Detecting Malicious Accounts in Social-Network-Based Online Promotions

Neha Kuril, Poonam Dongre, Prajakta Panekar, Yamini Dubey, Pooja Telgote

Dept.of Computer Science And Engineering Tulsiramji Gaikwad Patil College Of Engineering And Technology Nagpur,INDIA

Dept.of Computer Science And Engineering Tulsiramji Gaikwad Patil College Of Engineering And Technology Nagpur,INDIA

Dept.of Computer Science And Engineering Tulsiramji Gaikwad Patil College Of Engineering And Technology Nagpur,INDIA

Dept.of Computer Science And Engineering Tulsiramji Gaikwad Patil College Of Engineering And Technologys Nagpur,INDIA

Dept.of Computer Science And EngineeringTulsiramji Gaikwad Patil College Of Engineering And Technology Nagpur,INDIA

Abstract—*The Online social networks (OSNs) gradually integrate financial capabilities by enabling the usage of real and virtual currency. They serve as new platforms to host a variety of business activities, such as online promotion events, where users can possibly get virtual currency as rewards by participating in such events. Both OSNs and business partners are significantly concerned when attackers instrument a set of accounts to collect virtual currency from these events, which make these events ineffective and result in significantfinancial loss. It becomes of great importance to proactively detecting these malicious accounts before the online promotion activities and subsequently decreases their priority to be rewarded. In this paper, we propose a novel system, namely ProGuard, to accomplish this objective by systematically integrating features that characterize accounts from three perspectives including their general behaviors, their recharging patterns, and the usage of their currency. We have performed extensive experiments based on data collected from the Tencent QQ, a global leading OSN with built-in financial management activities. Experimental*

Pooja Telgote

Keywords—*malicious accounts, online social network, existing methods, advanced technology, blocking accounts*

I. Introduction

Online social networks (OSNs) that integrate virtual currency serve as an appealing platform for various business activities, where online, interactive promotion is among the most active ones. Speci_cally, a user, who is commonly represented by her OSN account, can possibly get reward in the form of virtual currencybyparticipatingonlinepromotionactivities organized by business entities. She can then use such reward in variousways such as online shopping, transferring it to oth- ers, and even exchanging it for real currency [1]. Such virtual- currency-enabled online promotion model enables enormous outreach, offers direct _nancial stimuli to end users, and meanwhile minimizes the interactions between business enti- ties and _nancial institutions. As a result, this model has shown great promise and gained huge prevalence rapidly. However, it faces a signi_cant threat: attackers can control a large number of accounts, either by registering new accounts or compromising existing accounts, to participate in the online promotion events for virtual currency. Such malicious activities will fundamentally undermine the effectiveness of the promotion activities, immediately voiding the effective-

ness of the promotion investment from business entities and meanwhile damaging ONSs' reputation. Moreover, a large volume of virtual currency, when controlled by attackers, could also become a potential challenge against virtual cur- rency regulation [2].

It therefore becomes of essential importance to detect accounts controlled by attackers in online promotion activ- ities. In the following discussions, we refer to such accounts as malicious accounts. The effective detection of malicious accounts enables both OSNs and business entities to take mit- igation actions such as banning these accounts or decreasing the possibility to reward these accounts. However, designing an effective detection method is faced with a few signi_cant

1990 VOLUME Transactions on Secure Computing,Volume:5,Issue Date:17.January.2017 Y. Zhou et al.: ProGuard: Detecting Malicious Accounts in Social- Network-Based Online Promotions challenges. First, attackers do not need to generate malicious content (e.g., phishing URLs and malicious executables) to launch successful attacks. Comparatively, attackers can effec- tively perform attacks by simply clicking links offered by business entities or sharing the benign content that is orig- inally distributed by business partners. These actions them- selves do not perceivably differentiate from benign accounts. Second, successful attacks do not need to depend on social structures (e.g., ``following" or ``friend" relationship in pop- ular social networks). To be more speci_c, maintaining active social structures does not bene_t to attackers, which is funda- mentally different from popular attacks such as spammers in online social networks. These two challenges make the detec- tion of such malicious OSN accounts fundamentally different from the detection of traditional attacks such as spamming and phishing. As a consequence, it is extremely hard to adopt existing methods to detect spamming and phishing accounts.

