ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Survey on Malicious Application Detection on Social Network

Vidya Dhamdhere[1], Sheetal Gund[2], Tejaswini Zade[3], Radhika Tiwari[4], Ashish Salunkhe[5]

Asst. Professor**,** G.H. Raisoni College of Engineering and Management, Wagholi, India[1]

Student, G.H. Raisoni College of Engineering and Management, Wagholi, India[2,3,4,5]

ABSTRACT*:* Online social media services like Face book 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 rumors, 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 analyzed the content spread on social networks during real world events. However, little work has explored the Face book social network. Two of the main reasons for the lack of studies on Face book are the strict privacy settings, and limited amount of data available from Face book, 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 analyze 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: Intrusion Detection Systems, Digital Forensic Logs, Cryptography**.**

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) [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. 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 URL on to the specified sites are recognize d by some method like feature extraction.
Malicious URL and data have a natural Progression between using traditional internet technologies, such as web browsing exploiting the inherent trust and size of social networks to help spread their attacks. appearing to come from one of yours friends ,usuallyadvertising a funny video .when the victim clicks the link to watch the video they are make with a pop-up message stating that they need to update their links when the user clicks to download the update,they are actually downloading malicious data .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

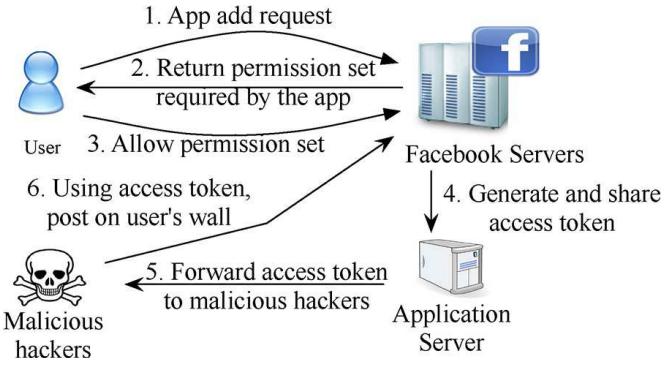
Vol. 4, Issue 9, September 2016

II. EXISTING SYSTEM

Ever since the personal computer changed the lives of people around the world, we have become accustomed to the notion of software applications. The personal computer world started out with completely open platforms where all applications (apps) ran with the same complete set of privileges available to the user. This quickly gave rise to the phenomenon of malicious and inappropriate software [7]. Operating system and runtime platform security schemes can be used to apply the principle of least authority to applications. Although various platform security schemes were developed since the 1960s, they saw widespread deployment only when they were incorporated into Java Security Architecture and into mobile device platforms.

On the other hand, the Normal permissions govern the functionalities which can be annoying (e.g., vibrating the phone), while the Dangerous permissions protect the user from operations that can be potentially harmful including those that cost money or potentially privacy intrusive [8]. The details of individual Android permissions can be found on [9].

All current OSNs adopt the client-server architecture. The OSN service provider acts as the controlling entity. It stores and manages all the content in the system. On the other hand, the content is generated by users spontaneously from the client side. The OSN service provider offers a rich set of well-defined interfaces through which the users can interact with others. Currently two popular ways of interaction exist. Facebook is representative of OSNs that adopt the interaction between a pair of sender and recipient as their primary way of interaction, although they also support other ways. Twitter is representative of OSNs that adopt broadcasting as their primary way of interaction



III. PROPOSED SYSTEM

Connectively Me is the system which provides a secure way to handle the OSN wall and its related difficulties. The system able to filter out unwanted messages, images and links from social network user walls. In this module first we can create user GUI like user can login with our application by adding his personal information like his name, password, address etc.

a) User Registration (Sign In / Signup)

In this module first user register with our application by adding his personal information like his name, password, address and his hobbies etc. After registering with our application he can login with us using userid and password.

b) Adding / Inviting Friends

After login into the system a user can add friends by seeing there profiles, in this module user sends requests to the friends when user accepts the request, he becomes his friends. Also user can Invite friends regarding any invent.

c) Chatting / Messaging

After adding friends user can see online friends andselect a particular friend for chatting.Figureshows data flow diagram a simple connectivitybetween user and server are shown.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

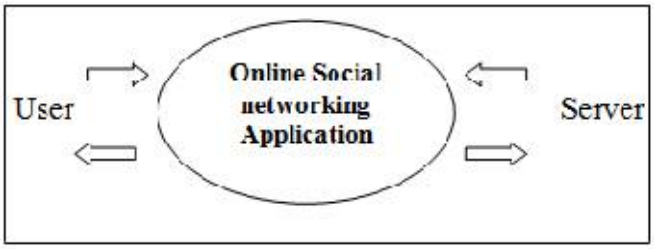


Figure 1: Data flow diagram 0

B. FILTERING PATTERN

In defining the language for FRs specification, we consider three main issues that, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on their profile s attributes. In such a way it is, forinstance, possible to define rules applying only to young creators or to creators with a given religious/political view. Given the social network scenario, creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth and trust values of the relationship creators should be involved in order to apply them the specified rules.

