Impact Factor Value 4.046 e-ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 3, No.5, 2018
www.ijies.net

Detecting Malicious Data Using Fidget

Manjula V, Parth Purohit , Puneet Purohit, NishantNishu, Sangeetha V

manju6476@gmail.com, parthpurohit1710@gmail.com,ppunit02@gmail.com,
nishantnishudps@gmail.com,sangeethajaiprakash@gmail.com
Assoc.professor
Department of Computer Science and Engineering
Visvesvaraya Technological University, Belagavi,Karnataka,India

Abstract– *In this era of internet social media plays a very vital role and is thus becoming the next generation of communication. Communication technology has completely occupied all the areas of applications. Last few decade has however witnessed a drastic evolution in information and communication technology due to the introduction of social media network which has been very phenominal and is a world phenomenon.In some cases even Business growth is achieved by these social media looking to the present scenario of the usage of social media and looking in the future social media is very profitable thus,this also has attracted hackers all over the world and has created a trap for people using the social media platform Number of peoples is affected by a fake account or app is enormous over the internet. The hackers thus tend to infiltrate the victim's social network profile.This is done basically by copying the profile picture,,photos etc. of their targeted victim.Then they go on further and block the person's account whom they are impersonating and send requests to the friend list of that person and get profit both personally and economically.Third party applications are thus used to enhance user's experience on certain platform which is enabled and encouraged by Online social network(OSN).We can here take the example of Facebook as there are 500K apps available and on an average 20M apps are installed every day,we can also see such apps have maintained large user base.Only in Facebook alone there was 200K application available and whose numbers are suppose to increase to about 400k and the range in every day is 20M. Malicious applications are those applications which hack personal information like e-mail id, phone -number of Facebook users. These malicious applications also provide the business for hackers by using the popularity of online social network.By using malicious applications only hackers are getting benefited in so many ways.*

(a)The malicious applications reach the huge number of users to hacktheir personal information and use their friends also to spread spam

(b) when signing in,user's personal information are also acquired by such apps like their personal email address,home, number etc.

(c)these information collected are therefore used against the user itself or even manipulate their contactsthus resulting in personal and most of the time economical loss.

Key Words - Facebook Applications, Malicious Data, Benign data, Profiling Apps, Online Social Networks

I. INTRODUCTION

In this era of technology internet serves as a global internet connected network which uses internet protocol suite. It is a network of networks that consists of private, public, academic, business and govt networks of local to global scope. The internet carries vast range of information resources and services ex electronic mail,telephonya and file sharing. The development of online social network is thus facilitate by social media to a very large extent. We can take example of most used social media platforms such as are facebook, Google +, instagram,linkdln,tumbler,wechat,snapchat,my space and many more. We can take example of Facebook which is the biggest social networking website intended to connect friends,family, and business associates. With a increase of over 1.50 billion users and counting when compared with previous year's 1.35 billion users, application developers are in need of user information integration with the biggest social network. Among the 1.50 billion users and apps the number of running fake profiles and apps are enoromous. Creating a fake account is very easy as there are number of resources on the internet which provide utility and information to create a fake account and Number of peoples is affected by a fake account or app is also increasing. Someone copying the name,profile picture and photos is the most common thing which leads to hacking of account thus,making the user a victim. Then hackers block the person they are impersonating and send friend requests to everyone who so ever is in the friend list of the user. This is known as infiltrating the account of user.Given the popularity of OSN's malicious apps can be a very profitable business for the

hackers which has drastically increased as social media is expanding on a very high rate.For explaining this in a better way we can see the example of facebook which has 500K applications and on an average 20M applications are installed almost on a daily basis this has therefore provided a very large platform for hackers to carry on malicious activity and also nowadays hackers have started taking the advantage of third party applications to their profit as they realized it can provide a profitable business for them by carrying malicious activity. We can also notice that in past few years social media is the biggest propogators on internet.online social network is therefore the new way of cybercrime which is introduced by the hackers we can thus say hackers have found a illegal way to advertise and forward the spam messages thereby damaging the computer system with various ideas.This is called as social malware.We can take the example of Facebook again as Social malware is present everywhere in Facebook. Facebook is therefore the biggest social network to date as it alone has more then 2.2 billion users and for a networking site like Facebook it is important to detect a malware detection technique and so is for all the other social network or media.It is thus very essential and important to provide security and efficiency to billions of users using social networks. Thus,malware detection technique should be very efficient and reliable which can overcome the threats offered by hackers.As the hackers from past few years have started all social networking site to deploy malicious applications.And as we know for this task to be carried out by hackers they take use of third party applications and create a very strong business given the popularity of OSN's.to spread spam and reach huge number of users and their friends they put in a lot of ideas to gather personal and confidential information of user. Therefore, looking into these problems and issues it has been very important to develop a tool that can stop such malicious activities or atleast predict them with better result.Thus,the main goal of fidget is focused on detection of any form of malicious data with better accuracy and efficiency to guarante and ensure security of the user.

II-LITERARY SURVEY

Md Sazzadur Rahman, Ting-kai Huang, Harsha V.Madhyastha, and Michalis Faloutsos [01] In this paper the main concept is to detect whether to find the given app, in that can we find it is malicious are not. For that they compared with malicious apps and benign apps. They used set of features that distinguishes malicious apps from the benign apps. They used a MypageKeeper concept in this paper. MypageKeeper concept primarily relies on SVM based classifier that evaluates every URL. MyPageKeeper mainly designed for detecting malicious post on facebook. This paper mainly focuses on detecting malicious apps in facebook.

RosenSanae, Zhiyun Qian, and Z. MorelyMao[02] described a system for methodically identifying privacy connected appliance behaviour in mobile system where mainly significant aspect of the appliance behavior can be arbitrated during a well defined appliance structure. This system contains two components creating an acquaintance base of the API call by privacy pertinent behavior, with this information base to create a behavior outline for requests. They have established that it can be an extremely efficient process of permitting both end users as well researcher to improve appreciates how the application behaves.

Monika Verma, Divya, Sanjeev Sofat [03] This paper presents many methods have been developed and used by various researchers to find out spammers in different social networks. Most of the work has been done using classification approaches like SVM, Decision Tree, Naive Bayesian, and International Random Forest. Detection has been done on the basis of user based features or content based features or a combination of both.

Sonal S Khobragadeprof.MrudulaNimbarte [04] This paper gives the details about building a tool called FRAppE which focused on detecting malicious apps on facebook. In this they proposed a system which will provide a user to save their facebook profile from different malicious apps, posts .In this they used a FRAppE client, it is a app which created by the user to access token from the facebook server for accessing the user's profile. To view user's posts and information about their profiles. The called FRAppE they created can only get the details of user from facebook. This is done by facebook by giving access to tokens after getting the details via user. This FRAppE tool requests app installation permission from the user, to access data of the users, user then ask permission from facebook server, facebook then ask many information and then it grants access to the token the FRAppE client to access user profile. In this overall interface is created by using jsp,html5,javascript and bootstrap framework. Then they will compare malicious data with the selected data to determine wheather it is malicious.

Kiran Bhise, MsR.S.Shishupal [05] In this paper they used many classification technique to identify malicious app. They used parameters such has number of user data and user review. The input is malicious and benign app datasets. In this they considered two features for improving accuracy and decrease false positive rate. They used these two points to improve accuracy. They used SVM algorithm for better accuracy.

Shital B, Mandhane,Ismail Mohammed [06] In this paper they used mypagekeeper concept, it is a security application in facebook. In this they focused on profiling,qualifing and understanding malicious application. They introduced two features to detect malicious apps that is FRAppE Lite and FRAppE. The first detects identity number, name and source. The second detects actualdetection of malicious application.

They used orthogonal transformation and dimension reduction then only significantfeatures are preserved. They used hash concept to store.

Girisha Khurana, MrMarishKurma [07]. In this paper it is focused on detecting spam users in twitter social network. It can be done by based on content based or spam classifier method. They also included concepts of types of spammers, motives of spammers, the twitter social concepts. They used Honey-profile approach. In this they created 900 profiles on facebook, My-space and Twitter,300 on reach platform. The purpose of these accounts was to log the traffic they receive from other user of the network. These accounts are called honey profile. In this they did not sent any friend request but accepted all friend request. After having request accepted they logged all information to detect all malicious activity.

