International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Detecting Malicious Apps on Online Social Network's

Pravin Masal[1], Abhilash Lokhande[2], Avinash Adhav[3] ,Suraj Ghodake[4]

1234 Bachelor of Computer Engineering, Department of Computer Engineering, MMIT, Maharashtra, India.

Abstract - ***Now a day's use of social networking site like facebook, Twitter, Google+ for Communication and maintaining relationship among various users 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 theft and sexual l 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 unauthorized 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 MyPage-Keeper that is our base data, cannot detect malicious apps; it only detects malicious posts on Facebook. Though malicious apps contains 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 powerful than MyPage-Keeper to develop FRAppE, we use information gathered by observing the posting behavior of basic Facebook apps that are running on it. So, first we try to find out the features of malicious apps and other characteristics of malicious apps that are harmful to users.***

Keyword: Malicious Apps, Privacy, Online Social Networks, Security, Social Networking Applications, Facebook Apps, Naïve Bayes, Machine Learning.

I.INTRODUCTION

Online social network sites (OSN's) such as Twitter, google+, linkedIn and others are experiencing incredible user's growth with millions of active users. Away from just creating profiles and linking with friends, several sites are building a platform for a different applications built on top of users profiles. These social applications will become a new example of online communication where services make use of user's private information and social links. Online social networks (OSNs) are very popular cooperation and communication tools that have involved millions of Internet users.

Presently, social network sites provide few mechanisms for limiting the disclosure of user profile data to applications. Facebook, for example, takes an all-or-nothing approach: when users visit an application for the first time, they must give permission to allow that application to access all permissible profile data. The single choice is to not use or visit the application at all. However, even this does not give any genuine safety. The application can still demand a user's information on behalf of a friend who did install the application. Earlier research proposes to protect user data by approximately totally limiting what an application can access. We trust that there exists stability between the privacy of the user and the communal value of applications consuming users and friend's data. We are implementing a new model for social network application platforms.

In this paper, we develop system of efficient categorization technique for identifying whether an app is malicious or not. To build this system, we employ data from MyPageKeeper. This is possibly the first complete revision focusing on malicious apps.

2. LITERATURE SURVEY

1] G. Magno, T. Rodrigues, and V. Almeida." Detecting spammers on Twitter. "Benefits of this technique are it can identify spam by using attributes by checking proxy settings And disadvantages is Overhead on internet settings.

2]Hongyu Gao, Yan Chen, Kathy Lee† Northwestern University Evanston, IL, USA has present an" Online Spam Filtering System On Social Network" that can be deployed as a component of the online social network platform to inspect messages generated by users in real-time.SVM is reported to achieve good correctness on a broad variety of problems such as hand writing detection, face detection, text categorization,

3]Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek,."Social Applications: Exploring a More Secure Framework."It gives a practical balance between safety and privacy needs of the users, and the needs of the applications to access users' information.

4] Sundus Hassan, Muhammad Rafi, Muhammad Shahid Shaikh "Comparing SVM and Naïve Bayes Classifiers for Text Categorization with Wikitology as knowledge enrichment" we are comparing Support Vector Machine (SVM) and Naïve Bayes (NB) classifiers under text enrichment through Wikitology. We have shown that NB gives an enhancement of +28.78%, on the other hand SVM gives an improvement of +6.36% when compared with baseline results. Naïve Bayes classifier is better choice when external enriching is used through any external knowledge base.

3. EXISTING SYSTEM

Hackers have started taking benefit of the attractiveness of this third-party apps platform and deploying malicious applications. Malicious apps can provide a beneficial business for hackers, given the popularity of OSNs, with Facebook in important way with 900 Million active users. There are many ways that hackers can benefit from a malicious app.

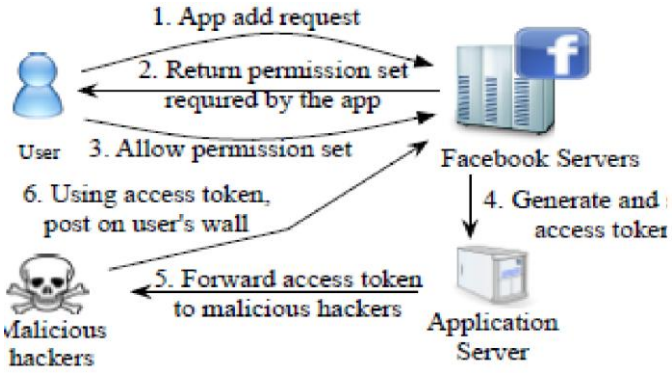

Fig. 1. Architectural Diagram of Existing System.

Disadvantages

(a) The app can get in touch with large numbers of users and their friends to spread spam.

