AUTOMATIC DETECTION OF FAKE PROFILES

[1]Sanju, [2] Dinesh

[1,2]Computer Science & Engineering Department, M.D.U, (India)

ABSTRACT

This paper presents the study of various methods for detection of fake profiles.In this paper a study of various papers is done, and in the reviewed paper we explain the algorithm and methods for detecting fake profiles for security purpose. The main part of this paper covers the security assessment of security on social networking sites.

Keywords: Objective, Problem Statement, Scope, Conclusion, Survey

I. INTRODUCTION

A social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people who have the same interests. These Online Social Networks (OSN) uses web2.0 technology, which allows users to interact with each other.

These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends.There are no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method**,**it can be applied easily by online social networks which has millions of profiles whose profiles can not be examined manually.. These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends. In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their up- dates has become easier.

The online social networks have impact on the science, education, grassroots organizing, employment, business, etc. Researchers have been studying these online social networks to see the impact they make on the people. Teachers can reach the students easily through this making a friendly environment for the students to study

II OBJECTIVE

In todays online social networks there have been a lot of problems like fake profiles,online impersonation, etc. Till date, no one has come up with a feasible solution to these problems.In this project we intend to give a framework with which the automatic detection of fake profiles can be done so that the social life of people become secured and by usingthis automatic detection technique we can make it easier for the sites to manage the huge number of profiles, which cant be done manually.

III. LITERATURE SURVEY

Fake profiles are the profiles which are not genuine i.e. they are profiles of persons who claim to be someone they are not, doing some malicious and undesirable activity,causing problems to the social network and fellow users.

Social Engineering in terms of security means the art of stealing confidential information from people or gaining access to some computer system mostly not by using technical skills but by manipulating people themselves in divulging information. The hacker doesnt need to come face to face with the user to do this.

The social engineering techniques are like Pretexting, Diversion theft, phishing, baiting, quid pro quo, tailgating, etc. Social bots are semi-automatic or automatic computer programs that replicate the human behavior in OSN. These are used mostly by hackers now-a-days to attack online social networks. These are mostly used for advertising,campaigning purposes and to steal users personal data in a large scale.

These social bots communicate with each other and are controlled by a program called botmaster. The botmaster may or may not have inputs from a human attacker. The social bots look like human profiles with a randomly chosen.

IV. CLASSIFICATION

Classification is the process of learning a target function f that maps each records,x consisting of set of attributes to one of the predefined class labels, y. A classification technique is a approach of building classification models from an input data set. This technique uses a learning algorithm to identify a model that best fits the relationship between the attribute set and class label of the training set. The model generated by the learning algorithm should both fit the input data correctly and correctly predict the class labels of the test set with as high accuracy as possible. The key objective of the learning algorithm is to build the model with good generality capability

V. SCOPE

The proposed framework shows the sequence of processes that need
to be followed for continues detection of fake profiles with active leaning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by the social networkingcompany.By using method and parameters fake profiles detection becomes easy.As a result of this cyber crime may be reduced.

VI. CONCLUSION

From the above study we conclude that we an detect the fake profiles on social networking sites

VII. ACKNOWLEDGMENT

I show my thanks to all the departments' personals and sponsors who give us an opportunity to present and express my paper on this level. We wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers, books, websites etc.

REFERENCES

[1] T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems, SNS, volume 11, page 8,2011.

[2] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93{102. ACM, 2011.

[3] C. Wagner, S. Mitter, C. K□orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. InProceedings of the WWW, volume 12, 2012.

[4] G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops),2011 IEEE International Conference on, pages 295{300. IEEE, 2011.

[5] A. Wang. Detecting spam bots in online social networking sites: a machine learning approach.Data and Applications Security and Privacy XXIV, pages335{342, 2010.

[6] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35{47. ACM, 2010.

[7] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21{30. ACM, 2010.

[8] S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam based on header and _le properties using c4. 5 decision trees and support vector machine learning.In Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC, pages 255{261.IEEE, 2007.

[9] G.K. Gupta. Introduction to Data Mining with Case Studies. Prentice Hall India, 2008.

[10] Rajan Chattamvelli. Data Mining Methods. Narosa, 2010.

[11] Spies create fake facebook account in nato chief's name to steal personal details, http://in.news.yahoo.com/spies-create-fake-facebook-account-nato-chiefs-name-114824955.html.

[12] Man arrested for uploading obscene images of woman colleague, http://www.ndtv.com/article/andhra-pradesh/man-arrested-for-uploading obscene-images-of-woman-colleague-173266.

[13] How obamas internet campaign changed politics, /bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics.

[14] S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, and N. Borisov. Stegobot:A covert social network botnet. In Information Hiding, pages 299{313. Springer, 2011.

[15] M. Huber, M. Mulazzani, and E. Weippl. Who on earth is mr. cypher: Automated friend injection attacks on social networking sites. Security and Privacy{Silver Linings in the Cloud, pages 80{89, 2010. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93{102. ACM, 2011.

[16] C. Wagner, S. Mitter, C. K□orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. In Proceedings of the WWW, volume 12, 2012.

[17] G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops),2011 IEEE International Conference on, pages 295{300. IEEE, 2011.

[18] A. Wang. Detecting spam bots in online social networking sites: a machine learning approach. Data and .

[19] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35{47. ACM, 2010.

[20] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21{30. ACM, 2010.

[21] S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam