ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 644-648
doi: 10.18178/wcse.2017.06.112

Research on Security of Online Social Network

Liping Teng[1 +, 2], Bugen Huang [1] , Dong Cai [1,2]

[1] Jiangsu Police Institute

[2] Key Laboratory of Police Geographic Information Technology, Ministry of Public Security

Abstract. Online social network is a new tool for the publics to exchange information and establish interpersonal interaction by using computing technology and information technology. The security threats hidden in online social network have never stopped for a moment, therefore online social network security risks and hazards attract widespread attentions. This paper introduces the concept, characteristics and current security situation of online social network, analyzes the common attacks to social network and the current security strategies. The prospects of security research of online social network are discussed at the end of the paper.

Keywords: attacks, online social network, security threats.

1. Introduction

Online Social Networks (OSN), also known as Social Media Networks (SMN) or Social Network Sites(SNS), refers to Online network platform for people who have common interests, behaviors, backgrounds to establish social relations [1]. Today, Twitter, Facebook, Sina micro-blog and so on are very popular social networks. Users can share news, logs, pictures, videos and maintain interpersonal relationships through online social networks. Due to the openness of social networks, people can establish relationships easily and be free from time and space constraints. Compared with traditional websites, the spread of information among social networks has random, uncontrollability and unprecedented spreading influence, making it a powerful tool for the spread of public opinion.

Online social networks provide much convenience for human's social interaction, having the following characteristics: First of all, the number of users is very large, and the user types are complex and the interaction modes are diversified. Secondly, flexible using and more functions make it is hard to control users' behavior. Then, a high degree of openness and a large amount of information lead it is difficult to manage. These features make online social network security issues particularly prominent. In order to interact by utilizing the online social networking platform, people are willing to share their own personal information with others on the social network, such as nickname, photos, gender, company, even the real name, birthday . If lacking good protection, users' privacy information will be exposed to serious threats. The massive number of online social network users also attracts the attention of the attackers, and the attackers can gain huge interests in this park. The attackers publish malicious ads, pornographic videos, phishing links, and other malicious information in social networking sites through many false accounts. Due to the trust relationship among online social network users, the malicious information is more dangerous than traditional spam, etc. The study found that the click rate of spam links in Twitter is two orders of magnitude higher than that in traditional spam [2]. These malicious attacks pose a serious threat to the normal users' information privacy, account security and user experience. In addition, attackers gain interests through some abnormal accounts for adding friends, malicious mutual fans, pointing likes and other acts. As the global

+ Corresponding author. Tel.: + 86-13951861896.
E-mail address:780980050@qq.com.

wide using and the hidden potential huge benefits of online social networks, much of hackers' attention and interest is aroused, which leading to endless network attacks to social network platforms.

2. Common Attacks of Online Social Networks

2.1. SQL Injection Attack

SQL injection attack is the most commonly attack in the Web [3]. SQL injection is that an attacker finds the loopholes in the WEB server and inserts the illegal SQL command to the Web server-side database in order to spoof the server to execute malicious SQL commands to obtain user permissions, and then the attacker operates the database and has access to the unlisted data of the database. Even worse attackers use malicious SQL command to delete or destroy the data in the database.

Online social networks need to use the database to store information, whether user information, publishing information or other types of data, so the database is a very important part of the online social networking environment. The SQL command is the interface between the front-end Web and the back-end database, so that the data can be passed to or from the Web applications. But SQL query request is often generated by using the parameter dynamic which users input, which helps the attackers who visit the Web page to open a window. The attackers enter their SQL command through the URL, form fields or other input fields in order to query properties, fool the application, so as to visit the database without restriction.

2.2. Sybil Attack

Traditional sybil attack means that malice user set up a lot of false identifications, keep away form the prestige system through the trust relationships between nodes. Social networks contain many friendships; users get the privacy information access authorities through trust relationships, this give the convenience for sybil attack. Researcher find that there are a lot of sybil nodes transmitting junk mail and malice software in Twitter and Facebook. When the attacker get the trust of normal node, he set up new identification and sybil node, send illegal data to goal nodes pretend to be a normal node, these actions occupy the resource of networks, degrade the prestige of the normal node. If there is no identification mechanism, attacker can compile program to build random sybil identification, or sent information to sybil node through steeling other user's legal identification.

2.3. Abnormal Account Attack

Zombie accounts [4] are fake accounts created by attacker through some automatic tools. These fake accounts are used to send messages or add friends. Zombie accounts are reflections of creating period of anomaly accounts. They focus on the creating process and the purpose of creating these accounts is not taken into account. Creating features, such as naming features of these accounts nicknames are mainly used to detect zombie accounts.

