International Journal of Pure and Applied Mathematics
Volume 120 No. 5 2018, 905-918
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Detecting Malicious Accounts in Social-Network-Based Online Promotions

[1]Dr M Praveen Kumar, Professor, Department of Computer Science & Engineering, Malla Reddy Institute of Technology, Hyderabad, India.
[2]Dr G PabhakarRao and HOD, Professor, Department of Computer Science & Engineering, Scient Institute of Technology, Hyderabad, India.

Abstract: Online social networks 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 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 significant financial 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 Tencent QQ, a global leading OSN with built-in financial management activities. Experimental results have demonstrated that our system can accomplish a high detection rate of 96.67% at a very low false positive rate of 0.3%.

Keywords: Online social networks, virtual currency, malicious accounts, intrusion detection, network security

1. 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. Specifically, a user, who is commonly represented by her OSN account, can possibly get reward in the form of virtual currency by participating online promotion activities organized by business entities. She can then use such reward in various ways such as online shopping, transferring it to others, and even exchanging it for real currency. Such virtual- currency-enabled online promotion model enables enormous outreach, offers direct financial stimuli to end users, and meanwhile minimizes the interactions between business entities and financial institutions. As a result, this model has shown great promise and gained huge

prevalence rapidly. However, it faces a significant 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 effectiveness 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 currency regulation.

It therefore becomes of essential importance to detect accounts controlled by attackers in online promotion activities. 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 mitigation 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 significant challenges. First, attackers do not need to generate malicious content (e.g., phishing URLs and malicious executable) to launch successful attacks. Comparatively, attackers can effectively perform attacks by simply clicking links offered by business entities or sharing the benign content that is originally distributed by business partners. These actions themselves 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 popular social networks).

To be more specific, maintaining active social structures does not benefit to attackers, which is fundamentally different from popular attacks such as spammers in online social networks. These two challenges make the detection 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 phishingaccounts.

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namely ProGuard. ProGuard employs a collection of behavioral features to profile an account that participates in an online promotion event. These features aim to characterize an account from three aspects including i) its general usage profile, ii) how an account collects virtual currency, and iii) how the virtual currency is spent. ProGuard further integrates these features using a statistical classifier 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 first effort to systematically detect malicious accounts used for online promotion activity participation. We have evaluated our system using data collected from Ten cent QQ, a leading Chinese online social network that uses a widely-accepted virtual currency (i.e., Q coin), to support online financial activities for a giant body of 899 million active accounts. Our experimental results have demonstrated that ProGuard can achieve a high detection rate of 96.67% with a very low false positive rate of 0.3%.

2. Literature Review

2.1 Detecting Clusters of Fake Accounts in Online Social Networks

Fake accounts are a preferred means for malicious users of online social networks to send spam, commit fraud, or otherwise abuse the system. A single maliciousactor may create dozens to thousands of fake accounts in order to scale their operation to reach the maximum number of legitimate members.

Detecting and taking action on these accounts as quickly aspossible is imperative in order to protect legitimate members and maintain the trustworthiness of the network. However, any individual fake account may appear to be legitimate on first inspection, for example by having areal-sounding name or a

believable profile.

2.2 ImpactofSocialNetworking on IndianYouth

The objectives of this study are an attempt to investigate the extent of social networking impact on the Indian youth. The reason for selecting youth as the target audience is because the direction of a country and culture is decided by the direction taken by youths of that country. This paper is an attempt to analyze the pattern of social networking usage and impact in order to determine the social networking addiction.

Off the 7.3 billion global population worldwide, social networking has 2.3 billion active users which has seen a rise of 176 million just last year Social networking advertising earnings are estimate dat $8.3 billion in 2015 even as 385 organizations spent over 20% budget on social media channels which has been up by 15% compared to 2015 [The increased use of social networking culture and social networking sites by youth has helped bring friends and family closer for those living in distant locations.

2.3 Towards detecting Compromised Accounts on Social Networks

Compromising social network accounts has become a profitable course of action for cybercriminals. By hijacking control of a popular media or business account, attackers can distribute their malicious messages or disseminate fake information to a large user base. The impacts of these incidents range from a tarnished reputation to multi- billion dollar monetary losses on financial markets. In our previous work, we demonstrated how we can detect large-scale compromises (i.e., so-called campaigns) of regular online social network users.

