An Approach for Detecting Malicious Applications on Online Social Networks

Sharad Laxman Pawar[1], Kishor Ashok Jadhav[2], Bhushan Eknat Gaikwad[3], Kiran Bhagwat Chormale[4], Prof. S. A. Kahate[5]

[1] Student, Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, Maharashtra, India.
[2] Student, Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, Maharashtra, India
.[3] Student, Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, Maharashtra, India.
[4] Student, Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, Maharashtra, India.
[5] Assistant Professor, Computer Engineering, SPCOE, Dumberwadi, Otur, Pune, Maharashtra, India.

ABSTRACT

As online social networks are used by everyone now a day's which enhances the information sharing between the peoples those are interconnected with each other's. Due to this tremendous use of specific online social networks a third parties are involving to do certain their advertisement on such networks. But here is the place that the malicious and viral applications are come up to access your secure information through this social network. The real fact behind this studies are for detecting such malicious applications those are trying to access secure information and share to third parties.

Keywords: *Facebook apps, malicious, online social networks, spam.*

1. INTRODUCTION

Today online social networks play an important role in daily life. There are various online social networks such as Facebook, twitter etc. are there and these shows tremendous growth in recent years. These kind of social networks allow users to make social connection with others. Apart from all these there are some security issues or security violations are there. A social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people who have the same interests. These Online Social Networks (OSN) uses web2.0 technology, which allows users to interact with each other. These social networking sites are growing rapidly and changing the way people keep in contact with each other.

The online communities bring people with same interests together which makes users easier to make new friends. There are no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method, it can be applied easily by online social networks which has millions of profiles whose profiles cannot be examined manually. These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends. In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their up- dates has become easier.

Social Engineering in terms of security means the art of stealing confidential information from people or gaining access to some computer system mostly not by using technical skills but by manipulating people themselves in divulging information. The hacker doesn't need to come face to face with the user to do this. The social engineering techniques are like Pretexting, Diversion theft, phishing, baiting, quid pro quo, tailgating, etc. Social bots are semi-automatic or automatic computer programs that replicate the human behaviour in OSN. These are used mostly by hackers now-a-days to attack online social networks. These are mostly used for advertising, campaigning purposes and to steal users personal data in a large scale. These social bots communicate with each other and are controlled by a program called botmaster. The botmaster may or may not have inputs from a human attacker. The social bots look like human profiles with a randomly chosen.

2. LITERATURE SURVEY-

Online Social Networks (OSNs) such as Facebook1 and Twitter2 have far exceeded the traditional networking service of connecting people together. With millions of users actively using their platforms, OSNs have attracted third parties who exploit them as an effective media to reach and potentially influence a large and diverse population of web users.

Yazan Boshmaf et all defines Online Social Networks (OSNs) have become an integral part of today's Web. Politicians, celebrities, revolutionists, and others use OSNs as a podium to deliver their message to millions of active web users. Unfortunately, in the wrong hands, OSNs can be used to run astroturf campaigns to spread misinformation and propaganda. Such campaigns usually start by infiltrating a targeted OSN on a large scale. In this paper, we evaluate how vulnerable OSNs are to a large-scale infiltration by socialbots: computer programs that control OSN accounts and mimic real users. As socialbots infiltrate a targeted OSN, they can further harvest private users' data such as email addresses, phone numbers, and other personal data that have monetary value. To an adversary, such data are valuable and can be used for online profiling and large-scale email spam and phishing campaigns.

Fabrıcio Benevenuto et all introduces In this paper we consider the problem of detecting spammers on Twitter. Here they had first collected a large dataset of Twitter that includes more than 54 million users, 1.9 billion links, and almost 1.8 billion tweets. Using tweets related to three famous trending topics from 2009, we construct a large labelled collection of users, manually classified into spammers and non-spammers. We then identify a number of characteristics related to tweet content and user social behaviour, which could potentially be used to detect spammers. They used these characteristics as attributes of machine learning process for classifying users as either spammers or no spammers. Our strategy succeeds at detecting much of the spammers while only a small percentage of non-spammers are misclassified. Approximately 70% of spammers and 96% of non-spammers were correctly classified. Our results also highlight the most important attributes for spam detection on Twitter. Tweet spammers are driven by several goals, such as to spread advertise to generate sales, disseminate pornography, viruses, phishing, or simple just to compromise system reputation. They not only pollute real time search, but they can also interfere on statistics presented by tweet mining tools and consume extra resources from users and systems. All in all, spam wastes human attention, maybe the most valuable resource in the information age.

