Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Approach for Detecting Profile Cloning in Online Social Networks

Amar B.Ghodke*

Prof. Sonali Kulkarni, Assistant Professor

Department of Information Technology

Nutan Maharashtra Institute of Engineering And Technology.

University of Pune, India

Abstract— Social Network is popular nowadays in last decades. A person have to do is to sign up for the any social networking websites i.e. giving the personal details or information such as name ,address, date of birth etc. After that the person who completes the process of sign up can login in that websites. The Online Social Network (OSN) such as Facebook, Twitter, MySpace, Yahoo, Gmail, linked-in ,allow people to interact with others i.e. they can chat with one or more people's, regardless the geographical position of their own. Due to this the OSN helps to people to create and manage their relationship between others. Apart from that The OSN also transfer the data in forms of files, documents, texts, multimedia, etc. Thus the OSN are now really in demand and popular. Nowadays the Identity Clone Attack (ICA) is increased in the many social networking websites that causes the frustration between the peoples and social networking websites too. This attack is done by retrieving the information of the individuals profile by anonymous person i.e. individual information is leaked and clone or fake profile is created which shows as real one. Thus this leads to the ambiguity between the owner of the profiles and the person associated to their profile i.e. we cannot have control to create over creation of clone profiles in the OSN and impacts it to the person having his or her own profiles. In this paper we introduced the attacks on the OSN and then our proposed system. The proposed system constituents profile attributes similarity and friend's similarity of both real and clone profiles. After these similarity calculation the real and clone profile evaluation is done.

Keywords— Online Social Network (OSN), Friends List, Victim Profile, Fake Profile, Profile Cloning.

I. INTRODUCTION

The Online Social Network's (OSN) are getting more popular and more in use. The OSN websites allows to people connect through each other with the help of their own user profiles. The OSN websites such as Facebook, Twitter, MySpace, Linked-In etc. are allow to create the accounts. After successful creation of user account, OSN authenticate the person via user credentials such as user name and password. While accessing own profile, the person can search for the person that he or she knows him or her personally. In the websites such as Facebook, linked-in etc. a person sends a request to add himself in his or her connections in Facebook it is known as sending friend request and adding to the person in the friend list. Thus people can communicate with each other on the OSN regardless the geographical location of them. Operating the OSN on the websites on the devices such as laptop, mobile, tablets, computer are relatively easy, due to this it makes age group above eighteen can use the features of OSN effectively. Now the OSN has the millions of peoples profile along with their private, sensitive information and tremendous Posts, comments, etc.

In the last decades these popular OSN websites as well as the people facing the problem of profile cloning i.e. an existence of a fake profile of a person having all the details of the person having the real profile in the same or different OSN that leads to the conflict between the people and the genuine profile owner. The clone profile is created by any anonymous person, called as attacker, it might be any person in the world and this term is known as identity clone attacks (ICAs) [1]. The creation of clone profile can be done at anytime, anywhere, any instance, due to this no one has control over creation of clone profile and also there is no mechanism to control to it or by anyone or the OSN.[3]The clone profile is created by an attacker by extracting the profile's private, sensitive information of the genuine profiles, along with their connection. a victim profile has no control to leak the sensitive, private information. as soon as information get by an attacker it creates a clone profile in the same OSN or different OSN then finally that attacker looks for the friends connection of victims profile to add in his or her friends network i.e. sends the friend requests. Once the friends connections are added by clone profile, then an attacker can also access the friends profile information and connections. The clone profile created at same OSN is known as profile cloning while the clone profile created at the different OSN is known as cross-site profile cloning as shown in figure 1.

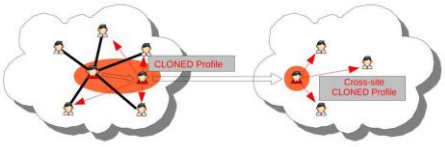

Figure1. Profile cloning and Cross-site profile cloning

II. PROBLEM STATEMENT

The OSN now days having the no. of profile of users typically in millions in that the clone profiles are added too. [2]There is no way to control the activity of clone profile and there creation. This leads the frustration between the many people and OSN.[4]Therefore there is need arises at least to detect this kind of activities and to take necessary actions. In this paper the framework for clone profile detection in OSN is explained. The clone profile in the OSN is searched and detected. Then similarity between the clone profile and the genuine profile is detected on the basis of profile similarity and friend's similarity network. The clone profile detection has 3 phases: in first phase the genuine profile information is considered. In the second phase on the basis genuine profile information its relative profile i.e. clone profiles are detected in the OSN which shows itself as genuine profile. In the final phase the similarity calculation performed between the clone and genuine profiles. On the basis of calculation the clone profile is evaluated.

