errors," Commun. ACM, vol. 7, no. 3, pp. 171–176,Mar. 1964.
[5] C. Wueest, "Fast-flux Facebook application scams," 2014 [Online].