FRAPEE: Securing Facebook from Malicious Applications

[1]P. HimaBindu, [2]K.Archana
[1,2]University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India

Abstract
The online social network, with 20 million installs per day, third-party applications are a major reason for the popularity of and dependence on Facebook. Unfortunately, hackers have realized the potential of using applications to spread malware and spam. The problem is more significant, as we have to be at least 13% of the applications in our collection are malicious. So far, the research community has focused on detecting malicious messages and campaigns. In this paper, we ask the question: given the Facebook application, we can determine whether it is malicious? Our key contribution to the development of a malt Facebook Rigorous application of evaluator-probably the first tool aimed at detecting malicious applications on Facebook. For the development of Frappe, we use the information gathered by observing the behavior of posting 111k Facebook application saw across 2.2 million users on Facebook. First, identify a set of functions that help us to distinguish Malicious applications from benign. For example, we find that the Malicious applications often share names with other applications, and they usually look for fewer licenses than benign applications. Secondly, using these features, we show that smoothie can detect Malicious applications with 99.5% accuracy, with no false positives and low false negative rate (4.1%). Finally, we explore the ecosystem of malicious Facebook applications and identify the mechanisms that these applications use for propaganda. Interestingly, we find that many applications in connivance and support each other; in our collection, we find the 1584 application allows viral propagation 3,723 other applications through your messages. In the long term, we see a smoothie as a step towards the creation of an independent watchdog to assess the application and ranking, so to warn Facebook users before installing applications.

Keywords
Facebook Apps, Malicious, Online Social Networks, Spam

I. Introduction

Online social networks allow and encourage third-party applications to improve the user experience on these platforms. These improvements include interesting or fun ways to communicate with online friends and activities such as playing games or listen to songs. For example, Facebook is an application where the user must first register and users can create a profile, add other users as "friends", exchange messages, updates, post status updates and photos, share videos, use various applications and receive notifications when others update their profiles. Additionally, users can join groups of users of common interest, organized by workplace, school or college, or other characteristics Facebook provides developers with an API [1] which facilitates integration of the application into the Facebook user experience. There 500K apps on Facebook [2], and on average, 20M applications are installed every day [3]. In addition, many applications have acquired and maintain a large number of users. For example, FarmVille and CityVille applications 26.5 and 42.8 users to date.

To make matters worse, the deployment of malicious applications is simplified by boxes ready to use tools from $ 25 [4]. In other words, it is mobile and used, and therefore, there are many malicious applications spreading on Facebook each day [5].

Despite disturbing trends above, a user now very limited information at the time of installing an application on Facebook. In other words, the problem is this: Given the ID number of an application (the unique identifier assigned to the application by Facebook), do you detect if the application is malicious? Currently, there are no commercial service, publicly available information, or tool based on research to advise a user on the risks of an application.

Most research related to spam and malware on Facebook has focused on detecting malicious messages and social spam campaigns [6] [7-8]. At the same time, in a step apparently back, dismantled its Facebook app functionality rating recently. A recent work studies how applications and community assessments correlated authorizations with the risk of privacy Facebook applications. [9] Finally, there are community-based efforts feedback led to classify applications, such as WhatApp? [10]; although these could be very powerful in the future, so far they have received little adoption

II. Existing System

The pirates started to take advantage of the popularity of this third-party application platform and deployment of malware [11] [12-13]. Malicious apps can provide a lucrative business for the hackers, given the popularity of OSN, with Facebook leading with 900M active users [14]. There are several ways that hackers can take advantage of a malicious application:

- The application can reach a large number of users and their friends to spread spam.
- The application can obtain personal information from users such as e -mail, hometown, and sex.
- The application can "reproduce" by other popular malicious applications.

III Proposed System

In this work , we develop Frappe, a series of effective classification techniques to identify whether an application is malicious or not . To build Frappe, we use data MyPageKeeper, a security application in Facebook that monitors Facebook profiles of 2.2 million users. We analyze 111K applications that made 91 million messages over nine months. This is probably the first completestudy of malicious Facebook applications that focuses on quantifying, profiling and understanding of malicious applications and synthesizes this information into effective detection approach .

