ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Detection of Compromised Accounts in Online Social Network

[1] Sneha Rane, [2] Megha Ainapurkar, [3] Ameya Wadekar.
[2][3]Asst Prof
[1][2][3] Department of Information Technology, PCCE, Verna, India

Abstract - **Compromised accounts are of a severe risk to the social network users. People nowadays are mostly dependent on Online Social Networks. While some persistent spams feat the relationship between the users by spreading spams. Therefore time to time detection of the compromised accounts is a necessity. In this paper, we will study different social user behaviour and detect the compromised accounts and spam users. Spam behaviour in social networks has a wide range of illegal activities. Such activities need to be evaluated and effect of spam users' needs to be reduced. To reduce such effects, we require proper detection strategy. We validate the effectiveness of this behaviour by collecting the clickstream data on a social network website. Social behaviour reflects the users' behaviour online. While a legitimate user coordinates its social behaviour carefully, it is hard for the fake users to pretend to be affected. Different studies are performed in spam behaviour analysis and define a structure for spam account detection.**

Index Terms: Clickstream, compromised accounts, social networks.

I. INTRODUCTION

We live in the generation of social networks. Like online social networks facebook and twitter have become quite popular in couple of years. Many people use social networks to perform different activities online like staying in contact with relatives, friends, chatting and also acquiring information and news. This creates interactions between different users forming an activity log. These information are stored by the social network service providers. The access of such information to a spam user may expoit the privacy and security of the social network. It may also spread some illegal content and wrong information. These users or accounts gain access to information of other users or spread unwanted messages. Comman spam behaviors like Sybil attacks occur in online social networks. Therefore identifying the spam user is a necessity.

Now hacking someone's social network profile and and using it to perform any vulgularities has been a serious threat. There are many systems that have been suggested to be aware of the profiling attacks however most of them communicate information about the accounting which takes lot of time to notice the attacks. So we need to decrease the time of detection of these attacks. The main idea is to increase the early detection and avoid serious threats.

Compromised accounts are those that might have been hacked and used by the hacker. Many people now a days are engaged in social networking sites for many purposes. Many threats has been occurred in this network such as spam accounts and Sybil attacks. The main cause of these spam accounts is that spammers exploit the trust relationship between the legitimate user and his friends on the network. Latest news shows many incidents of hacking accounts. Everytime a user behavior is recorded we need to classify whether it is compromised or not. Assessment of the profile needs to conducted on each and every behavior that comes into account. Profile assessment includes the activities of the legal users. These functions include which friends he made , or any sorts of photo uploads or status posts, messages he sent to his friends in his account and messages received and the sort of clicks he chooses and so on.

The paper is organized as follows. In section II, we discuss the related studies conducted in compromised account detection. We discuss the framework, proposed system , cliskstream , the social behavior and compromised account detection in section III. Finally we conclude in section VI.

II. RELATED STUDY

A lot of research has been conducted to categorize social network user accounts as being used for spreading malicious spams or not. Sybil accounts which were created with the idea of sending out spams or unwanted messages with spreading spams. Some algorithms used to detect these Sybil accounts made use of supervised learning methods. While Sybil accounts can be easily

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

created for getting large viewers , one disadvantage is that they can be quickly be discovered and thus it is difficult for them to gain enough reliability. Cause of this it can be highly significant to attempt to capture the exsisting user accounts.

Another unsupervised approach has been discussed in [7]. They made use of the principal component analysis (PCA). PCA is used to represent the behavior of the normal user using small set of latent temporial or spartial and spatio-temporal features which can be used to differentate from a normal user. This makes it possible to detect various types of abnormal behavior, like Sybil accounts.

COMPA system [2] is another algorithm used based on supervised learning classification based on anamoly detection approach. COMPA builds a behavior feature for individual user on their personal interest and their previous actions.

Stringhini [6] set up honey pots for identify spam accounts and identify the features od spammers such as URL ratio is their messages, friends selection etc. Using these features , they used clasificaion algorithm to detect spammers.

III. FRAMEWORK

1) Proposed system

In this paper, we first build a social behavior profile of the online social network to distinguish between different users and their behavior patterns. We will consider two types of behavior for the online social users, extroversive and introversive behavior , based on these features we will be able to distinguish spam users from the legitimate owners.

Specifically, we introduce different featured to represent a users social behaviors, including extroversive and introversive behavior. A user's feature values consists of its behavior profiles. The analysis is not only conducted on user profiles and message contents, but we try to discover the users history of his social activities. Online social networks provide various features like sending messages, chatting, uploading photos, browsing content, browsing friends, uploading status, downloading pictures etc.

These activities are totally based on the users personal interests and his social behavior patterns. It is easy for a hacker or a spam user to hack an account if he has a slight idea about the user behavior on social network. Firstly we try to collect the user clickstream data by collecting the number of clicks on a social network site. We propose new behavior features that evaluate user differences in social activities. Or each behavior we measure the clicks observed from each users clickstream. Lastly combination of all the behavior into a social networking behavioral profile.

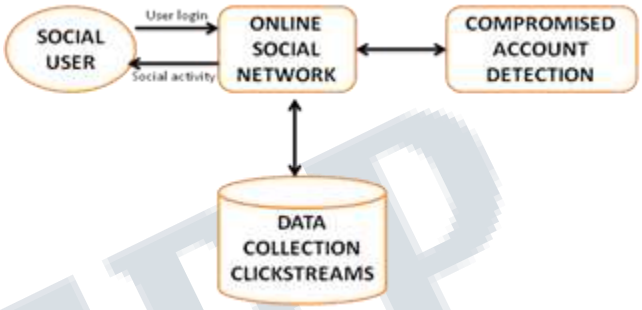

Fig: System Architecture

2) Clickstream

Clickstreams record the users clicks same time as web browsing. The clicks are recorded when the user clicks on any webpage, website or any software application. All thse clicks are recorded on the server side or sometimes on the client machine. Clickstream analysis involves analyzing each individual page in the website made by the users and sent to the server machine. The benefit of clickstreams is that it evaluates the online social behavior of the users. The authentic users patterns are recorded.

