Detecting Malicious Accounts in Social Network Based Online Advertisements using ProGuard

Suvarna Ramyakrishna[1], Dr.Gulab Singh[2]

1. **M.Tech Scholar, Department of CSE, Vaageswari College of Engineering, Karimnagar, Telangana, India --krishsuvarna9@gmail.com, 9652655440**
2. **Research Supervisor, Associate professor, Vaageswari College of Engineering, Karimnagar, Telangana, India --gulsinchu@gmail.com, 8121141303**

ABSTRACT:

Now a day's Online Social Networks(OSN) plays an important role that integrate financial capabilities by enabling the usage of real and virtual currency. OSN serves as great platforms to host a large variety of business activities such as online advertisements, where users can possibly get virtual currency as rewards by participating in such events. Both OSN and business organizations are highly concerned when attackers uses a set of accounts to collect virtual currency from these events, which make these events unsuccessful and leads to financial loss and OSN reputation is also damaged. It becomes a great importance to proactively detecting these malicious accounts before the online promotion activities and eventually decrease their main concern to be satisfied. In this paper, a novel system is proposed, namely ProGuard. ProGuard employs a collection of general behaviors, recharging patterns, and the usage of currency of the participants. ProGuard is evaluated using data collected from Tencent QQ, a Chinese online social network that uses virtual currency i.e., Q coin to support financial activities on online social networks. Experimental results have analyzed that ProGuard can accomplish a high detection rate of 96.67% at a very low false positive rate of 0.3%.

Keywords—*Online Social Networks(OSN's), Virtual Currency, Malicious Accounts, Detection, ProGuard.*

INTRODUCTION:

In an online social network a user can create a profile and build a personal network that connects the user to other users. It is ideal for exchanging of ideas, views and also a biggest platform in multilevel marketing. In online promotion events conducted by business organizations, the users get rewards in the form of virtual currency which can be used for shopping, transferring currency and exchanging currency vice versa to others. As a result, it is gained public interest at a great demand.

But, it faces a threat from attackers who can control large number of accounts to participate in promotional events for virtual currency. Due to these malicious activities, it is not only lessen the effectiveness of promotional events. But also defame of the reputation.

It is more important to detect these malicious accounts and designing a detection method is faced with few challenges like, the attackers can attack by simply clicking links offered by business organizations or sharing the original content distributed by business organization through different attractive advertisements. So, it is hard to distinguish between benign and malicious accounts by existing methods.

In order to detect these malicious accounts effectively, we have designed a novel system namely ProGuard. The main aim of the system is to characterize an account from three aspects including its general usage profile, how a participant collects money, and how the virtual currency is spent, which further incorporates these features using a statistical classifier to differentiate the benign and malicious accounts.

EXISTING SYSTEM:

Lin et al ranked the importance of fraud factors used in financial statement fraud detection, and investigated the correct classification rates of three algorithms including Logistic Regression, Decision Trees, and Artificial Neural Networks. Throckmorton et al proposed a corporate financial fraud detection method based on combined features of financial numbers, linguistic behavior, and non-verbal vocal.

Networking and online promotion events involving financial activities, predicts the participant behaviors of collecting and using the virtual currency in online promotion activities are different from traditional financial systems. Our system aims to address a new problem caused by the new trend of integrating online social networks and financial activities. ProGuard features combines networking and financial characteristics for detection and to enhance the security of online social networks.

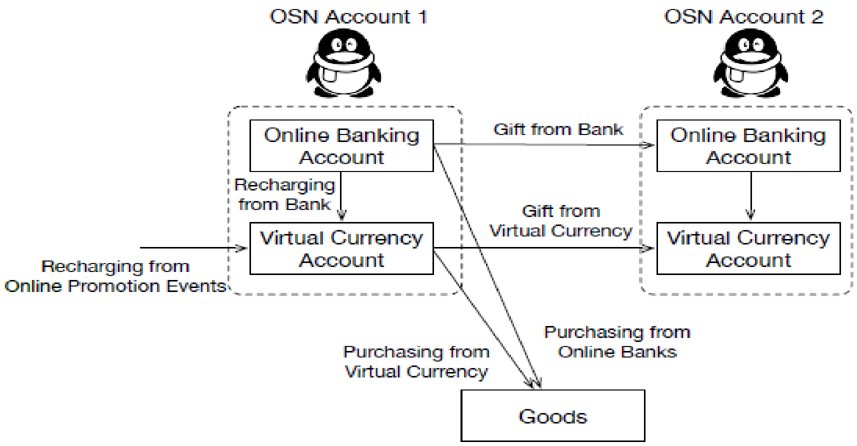

Fig. 1. The integration of financial accounts and OSN accounts

PROPOSED SYSTEM:

We proposed a novel system namely ProGuard. Its purpose is to identify the malicious accounts that participate in online promotion events for virtual currency collection. To prevent freshly registered accounts that are likely to be participated, business organization usually require the participating accounts to be registered for a specific amount of time. The detected malicious accounts cannot be quickly replaced by the newly registered accounts, thereby drastically limiting the number of attackers.