We are going to provide below Advantages for users:

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.

IV System Architecture

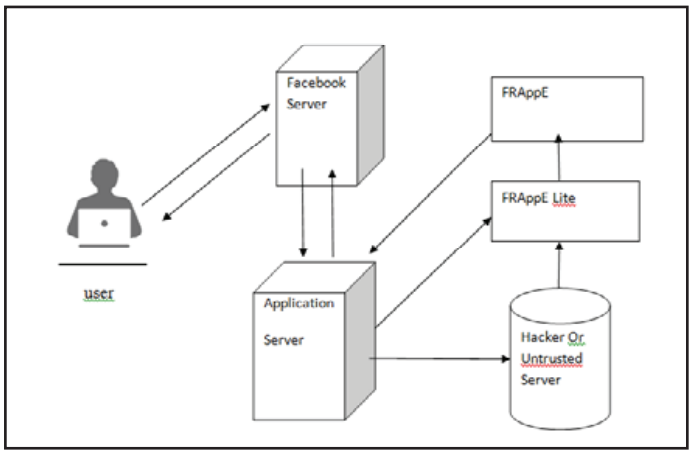

Fig. 1: Detection System Architecture

V. Detecting Malicious Apps

After analyzing the characteristics of differentiation of benign and malicious applications, we then use these features to develop effective classification techniques to identify malicious apps on Facebook . We present two variants of this malicious application classifier - FrappeLite and Frapee

A. FrappeLite

FrappeLite is a lightweight version that uses only the features of the application are available on request. Given a specific application ID, FrappeLite explores the features of the demand for this application and evaluates the request based on these characteristics in real time. We expect FrappeLite can be incorporated, for example, a browser extension that allows to evaluate any Facebook application when a user intends to install his profile.

In this work, we develop Frappe, a series of effective classification techniques to identify whether an application is malicious or not. To build FRAPPE, we use data MyPageKeeper, a security application in Facebook [15] which monitors the Facebook profiles of 2.2 million users. We analyze 111K applications that made 91 million messages over nine months. This is probably the first comprehensive study focusing on malicious Facebook applications that focuses on quantifying, profiling and understanding of malicious applications, and synthesizes this information into effective detection approach. Our work makes the following key contributions:

- We find that 13% of applications are malicious .
- The malicious and benign application profiles differ significantly.
- FRAppE can detect malicxious apps with 99% accuracy.

VI. Conclusion

An application provides a convenient way for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of the malicious application and how they work. In this project, using a large corpus of malicious Facebook applications observed over a period of nine months and found that malicious applications to differ benign applications over several characteristics. Leverage our observations , developed HITS, a specific classifier to detect malicious applications on Facebook.

References

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

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

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

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

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

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

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

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

[9] P.Chia,Y.Yamamoto, N.Asokan,"Isthisappsafe?Alargescale study on application permissions and risk signals," In Proc. WWW, 2012, pp. 311–320.

[10] "WhatApp? (beta)—A Stanford Center forInternet and Society Website with Support from the Rose Foundation," [Online]Available: https://whatapp.org/facebook/

[11] "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_2012_4_4

[12] "Whiich cartoon characterare you Facebooks u r v e y scam," 2012 [Online] Available: https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30

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

[14] Goldman,"Facebook tops 900 million users," 2012 [Online] Available: http://money.cnn.com/2012/04/23/technology/facebook- q1/index.htm

[15] "MyPageKeeper," [Online] Available: https://www.facebook.com/apps/application.php?id=167087893342260

P.HimaBindu completedM.Sc,M.Phil, M.Tech (IT), working as Asst. Professor, having 19 years of Experience, currently working in University College of Science, Saifabad, Osmania University, Hyderabad, India.

K.Archana Completed MCA and working as Asst. Professor, having 8 years of Experience, currently working in University College of Science, Saifabad, Osmania University, Hyderabad, India.