Aamir Suhial et all explains In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates have become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There are no feasible solutions that exist to control these problems. Nowadays, the web is all about Facebook, Twitter, YouTube, Tumblr. But seven years ago, all these services didn't exist, portals and search engines where still king. So what happened during this period? To make a long story short: users took the control of the web. Or, to be more accurate: the market shifted to a click based engagement model to a fan-based engagement model. Which means, clicks are no longer the premium currency for advisers, fans are: they want to be followed, to be shared, to be mentioned, even to be pinned? Fan is the new click. With the advent of user generated content and sharing features, social platforms are the new kings of the web. This being said and I assume you already knew it, not every social platform is the same.

Within the last seven years, we have been through three waves of social domination: The publishing wave (with blogs), the sharing wave (with Facebook and Twitter), and the curating wave (with Quora, Pinterest and alike). The main reason for this shift in users' behavior is the amount of content: the more content, the more precious it is to find the value-added content; this is why we are currently in the curating wave. The second reason is the evolution of users' expectations: the more they use social media, the more sophisticated their needs are. Thus, every six month, we are witnessing the arrival of "the new Facebook". But as you can experience it every day, we still have the same three dominant players (Facebook, Twitter, and Google) and a dense ecosystem of niche players.

Minas Gjoka et all defines Facebook is one of the most popular Internet sites today. A key feature that arguably contributed to Facebook's unprecedented success is its application platform, which enables the development of third-party social-networking applications. Understanding how these applications are installed and used is important for the function and utility of web-based online social networks, e.g. to better engineer them and/or to design advertising campaigns. OSNs nowadays are up against the problem associated with uncovering bogus records in the remarkably adversarial setting. The problem becoming more challenging as such account have become sophisticated within cloaking the operations with behavior similar to real individual habits. In this perform, we all introduced Íntegro, scalable defense system that will facilitates OSN operators to find are records by using a meaningful individual standing plan. Your evaluate final results indicate that will SybilRank, the particular state-ofthe-art within bogus account detection, is usually inadequate when the reproductions infiltrate the objective OSN through befriending quite a few real consumers. Íntegro, however, has verified more resilient for this effect by leveraging the ability associated with civilized sufferer records in the story way.

3. PROPOSED WORK-

Facebook enables third-party developers to offer services to its users by means of Facebook applications. Unlike typical desktop and smartphone applications, installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a user adds a Facebook ap plication to her profile, the user grants the application server: 1) permission to access a subset of the information listed on the user's Facebook profile (e.g., the user's e-mail address), and 2) 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 OAuth 2.0 [17] 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 operation of a Facebook application.

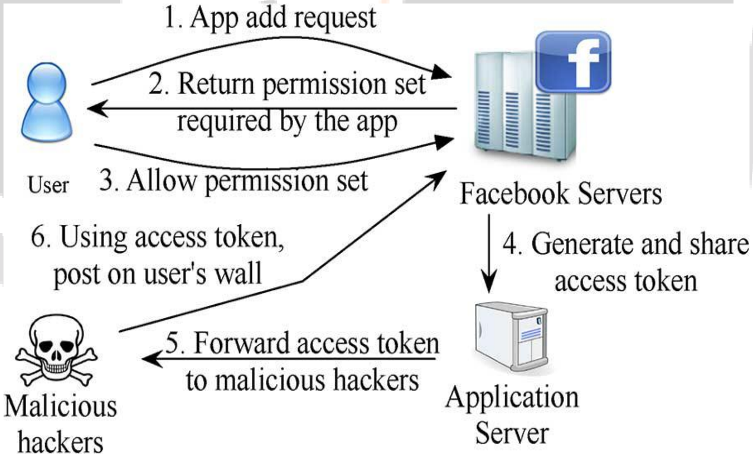
1. App add request
2. Return permission set required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

Fig-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 convince 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 perform 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 potentially 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 (or some other malicious app).

This way the cycle continues with the app or colluding apps reaching more and more users. Personal information or surveys can be sold to third parties [18] to eventually profit the hackers.

