International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 389 - 393

FRAppE: Detecting Malicious Facebook Applications

Shital B, Mandhane[1]
ME Student in Computer Dept., ACEM
Pune,India
s.mandhane@gmail.com

Ismail Mohammed[2]
Prof. in Computer Engg. Dept, ACEM
Pune,India
ismail_009@yahoo.com

Abstract:- Online social media services like Facebook witness an exponential increase in user activity when an event takes place in the real world. This activity is a combination of good quality content like information, personal views, opinions, comments, as well as poor quality content like rumours, spam, and other malicious content. Even if the good quality content makes online social media very good source of information, uses of bad quality content can degrade user experience, and could have an inappropriate impact in the real world. It could also impact the enormous promptness, promptness, and reach of online social media services across the globe makes it very important to monitor these activities, and minimize the production and spread of bad quality content. Multiple studies in the past have analysed the content spread on social networks during real world events. However, little work has explored the Facebook social network. Two of the main reasons for the lack of studies on Facebook are the strict privacy settings, and limited amount of data available from Facebook, as compared to Twitter. With over 1 billion monthly active users, Facebook is about times bigger than its next biggest counterpart Twitter, and is currently, the largest online social network in the world. In this literature survey, we review the existing research work done on Facebook, and study the techniques used to identify and analyse poor quality content on Facebook, and other social networks. We also attempt to understand the limitations posed by Facebook in terms of availability of data for collection, and analysis, and try to understand if existing techniques can be used to identify and study poor quality content on Facebook.

Keywords-(OSN) – *Online social network, (OSM) Online Social Media, (PCBIR) Privacy-preserving CBIR System.*

*****

1. INTRODUCTION

Online social networks enable and encourage 3rd party applications to enhance the user experience on these platforms. Such enhancements consists of entertaining or interesting ways of communicating among online users, groups and friends,and very different unrelated activities like watching videos, playing games or listening to songs. Few examples are Facebook provides developers an API which facilitates an app integration in the FB user experience. There are 600K app present on FB, and on an average, 30M applications are installed daily]. In addition, many applications have also acquired and maintain a large user database. Like instance, Farm Ville and City Ville applications have 36.5M and 52.8M users as of today.

Today users are forced to trust the service providers for the use of their profiles. People across the globe actively use social media platforms like FB and Twitter, Facebook for distributing information, and learning about real world events now a days. A recent study shows that social media activity increases up to 300 times during major events like sports, festivals, and during natural calamities. This enflamed activity contains a lot of data about the events, but it also likely to to severe misuse like spam, misleading information, and rumour broadcast, and has thus drawn great attention from the computer science research community. Since this stream of information is generated and consumed in real time, and by common users, it is inflexible to extract useful and actionable content, and later out unwanted feed. Twitter, in particular, has been extensively studied by academics during real world events. But some of the studies have also looked at the content distributed on social media platforms other than FB and Twitter to study real-world events. Astonishingly, there has been little work on studying content on FB during real world events, which is six times bigger than Twitter in terms of the number of active users. Range of research attempts which would help to explore malicious content spread on Facebook during events. In particular, we look at 3 diverse areas, like. 1) the Facebook social graph, 2) attack and detection techniques with respect to malicious content on FB, and 3) analysis of events using online social media data. Then, we look at the various boundaries that FB poses, which makes event analysis, and detection of malicious content on this network a very hard problem. We also discuss the suggestions and study gaps in identifying and analyzing malicious user generated content on Facebook during these events.

2. PROBLEM STATEMENT

Currently, malicious applications often do not include a category, company, or description in their app summary. To detect the malicious facebook applications which may affects to user's private information on his/her profile. As we see user did not get much information about application expect name of that application while installing as a result no security available on Facebook.

3. MALICIOUS CONTENT ON FACEBOOK

The popularity and reach of Facebook has also attracted a lot of spam, phishing, malware, and other types of malicious activity. Attackers lure victims into clicking on malicious links pointing to external sources, and in literate their network. These links can be spread either through personal messages (chats), or through wall posts. To achieve maximum visibility, attackers prefer to post links publicly. Typically, an attacker initiates the attack by posting memes with attention grabbing previews, which prompt users to like, share, or comment on them in order to view them. The actions of liking, commenting or sharing spread these memes into the victim's network. Once the meme is spread, the victim is redirected to a malicious website, which can further

infect her computer, or friends network through phishing, malware, or spyware. This phishing page asks the victim to share this video with their friends in order to view it. However, once the victim shares this video, the page redirects to a random advertisement page. The video corresponding to the preview / thumbnail shown in the post does not actually exist.

Multiple other sources have cited such examples of scams and malicious posts on Facebook in the past few years. 11, 12 In addition to phishing scams, other malicious activity on Facebook includes unsolicited mass mentions, photo tagging, post tagging, private / chat messages etc. Intuitively, a user is more likely to respond to a message or post from a Facebook friend than from a stranger, thus making this social spam a more effective distribution mechanism than traditional email. This increased susceptibility to such kind of spam has prompted researchers to study, and combat social spam and other malicious activity on Facebook. We now look at the various attack and detection techniques that have been used in the past to identify and spread malicious content on Facebook respectively.

3.1 Attack techniques

In order to identify and contain malicious posts on Facebook, or any OSM, it is essential to explore and understand the techniques that are, or can potentially be deployed by attackers to spread such content. To this end, Patsakis et al. [Patsakis et al. 2009] described how Facebook can be exploited and converted into an attack platform, in order to gain some sensitive data, which can complete a perfect attacking pro le against a user. Authors created a Facebook application for demonstration purposes that on the surface was a simple application, but on the background it collected useful data. This app executed malicious code on the victim's browser, and collected the IP address of the user-victim, the browser version, the OS platform and whether some specific ports are open or closed. This data was then transmitted to the authors over email. Authors also pointed out that their app was indexed on the main list of Facebook applications, despite the fact that the description of app clearly stated that it was generating malicious transaction, and had been created for penetration testing purposes. Huber et al. presented a friend-in-the-middle attack through hijacking session cookies. Authors explained how it was possible to impersonate the victim using this technique, and interact with the network without proper authorization. However, this technique was proposed in 2011, when using HTTPS to connect to the website was optional. 13 Post 2013, all communication on Facebook uses encryption (HTTPS) by default, which means that such attacks are no more possible.

Fan et al. [Fan and Yeung 2010] proposed a virus model based on the application network of Facebook. Authors also modelled the virus propagation with an email virus model and compared the behaviours of virus spreading in Facebook and email network. Their findings revealed that while Facebook provides a platform for application developers, it also provides the same chance for virus spreading. In fact, the virus was found to spread faster on the Facebook network if users spend more time on it. The result of their simulation showed that, even though a malicious Facebook application attracts only a few users in the beginning, it can still spread rapidly. That is because users may trust their friends of Facebook and install the malicious application.

It is important to understand that in addition to the techniques described above, a large proportion of attacks on Facebook, and even other social networking platforms, make use of social engineering. This is evident since it is hard to initiate the spread of a malicious piece of content on a network without any human involvement. Attackers lure victims into using malicious applications, clicking malicious links, and sharing pieces of content, and in some cases, even pretend to provide various kinds of profits in return. Since these attacks are well-crafted in most cases, it becomes hard for a legitimate user to be able to comprehend the results of her actions. We now look at the various techniques that have been proposed to detect malicious content on the Facebook social network.

3.2 Detection techniques

Facebook has its own immune system to safeguard its users from unwanted, malicious content [Stein et al. 2011]. Researchers at Facebook built and deployed a coherent, scalable, and extensible real time system to protect their users and the social graph. This system performs real time checks and classifications on every read and write.

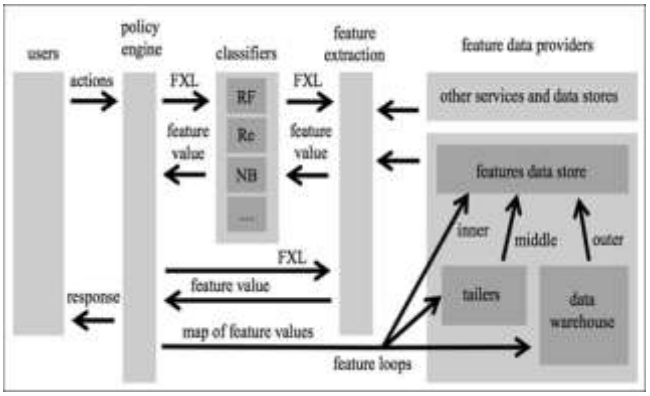

Fig 3.2. High level design diagram of the immune system deployed by Facebook.