3. Existing System

Since online social networks play an increasing important role in both cyber and business world, detecting malicious users in OSNs becomes of great importance.

Many detection methods have been consequently proposed. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts that send 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 detectionincluding

a. The content of the spam message,
b. The network infrastructure that hosts the malicious information (e.g., phishing content or exploits)and
c. The social structure among malicious accounts and victim accounts.

3.1 Disadvantages of Existing System

However, it faces a significant 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.

4. Proposed Method

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namely ProGuard.

ProGuard employs a collection of behavioral features to profile an account that participates in an online promotion event.

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.

4.1 Advantages of Proposed System

This work represents the first effort to systematically detect malicious accounts used for onlinepromotionactivityparticipation

5. System Design

System Architecture:

System Design Introduction:

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human- machine interfaces, detailed design, processing logic, and external interfaces.

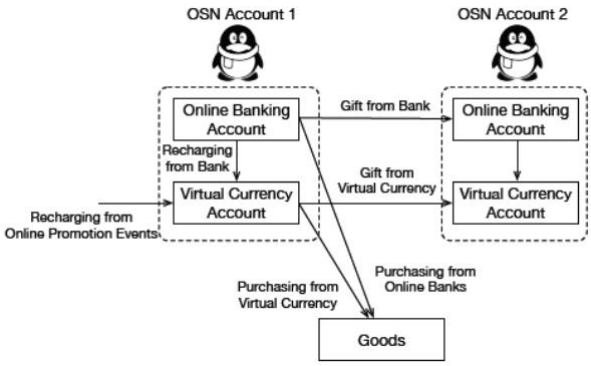


Figure.1. Architecture and Flow Diagram

5.2 UML Diagrams

Global Use Case Diagrams:

Identification of actors:

Actor: Actor represents the role a user plays with respect to the system. An actor interacts with, but has no control over the use cases.

Graphical representation:

An actor is someone or something that:

Interacts with or uses the system.

I. Provides input to and receives information from the system.

II. Is external to the system and has no control over the use cases.

Actors are discovered by examining:

I. Who directly uses thesystem?
II. Who is responsible for maintaining the system?
III. External hardware used by the system.
IV. Other systems that need to interact with the system.

Questions to identify actors:

I. Who is using the system? Or, who is affected by the system? Or, which groups need help from the system to perform a task?
II. Who affects the system? Or, which user groups are needed by the system to perform its functions? These functions can be both main functions and secondary functions such asadministration.
III. Which external hardware or systems (if any) use the system to perform tasks?
IV. What problems does this application solve (that is, for whom)

Construction of use case diagrams:

The Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions is performedforwhichactor.Rolesoftheactorsinthesystemcanbedepicted.

