ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

Aiding the Detection of Compromised Accounts

Neha M. Yadav[1], Prof. Dr. P. N. Chatur[2]

P.G. Student, Department of Computer Science and Engineering, Government College of Engineering, Amravati, India[1]

Professor, Department of Computer Science and Engineering, Government College of Engineering, Amravati, India[2]

ABSTRACT: Nowadays, due to the rapid increment in the use of internet, different types of threats has been occur. Users are more inclined towards the social networks and it is also known as the Online Social Networks(OSNs). Suspicious account also called as compromised account or the account that has been hacked by the hacker. In order to provide a secure Online Social Network(OSN), various detection techniques has been used to detect compromised account. In this survey paper, for detecting the compromised account, the behaviour of the user is tracked. That is, the Online social behaviour of the user is studied which includes various factors such as the different activities performed by the user and the sequence of the activities is also taken into consideration. Various measurement factors are also considered such as the time spent by the user on a particular module, etc.Based on the mentioned measures and the activities, the behaviour of the OSN user, user is validated. By evaluating the results helps in distinguishing the user's OSN behaviour and thus, detects the compromised account.

KEYWORDS: Compromised account detection, Online Social Networks, Suspicious account, Online Social Behaviour.

I. INTRODUCTION

Compromised accounts are those accounts that are hacked and used by the hacker. Due to the rapid increase in the OSN users, millions of people are getting addicted to the use of Social network. Generally there are several and different types of threats that has been occur in this network. Spam accounts and the sybil accounts are few of them. The main purpose of Spam accounts is to exploit the well established connection occurred at time of communication between the authorised user and his friends in the network.

Sybil accountsare the accounts that sends the malicious spam ads to the user's friends. But compromised accounts are more favourable to the increasing OSN. Nowadays, large amount of hacking incidents came into existence. Compromised are not like sybil or spam accounts. In compromised account every time the user behaviour is tracked so that to detect whether is compromised or not. Profile analysis needed to be done each and every time to detect account. Also the concept of filtering is also applied on the different fields such as messages in the account. Profile analysis includes the activities and keeps track of all the activity by the original user . These online features includes the nature of the original user like how and which type of connections he likes to make or made, types of photos he uploads and downloads, which type of people he adds to his connection, which types of messages he sends and receives from his connections, type of clickstreams he chooses, the way accesses his friends profile, etc.

In this survey paper, the proposed system includes different modules which of them are :

1. It includes all the social activities controlling mechanism. The activities such as the uploading photos, updating status, users behaviour tracking.
2. The second is the user management module, where all the friends in the account aremanaged.
3. Third is to study the user behaviour. It includes the extroversive behaviour tracking.
4. Fourth is to study the users introversive behaviour.
5. The last is to study the user access permission wise behaviour .

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

In Access permission wise behaviour, System automatically keep a track of document category wise access permission specification. If a user is trying to specify access permission to unusual group/person, system will consider that activity as a suspicious activity. In order to perform activity, user needs to access the permission. This helps to differentiate the user behaviour anamoly.

In this survey paper, section II shows the related work. Section III explains the users behaviour study in order to characterised the user study behaviour. Hence helps in detecting the compromised account.

II. RELATED WORK

The users behaviour study is more beneficial in detecting the different types of threats occurring at the time of OSN. Some of the threats may include the traffic in the network for sending and receiving data. Here data can be of any type, it may be a text message or it may be a photo.

Schneider and Benevenuto has made the study of the user Online Social Network behaviour that based on the network traffic that are collected from the different ISPs. Both makes the study on the network analysis over which the user interacts. It includes the length of the communication that has been developed. It also includes the clickstreams that is the clicksequences made by the user. In additional to this, Benevenuto makes further study that includes the interaction of user with his friends and the other over the OSN. But this is not sufficient to detect the compromised account, so it is to be needed to characterised the users social behaviour and to detect the OSN account usage anamoly. Hence, additional and the measurement study is required for fine and accurate results.

Further, Vishwanath also aims to detect the users social behaviour in social network that is in Facebook. But he fully focused on the 'like' type of behaviour in order to detect whether the account is spam or not. Many previous researches has been made to detect the compromised account by analysing the users social behaviour.

Furthermore, Egele studied indetail to detect the compromised account by mainly focusing on the users social behaviour analysis with different features. These features includes the timie evealuation, the users behaviour and bonding with the friends and the types of the friend he made by sendind the request and accepting the request. He also focused on the users users photos posting behaviour , commenting behaviour, time evaluating. The more advancement is needed, so, the method of clustering is applied on the messages.

Wang also proposed the mechanism in which it can detect the fake account or an sybil account by analysing the clickstreams. He mainly proposed by onsidering the factos such as the inter arrival time and the click sequences in an account in OSN. Thus this mechanism is useful in detecting sybil account.

