International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Recognizing Vindictive Social Network Applications

A.Raghava Rao, K.Sasank, P.Subash, K.C.Anu (Guide)

SRM University,Chennai, India

Abstract - Online social networks (OSN's) users are attracted towards their platform by Third party applications. OSN's let and support third-party apps to increase the user usage on these social networks. Third party applications are divided into two types Trusted and Non – Trusted. Non-Trusted apps divide into two categories benign apps and vindictive apps. Vindictive applications show harmful apps by giving fake advertisements like rewards, electronics as gifts and make users redirect to their page, when users visits these pages it will collect the secured data of users by providing fake login or URL's. This fake login lets the hacker in your profile to spread or post spam to your online friends through your profile. In this paper, we have taken Facebook as OSN and developed TPAppE – Third-party Application Evaluator which is the tool for detecting or recognizing vindictive apps with high accuracy. We develop Third-Party Application Evaluator to recognize user harmful apps using features using both demand and based on aggregation. To develop TPAppE, we include data assembled by watching the posting nature of 550K third-party applications in Facebook used by 1.86 billion users. We used a suite of classifiers that help us in recognizing vindictive applications from non-malicious ones. To warn Facebook users before installing apps ,TPAppE is a step toward creating an independent watchdog for app.

Key terms: Social networks, Non- trusted, Vindictive, TPAppE, Spam.

I. INTRODUCTION

The usage of Third-party applications in online social networks (OSN's) is huge now a days. OSN's let the third-party apps to improve the user experience. These third-party applications are being used by many users and the demand for third party applications is increasing day by day. Third-party apps are the only reason for the publicity, popularity and attractiveness of social networks. The new created application requests the social network to enter their platform, the social network investigates the app and what permissions it is asking from user. If the requested application is as per the OSN terms , it will furnish and generates the unique access token for that app or page to let their app used by users on their platform. The Third-part application are categorized in two types Trusted and Non – Trusted. Trusted applications will collect the required user needed for the app and stores it securely, where as a Non-Trusted Applications makes fake promises to the user, collects all the user personal data (email, phone number, age, gender, friend's names) and uses it to spread spam using your profile. Non-Trusted apps divide into two categories benign apps and vindictive apps. Vindictive apps will display fake ad's like free rewards, phone, money etc. and targets user to show-up in their particular page, it recovers or collects the secured or personal data of user when the user visits their page by manipulating user to enter details in fake login . Using the details provided in fake login it makes the hacker to let in user profile to spread or post spam to your friends in the network. Through this spam posts or shares so many users and their personal details can be affected.

II. EXISTING SYSTEM

In Existing concept, Hackers bring started exploiting the profit from this third-party apps used in social networks and sending vindictive requests to users. These vindictive apps providing a huge benefits and business for hackers, leading the way with 1.15B active users in Facebook. In many ways a hacker can benefit through a vindictive app: 1) to spread spam application mau do promotions to get top rank; 2) the

app can recover user's secured details 3) apps can portray by making other vindictive apps popular spreading on social network everyday.

To easily hack , the development of vindictive apps is stream lined by ready-made toolkits starting at $30. There are so many black websites which are using proxy to make themselves static and they giving fake URL's or ready-made apps for the hackers to share the app . At the end of the day, there is thought process and opportunity, and accordingly on Facebook consistently. There is no recognizing and detection in the current framework to check whether an application is unsafe to user or not.

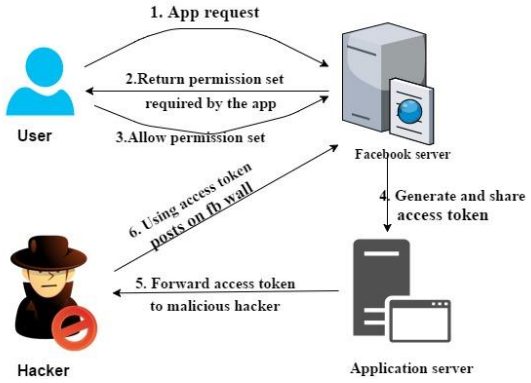


FIG 1. Access from the User through OSN

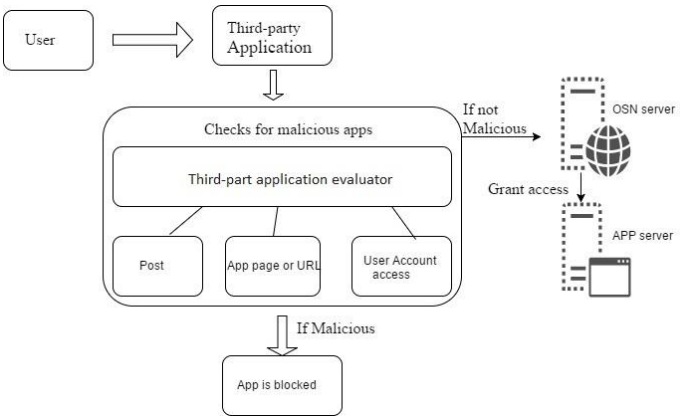
EXISTING TECHNIQUE

Efficient Classification Technique.

"Photo of the Day" to show and tell how pernicious applications on Facebook can dispatch distributed denial-of-service (DDoS) assaults utilizing the Facebook platform. Facebook conducted a study to comprehend user's communication with third-party applications. It is just used to know how users are attracting or reacting towards the third-party apps.

