ISSN: 2321-7782 (Online)
Volume 3, Issue 11, November 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on a FRAppE: Detecting Malicious Facebook Applications

Shital B. Mandhane[1]
ME Student in Computer Dept., ACEM
India

Ismail Mohammed[2]
Prof. in Computer Engg. Dept, ACEM
India

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. Although, the good quality content makes online social media a rich source of information, consumption of poor quality content can degrade user experience, and have inappropriate impact in the real world. In addition, the enormous popularity, promptness, and reach of online social media services across the world makes it essential to monitor this activity, and minimize the production and spread of poor 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: (CBIR) Content Based Information Retrieval, (OSM) Online Social Media, (PCBIR) Privacy-preserving CBIR System.

I. INTRODUCTION

In the Internet era, multimedia content is massively produced and distributed. In order to efficiently locate content in a large-scale database, content-based search techniques have been developed. They are used by content based information retrieval (CBIR) [1] systems to complement conventional keyword-based techniques in applications such as near-duplicate detection, automatic annotation, recommendation, etc. In such a typical scenario, a user could provide a retrieval system with a set of criteria or examples as a query; the system returns relevant information from the database as an answer. Recently, with the emergence of new applications, an issue with content-based search has arisen sometimes the query or the database contains privacy-sensitive information [3][1]. In a networked environment, the roles of the database owner, the database user, and the database service provider can be taken by different parties, who do not necessarily trust each other. A privacy issue arises when an untrusted party wants to access the private information of another party. In that case, measures should be taken to protect the corresponding information.

The main challenge is that the search has to be performed without revealing the original query or the database. This motivates the need for privacy-preserving CBIR (PCBIR) systems. Privacy raised early attention in biometric systems, where the query and the database contain biometric identifiers. Biometric systems rarely keep data in the clear, fearing thefts of such highly valuable data. Similarly, a user is reluctant in sending his biometric template in the clear. Conventionally, biometric systems [5] rely on cryptographic primitives to protect the database of templates. In the multimedia domain, privacy issues recently emerged in content recommendation. With recommendation systems, users are typically profiled. Profiles are sent to service providers, which send back personalized content.

Users are today forced to trust the service providers for the use of their profiles. Although CBIR systems have not been widely deployed yet, similar threats exist. Recently, the one-way privacy model for CBIR was investigated [1]. The one-way privacy setting assumes that only the user wants to over the past decade, online social media (OSM) has stamped its authority as one of the largest information propagators on the Internet. OSN services have deled all regional, cultural, and language boundaries, and provided every Internet user on the planet with an equal opportunity to speak, and be heard. Nearly 25% of the world's population uses at least one social media service today. 1 People across the globe actively use social media platforms like Twitter and Facebook for spreading information, or learning about real world events these days. A recent study revealed that social media activity increases up to 200 times during major events like elections, sports, or natural calamities [Szell et al. 2014]. This swollen activity contains a lot of information about the events, but is also prone to severe abuse like spam, misinformation, and rumour propagation, 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 hard to extract useful and actionable content, and later out unwanted feed. Twitter, in particular, has been widely studied by researchers during real-world events [Becker et al. 2011; Hu et al. 2012; Kwak et al. 2010; Sakaki et al. 2010; Weng and Lee 2011]. However, few studies have looked at the content spread on social media platforms other than Twitter to study real-world events [Chen and Roy 2009; Hille and Bakker 2013; Osborne et al. 2012]. Surprisingly, there has been little work on studying content on Facebook during real world events [Westling 2007], which is five times bigger than Twitter in terms of the number of monthly active users. Range of research attempts which would help to explore malicious content spread on Facebook during events. In particular, we look at three distinct areas, viz. a) the Facebook social graph, b) attack and detection techniques with respect to malicious content on Facebook, and c) analysis of events using online social media data. Then, we look at the various limitations that Facebook poses, which makes event analysis, and detection of malicious content on this network a hard problem. Towards the end, we discuss the implications and research gaps in identifying and analysing malicious user generated content on Facebook during events.

II. Problem Statement

Currently, malicious apps 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.

III. 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 profile 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 apps, 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.

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.