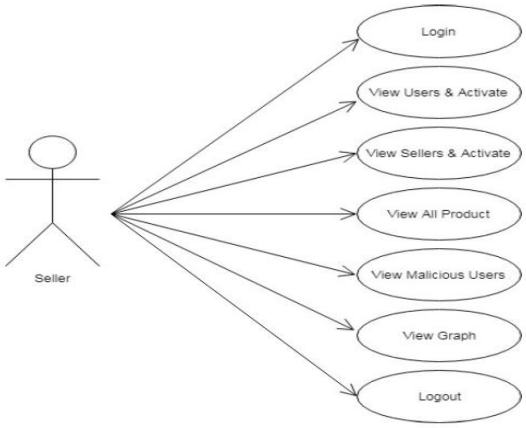


Figure.2. Admin Use case Diagram

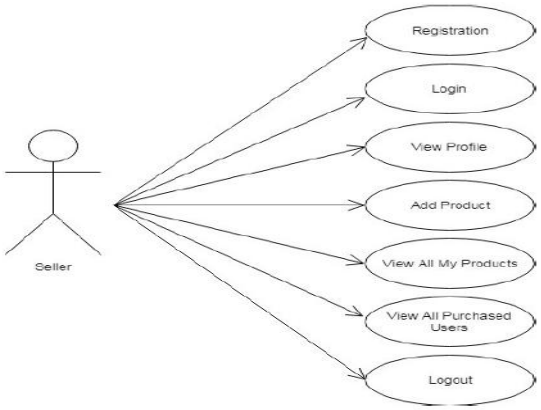
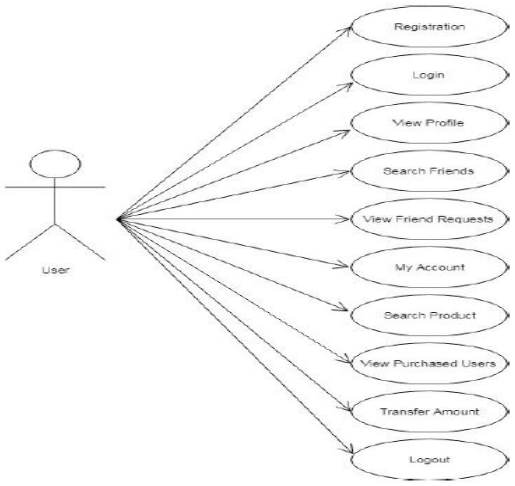


Figure.2.1.Seller Usecase Diagram



Fifure.2.2. User Use Case Diagram

5.4 Activity Diagram

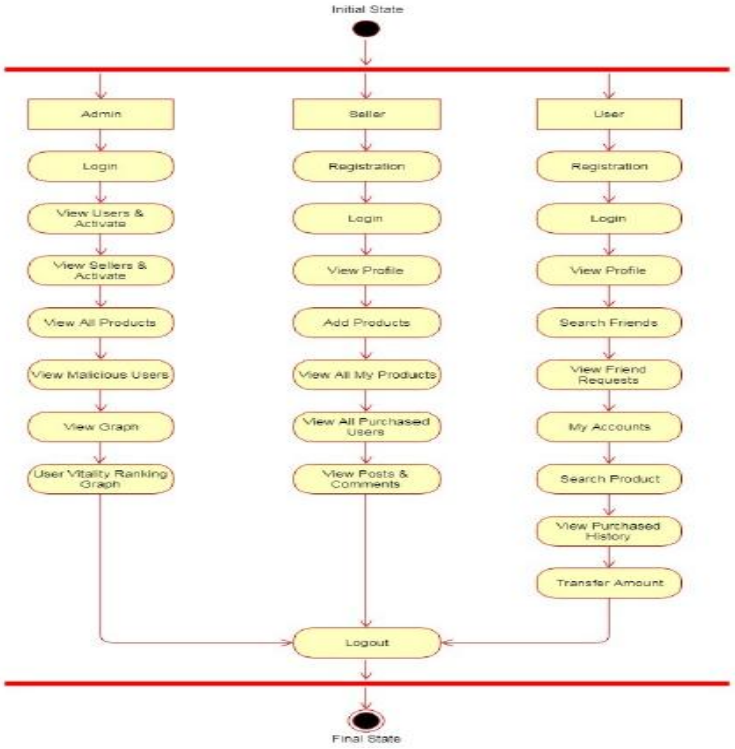


Figure.2.3Activity Diagram

Module Description

For detecting malicious accounts in social networks based on online promotion it has three modules to test them functionality:

1. Admin
2. Seller
3. User

Admin functionality:

Admin play a main important role in this protect, admin detect malicious accounts in both seller and user. Once seller and user register for social network in order to get login into his account first admin should activate his account and authorize him.

When user and seller click shorthand three time so the payment of product by using fake account then admin detect them as a malicious user and block the account.

Seller functionality:

Seller is the second module after getting registration in social networks by participating in online promotion event , he should wait for admin until he activate his account and authorize him , next seller can send friends request to his friends by using online social networks he can share the product to user by using credit or debit card payment and by virtual payment if seller share the product by using virtual payment more than 3 times he is detecting as malicious user and block .

User functionality:

User is the second module after getting registration in social networks by participating in online promotion event , he should wait for admin until he activate his account and authorize him. In this the user can add money in to his accounts , view product and purchase the product by using online payment . user doesn't have enough money in his account and even try to purchase the product more than three times and then user is detected as malicious user in social networks based on online promotions and user get block by the user .

6. System Testing

Testing is the debugging program is one of the most critical aspects of the computer programming triggers, without programming that works, the system would never produce an output of which it was designed. Testing is best performed when user development is asked to assist in identifying all errors and bugs. The sample data are used for testing. It is not quantity but quality of the data used the matters of testing. Testing is aimed at ensuring that the system was accurately an efficiently before live operation commands.