III. PROPOSED SYSTEM

In proposed system, we developed Third-party Application Evaluator(TPAppE) , which is a tool completely centered on analysing or recognizing vindictive apps on Facebook. It recognizes the harmful apps with high accuracy and with positive results. To develop TPAppE, we utilize data assembled by watching the posting nature of 550K Facebook applications seen over 1.86 billion users on Facebook We recognize a suite of components that help us recognize vindictive applications from generous ones. Interestingly, we asset that lot of applications intrigue and backing each other in our data-set, we find 1585 applications sanctioning the viral propagation of 3725 different applications through their posts. We also introduced a secondary authentication otp in social network, the otp password will be received by user to his\her email-id. This OTP process will keep the user's account securely and block the unauthorized login's.



VI. ALGORITHMS USED

1. **Naive Bayes Algorithm**
2. **One time password**

1.Naive Bayes Algorithm

Naïve Bayes is a classifier technique in finding harmful vindictive apps. According to permission set, it contains the number of permissions required to access any app, but as we know that malicious app need fewer permissions to access anyone's info as compared to benign apps that needs to satisfy all the criteria to access the same things. In our app, we are using naïve Bayes algorithm which fills the information in the

feature table like 1 or 0 according to whether the app asked for permission or not.

Bayes theorem provides a way of calculating posterior probability P(c—x) from P(c), P(x) and P(x—c). Look at the equation below:

1. P(c—x) is the posterior probability of class (c, target) given predictor (x, attributes).
2. P(c) is the prior probability of class.
3. P(x—c) is the probability which is the likelihood of indicator given class.

Now, we need to classify whether Application is malicious or not based on permission set condition. Let's follow the below steps to perform it.
1. Here we are considering permission set. We are assuming 1 means permission is required and 0 means permission is not required.

Dataset Table according to our Project as follows:

Table 1. Data set Table

Permission Set	Condition Values
Publish Stream	0
Offline Access	1
User Birth Date	1
Email	1
Publish Access	1
Publish Stream	1
Offline Access	1
User Birth Date	0
Email	0
Publish Access	0

Table 2. Frequency Table

Permission Set	0(permission not required)	1(permission required)
Publish Stream	1	1
Offline Access	0	2
User Birth Date	1	1
Email	1	1
Publish Access	1	1

2. Finding the probabilities like Publish Stream probability = 0.20 and probability of Non-malicious app is 0.60

Permission Set	0	1
Publish Stream	1	1
Offline Access	0	2
User Birth Date	1	1
Email	1	1
Publish Access	1	1
	All=4	All=6
	4/10=0.40	6/10=0.60

Table 3. like Hood table

3. Now, use Bayesian equation to calculate the posterior probability for each with positive likelihood in the result.
4. **Problem:** App is trustable if permission set is 1 for Publish Stream.
Consider Yes=1 and 0=No We can solve it by probability. P(Yes | Publish Stream) = P(Publish Stream | Yes) * P(Yes) / P (Publish Stream) Here we have

P (Publish Stream |Yes) = 1/6= 0.16, P(Publish Stream) = 2/10= 0.36, P(Yes)= 6/10 = 0.60 Now, P (Yes | Publish Stream) = 0.16*0.6/0.2=0.48, which has lower probability. The strategy to guess the likelihood of various class in different attributes is used by Naïve Bayes.

2.One Time Password

A **OTP** is a secret key that is substantial for just a single login session or exchange, on a PC framework or other advanced gadget. The strategic methodologies from various inadequacies that are similar to static key based used as OTP authentication for example, a PIN). OTP calculations ordinarily make utilization of pseudo changeability or volatility, making guess of successor OTPs by an aggressor troublesome, and furthermore hash capacities, which can be utilized to determine an esteem however are difficult to turn around and accordingly troublesome for an assailant to acquire the information that was utilized for the hash. OTPs are listed below:

- Based on **time-synchronization** and **Mathematical algorithm** between the server which verifies and the

user entering the password (OTPs are valid only for a short period of time)

- Utilizing a numerical calculation to create another secret key in view of the past watchword (OTPs are successfully a chain and should be utilized as a part of a predefined arrange)

VII. FUTURE ENHANCEMENT

We can use different classifiers as the techniques for further improvement in the validation. Collaborative Filtering is an algorithm can be used for rating process for the third-party applications reduces time for validating applications by user. Details about apps whether it is malicious or not can be known quickly. Security can be improved which will work as Anti-Malicious app checker.

VIII. CONCLUSION

Applications introduce advantageous means for hackers to spread vindictive posts on Facebook. One should understand how a non-trusted app attracts and should know how a vindictive app works in the background process. Malicious applications differ from benign applications. The main aim of benign application is to publicize their page and app. Non-trusted apps will hack the user details and spreads spam. To stop this type of spamming and hacking user account we developed TPAppE using Naive Bayes theorem and suite of classification techniques to detect and block the vindictive applications accurately.

References

[1] "Which cartoon character are you—Facebook survey scam," 2012 [Online]. Available:https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30/

[2] H. Gao *et al.*, "Detecting and characterizing social spam campaigns," in *Proc. IMC*, 2010, pp. 35–47.

[3] E. Protalinski, "Facebook kills app directory, wants users to search for apps," 2011 [Online]. Available: http://zd.net/MkBY9k.

[4] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs," in *Proc. KDD*, 2009, pp. 1245–1254.

[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 447–462.

[6] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek, "Social applications: Exploring a more secure framework," in *Proc. SOUPS*, 2009, Art. No. 2

[7] A. Makridakis *et al.*, "Understanding the behavior of malicious applications in social networks," *IEEE Netw.*, vol. 24, no. 5, pp. 14–19, Sep.–Oct. 2010.