4. SYSTEM ARCHITECTURE-

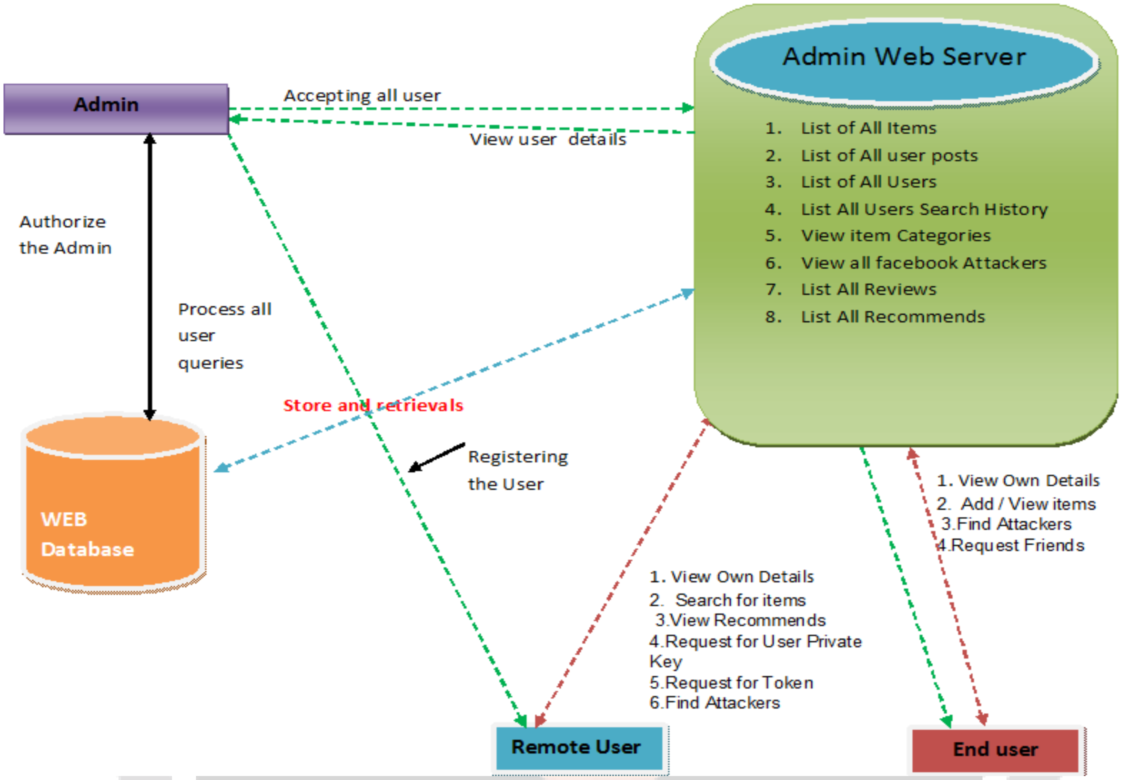

Fig-System Architecture

The proposed system consists of main three subsystems such as web server, web database, and user. Web server having a number of tasks as maintaining all the information related to individual users defines a strategy for detecting attacks and review sheets. As apart from these it maintains all the history related to users search which can be further useful to tract the attacker activities since it makes system efficient and effective. Web database is second part of system which processes all the user queries and having a responsibility to define authorizes users which are going to access the entire system. In user part there are three classes of users are such as admin, remote user, end user which are going to use system. As entire figure shows all the details related to each entity in the system.

5. CONCLUSIONS

The above defined system detects malicious applications on the Facebook by tracking the entire activities of numbers of users and malicious applications are detected effectively by defining FRAppE lite. As system architecture is very simple and effectively tracks the malicious applications on the online social networks. As apart from study, now a days the security measures should enhance of Online Social Network since hackers are attempting to hack crucial information of users from the same due to wide use of online social networks.

6. ACKNOWLEDGEMENT

Here we are going to thanks everyone those who had helped us during completion of this paper. We would like to thank our guide Prof. S. A. Kahate and head of department Prof. Gajanan Deokate for entire support and guidance. At last we thank to our friends and family members for their encouragement for doing same.

7. REFERENCES

[1]. Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos "Detecting Malicious Facebook Applications" IEEE/ACM TRANSACTIONS ON NETWORKING 2015.
[2]. Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu "The Socialbot Network: When Bots Socialize for Fame and Money" ACSAC 11 Dec. 5-9, 2011
[3]. Fabr´ıcio Benevenuto, Gabriel Magno, Tiago Rodrigues, and Virg´ılio Almeida Detecting Spammers on Twitter CEAS 2010 Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference July 1314, 2010, Redmond, Washington, US.
[4]. Aamir Suhial "Privacy & Security a Concern in Social Networks" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 4, Issue 1, January-February 2015
[5]. Minas Gjoka, Michael Sirivianos, Athina Markopoulou, Xiaowei Yang Poking Facebook: Characterization of OSN Applications WOSN'08, August 18, 2008, Seattle, Washington, USA.
[6]. Shuliang WANG, Hanning YUAN, "Spatial Data Mining in the Context of Big Data", IEEE International Conference on Parallel and Distributed System,2013.
[7]. L. Parfeni, "Facebook softens its app spam controls, introduces better tools for developers," 2011 [Online]. Available: http://bit.ly/LLmZpM
[8]. "Norton Safe Web," [Online]. Available: http://www.facebook.com/ apps/application.php?id=310877173418