Different methods are available to record the clickstream data of the online social users. By making the use of server log files, URL or HTTP requests and recording ISP requests. An user directs from one page to another, by clicking on different menus and buttons. These clickstream information can be used for a variety of purposes, such as marketing etc. Clickstream tells where the user has clicked and how many times on a page he has clicked. Many different clickstreams can be combined together to give better analysis. Clickstream data can be used to restructure large websites based on their past performances.

Another method to evaluate clickstreams data is by making use of the sessions and cookies. We identify each requests and determine individual sessions of each pages in the website. We represent the start of a session, when the user visits the social networking site in a browser, and the end of the session is represented when the user closes

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

all the windows or tabs . Clickstream from each tabs or pages are grouped into individual sessions and are not combined with those from other pages or tabs. Clickstreams fro inactive period --pages in which no activity has occurred for a long duration, are evaluated separately. For example, an user may go away from a website leaving behind the browser open and running. We plot a graph by eliminating these types of idle periods.

For each incoming request we define a cookie a value, this cookie will contain an ID, which will be able to track each individual users. If the ID is already existing then we use the existing one , or ese create a new ID.. Sessions have a time span such as five minutes and they expire soon as it is over.

3) Social behaviour

We have defined two types of social behavior features as;

1. Extroversive Behavior
2. Introversive Behavior

Extroversive Behavior

Extroversive behavior shows how a user interacts with his online social friends and consequently characterize user behavior.these behaviours like uploading pictures, sending messages to friends online ,etc. The first activity in the extroversive behavior is when the user is logged on to the website. Some users may start commenting on the users status or a picture while others may upload his own status or photos. This typically depends on the users personal interests and preferences. While some activities are consistent which lead from one activity to another. Some users after liking friends status may update their own status or may start chatting with his friends online etc. Many activities in socal network are time consuming as they require various steps to complete.

Introversive Behavior

Introversive behavior such as browsing other users profile or friends online, visiting friends profiles, searching messages in inbox etc, which do not make any visible effects to other users. This behavior is invisible to other users, but makes up the majority of the social activities, i.e browsing. Browsing different profiles helps the user to collect informations about different users and their personal profiles and generate ideas and opinions to establish connections and communications with them. Intoversive behavior makes the the most important part of the social activity.

4) Compromised Account Detection

For detection of compromised accounts , we study the structure of the users social behavior using the behavior defined. Building this profile we can make a decision, whether the arriving clicks is from a legal user or from a spam user. If it is authentic, then it should obey the behavior patterns represented by the behavior profiles.

When an account is compromised, it is most likely to post spams, and differentiating it from a legal user is much higher. The main purpose of the spammers are to send spams and they can be planned and focused mainly on posting spams. Thus their behavior obviously diverges from the normal users. Thus there is a much higher chance that these clickstream will contain postings that are very different from the behavior profiles built.

Not all spammes will implement stratergies that will post spams and control the compromised accounts, whereas they will try to slow down their browsing speed as to look like a normal user. But is is really difficult to predict a normal user behavior pattern. Our method does not detects compromised account based on spreading spams in a particular way. Most of the existing systems detect the spam messages, but does not detect any suspicious data related to photos or sharing etc. However detecting of spams depends on different forms of spams.

Our method will make use of a combinations of different clickstreams and message content analysis which will be based on the different behavior.

IV. CONCLUSION

In this paper, we study the users behavior in social network according to different behavior defined. We also plan to build a social behavior profile for individual social network user to distinguish their behavior patterns. By considering both types of behaviors defined above , we try to identify the compromised accounts from online social network data. We can get accurate data when the behavior profiles are buit in a complete and perfect fashion. We belive that future researches of social network will create interesting research problems and appropriate solutions in this field.

REFERENCES

1) F.Benevenuto, T. Rodrigues, M. Cha, and V. Almeida. “Characterizing user behavior in online social networks”, Chicago, Illinois, USA, 2009. ACM.

2) M. Egele, G. Stringhini, C. Kruegel,and G.Vigna.”Compa:2}Detecting compromised accounts on social networks”. , San Diego, CA USA.

3) H. Gao, Y. Chen, and K. Lee.” Towards online spam filtering in social networks,” San Diego, CA USA.

4) H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. “Detecting and characterizing social spam campaigns”. Melbourne, Australia, 2010. ACM.

5) F. Schneider, A. Feldmann, B. Krishnamurthy, and W. Willinger. “Understanding online social network usage from a network perspective”. Chicago, Illinois, USA, 2009. ACM.

6) G. Stringhini, C. Kruegel, and G. Vigna. “Detecting spammers on social networks”.Austin, Texas, USA,2010. ACM.

7) B. Viswanath, M. A. Bashir, M. Crovella, S. Guha, K. P. Gummadi, B. Krishnamurthy, and A. Mislove.“Towards detecting anomalous user behavior in online social networks”. San Diego, CA, Aug. 2014.USENIX Association.

8) G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao.”You are how you click: Clickstream analysis for sybil detection”,Washington D.C., USA, 2013.

9) C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu. “Analyzing spammers’ social networks for fun and profit: a case study of cyber criminal ecosystem on twitter”,Lyon, France,2012. ACM.

10) Nils Kammenhuber, Julia Luxenburger, Anja Feldmann, Gerhard Weikum. “Web Search Clickstreams”. Rio de Janeiro,2006.