In order to identify and contain malicious posts on Facebook, or any OSM, it is essential to explore and understand the techniques that are, or can potentially be deployed by attackers to spread such content. To this end, Patsakis et al. [Patsakis et al. 2009] described how Facebook can be exploited and converted into an attack platform, in order to gain some sensitive data, which can complete a perfect attacking pro le against a user. Authors created a Facebook application for demonstration purposes that on the surface was a simple application, but on the background it collected useful data. This app executed malicious code on the victim's browser, and collected the IP address of the user-victim, the browser version, the OS platform and whether some specific ports are open or closed. This data was then transmitted to the authors over email. Authors also pointed out that their app was indexed on the main list of Facebook applications, despite the fact that the description of app clearly stated that it

was generating malicious transaction, and had been created for penetration testing purposes. Huber et al. presented a friend-in-the-middle attack through hijacking session cookies. Authors explained how it was possible to impersonate the victim using this technique, and interact with the network without proper authorization. However, this technique was proposed in 2011, when using HTTPS to connect to the website was optional. 13 Post 2013, all communication on Facebook uses encryption (HTTPS) by default, which means that such attacks are no more possible.

Fan et al. [Fan and Yeung 2010] proposed a virus model based on the application network of Facebook. Authors also modeled the virus propagation with an email virus model and compared the behaviors of virus spreading in Facebook and email network. Their findings revealed that while Facebook provides a platform for application developers, it also provides the same chance for virus spreading. In fact, the virus was found to spread faster on the Facebook network if users spend more time on it. The result of their simulation showed that, even though a malicious Facebook application attracts only a few users in the beginning, it can still spread rapidly. That is because users may trust their friends of Facebook and install the malicious application.

It is important to understand that in addition to the techniques described above, a large proportion of attacks on Facebook, and even other social networking platforms, make use of social engineering. This is evident since it is hard to initiate the spread of a malicious piece of content on a network without any human involvement. Attackers lure victims into using malicious applications, clicking malicious links, and sharing pieces of content, and in some cases, even pretend to provide various kinds of benefits in return. Since these attacks are well crafted in most cases, it becomes hard for a legitimate user to be able to comprehend the results of her actions. We now look at the various techniques that have been proposed to detect malicious content on the Facebook social network.

Facebook itself has confirmed that spam as a serious issue, and taken steps to reduce spam content in users. Identifying spam on Facebook, is still a very rigid problem. Even though the Facebook having a high performance immune system of their own [Stein et al. 2011], users still faces an enormous number of spam and malicious content daily. Existing approaches to detect spam in other online social media services like Twitter [Benevenuto et al. 2010; Grier et al. 2010; McCord and Chuah 2011; Wang 2010], cannot be directly ported to Facebook due to multiple issues. These include the public unavailability of critical pieces of information like pro le, and network information, age of the account, no limit on post length, etc. There exists dire need to study spam content on Facebook, and develop techniques to identify it cogently, and automatically.

4. THE PROPOSED FRAMEWORK AND ARCHITECHTURE

In this area of work, we develop FRAppE as a suite of efficient classification techniques for identifying whether an application is malicious or not. We have to use data from MyPageKeeper to build FRAppE, a security application in FB that screens the Facebook profiles of 2.5 million users. We analyse 150K applications those made 95 million posts over nine months. This is tably the first complete study focusing on malicious Facebook applications that focuses on profiling, quantifying and understanding malicious applications, and synthesizes this information into an effective detection approach.

We have also introduced two features that is classifiers to detect the malicious applications FRAppE Lite and FRAppE . In the first classifier it detect the initial level detection that is applications identity number , name and source etc. and in second level detection the actual detection of malicious application has been done.

Advantageous

- Facebook Rigorous Application Evaluator is arguably is the tool to detect malicious applications.
- It provides security to users profiles from malicious applications.