III. PROPOSE SCHEMES

This section presents our profile cloning detection system in OSN which will detect the clone profiles.

A. Attribute similarity measure:

The attribute similarity measure is used for calculating the similarity of two profiles' attributes. Here by using rank-sum weighting formula, the weight of each attribute is identified, as per the rank of the groups of attributes; with respective to domain, it is possible to be expressed.

$$Sim_{att}\,(Pv, Py) = \frac{\sum i \epsilon z\, Wiy \;\times\; Wiv}{\sum i \in Attv\, Wiv \;\times \sum i \in Atty\, Wiy}$$

Where
Attv : attributes in profile V.s

Atty : attributes in profile Y.

Z: a set of attributes have similar values
in both profiles.

Wiv: weight of profile v

Wiy: weight of profile y

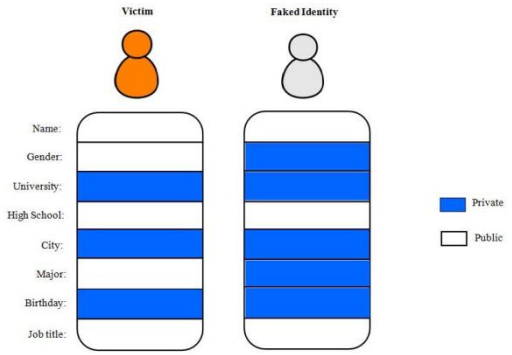

Figure2. Victim and Faked identity profiles

For example there are two profiles in fig 2. The public attributes of profile are ranked with respective to this order as:

name>gender> major > job title > high school

For victim profile Pv and rank order,
name>gender> major > job title > high school
the weights for each attributes are as follows for attributes of Pv

For attributes of Pv

Wname = 0.7

Wgender = 0.36

Wmajor = 0.7

Wjob title = 0.11

Whigh school = 0.19

For victim profile Py and rank order,
name> job title > high school
the weights for each attributes are as follows for attributes of Py
.
For attributes of Py

Wname = 0.8

Wjob title= 0.16

Whigh school = 0.13

Then the attribute similarity measure for both Pv and Py is Calculated as:

$$Sim_{att}(Pv, Py) = \frac{(0.7\times 0.8) + (0.11 \times 0.16) + (0.19 \times 0.13)}{1+1}$$

= 0.30115

B. Friend network similarity:
The other similarity measure is friend network similarity where the groups of friends are present in OSNs of that profile. The groups friends are friends list, excluded friends list and recommended friend list as shown in fig.3

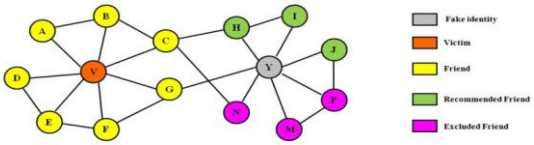

Figure3. Victim and Faked identity Friends Network

The victim profile and clone profiles, similarity measure is calculated according to friends list, excluded friends list and recommended friend list of both profiles. The social network graph and users' connections with their friends in OSN for both profiles are defined in the following ways:

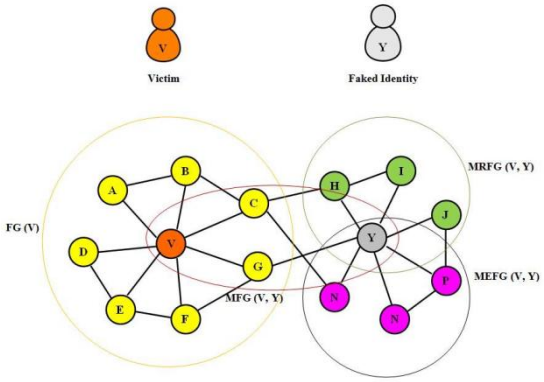

Figure4. Victim and Faked identity's relations are denoted by edges in OSN graph

Where MFvy is the set of mutual friends common in the FLs of Py and Pv

MRFvy is the set of mutual friends common in FL of Py and RFL of Pv

MEFvy is the set of mutual friends common between FL of Py and EFL of Pv

Then friends network similarity of node v to y is expressed as:

$$S_{ff}(p_v, p_y) = \frac{\log(|MFG(v,y).E|)}{\log(2|FG(v).E|)}$$

$$S_{frf}(p_v, p_y) = \frac{\log(|MRFG(v,y).E|)}{\log(2|FG(v).E|)}$$

$$S_{fef}(p_v, p_y) = \frac{\log(|MEFG(v,y).E|)}{\log(2|FG(v).E|)}$$

Where |MFG(v,y).E|,|MRFG(v,y).E|, |MEFG(v,y).E| and |FG(v).E| are the number of edges in MFG(v,y), MRFG(v,y), MEFG(v,y) and FG(v), respectively.