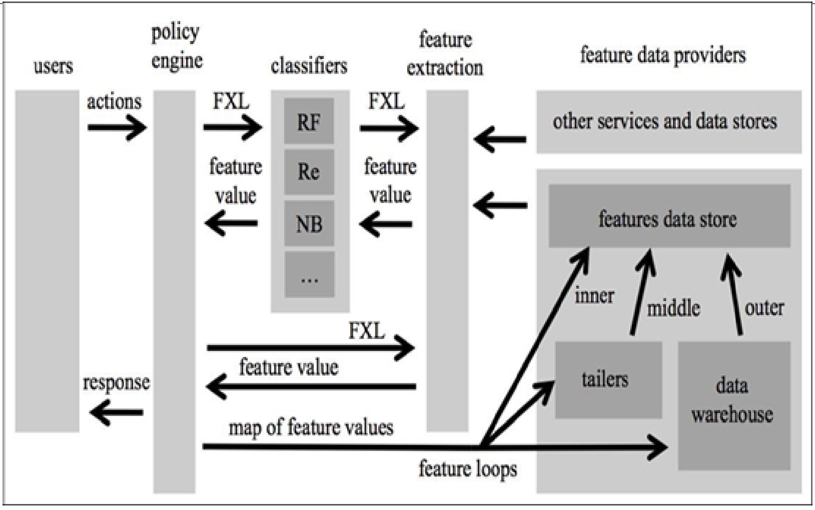

Fig 3.2. High level design diagram of the immune system deployed by Facebook.

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 profile 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 apps, 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 spam as a serious issue, and taken steps to reduce spam content in users, newsfeed recently [Owens and Turitzin 2014]. Identifying spam on Facebook, however, evidently remains a hard problem. Despite of Facebook having a high performance immune system of their own [Stein et al. 2011], users still encounter an enormous number of spam and malicious content on regular basis. 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.

IV. The Proposed Framework

In this work, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from MyPageKeeper. To build FRAppE, we use data from MyPageKeeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyse 111K apps that made 91 million posts over nine months. This is arguably 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 detection approach.

We have introduced two features i.e. classifiers to detect the malicious apps FRAppE Lite and FRAppE . In first classifier it detect the initial level detection e.g. apps identity number , name and source etc. and in second level detection the actual detection of malicious app has been done.

Advantageous

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

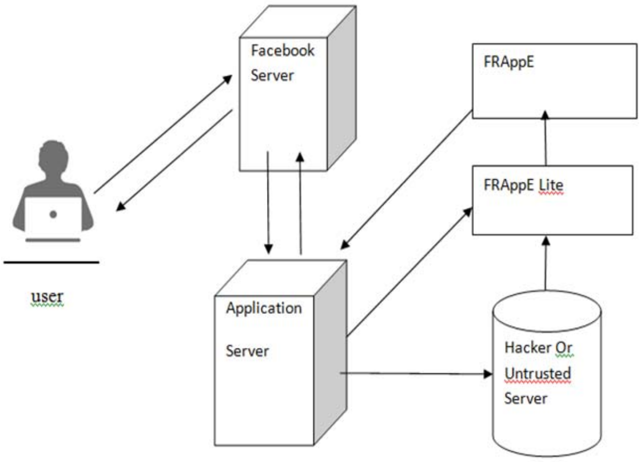

Fig.4.1. System Architecture of proposed framework

Feature extraction component. The extracted feature vectors are capable 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 divided 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 value. Finally, a multimedia object in the database is indexed by the overall hash value H = h0||h1||···||hn−1, i.e., the concatenation of sub-hash values.

Each sub-hash value is associated with an inverted index list (also called a hash bucket). The list contains the IDs (identification information) of multimedia objects corresponding to the sub-hash value. The size of a sub-hash value l depends on the significance of its corresponding feature elements

V. 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.

VI. Conclusion

In this survey, we explored various research attempts towards exploring the Facebook network, analyzing malicious content on it, and analyzing events on online social media in general. The aim of this survey was to look at relevant literature, which could aid in studying and combating malicious user generated content spread on Facebook during events. In order to keep this survey focused, we did not cover a variety of possibly relevant research areas including detection of compromised / fake accounts, and sybil nodes in the Facebook network, detection of spam on other social networks like Twitter, credibility / trustworthiness of information of user generated content, and event detection in online social media. We also looked at the various challenges and limitations posed by Facebook (as discussed in Section 3). Apart from technical limitations, there exist various research gaps in existing literature, which are yet to be addressed and explored.

References

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.