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned chal- lenges, we have designed a novel system, namely ProGuard. ProGuard employs a collection of behavioral features to pro_le an account that participates in an online promotion event. These features aim to characterize an account from three aspects including i) its general usage pro_le, ii) how an account collects virtual currency, and iii) how the virtual currency is spent. ProGuard further integrates these features using a statistical classi_er so that they can be collectively used to discriminate between those accounts controlled by attackers and benign ones. To the best of our knowledge, this work represents the _rst effort to systematically detect malicious accounts used for online promotion activity partic- ipation. We have evaluated our system using data collected from Tencent QQ, a leading Chinese online social network that uses a widely-accepted virtual currency (i.e., Q coin), to support online _nancial activities for a giant body of 899 million active accounts. Our experimental results havedemonstrated that ProGuard can achieve a high detection rate of 96.67% with a very low false positive rate of 0.3%. proper way.

II. Literature Review

Isodje, A. [1] presented an overview on the use of Social Media for business promotion, since social media as an online collaborative platform has the power to impact cultures and business. This further infiltrates communities, professional groups, peer bodies, which can be successfully used for promoting ones business.

Mamta et al. [10] tested for affiliation that exists between Higher Education and Social Networking Site. Mining algorithms provided by NASA tools like Like-Analyser, Gephi, Wolfram Alpha and NodeXL to assess presence and participation factor of students and education professionals in social network graphs are utilized in this study and analysis finding related to social network analysis predicted that social networking on Facebook and higher education work in parallel units. n times of traditional print media, there used to be one- way information dissemination which was restricted to geographical limits and presence. The process of information diffusion with arrival of Internet transformed significantly.

Purva et al. [12] presented that online social networking like Facebook and Twitter have the fastest means of communication and having gained wide popularity, have revolutionized interpersonal communications by providing a platform to individuals for expressing themselves for a particular at a global level, beyond their immediate geography. The authors present the study on diffusion dynamics of specific real world events, discussed on Twitter, with respect to location and time.its The events were categorizes into broad categories based temporal (short or long), geographical distribution (local or global), information diffusion (viral or gradual), influence (popular or unpopular) and the cause (natural or planned). It was conclude that the three-dimensional analysis of real-world events by exploring relationships among them. The number of social networking site users is increasing immensely not only in India but also across the globe.

Davmane et al. [3] analysed the factors for the online social networking sites as per users behavior regarding user friends, the peer groups, access patterns, amount of time spend, the effect on personal and professional life. User attitude and behavior is also surveyed for over seven hundred users using a questionnaire consisting of 27 questions which focused on behavior of Indian users in terms of usability, trends and access.

Singh et al. [14] presented the research effort in ensuring awareness about the social networking site concept, merits, demerits and meaning. The research methodology in this paper was based on primary and secondary data regards to groupingof users having similar type of interests, jobs, activities, backgrounds or some other type of real life similarities.

Purti at al. [2] focused on Big Data Management for Social Networking Sites by review and analysis of how Big Data is being managed for social networking sites by Facebook and Twitter. The data size for social networking sites constitutes almost 105 terabytes of data for every thirty minute, which in itself is a huge chunk of the data, unlike other data sources which has structured, limited data to handle. Facebook uses Hive for storing the data on HDFS (Hadoop Distributed File System) while Twitter has implemented a set of solutions storage inside Hadoop to store the data in LZO compressed format

Kumar et al. [9] propose a sentiment analysis method on the tweets in Cloud environment and utilized Hadoop for intelligent analysis and storage of big data on Facebook and Twitter. The reason is that I.J. of

Electronics and Information Engineering, Vol.7, No.1, PP.41-51, Sept. 2017 (DOI: 10.6636/ IJEIE.201709.7(1).05).