C. IMAGE FILTERING

In this we are using the LSB algorithm to filter the images and decode the text from the images and display it. In this we are avoiding the misuse of Social Networking by the terrorist to pass their secrets messages through images.

D. PHISHING PREVENTION FOR LINKS POSTED ON USER WALLS

Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a faked Web site by sending them faked e-mails (or instant messages), and stealthily get victim's personal information such as user name, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). So we are providing here antiphishing environment for the links posted on user wall.

IV. SYSTEM ARCHITECTURE

Three Tier architecture is used in OSN services. These three layers are:
A) Social Network Manager (SNM)
B) Social Network Application (SNA)
C) Filtered Wall (FW)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

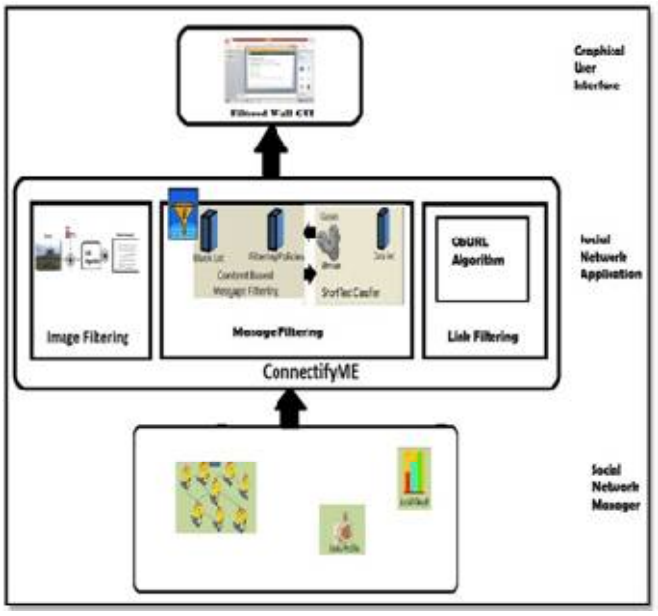


Figure 2: Block diagram

Above figure shows the Filtering of Unwanted Message, Images and Phish Links on OSN.

IV. FUTURE SCOPE

Applications present a convenient means for hackers to spread malicious happy on Facebook. However, little is tacit about the characteristics of malicious apps and how they operate. In this work, using a large body of malicious Facebook apps observed over a nine month dated, we exhibited that malicious apps differ significantly from benign apps with respect to several features. For example, malicious apps are much more likely to share names with other apps, and they typically request fewer permissions than benign apps. Leveraging our explanations, we developed FRAppE, an correct classifier for detecting malicious Facebook applications. Most interestingly, we painted the emergence of App Nets— large groups of tightly connected applications that promote each other. We will continue to dig deeper into this system of malicious apps on Facebook, and we optimism that Facebook will benefit from our endorsements for reducing the menace of hackers on their podium. REFE

V. CONCLUSION

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

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

[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] A. Le, A.Markopoulou, and M. Faloutsos, PhishDef: URL names say it all,‖ in Proc. IEEE INFOCOM, vol-1, pp. 191–195,2011.
[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D.Song, Design and evaluation of a real-time URL spam filtering service,‖ in Proc. IEEESymp.
[6] Security Privacy, pp. 447–462, 2011.
A. Makridakis et al., ―Understanding the behavior of malicious applications in social networks,‖ IEEE Netw., vol. 24, no. 5, pp. 14–19, Sep.–Oct.2010.
[7] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," Trans. Intell. Syst. Technol., vol. 2, no. 3, 2011, Art. no. 27.
[8] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs," in Proc. KDD, 2009, pp. 1245–1254.
[9] A. Le, A. Markopoulou, and M. Faloutsos, "PhishDef: URL names say it all," in Proc. IEEE INFOCOM, 2011, pp. 191–195.
[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.