Testing objectives:

The main objective of testing is to uncover a host of errors, systematically and with minimum effort and time. Stating formally, we can say, testing is a process of executing a program with intent of finding an error.

a. A successful test is one that uncovers an as yet undiscovered error.
b. A good test case is one that has probability of finding an error, if it exists.
c. The test is inadequate to detect possibly present errors.
d. The software more or less confirms to the quality and reliable standards.

Level of Testing

Code testing:

This examines the logic of the program. For example, the logic for updating various sample data and with the sample files and directories were tested and verified.

Specification Testing:

Executing this specification starting what the program should do and how it should performed under various conditions. Test cases for various situation and combination of conditions in all the modules are tested.

Nnit testing:

In the unit testing we test each module individually and integrate with the overall system. Unit testing focuses verification efforts on the smallest unit of software design in the module. This is also known as module testing. The module of the system is tested separately. This testing is carried out during programming stage itself. In the testing step each module is found to work satisfactorily as regard to expected output from the module. There are some validation checks for fields also. For example the validation check is done for varying the user input given by the user which validity of the data entered. It is very easy to find error debut the system.

System testing:

Once the individual module testing is completed, modules are assembled and integrated to perform as a system. The top down testing, which began from upper level to lower level module, was carried out to

check whether the entire system is performing satisfactorily.

Test Cases

	TE T APP	TE T CA E DE CRIPTI	ACTU AL	A TICIPATED VALUE	RE ULT
1	Unit Testing	User Registration: Enter Username, Password, Email, Gender, #o#ile no, and click on Register. Values: Username: ramya Password : 1 Email:Ramya1@gamil.com Gender: Female #o#ileno:9988774455	*ogin +orm will #e opened	*ogin +orm is opened	Pass
	Unit Testing	User Login: Enter Username, Password and Email, Gender, #o#ile no then !lick on *ogin. Values: Username: ramya Password : 4 Email : Ramya1 @gmail.com #o#ileno:9988774455	*ogin +orm Will #e opened	Incorrect Username*f* Password	Fail

7. Results

Figure. 7 .Home Admin Login

Figure.7.1 Admin Home

Figure.7.2 View user and Active

Fig.7.4 View seller and activate

Fig.7.5 View All Product

Fig.7.6 Seller login

Fig.7.7 View Profile

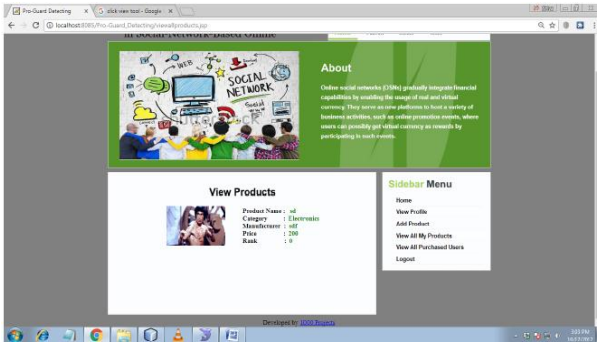


Fig.7.8 View Product

Fig.7.9 Purchased product

Conclusion

This paper presents a novel system, ProGuard, to automatically detect malicious OSN accounts that participate in online promotion events. ProGuard leverages three categories of features including general behavior, virtual-currency collection, and virtual-currency usage. Experimental results based on labeled data collected from Tencent QQ, a global leading OSN company, have demonstrated the detection accuracy of ProGuard, which has achieved a high detection rate of 96.67% given an extremely low false positive rate of 0.3%.

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.GansandH.Halaburda,"Someeconomicsofprivatedigitalcurrency,"RotmanSchool ofManagementWorkingPaper,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.

[5] Chu,S.Gianvecchio,H.Wang,andS.Jajodia,"Detectingautomationoftwitteraccounts: Are you a human, bot, or cyborg?" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, 2012.

[6] Chu,S.Gianvecchio,A.Koehl,H.Wang,andS.Jajodia,"Blogorblock:Detectingblog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

[7] 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.

[8] Y.-R.ChenandH.-H.Chen,"Opinionspammerdetectioninwebforum,"inProceedingsof the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval.ACM,2015,pp.759–762.