Spam accounts are common names of these false accounts in application period. These accounts are primarily used to post ads, fishing, pornography and other information, or to maliciously change social network reputation, such as malicious acts, add fans, add friends, praised each other.

Compromised accounts are Hijacked accounts, The account was originally a normal account, but be hijacked by an attacker to perform malicious acts. Normal user account has a lot of friends, and have a normal behavior, so the attackers through a variety of methods to steal accounts properly for malicious behavior. As the Compromised accounts are created by normal users, there is no creating or developing period features, these mutations of accounts activities are mainly used to detect the Compromised accounts.

Spam Campaign means attacker creates a large number of false accounts and steals Compromised account during the set time period to spread malicious information or perform other malicious acts. The Spam Campaign is mainly detected by the behavior of these accounts during the same time period, such as publishing the same message or praising the same page.

2.4. Cross Site Scripting Attack

Cross Site Scripting (XSS) attack is a common form of attack that threatens the security of social network platforms. It is the focus of research on social network attacks. The existence of XSS vulnerability brings security risks and threats to social network security and user information. XSS attack means malicious attackers find the XSS vulnerabilities or code vulnerabilities of the WEB server. The attacker can choose to

upload the malicious code to the WEB server, or send the URL address of the WEB site containing the malicious script code to the user. When the user access the Web interface with malicious code or open a malicious URL link, the malicious code will be executed automatically by the user's browser, so as to achieve the purpose of the attacker.

Ajax technology is applied to the background of social networking, and the HTML language that the technology used has strong interaction. The user can provide the script to the background, so WEB-side is vulnerable to attacks and threats. The attack program mainly exists between the user node and the site node, and the site node take up most of the resource consumption, not leading to network congestion and collapse. Social networking users are highly active and have high interactivity, which increases the probability that latent XSS worms are activated.

3. The Security Strategies of Online Social Network

Different types of secure social networking solutions are emerging for the different types of security problems described above. This article focuses on Sybil attacks and abnormal account attacks.

3.1. Detection Method for Sybil Attack

The detection of Sybil attacks should be based on a certain network structure model, and the basic network structure model is shown in Figure 1:

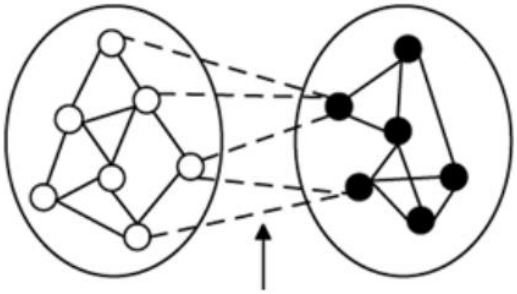

Fig. 1: Sybil network structure model.

In recent years, more and more researches have been devoted to the research of Sybil attacks. Wei Wei et al. proposed a centralized Sybil Defender algorithm in 2012[5]. The hypothesis is based on the fact that the Sybil node needs to reach the honest node through the small grid in the social network graph. This algorithm can be applied to large-scale Social network efficiently, but this algorithm over depends on the fast self-construction of social network graphs.

AB Potey et al. proposed an improved Sybil attack detection scheme based on Sybil Guard in 2013[6]. Using edge crossing to replace node crossover, this paper proposed new conditions to reduce the false positive rate, but people only theoretically analyze the feasibility of the scheme , and do not test on the actual data set.

There is also a kind of methods to detect Sybil attacks in social networks, which does not explicitly mark every node in network as real node or Sybil node. Instead, they use application-oriented historical information with the structure of a social network to restrict the number of identities that can be created in the system by Sybil nodes, so that the communication of the nodes and the number of node identities the nodes have are independent and irrelevant.

At present, there is little domestic research on Sybil attacks in social network. In 2011, Zhi Yang et al. of Peking University cooperated with Renren to provide a Sybil detection scheme based on supporting vector machine [7], and trained classifier in the real data sets provided by Renren, and then conducted classification detection of the Sybil nodes in the nodes of the social network. In 2012, Jing Jiang in Peking University analyzed the number of nodes visited and the actual degree relationship in the real network data provided by Renren, also analyzed the login time and registration time of the nodes and effectively detected Sybil Groups of Renren [8].