Then from above relation friends similarity measurement of both profiles is given as:
NS(pv, py)= (αSff + βSfrf + γSfef), α+β+γ=1

Where a, ß and γ are parameters to balance the weights of similarities to both profiles of FL, RFL and EFL.

C. Profile similarity:

Profile Similarity measurement is based on attribute similarity and friend network similarity measurement of both profiles is calculated as follows:

Given a public profile Pv of a victim identity v and a public Profile Py of a clone identity y, we calculate the Basic Profile Similarity of these two identities as Sps:

$$S_{ps}(p_v, p_y) = \frac{\sqrt{(kS_{att})^2 + (xS_{fn})^2}}{\sqrt{k^2 + x^2}}$$

Where κ and χ are the parameters to balance the effect of attribute similarity and friend network similarity on the PS..

S_{att} is the attribute similarity measure and S_{fn} is the friends similarity measure.

D. Detection Process

The detection process is will be as follows:

-The victim profile information such attributes and friends network is extracted.

- Profiles in OSN will be searched based on attributes such as name same as victims name.

- The result of search is a set of clone profiles.

- The attributes and friend network will be extracted from each clone profile.

- Based on similarity measures of victim and clone profiles, profile similarity will be calculated.

-According to the calculation and measurements, the decision will be taken that which profiles are clone and which is real as shown in fig.5.

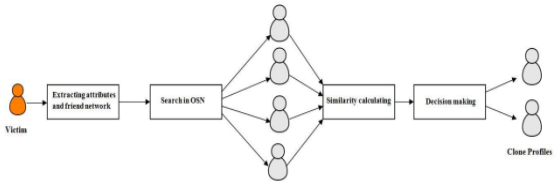

Figure 5 Clone profiles detection process.

IV. RESULTS

The proposed system will be in action as soon as the user log-in to the system. After log-in, the results of clone profile will be displayed by similarity calculations of both real and fake profiles. The results of clone profile will be shown to user as follows:

A. Attribute Based Matching :
- How many attributes of both profiles are similar. e.g. if both real and fake profile have ten attributes and clone profile has six attribute same out of same.

B. User Friend-list wise matching:
- How many friends are same in both profiles.

C. User Content (Post) wise Matching:
- Any posts which is same in both profiles.

The results of clone profile will be shown to user and we take request, command from user's to block fake account then clone profile will not be exists forever.

V. CONCLUSIONS

In this paper, we propose a profile cloning detection system in Online Social Networks. We utilizes the profile cloning detection approaches, like similarity calculations of profiles of both the real and clone profiles, as well as the friend list of both real and clone profiles. Using similarity calculations we can find the fake profiles those are really costing to the OSN and the genuine profile users.

REFERENCES

[1] Mohammad Reza Khayyambashi, Fatemeh Salehi Rizi (2013).'An approach for detecting profile cloning in online social networks, 'Paper presented at the 7th international conference on e-Commerce in developing Countries with focus on e-Security, 17-18 April, in Kish Island, Iran.

[2] Akcora. C. G, B. Carminati and E. Ferrari (2011). 'Network and Profile Based Measure for user Similarities on Social Networks.' Paper presented at the 11th international workshop on Web information and data management, August 35, in Las Vegas, USA.

[3] Bhumiratana. B (2011).'A Model for Automating Persistent Identity Clone in Online Social Network.' Paper presented at the 11th international workshop on Web information and data management, November 1618, Changsha, Hunan Province, China.

[4] Jin. L, H .Takabi and J. Joshi (2011).'Towards Active Detection of Identity Clone Attacks on Online Social Networks.' Paper presented at the first ACM conference on Data and application security and privacy, February 21-23, in San Antonio, TX, USA.

[5] Kontaxis. G, I. Polakis, S. Loannidis and E.Markatos (2011). 'Detecting Social Network Profile Cloning.' Paper presented at the Ninth Annual IEEE International Conference on Pervasive Computing and Communications, March 21-25, in Seattle, WA, USA.