III. System Architecture

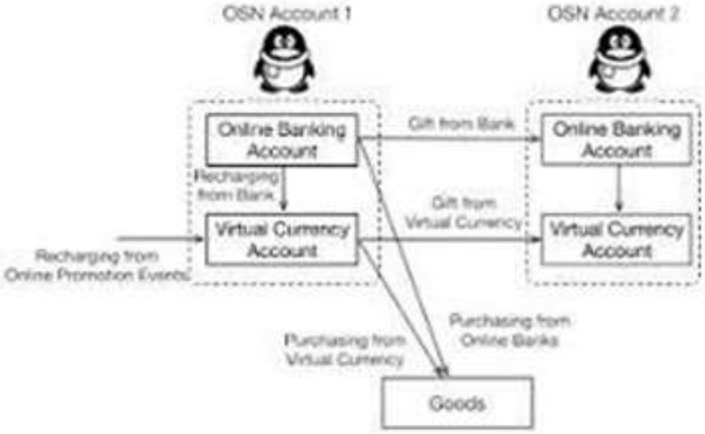

Fig: Working process

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namelyProposed system. Proposed system employs a collection of behavioral features to profile an account that participates in an online promotion event

IV. Our Old Work

Since online social networks play an increasing important role in both cyber and business world,detecting malicious users in OSNs becomes of great importance.For the further experiments for Many detection methods have been consequently proposed. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts thatsend maliciouscontent. Spamming attack can be considered as an information flow initiated from an attacker, through a series of malicious accounts, and finally to a victim account. Despite the diversity of these methods, they generally leverage partial or all of three sources for detection including,The content of the spam message,The network infrastructure that hosts the malicious information .The social structure among malicious accounts and victim accounts.

1. In the existing system, many detection methods have been consequently proposed. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts that send malicious content. A spamming attack can be considered as an information follow initiated from an attacker, through a series of malicious accounts, and finally to a victim account.
2. Despite the diversity of these methods, they generally leverage partial or all of three sources for detection including

i) the content of the spam message
ii) the network infrastructure that hosts the malicious information (e.g., phishing content or exploits)
iii) the social structure among malicious accounts and victim accounts. and then propagated maliciousness score using the derived graph.

3. For example, Gao et al. designed a method to reveal campaigns of malicious accounts by clustering accounts that send messages with similar content. Lee and Kim [devised a method to rst track HTTP redirection chains initiated from URLs embedded in an OSN message, then grouped messages that led to web pages hosted in the same server, and finally used the server reputation to identify malicious accounts. Yang et al. extracted a graph from the ``following" relationship of twitter accounts.

V. Proposed System

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namely Proposed system. Proposed system employs a collection of behavioral features to profile an account that participates in an online promotion event . Also,These features aim to characterize an account from three aspects including,

i) Its general usageprofile,
ii) How an account collects virtual currency and

iii) How the virtual currency is spent.

iv) In the proposed system, the system proposes a novel system, namely Proposed system, to accomplish this objective by systematically integrating features that characterize accounts from three perspectives including their general behaviors, their recharging patterns, and the usage of their currency.

v) The system has performed extensive experiments based on data collected from the Tencent QQ, a global leading OSN with built-in financial management activities. to predict the disease more accurately.

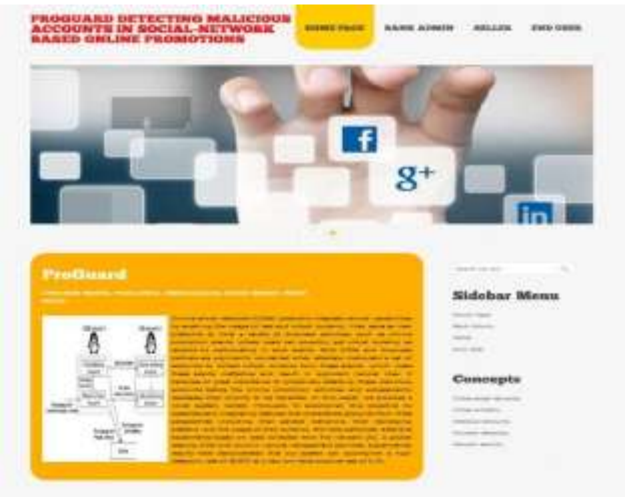
PROGUARD DETECTING MALICIOUS ACCOUNTS IN SOCIAL-NETWORK BASED ONLINE PROMOTIONS
HOME PAGE
BANK ADMIN
SELLER
END USER
ProGuard
Sidebar Menu
Concepts