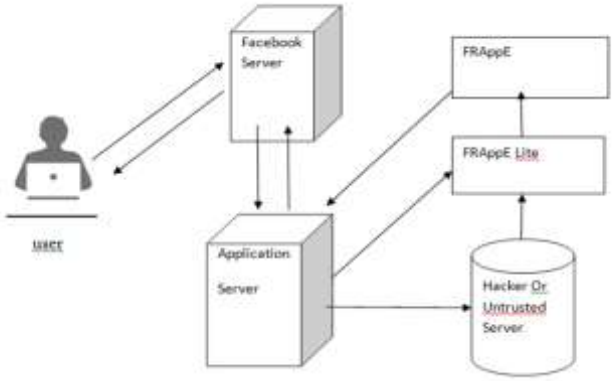

Fig.4.1. System Architecture of proposed framework

Feature removal component. The extracted feature vectors are accomplished of characterizing the underlying content. They first undergo an orthogonal transform and dimension reduction. Only significant features are preserved. The elements of a feature vector are splited into ‘n’ groups. A robust hash value hi (i = 0,1,⋯,n − 1) is computed from the ith group. We call it asub-hash value. The above step creates a new coordinate system, with each coordinate represented by a sub hash values. Finally, a multimedia object in the database is indexed by the overall hash value H= h0||h1||⋯||hn−1 that is., the concatenation of sub hash values.

Each sub hash value is associated with an inverted index list. The list contains the identification information of multimedia objects matching to the sub hash value. The size of a sub hash value l depends on the significance of its corresponding feature elements.

5. MATHEMATICAL MODEL

Let S is the Whole System Consists:

S = {U, P, Req, A, APP}.

1. U is the set of number of user on the facebook.

U={u1,u2,……..un}.

2. P is the set of number of permission set for user .

P={p1,p2,……pn}.

3. Req is set of number of add app request from user to server.
Req={a1,a2,……an}.

4. A is the set of number of set of access tokens of user.

5. APP is the set of number of facebook benign application available on facebooks application server.

APP = {ap1,ap2,……apn}.

6. LITERATURE SURVEY

Paper Name	Published Year	Author	Description
FRAppE: Detecting Malicious Facebook Applications	2015	Md S. Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos	Developed FRAppE, an accurate classifier for detecting malicious Facebook applications. uses data from mypagekeeper app, a security app in facebook that monitors the facebook profiles.
LIBSVM: A library for support Vector machines. Analysing Facebook Privacy Settings: User Expectations vs. Reality	2011	C.-C. Chang and C.-J. Lin.	LIBSVM is a library for Support Vector Machines (SVMs). This paper helps users to easily apply SVM to their applications. The article presents all implementation details of LIBSVM. Issues such as solving SVM optimization problems, multi-class classication, probability estimates, and parameter selection are discussed in detail
Analysing Facebook Privacy Settings: User Expectations vs. Reality	2011	Y. L. Krishna, P. G. Balachander , Krishnamurthy Alan Mislove	The paper focus on measuring the disparity between the desired and actual privacy settings, quantifying the magnitude of the problem of managing privacy
WARNINGBIRD: Detecting Suspicious URLs in Twitter Stream	2012	Sangho Leey and Jong Kimz	WARNINGBIRD, a suspicious URL detection system for Twitter. Instead of focusing on the landing pages of individual URLs in each tweet, considered correlated redirect chains of URLs in a number of tweets. Because attackers have limited resources and thus have to reuse them, a portion of their redirect chains will be shared.

7. DISCUSSION

In this section, we discuss potential measures that hackers can take to evade detection by FRAppE. We also present recommendations to Facebook about changes that they can make to their API to reduce abuse by hackers. Robustness of features. Among the various features that we use in our classification, some can easily be obfuscated by malicious hackers to evade FRAppE in the future. For example, we showed that, currently, malicious applications often do not include a category, company, or description in their app summary. However, hackers can easily fill in this information into the summary of applications that they create from here on. Similarly, FRAppE leveraged the fact that profile pages of malicious applications typically have no posts. Hackers can begin making dummy posts in the profile pages of their applications to obfuscate this feature and avoid detection. Therefore, some of FRAppE's features may no longer prove to be useful in the future while others may require tweaking, e.g., FRAppE may need to analyze the posts seen in an application's profile page to test their validity. In any case, the fear of detection by FRAppE will increase the onus on hackers while creating and maintaining malicious applications. On the other hand, we argue that several features used by FRAppE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are robust to the evolution of hackers. For example, to evade detection, if malicious app developers were to increase the number of permissions required, they risk losing potential victims; the number of users that install an app has been observed to be inversely proportional to the number of permissions required by the app. Similarly, not using different client IDs in app installation URLs would limit the ability of hackers to instrument their applications to propagate each other. We find that a version of FRAppE that only uses such robust features still yields an accuracy of 98.2%, with false positive and false negative rates of 0.4% and 3.2% on a 5-fold cross validation.