Peng ZY etc presented a method based on random wandering tactic in social networks to detect Sybil attack in 2014[9]. This method effectively resolved the limit for current sybil attack detecting methods used for large scale social networks. The method can not only detect sybil nodes by label spreading but also reduce the damage of sybil attacks to social networks.

WangYC etc presented a Sybil detection method named SybilGrid used for directed social networks in 2016[10]. This method adopts the random wandering tactic to detect sybil nodes in directed social networks topology. This method was evaluated and was proved to be valid through getting the real social networks topology data from the Sina micro-blog.

3.2. Detection Method for Abnormal Account Attacks

Academia and industry put forward many detection schemes for the abnormal account online social network threats. According to the different core algorithm, these detection schemes mainly divided into four categories: the detection scheme based on the behavior characteristics, the detection scheme based on content, the detection scheme based on chart and the detection scheme based on unsupervised learning.

In the detection schemes Based on the behavior characteristics and content, the abnormal account is regarded as a classification problem, that is, using the behavior characteristics and the content of the account to distinguish the normal account and the abnormal account. The relationship between the accounts in a social network has the chart character.The detection scheme based on char utilizes that the use of normal and abnormal account have different modes of the structure in the form of or connection, the abnormal detection problems transform into the abnormal detection problems in chart, and then using some algorithms of graph mining to distinguish normal account and abnormal account. the detection scheme based on unsupervised learning has the same characteristics or conform to a certain model, through the characteristics of the cluster or the establishment of a model to detect abnormal accounts.

There is no clear boundary between the different detection schemes, some detection schemes may use a variety of detection technologies, such as the combination based on the behavior characteristics and content, or based on the behavior characteristics and based on the chart. Combining different techniques in the detection of specific program maybe achieve better results.

4. Conclusion

With the rapid development of online social network, more and more attackers focus on the online social network, and the harm caused by various attacks seriously threaten the users' information security and the development of online social security sites. This paper analyzes and summarizes the typical attacks of online social network, and researches and compares the related attack detection methods. Online social network security research is still a relatively weak part at home, so social networks will always face new attacks. Driven by interests, the attackers will change the original attack when they face to the social network detection system, and form new attack method. We believe that with the depth of the study, more comprehensive security mechanisms will be proposed.

5. Acknowledgements

This work is kindly supported in part by The Key Research Program of Jiangsu Police Institute (2015SJYSZ03), the scientific research innovation team of Jiangsu Police Institute (2015SJYTZ03), Top-notch Academic Programs Project of Jiangsu Higher Education Institutions (TAPP), the open project of Key Laboratory of Police Geographic Information Technology, Ministry of Public Security(2016LPGIT04), National Social Science Foundation of China (13BTQ046), and the theory soft science program for the Bureau of Public Security for Jiangsu Province (2013LX028).

6. References

[1] N.B. Ellison, "Social network sites: definition, history, and scholarship," *Journal of Computer-Mediated Communication*, vol. 13, pp. 210-230, July 2007.

[2] C. Kanich, C. Kreibich, and K. Levchenko "Spamalytics: An empirical analysis of spam marketing conversion," *Proceedings of the 15th ACM conference on Computer and communications security*, pp. 3-14, 2008.

[3] C. M. Zhong, S. P.Xu, “Web Front Hacker Technology Disclosure,” *Electronic Industry Publishing House.*, 1st ed. C.H.: Beijing, 2012.

[4] Y.Q. Zhang, S.Q. Lv, D.Fan, “Anomaly Detection in Online Social Networks,” *Chinese Journal of Computers,* vol. 38, 2015.

[5] Wei W, Xu F, Tan C C, et al. Sybildefender: Defend against sybil attacks in large social networks[C]//INFOCOM, 2012 Proceedings IEEE. IEEE, 2012: 1951-1959.

[6] Potey A B, Raut A B. Combating Sybil Attacks using Sybil Guard[J]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013, 2(2): 452-455.

[7] Z. Yang, C. Wilson, X. Wang, “Uncovering social network sybils in the wild,” *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pp. 259-268, 2011.

[8] J. Jiang, Z. Shan, W. Sha, “Detecting and validating sybil groups in the wild,” Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. IEEE, pp. 127-132, 2012.

[9] Z.Y. Peng, “Research on Sybil Attack Detection Algorithm Based on Random Walks Betweenness in Social Networks,” *YanShan University,* 2014.

[10] Y.C.Wang, Y.H.Meng, “SybilGrid: Sybil Detection Method Based on Directed Social Networks,” J*ournal of Xidian University,* vol. 43, pp. 199-204, 2016.