Fig 5.1.1 Home page

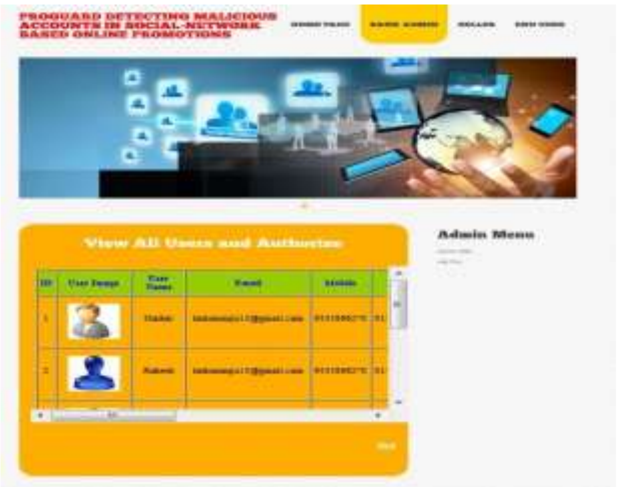
PROGUARD DETECTING MALICIOUS ACCOUNTS IN SOCIAL-NETWORK BASED ONLINE PROMOTIONS
HOME PAGE
BANK ADMIN
SELLER
END USER
View All Users and Authorize
ID
User Image
User Name
Email
Mobile
Admin Menu

Fig5.1.2 Malicious accounts detection

5.2.Purpose

To the best of our knowledge, this work represents the first effort to systematically detect malicious accounts used for online promotion activity participation.

We have evaluated our system using data collected from online social network that uses a widely-accepted virtual currency (i.e., Q coin), to support online financial activities for active accounts.

Our experimental results have demonstrated that system can achieve a high detection rate of 96.67% with a very low false positive rate of 0.3%.This work represents the first effort to systematically detect malicious account used for online promotions activity participation.

VI. Conclusion And Suggested Work

This paper presents a novel system, Proposed system, to automati-cally detect malicious OSN accounts that participate in online promotion events. Proposed system leverages three categories of features including general behavior, virtual- currency collec- tion, and virtual-currency usage. Experimental results based on labelled data collected from Tencent QQ, a global lead-ing OSN company, have demonstrated the detection accu- racy of Proposed system, which has achieved a high detection rate of 96.67% given an extremely low false positive rate of 0.3%.

For future work, on one hand, we will further investigate the key features for classification. We hope to find more useful features in OSNs, and improve the accuracy of malicious account detection. On the other hand, we plan to expand the generality of OSNShield. We expect it can work well not only for Dianping, but also for other LBSN platforms.

References

[1]. Y. Wang and S. D. Mainwaring, "Human-currency interaction: learning from virtual currency use in china," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.

[2]. J. S. Gans and H. Halaburda, "Some economics of private digital currency," Rotman School of Management Working Paper, no. 2297296, 2013.

[3]. X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65. [4]"Leveraging knowledge across media for spammer detection in microblogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 2014, pp. 547– 556.

[4]. Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, 2012.

[5]. Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog or block: Detecting blog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

[6]. S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, "Collective spammer detection in evolving multi-relational social networks," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769–1778.

[7]. Y.-R. Chen and H.-H. Chen, "Opinion spammer detection in web forum," in Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2015.

[8]. F. Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in microblogging with social context regularization," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610.