Our detection system will label whether an account is malicious or not when it participates in an online promotion event, this enables business organizations to take immediate action such as neglecting this account from being rewarded in the event. Hence, it can proactively reduce the financial loss faced by business organizations more effectively.

SYSTEM ARCHITECTURE:

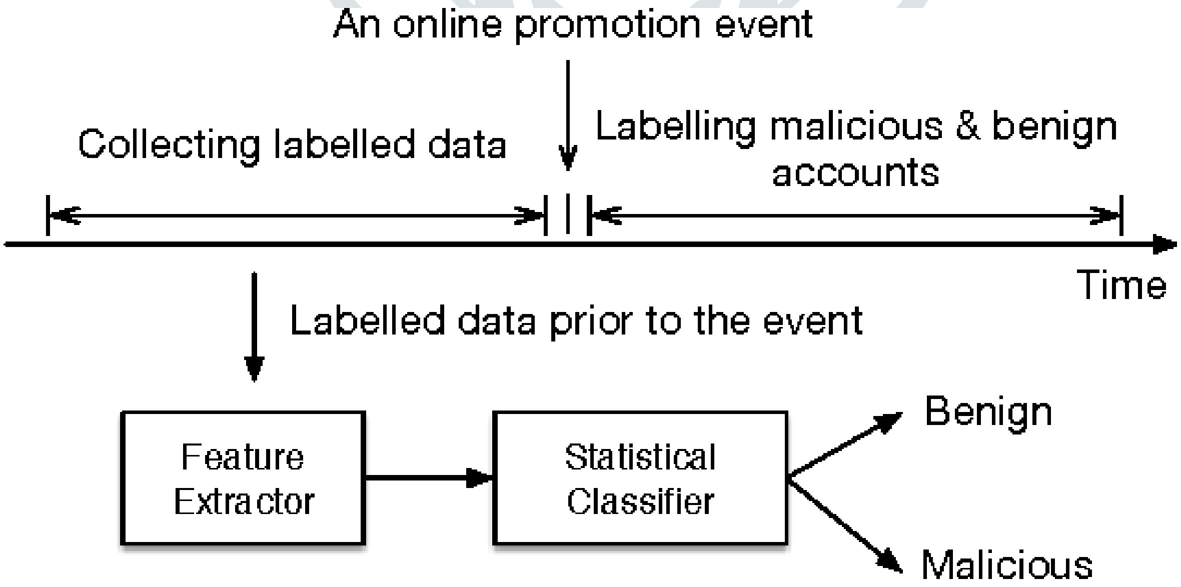
An online promotion event
Collecting labelled data
Labelling malicious & benign accounts
Time
Labelled data prior to the event
Feature Extractor
Statistical Classifier
Benign
Malicious

Fig. 2. The system architectural overview of ProGuard

CONCLUSION:

This paper presents a novel system namely ProGuard, which automatically detect malicious accounts that participate in online promotion events conducted by business organizations on online social networks. 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 to support online financial activities of 899 million accounts, have analyzed the detection accuracy of ProGuard, which has achieved a high detection rate of 96.67% with a low false positive rate of 0.3% effectively and efficiently.

Though the ProGuard can detect malicious accounts which participates and collect virtual currency from online promotional events, it cannot detect transferring and laundering of virtual currency, these detection capabilities falls into future work of ProGuard.

REFERENCES:

[1] Yadong Zhou, DaeWook Kim, Junjie Zhang, Member, IEEE, Lili Liu, Huan Jin, Hongbo Jin, Ting Liu, "ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions".

[2] J. West and M. Bhattacharya, "Intelligent financial fraud detection: Acomprehensive review, " Computers & Security, vol. 57, pp. 47 – 66, 2016.

[3] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering," Information Sciences, vol. 260, pp. 64–73, 2014.

[4] D. Olszewski, "Fraud detection using self-organizing map visualizing the user profiles," Knowledge-Based Systems, vol. 70, pp. 324 – 334,2014.

[5] C. S. Throckmorton, W. J. Mayew, M. Venkatachalam, and L. M.Collins, "Financial fraud detection using vocal, linguistic and financial cues," Decision Support Systems, vol. 74, pp. 78 – 87, 2015.

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

[7] 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.