Mohammad Rakib Amin, Mehedee Zaman, Mohammed Atiquzzaman, Md. Shohrab Hossain [08] In this paper they investigated the natures and identities of malicious application and device two approaches: Network based detection and system call based detection approach. To evaluate this they took 1260 malwares and 227 non malware applications. In network based malware detection, in this the method is divided into two steps. First log of Universal Resource Locator that are contacted for application for specific amount of time. Then they tried to match URL with the list of malicious domains, if a match is found then it is malicious otherwise it is not malicious. In system call based approach it uses system call traces of application to detect malicious activity. Then system call based detection approach detects malware with 87% accuracy.

Sneha C. Vishwakarma, Pooja R. Shejwalkar, Aishwarya R. Sadigale, Shyamal G. Palkhede, Prof. D. S. Thosar[9] In this paper they used a machine learning approach. They developed a secure u application to determine the given app is malicious or benign. In this if the app is found to be malicious then it displays it has malicious. If the app is benign app then it can be successfully shared on facebook.

III- EXISTING SYSTEM

3.1*Developing Mypagekeeper application*

In the existing system they used mypagekeeper to build FRAppE, which is a security application in facebook. This is related to application in facebook. Has shown in figure 1. This is related to application which concentrates on profiling, qualifying and understanding malicious application. In this they introduced two features i.eFRAppE lite and FRAppE. The first level detects identity number,name and source. The second level detects actual detection of malicious app.

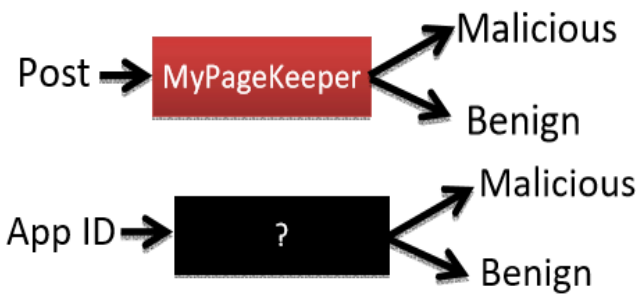


Figure 1

3.2*Developing FRAppE client*

To access user profile of face book user created FRAppE client to access token from facebook server this helps to view userwall, information and posts on user's wall. Facebook allows this by giving access to token after getting details from user. While installing FRAppE client app, it requests for app installation permissions such has users data,user in response to that ask for permission from facebook server then facebook ask various information and grant access token to FRAppE client to access user profile.

IV- METHEDOLOGY

The proposed topic Fidget basically detects malicious data based on the spam files and cookies generated. Fidget detects malicious data and application based on of spam file generated and gives the message to the users. Figure2 represents the general block diagram of detecting a malicious application.

The proposed model consists of three important modules that each perform specific task in the project.

1) Admin module- Admin is mapping the server details and web application details. In this module in the initial stage we will maintain two servers in the each server we will maintain few applications in various servers. Admin will keep track of the hosted applications, will have access to server settings and database where the details are stored. Admin will also be able to change password, add or remove applications.

2) Frappe agent module-The FRAppE agent module helps to map the IP address of the applications. It will track the IP address of server and the application accessing the user profile that is how many time it will access the application.

3) frappe attacker module-FRAppE attacker module will keep the track of all the applications. it keeps count of number of cookies and spam files. It maintains a table with application name, application id and the count of spam files and cookies and it will also check whether any application is misbehaved or not based on threshold value of the spam files and cookies.

