An Information Diffusion Model to analyze the Behavior of Online Social Network based Malwares

Akansha Pandey
pnakansha@hotmail.com

Ezhil Kalaimannan
Department of
Computer Science
University of West Florida
Pensacola, FL 32514
ekalaimannan@uwf.edu*

S. Venkatesan
Department of
Information Technology
Indian Institute of
Information Technology
Allahabad,India
venkat@iiita.ac.in

Abstract

In this paper, we report a work in progress research, which aims to analyze the information diffusion behavior of Online Social Networks (OSNs). To be able to do this, we intend to study various malware infection models in Social Networking Sites (SNSs). Our proposed research will mainly focus on analyzing multiple epidemic and malware infection models affecting popular SNSs like Facebook, Twitter, and LinkedIn etc. due to dissemination of information.

keywords: Online social network (OSN); Epidemic models; Information diffusion; Malware Analysis; Cybersecurity

1. Introduction

Social Networking Sites are continuously growing to be a "media" for socio-economic connection, learning, entertainment and business. The enormous amount of data flow and exchange in the form of text, audio, video, images etc. through SNSs have provided attackers with incredible abilities to exploit users vulnerabilities by spreading malware. Some of the privileged targets are:

- Online Social Networks (OSNs): With a low level of awareness about the existing cyber threats, OSN users are ideal victims for cyber crime such as social engineering and malware based attacks, which circumvent them toward malicious backdoors and remote servers.
- Organizations: Organizations are more prone towards cyber attacks such as cyber espionage, electronic fraud and several variants of phishing attacks.

In a typical social network model analysis, the whole network is represented as a graph, where people/organizations are represented by nodes and are then connected through various relationship patterns, which exist among them. We propose to develop a social network analysis framework using information diffusion and social contagion, which focuses on analyzing and modeling the characteristics of the information flow and exchange between various OSN users [1].

Further, information exchange is related to the disseminated content and social influence of nodes through which it flows through the entire network model. In the past, a significant number of researchers have studied the pros and cons of malware propagation models as mentioned in [2], where the author compares and contrasts various worm epidemic models such as KermackMckendrick Model and the Two Factor model. Hence, we intend to study various malware epidemic models and analyze how various these models outline the infectious behavior and dissemination of information flow found in popularly known OSNs.

2. Literature Review

Online Social Network has allowed researchers and adversaries to access unprecedented amount of information, which are exchanged through social interactions, advertisements, news alerts and event notifications. Having a knowledge about information diffusion in OSNs, will help to gain better understanding about the dynamics of malicious contents and comprehensive socio-technical systems. Sanzgiri et al. proposed a methodology to investigate Twitter by considering factors such as obfuscation of content by URLs,

*Corresponding author: Ezhil Kalaimannan (E-mail: ekalaimannan@uwf.edu)

978-1-4673-9795-7 2015

DOI 10.1109/CSCI.2015.57

broadcast nature of tweets and user-follower model for malware propagation [3]. Weng studied information diffusion process based on components like actors, content, network structure of SNSs and various diffusion mechanism affected by the homophile and social reinforcement [4]. Garg et al. analyses the Susceptible-Infected (SIS) disease model applied to SNSs based on the Erdos Renyi method [1]. This study shows that the diffusion increases when information is posted on a network of friends and the speed of diffusion is not related with the size of network. Cheng et al. proposed an epidemic model based on differential equations for malware propagation in a generalized social network context [5]. This model illustrates a methodology to approximate the severity and propagation speed of hybrid malware.

It is evident from the brief review of existing work that no light has been thrown on analyzing the OSN based malwares using a mathematical model. With this in view, we intend to develop an information diffusion model to analyze the behavior of SNS users and malware infection in OSNs.

3. Research Hypothesis

In the big data era, it is difficult to map the factors for contagion of malicious content in SNSs, where information diffusion process is governed by socio-economic influence and homophile connected people, who tend to share their attributes to promote similarities in behavior. Research studies in the past, have shown the aspect of how malware could affect the spread of information in different OSNs under the influence of various factors like social interactions, community structure and different type of information feeds.

To understand the influencing factors for the diffusion of information in SNSs, it is important to analyze the behavior of malwares like XSS worm, code red worm, beta box, koobface worm, webcam thingy, rainbow twitter worm etc. Further, the behavior of users such as periodic interests, leaving/joining groups and types of participant roles in information diffusion, must also be considered. Our objectives of research includes the following:

- Study various epidemic models like kermack mck- endrick, e-SEIR and the two factor Worm model.
- Simulate and analyze XSS worm, code red worm, beta box, koobface worm, web-cam thingy and rainbow twitter worm.
- Analyze user behavior, which can influence the dissemination of information in various SNSs like Facebook, twitter, LinkedIn etc.
- Propose an efficient information diffusion model based on the analysis results.

Thus, our proposed research will aim to understand:

- How SNSs can be better used for external communications, customer support and targeted marketing?
- With user and data production growing at a rapid rate, how spam (irrelevant information) and fake advertisements can be detected using a better approach?
- How a user can be protected from the popular OSN based attacks such as information leakage, clickbait attacks and hash tag traffic hijacking?

4. Conclusions

In this paper, we have presented our work in progress research to develop an improved and efficient information diffusion model, which aims to provide better insight about the malicious activities in OSNs. As a part of continued research work, we intend to present an information diffusion model based on how malware can spread in OSNs using information dissemination and what are the factors that an attacker can consider for his attack to be successful in SNSs

References

[1] Shweta, G and Sanjeev, Kumar, Modeling and Analyzing Information Diffusion Behavior of Social Networks, *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),IEEE*, pp.566 - 572, 2014.

[2] Aliyu, M., Sulaiman, M.N and Muhammad, N.M, Analysis of Internet Malware Propagation Models and Mitigation Strategies, *IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501*, Vol. 2, No. 1, 2012.

[3] Ameya, S., Jacob, J and Shambhu, U, The Early (tweet-ing) Bird Spreads the Worm: An Assessment of Twitter for Malware Propagation, *The 9th International Conference on Mobile Web Information Systems (MobiWIS)*, 2011.

[4] Lilian, W, Information diffusion on online social network, *Indiana University, in partial fulfillment of the requirements for the degree of Doctor of Philosophy*, 2014.

[5] Shin-Ming, C., Weng, C.A., Pin-Yu, C and Kwang-Cheng, C, On Modeling Malware Propagation in Generalized Social Networks, *IEEE communication letters*, Vol. 15, No. 1, 2011.