(b) The app can gain users private information such as email address, home town, and gender, and

(c) The app can "copy" users account by making other malicious apps popular.

4. PROPOSED SYSTEM

We are going to implement the system of efficient categorization technique for identifying whether an app is malicious or not. To build this system, we employ data from MyPageKeeper. This is possibly the first complete revision focusing on malicious apps. Our base data source MyPageKeeper is a facebook security application which can detects only malicious posts.

That's why we are going to implement system which will detect the malicious apps on online social networks, where the malicious apps are bunch of malicious post.

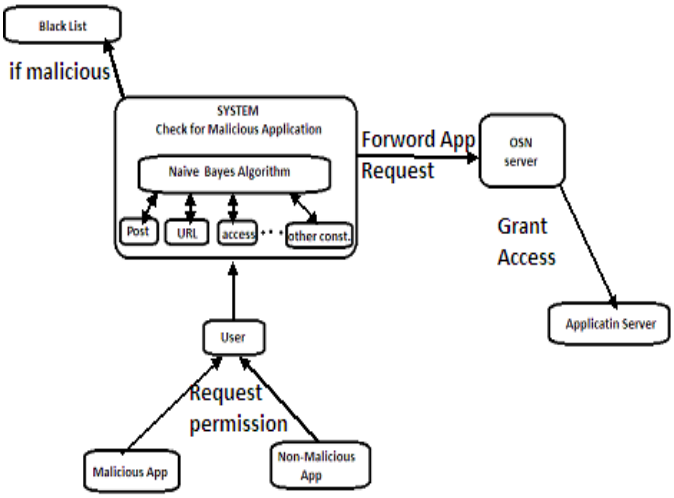

Fig. 2. Architectural Diagram of Proposed System

5. IMPLEMENTATION MODULES

1. Malicious and normal app profiles significantly differ

2. The appearance of AppNets: apps plan at huge scale

3. Malicious hackers impersonate applications.

4. FRAppE can spot malicious apps with 99% correctness

Malicious and normal app profiles significantly differ:

We scientifically profile apps and show that malicious app profiles are considerably dissimilar than those of normal apps. A striking inspection is the "laziness" of hackers; many malicious apps have the identical name, as 8% of unique names of malicious apps are each used by more than 10 dissimilar apps. generally, 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 necessary for the app and the posts in the application's profile page), and (b) others that require across-user view to collect information across time and across apps (e.g., the posting activities of the app and the comparison of its name to other apps).

The appearance of AppNets: apps collude at huge scale:

We perform a forensics inquiry on the malicious app bionetwork to spot and quantify the techniques used to encourage malicious apps. The most motivating result is that apps plan and work together at a huge scale. Apps support other apps via posts that point to the "promoted" apps. If we explain the collusion relationship of promoting-promoted apps as a graph, we find

1,584 advertiser apps that support 3,786 other apps. Furthermore, these apps form large and highly-dense connected components, furthermore, hackers use fast-changing indirection: applications posts have URLs that spot to a website, and the website dynamically redirects to a lot of different apps; we find 121 such URLs that point to 4,556 different malicious apps over the course of a month. These observed behaviors point to well-ordered offense: one hacker control a lot of malicious apps, which we will call an AppNet, since they seem a parallel concept to virus.

Malicious hackers impersonate applications:

We were amazed to find well-liked good apps, such as 'FarmVille' and 'Facebook for iPhone', posting malicious posts. On additional inquiry, we found a slack of authentication rule in Facebook that enabled hackers to make malicious posts come into view as though they came from these apps.

FRAppE can spot malicious apps with 99% accuracy:

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

6. CONCLUSION

OSN Applications present a suitable means for spammers to spread harmful content on Social networks. In this project, using a large amount of malicious social apps observed more than a nine month period, we showed that malicious apps differ drastically from normal apps with respect to a number of features. That's Why we are using naïve bayes classifier to classify the apps with respect to their feature for Example, post, URL, access permissions etc.

7. ACKNOWLEDGMENT

It gives great pleasure in submitting paper on "Detecting Malicious Apps on Online Social Network's". We would like to thank Prof. Chaitanya Bhosale(Guide) and Prof. S. K. Patil (Co-Coordinator)for giving timely & valuable guidance during successful completion of this project.

8. REFERENCES

1] G. Magno, T. Rodrigues, and V. Almeida., "Detecting spammers on Twitter."

2]Hongyu Gao, Yan Chen, Kathy Lee† Northwestern University Evanston, ILUSA "Online Spam Filtering System On Social Network"

3] Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek,"Social Applications: Exploring a More Secure Framework."

4] Sundus Hassan, Muhammad Rafi, Muhammad Shahid Shaikh "Comparing SVM and Naïve Bayes Classifiers for Text Categorization with Wikitology as knowledge enrichment"