8. RESULTS

Detecting spam on ONLINE SOCIAL NETWORKSs. Gao et al. [32] analyzed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. In other work, Gao et al. [31] and Rahman et al. [41] develop efficient

techniques for online spam filtering on ONLINE SOCIAL NETWORKSs such as Facebook. While Gao et al. [31] rely on having the whole social graph as input, and so, is usable only by the ONLINE SOCIAL NETWORKS provider, Rahman et al. [41] develop a 3rd application for spam detection on Facebook. Others [37,44] present mechanisms for detection of spam URLs on Twitter. In contrast to all of these efforts, rather than classifying individual URLs or posts as spam, we focus on identifying malicious applications that are the main source of spam on Facebook. Detecting spam accounts. Yang et al. [46] and Benevenuto et al. [26] developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot based approach [36, 43] to detect spam accounts on ONLINE SOCIAL NETWORKSs. Yardi et al. [47] analyzed behavioral patterns among spam accounts in Twitter. Instead of focusing on accounts created by spammers, our work enables detection of malicious applications that propagate spam and malware by luring normal users to install them. App permission exploitation. Chia et al. [29] investigated the privacy intrusiveness of Facebook applications and concluded that currently available signals such as community ratings, popularity, and external ratings such as Web of Trust (WOT) as well as signals from app developers are not reliable indicators of the privacy risks associated with an app. Also, in keeping with our observation, they found that popular Facebook applications tend to request more permissions. They also found that 'Lookalike' applications that have names similar to popular applications request more permissions than is typical. Based on a measurement study across 200 Facebook users, Liu et al. [38] showed that privacy settings in Facebook rarely match users' expectations. To address the privacy risks associated with the use of Facebook applications, some studies [27, 45] propose a new application policy and authentication dialog. Makridakis et al. [40] use a real application named 'Photo of the Day' to demonstrate how malicious applications on Facebook can launch DDoS attacks using the Facebook platform. King et al. [34] conducted a survey to understand users' interaction with Facebook applications. Similarly, Gjoka et al. [33] study the user reach of popular Facebook applications. On the contrary, we quantify the prevalence of malicious applications, and develop tools to identify malicious applications that use several features beyond the required permission set. App rating efforts. Stein et al. [42] describe Facebook's Immune System (FIS), a scalable real-time adversarial learning system deployed in Facebook to protect users from malicious activities. However, Stein et al. provide only a high-level overview about threats to the Facebook graph and do not provide any analysis of the system. Furthermore, in an attempt to balance accuracy of detection with low false positives, it appears that Facebook has recently softened their controls for handling spam applications [11]. Other Facebook applications [5,7,15] that defend users against spam and malware do not provide ratings for applications on Facebook. Whatapp [23] collects community reviews about applications for security, privacy and openness. However, it has not attracted much reviews (47 reviews available) to date. To the best of our knowledge, we are the first to provide a classification of Facebook applications into malicious and benign categories.

9. CONCLUSION AND FUTURE WORK

Applications present a convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious applications and how they operate. In this work, using a large corpus of malicious Facebook applications observed over a nine month period, we showed that malicious applications differ significantly from benign applications with respect to several features. For example, malicious applications are much more likely to share names with other applications, and they typically request fewer permissions than benign applications. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of AppNets— large groups of tightly connected applications that promote each other. We will continue to dig deeper into this ecosystem of malicious applications on Facebook, and we hope that Facebook will benefit from our recommendations for reducing the menace of hackers on their platform.

REFERENCE

[1] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2, 2011

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

[3] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 20124. J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011

[4] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011.

[5] Lee, J. Caverlee, and S. Webb. Uncovering social spammers: social honeypots + machine learning. In SIGIR, 2010

[6] Lee and J. Kim. Warningbird: Detecting suspicious urls in twitter stream. In NDSS, 2012.

[7] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In IMC, 2011.