RESEARCH ARTICLE OPEN ACCESS

FRAPPE: Making Facebook More Secure

Ritu Kumari, Utkarsha Mamidwar, Sanjoli Kapoor, Kritika Sharma
Mrs.Deepali Gothawal, Assistant Professor
Department of Computer Science and Engineering
D Y Patil College of Engineering, Akurdi
Pune - India

ABSTRACT

In Online Social Networking (OSN), With 20 million installs a day, third-party apps are a major reason for the addictiveness of Facebook (OSN) and hackers have realized the potential of using apps for spreading malware and spam which are harmful to Facebook users.

IN order to determine whether that application is malicious and let the user's identify that So, our key contribution is in developing "FRAppE—Facebook's Malicious Application Evaluator". There are 2.2 millions of people using Facebook in order to develop FRAppE, use gathering and observing information by posting behavior of Facebook user's.

Keywords:- Online Social Network, Social Applications ,Measurement

I. INTRODUCTION

Online social networks (OSN) enable and inspire third party applications to enhance the user knowledge on these platforms like FACEBOOK. Such improvements resulted in providing facilities like entertaining ways of interacting among online friends, and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app mixing into the Facebook user-experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a huge user base. It is observed that FarmVille and CityVille apps have users of range 26.5M and 42.8M users until now. Recently, hackers and malicious users have started taking advantage from these third-party apps platforms and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the status of OSNs, with Facebook leading the way with 900M active users. There can be these following ways that hackers can profit from a malicious app:

(a) The app can incur risks to huge numbers of users by spreading spam,

(b) The app can aquire users' personal information such as email address, address, and gender, And

(c) The app can be re-created by making other malicious apps popular.

As an outcome of the above problems, there are many malicious apps on Facebook every day. Because user has very incomplete material at the time of installing an app on his Facebook profile as user does not identify the proposed app is malicious or not only the identity number (the unique identifier assigned to the app by Facebook) Currently, there is no commercial service or research-based tool for advising a user about the risks of an app. Malicious apps are easily being spread, and because of it safety is compromised. There have been several researches done regarding spam and malware on Facebook which have focused on detecting malicious posts and social spam campaigns. A recent study has shown how app authorizations correlate to privacy risks of Facebook apps. Finally, there are some community-based feedback driven efforts to rank applications, such as What app; though these could be very controlling in the future, so far they have received little acceptance.

II. LITERATURE SURVEY

1) Detecting and Characterizing Social Spam Campaigns

Authors: Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao.

Description: Authors presented a primary study to calculate and analyze spam campaigns launched on online social networks. They calculated a huge anonymized dataset of asynchronous "wall" messages in between Facebook users. System detected generally 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that extra than 70% of all malicious wall posts advertise phishing sites. To study the distinctiveness of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts formed solely for the principle of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post in the early morning hours when users are normally asleep.

2) Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals

Authors: Pern Hui Chia, Yusuke Yamamoto, N. Asokan

Description: Third-party applications captures the attractiveness of web and platforms providing mobile application. Many of these platforms accept a decentralized control strategy, relying on explicit user consent for yielding permissions that the apps demand. Users have to rely principally on community ratings as the signals to classify the potentially unsafe and inappropriate apps even though community ratings classically reflect opinions regarding supposed functionality or performance rather than concerning risks. With the rising of HTML5 web apps, such systems relying on user-consent permission will be more widespread. To study the advantages of user-consent permission systems through a large data collection of Facebook apps, Chrome extensions and Android apps. The study confirms that the current forms of community ratings used in app markets today are not reliable for indicating privacy risks an app creates. We find some evidence indicating attempts to mislead or entice users for granting permissions: free applications and applications with mature content request; "lookalike" applications which have similar names as that of popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average

3) LIBSVM: A Library for Support Vector Machines.

Authors: Chih-Chung Chang and Chih-Jen Lin

Description:LIBSVM is a library for Support Vector Machines . Authors have been actively developing this package. The purpose is to help users to effortlessly apply SVM to their applications. LIBSVM has gained wide status in machine learning and many areas. In this, authors obtainable all implementation details of LIBSVM. Issues such as solving SVM optimization problems, theoretical convergence, probability estimates, and parameter selection are discuss in detail. Support Vector Machines are a popular machine learning method for categorization, regression, and other learning tasks.