In order to detect the spam account, Lee and Stringhini works on the URL ratio in the text messagegs and the the diffrent choices of the friends.

Our system aims at the increase the performance for detecting the compromised account detection along with decreasing the complexity and increasing the security in OSN.

III. USER SOCIAL BEHAVIOUR STUDY

In this section, several OSN users behavioural features are described in details so that it can help in distinguishing the account is compromised or not. Basically the behavioural features are the extroversive behaviour and the introversive behaviour. As the name only describes the features how it will help to distinguish the users behaviour. There are various activities such as the users message inbox, types of searches he made through his account, how he browse the others profile, clickstreams, etc. Whereas the extroversive behaviour includes the message outbox that is the messages send by the user to his friends and the which types of photos uploaded by the user.

Introversive Behaviour: In this type of behaviour, all the internal activities is recorded and traced to detect compromised account. This feature plays an vital role in detecting the compromised account. Since maximum activities can be easily traced here also. It also includes some additional more features to differentiate the users behaviour. The following are the various features:

1. User searching preference: Various classification has been made in the OSN Searching preferences. So that it became easy to depict the preference of browsing activity made by any user. For example, Users profile includes the photos section, upload file, name of user, different groups ,etc. But the homepage includes the updates and the friends only. It depends on the user that to which activity his actual interest is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

and which activity he prefers the most. Many users are interested in knowing the updates happening in the group that may includes photos uploaded in the group, commenting on the pics, some are interested in chatting, etc. Thus the user preferences differs from person to person.

2. User Searching Sequence: As we have seen how the users interest and the preferences varies from person to person, similarly, the preferring sequences also varies. In order to capture the users characteristics , this feature is useful. For example, navigating from users profile to his friends profile and so on. A very easy navigation has been provided by the OSN.
3. Visit time: After choosing the preference of searching to a particular account or any other type of search, the other important factor that helps to study the behaviour is the visiting time. It shows the total time duration of the user take to browse on a particular website or a profile reading. It also evaluate the time where the user spends more time and the less time. It shows the users interest characteristics. The main aim of this feature is to evaluate the type of information consumed by the user. For example, some user spend more time in commenting on the pictures uploaded, while some on chatting.

Extroversive Behaviour: Extroversive behaviour depicts the users actual behaviour, how he interacts with the other people. It became easy to study and characterized the users behaviour. It also further consist of some features:

1. The first feature is to tracking the users first activity when he first perform after logging in into the account. For example, some user after logging in into the account first see the news feed, while some in commenting, etc. Thus this helps to study the users habitual activity to which it first performs.
2. After capturing the users first activity, the other feature is to evaluate the time latency or the time duration he spends in doing to perform the first activity.
3. In extroversive behaviour also, like introversive behaviour, the users preferences is considered. But in extroversive behaviour feature, it keeps track of all the preferences the user choose in performing extroversive activities.

IV. SYSTEM WORKFLOW

Figure shows the actual workflow of the activity of detecting the sybil account. Here, firstly the user is needed to login to his/her account by using the user id and the password provided at the time of registration of account. The credentials provided by the user is validated with the help of the social database DB.

After authentication of the user, the number of activities and the behaviour of the user is traced with the help of mentioned different tracking ways which includes both the introversive behaviour as well as the extroversive behaviour. If any suspicious activity found then the account has been deactivated automatically.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

