Detecting Malicious Facebook Applications Using Classification Technique

Shivani Sundaram, Shruti V. Mhatre, Prof. Shilpa Satre
Bharati Vidyapeeth College of Engineering.
Sector-7, C.B.D, Belpada, Navi Mumbai-400614, India

Abstract

Online social media services like Facebook witness antremendous increase in user activity when an event takes place in the real world. Users also upload their personal information and photos to these sites without knowing much about the privacy of the site. With more than a thousand applicationsinstalls a day, third-party applications are a major reason for the popularity and addictiveness of Facebook. Unfortunately, hackers knows the potential of using applications for spreading malware and spam to get private or sensitive information and unauthorized access of the user's account. The researchers are working in this areas andso far, the research community has focused on detecting malicious posts and campaigns. In this proposed system we are developing an application which focused on detecting malicious applications on Facebook. To develop system, we use information gathered by observing the posting behavior of Facebook applications seen across users on Facebook. First, we identify a set of features that help us distinguish malicious applications from real ones. This will help in reducing malicious attack. The aim of the project is to observe at what extent can we train the system to correctly identify the malicious applications in Facebook to achieve ultimate objective to reduce the malicious attack.

Keywords: *Online social media, facebook, malicious, attacks, hackers.*

I. INTRODUCTION

The social networking sites like facebook enables third party applications to Boost up the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing a lots of exciting games or chaating with friends. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious applications can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with millions of active users There are many ways that hackers can benefit from a malicious applications:

1) These applications can reach large numbers of users and from them to their friends and so on to spread spam.
2) These applications can obtain users' personal information such as email address, birth date and many other sensitive Information
3) These applications can "re-produce" themselves by making other malicious applications popular. In other words, there is motive and opportunity, which results in many malicious applications spreading on Facebook every day.

Despite of these many risks which users are exposed to, users have very few or little information about these threats.

II. EXISTING METHOD

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 more 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) 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, Presentapplication platforms put users at risk by permitting the discovery of huge amounts of personal data and information to these applications and theirdevelopers. This paper generally abstracts main view and defines the current access control model gave to theseapplications, and builds on it to generate a more secure framework.

III. PROPOSED SYSTEM

In this work, we are going to build a system, which use classification technique to detect whether an applications is malicious or not. For this, the system will use data stored in our database.

For this, our work will contribute the following:

- First, we have designed a social networking site(like facebook).
- In that we can do all basic task like login, signup, make friend, like, comment, make post, etc.
- All the data related to all activities on the site is stored in the database.
- In our work if any application comes from the third party then first the system will check if that URL is present in active or block state in our database.
- If active, then the system will allow it to post application.
- If blocked, then the system will not allow it to post application.

If any application comes from a URL which is not in our database, that is for the first time that URL is hosting any application than the system will allow it to host.

In this way, we can suggest a way to secure user accounts from hackers.

Proposed System Architecture Diagram

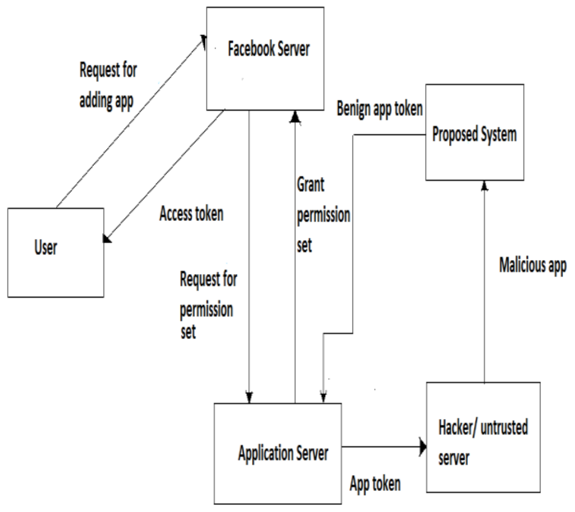

Fig: Architecture Diagram

The architecture diagram will show the functioning of our system. Whenever an application is popped out in front of user and if user wants to visit it then, the user will request the facebook server for access. The facebook server will pass request to application server after which the request will be received by our proposed system. Our system will look for it in our database that whether the URL from which the application has come is in active or blocked state, accordingly it will decide whether to grant the permission to user or not.

Advantages

1) The proposed system is a tool to detect a Malicious application.
2) It will provide security to the user's account form hackers.

IV. CONCLUSION

Till now, the researchers have found techniques to detect malicious posts and spams. But, due to these third party applications being hosted on facebook has put millions of users at security risk. Hence, in this work, we have proposed a system which will use classification techniques to detect whether an application is malicious or not.This work is a small contribution in this area for providing security to the users and reducing the malicious activity.

Hope, this small contribution will help in further research related to this area and improve the security over time.

REFERENCES

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

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

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

[4] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek. Social applications: exploring a more secure framework. In SOUPS, 2009.

[5]P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals. In WWW, 2012.

[6]M. Gjoka, M. Sirivianos, A. Markopoulou, and X. Yang. Poking facebook: characterization of osn applications. In Proceedings of the first workshop on Online social networks, WOSN, 2008.

[7] N. Wang, H. Xu, and J. Grossklags. Third-party apps on facebook: privacy and the illusion of control. In CHIMIT, 2011.

[8] Gaurav Parsewar, Yogesh Dalvi, Lalit Kothwade, “Detection of Malicious Application on Online Social Network” IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.

[9] Sushma Nallamalli, Loya Chandrajit Yadav, Karicharla Prasad, Gorla Siva Parvathi, “A Survey on Detecting Malicious Facebook Applications using FRApp” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.