LIBSVM is currently one of the most widely used SVM software.

4) Social Applications: Exploring A More Secure Framework

Authors: Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek

Description:OSNs such as Orkut, Facebook and others have grown-up rapidly, with hundreds to millions of active users. A new feature provided on several sites is social applications and services written by third party developers that supply additional functionality linked to a user's profile. However, present application platforms put users at risk by permitting the discovery of huge amounts of personal data and information to these applications and their developers. This paper generally abstracts main view and defines the current access control model gave to these applications, and builds on it to generate a more secure framework. So in the interest of preserving as much of the current architecture as possible, while seeking to practically provide balance between security and privacy needs of the users, and the require of the applications to access users' information. To present a user study of our interface design for setting a user-to-application policy.

III. EXISTING SYSTEM

Now a days, hackers have started taking advantage of the popularity of this third-party apps platform and deploying several malicious applications. These malicious apps can provide a lucrative business for hackers, given the popularity of online operating system, with Facebook leading the way with 900M active users. There can be enumeral ways that hackers can benefit from a malicious app, some of the them are:

(a) The app can reach huge number of users and their friends to spread spam,

(b) The app can obtain users' personal information such as email address,maritial status home town, and gender, And

(c) The app can be re-created by making other malicious application popular.

As a result of the above problems, there are many malicious apps spreading on Facebook every day. Because user has very limited information at the time of installing an app on his Facebook profile as user doesnot able to recognize the proposed app is malicious or not only the identity number

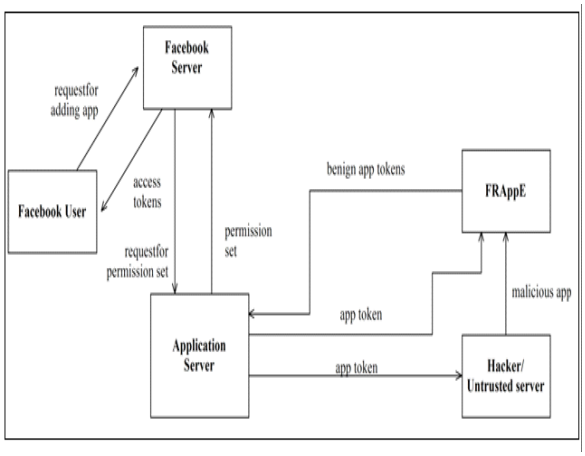
Problems with existing system:

Hackers spread malwares and spam in facing using app.

Many malicious apps are spreading on facebook.

IV. PROPOSED SYSTEM

To develop FRAppE, a suite of resourceful and efficient classification techniques for detecting whether an app is malicious or not. To build FRAppE, use data from MyPageKeeper, a security app in Facebook that monitors the Facebook profiles of no of users near about 2.2 million of user. Analyze 111K apps that made 91 million posts over nine months. This is debatably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective and fast detection approach.



There introduced two features , classifier to detect the malicious apps . In first step of classifier it detect the initial level detection e.g. apps identity number , name and source etc. and in second level of classifier do detection the actual detection of malicious app has been done.

V. EXPECTED OUTPUT

1. Application present a convenient means for hackers to spread malicious content on Facebook.

2. User on facebook can only get request from benign apps.

3. It provides security to users profiles from malicious apps.

VI. CONCLUSION

An application presents a convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious application and how they operate. In this project, using a large corpus of malicious Facebook apps observed over a nine month period and showed that malicious apps differ significantly from benign apps with respect to several features. Leveraging our observations, developed FRAppE, an accurate classifier for detecting malicious Facebook applications.

VII. REFERENCES

[1] C. Pring, "100 social media statistics for 2012," 2012 [Online]. Available: http://thesocialskinny.com/100-social-media-statistics-for-2012/

[2] Facebook, Palo Alto, CA, USA, "Facebook Opengraph API," [Online]. Available: http://developers.facebook.com/docs/reference/api/

[3] "Wiki: Facebook platform," 2014 [Online]. Available: http://en.wikipedia.org/wiki/Facebook_Platform

[4] "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report-_fb_survey_scam_pr0file_viewer_2012_4_4

[5] "Whiich 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

[6] G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam/

[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/ index.htm

[8] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI

[9] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5

[10] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in *Proc. USENIX Security*, 2012, p. 32.

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

[12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. NDSS*, 2012.