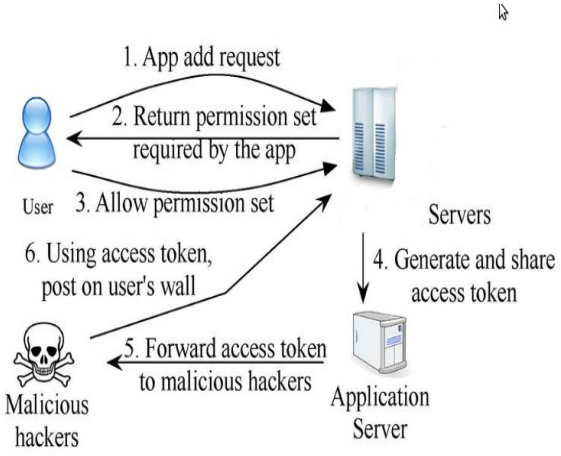
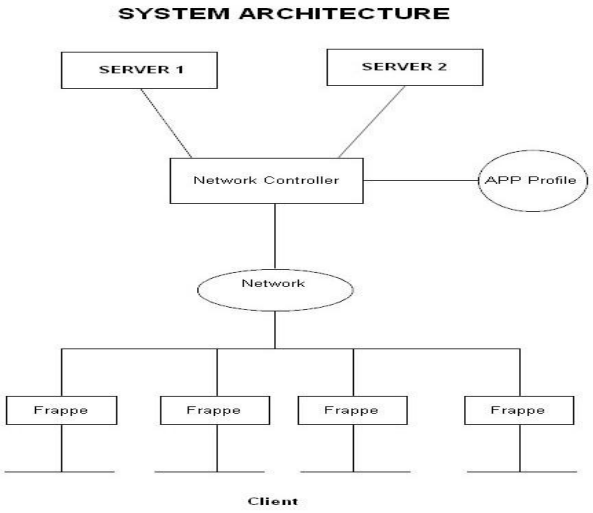


Figure 2

Spam file creation technique

If the application is not malicious only one file is created related to particular application and if the application is malicious many number of spam file is send to client irrelevantly

.



Design

Admin is mapping the surver details and web application details.In this module in the initial stage we will maintain two server,in each server we will maintain two application .

1.Server A

In this server two web applications.

Encryption

In this application we can process encryption and decryption process.

Numerology

By using this application we can see the numerology of the end user.

2.Server B

In this server two web application that is

Flames

This application is to find relationship between two persons,this is one of the entairtained games

Encoder

This application we can do encoding and decoding process

In this project we have maintained four web based application and initially we are going to induse one application as malicious.

IV-CONCLUSION

As the viral information increases on social media ,fake profiles increasing malicious things on internet, we have to prevent our profile from such fake profiles ,malicious links and from such fake people who now a days impersonate our account and use it for their profit. Fidget can detect malicious data, post and urls on social media. Fidget is not only used in detecting malicious data on our profile but also it detects the data of your friends whom you want to share in your timeline. It is also scheduling the malicious data detected on our mail. Evaluation of large variety of social network apps observed over time, it is seen that malicious third party apps or even data pose a constant threat to privacy and security and that malicious apps differ significantly from benign apps with respect to several features. For example, malicious data are much more likely to share names with other apps, or connected to app-nets etc. Based on these observations Fidget has been developed, as classifier for detecting malicious data.

ACKNOWLEDGMENT

The authors would like to thank to the reviewers for their best suggestions.

REFERENCES

[1] *Md Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos"FRAppE: Detecting Malicious Facebook Applications"IEEE Transaction on Networking vol: PP NO: 99 year 2015*

[2] *Rosen, Sanae, Zhiyun Qian, and Z. Morely Mao (2013), "Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users", In Proceedings of the third ACM conference on Data and application security and privacy, pp. 221-232, 2013*

[3] *Monika Verma, Divya, Sanjeev Sofat(2014) "Techniques to Detect Spammers in Twitter"International Journal of Computer Applications (0975 – 8887) Volume 85 – No 10, January 2014.*

[4] *Sonal S Khobragade, prof. MrudulaNimbarte "Overview on FRAppE" International Conference on Intelligent Computing and Control Systems ICICCS 2017.*

[5] *Kiran Bhise, MsR.S.Shishupal "A Method For Recognize Malignant Facebook Application" International Conference on Computing, Communication and Automation (ICCCA2016).*

[6] *Shital B, Mandhane ,Ismail Mohammed "FRAppE:Detecting Malicious Facebook Applications" International Journal on Recent and Innovation Trends in Computing and Communication.*

[7] *Girisha Khurana, MrMarish Kumar "Review: Efficient Spam Detection on Social Network " International Journal for Research in Applied Science & Engineering Technology June 2015.*

[8] *Mohammad Rakib Amin, MehedeeZamanMd, Shohrab Hossain "Behavioral Malware Detection Approaches for Android" IEEE ICC 2016.*

[9] *Sneha C. Vishwakarma, Pooja R. Shejwalkar, Aishwarya R. Sadigale, Shyamal G. Palkhede, Prof. D. S. Thosar "Detection ofMalicious Applications on Facebook using Machine Learning Algorithm" IJARIIE 2017*