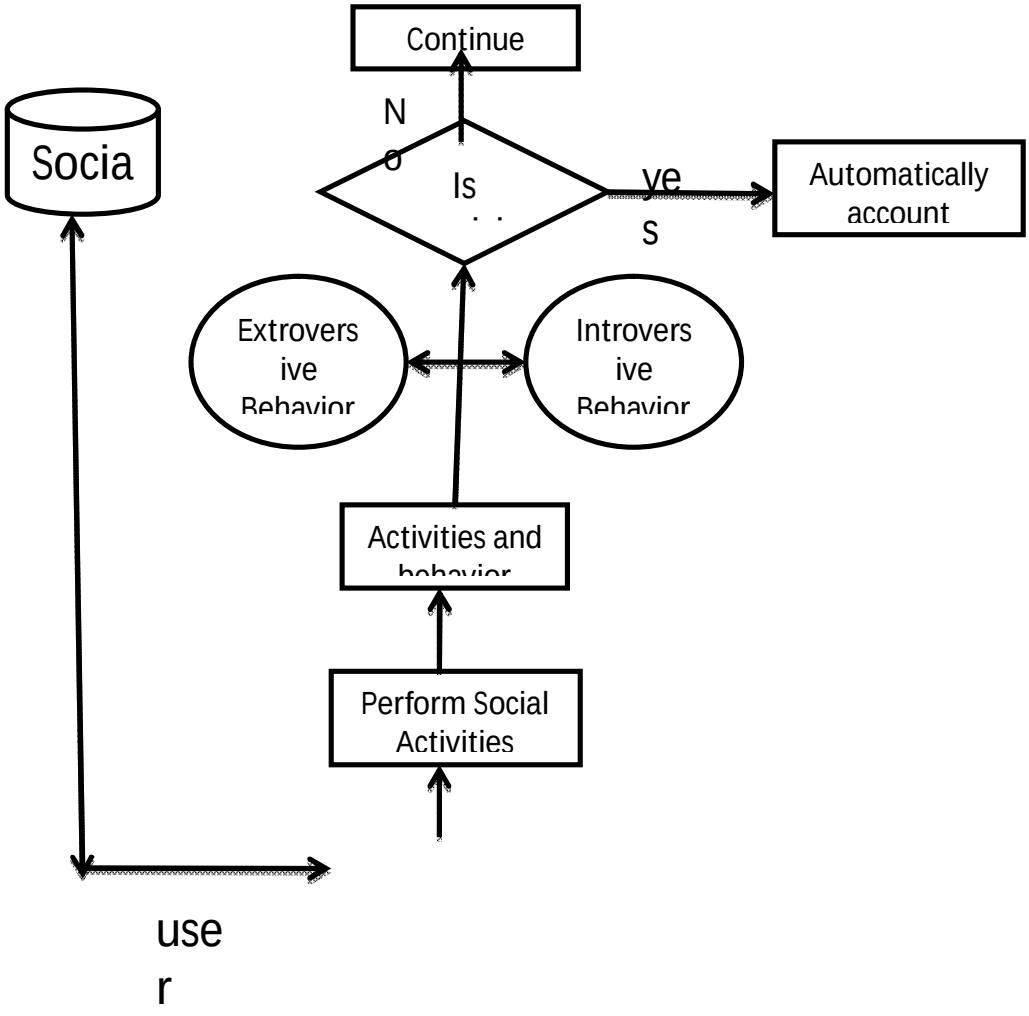

Fig. 1. Suspicious Account Detection System Workflow

V. CONCLUSION

In this our survey paper, we have proposed a Compromised account detection technique in the Online Social Network(OSN). All the approaches has taken into consideration such as an extroversive and the introversive types of behaviour that helps to easily identify the compromised account. Also by tracking the original users behaviour and maintaining the analysis of his various activities and evaluating the various factors helps to achieve the high detection accuracy.

REFERENCES

[1] MXin Ruan, Zhenyu Wu, *Member, IEEE, Haining Wang, Senior Member, IEEE, and Sushil Jajodia, Fellow* ,"Profiling Online Social Behaviors for Compromised Account Detection," *IEEE* TRANSACTIONS JANUARY 2016.

[2] Viswanath *et al.*, "Towards detecting anomalous user behavior in online social networks," in *Proc. 23rd USENIX Secur. Symp.*, San Diego, CA, USA, Aug. 2014, pp. 223–238.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 1, January 2017

International Conference on Recent Trends in Engineering and Science (ICRTES 2017)

20th-21st January 2017

Organized by

Research Development Cell, Government College of Engineering, Jalagon (M. S), India

[3] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxon, "Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse," in *Proc. 22nd USENIX Secur. Symp.*, Washington, DC, USA, 2013, pp. 195–210.

[4] Y. Bachrach, M. Kosinski, T. Graepel, P. Kohli, and D. Stillwell, "Personality and patterns of Facebook usage," in *Proc. 3rd Annu. ACMWeb Sci. Conf. (WebSci)*, Evanston, IL, USA, 2012, pp. 24–32.

[5] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proc. 9thUSENIX Conf. Netw. Syst. Design Implement. (NSDI)*, San Jose, CA, USA, 2012, p. 15.

[6] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. Symp. Netw. Distrib.Syst. Secur. (NDSS)*, San Diego, CA, USA, 2012.

[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proc. 10th ACMSIGCOMM Conf. Internet Meas. (IMC)*, Melbourne, VIC, Australia, 2010, pp. 35–47.

[8] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in *Proc. 33rd Int. ACM SIGIRConf. Res. Develop. Inf. Retr. (SIGIR)*, Geneva, Switzerland, 2010, pp. 435–442.

[9] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Austin, TX, USA, 2010, pp. 1–9.

[10] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao, "You are how you click: Clickstream analysis for Sybil detection," in *Proc. 22nd USENIX Secur. Symp., Washington, DC, USA, 2013*, pp. 241–256.

[11] 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," in *Proc. 21st Int. Conf. World Wide Web (WWW), Lyon, France, 2012, pp. 71–80.*

[12] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting compromised accounts on social networks," in *Proc. Symp. Netw. Distrib. Syst. Secur. (NDSS), San Diego, CA, USA, 2013.*