**ProGuard: Detecting Malicious Accounts inSocial-Network-Based Online Promotions**

**ABSTRACT:**

Online social networks gradually integrate financialcapabilities by enabling the usage of real and virtual currency.They serve as new platforms to host a variety of business activitiessuch as online promotion events, where users can possibly getvirtual currency as rewards by participating such events. BothOSNs and business partners are significantly concerned whenattackers instrument a set of accounts to collect virtual currencyfrom these events, which make these events ineffective and resultin significant financial loss. It becomes of great importance toproactively detecting these malicious accounts before the onlinepromotion activities and subsequently decrease their priorityto be rewarded. In this paper, we propose a novel system,namely ProGuard, to accomplish this objective by systematicallyintegrating features that characterize accounts from threeperspectives including their general behaviors, their rechargingpatterns, and the usage of their currency. We have performedextensive experiments based on data collected from Tencent QQ, aglobal leading OSN with built-in financial management activities.Experimental results have demonstrated that our system canaccomplish a high detection rate of 96.67% at a very low falsepositive rate of 0.3%.

**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.
* Compared to the studied financial fraud detection problems, account behaviors of collecting and using the virtual currency in online promotion activities are almost completely different with traditional financial systems since they do not only involve financial activities but also networking and online promotion activities
* Lee et al. devised a method to first track HTTP redirection chains initiated from URLs embedded in an OSN message, then grouped messages that led to webpages hosted in the same server, and finally used the server reputation to identify malicious accounts

**DISADVANTAGES OF EXISTING SYSTEM:**

* Attackers can control alarge number of accounts, either by registering new accountsor 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.
* None of existing methods is applicable to detecting malicious accounts in online promotion activities.

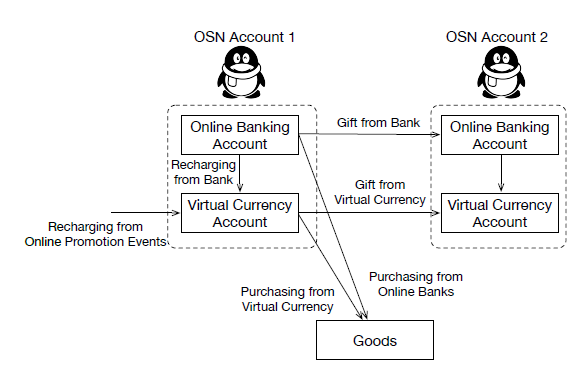
**PROPOSED SYSTEM:**

* 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.
* Our work aims to address a new problem caused by the new trend of integrating online social networks and financial activities. ProGuard features new capability of fusing features from both networking and financial aspects for detection. Nevertheless, we believe our method and existing approaches can complement each other to improve the security of online social networks.

**ADVANTAGES OF PROPOSED SYSTEM:**

* 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 ProGuard can achieve a high detection rate of 96.67% with a very low false positive rate of 0.3%.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL