ISSN 2319-7595

International Journal of Information Systems and Computer Sciences, Vol.7. No.1, Pages : 46-49 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJISCS/static/pdf/Issue/icsic2017sp21.pdf

How to Reduce Cloning of Facebook Accounts

Mohammad Al-Qudah

Department of Computer Science
Amman Arab University
Amman- Jordan
mmaq78@gmail.com

Mohammad Nassar

Department of Computer Science
Amman Arab University
Amman- Jordan
moanassar@aau.edu.jo

***Abstract*—Social media became an integral part in our lives. Where many people, companies and other various commercial fields started to use social media websites such as Facebook for the purpose of marketing, E-commerce, communicating with customers and even for entertainment. On the other hand, some people and organizations misuse the social media, especially in creating fake profiles aiming at deforming other people's images in front of their communities. Consequently, Social media providers should take into consideration the issue of profile cloning, given the wide spread of electronic crimes and the retaliation incidents against some social media users.**

In this paper we suggest a new methodology that tries to stop cloning of Facebook profiles before creating them by using the Normalization process which is part of "Name Entity Recognition" (NER) methodology, and image processing methodology. We are focusing on Facebook accounts due to the fact that Facebook is widely used more than the other social Media sites.

From our research and studies we found out that all these studies examined the cloning of exiting profiles, while none of them tried to prevent cloning of a profile before creating it.

Keywords— Facebook cloning; cloning, social media cloning; fake profile.

I. INTRODUCTION

Facebook is the most spread social Media web site, and is used by many people all over the world, where there are more than 1.86 billion active users.[1] Facebook doesn't make any restrictions on making profiles. Governments may use Facebook to analyze people's trends and thinking. Some people in our country use it to make decisions regarding their own lives including marriage, as he/she can build his/her decision depending on his/her posts and shares.

Anyone can make cloning for any Facebook profile, since it is easy to take the person's profile picture and the same name and make a fake account, then begin adding the original account holder's friends who might have forgotten whether their friend has deleted his/her account and created a new one, so these friends unhesitantly confirm the request. The fake person start to misuse the profile especially by obscene posts or sharing other posts that support terrorist and extremist organizations, which might result in causing serious issues for the original account holder with the security services in his/her country. Additionally, the fake user might also send reports to the Facebook provider in order to block the original profile and keep the fake one, while the original account holder remains the victim.

Most of social media websites provide open interfaces for third-party applications to interact with online social networks by accessing and publishing data (application programming interface (API)), leads to make social media networks lack security and privacy. Some users can use Trojans application to retrieve information about other users like their friends and posts. [8]

Since the social networks have sensitive information like email addresses, messages and photos, the attackers can use a spam attack by stealing HTTP sessions on a network layer, which is most of social networks providers fail to secure. [14]

The goal of social media campaign networks is to increase the spread of information on the network, with keeping the budget in the minimum, so they have to take into consideration the viral campaign. [9]

II. PROFILE CLONING

Some people who use Facebook don't know about the security and privacy terms, or how to tune these terms to match the users' rules. On the other hand, some other users may don't care about such security issues unless they fall a victim or get attacked by vandal users.

It is very important to try to reduce account cloning to mitigate cloning-related issues such as annoying others by

[1] Facebook news room

ISSN 2319-7595

International Journal of Information Systems and Computer Sciences, Vol.7. No.1, Pages : 46-49 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJISCS/static/pdf/Issue/icsic2017sp21.pdf

un-preferred comments, sending messages, pressing like or by any other potential activity.

In our everyday life we might come across with many accounts that belong to a famous person, while some other pages could belong to a certain company or university. Unfortunately, we as users cannot decide which is the right page that belongs to that famous person, company or university. Furthermore, it is very likely that we see on our Facebook wall one post or more telling us to press like or Share to win a prize. The aim of these posts is to collect the maximum number of likes to such pages to collect money.

Many companies use Facebook in marketing and E-commerce, and receive messages from users who may write comments on the companies' pages. If a user has a fake account, he/she can write anything with the victim name, or even request goods from some company and give any fake address. The company could be subject to lose the goods, wasting of time of delivery and money.

III. Normalization

Normalization is a process that enhances information retrieval and searching. It includes things like converting the word to lowercase, word stemming such as (drink, drinking, and drinks all stemming related to the word "drink"), and removing punctuation. We can use this process to match between two words or characters like AAU is matching Amman Arab University when searching the web. It's a very important method that helps in classification, summarization, and Name Entity Recognition (NER) and Natural Language Processing (NLP). [10][11][12]

In this paper, we will use normalization to make a matching on the Facebook profile names, to consider many different spelling names as one name, we can type Mohammad in different ways (Muhammad, Muhammed, Mohammed, Mohamad ...etc.). In our country, several people could have the same name (first and family name) but with different profile images, the fake account may have the same name with different spellings, the friends received the request will not look on the name spelling, rather they will just read the whole name and look at the profile image.

Normalization may use the famous company's names, universities, famous people, Facebook may reserve names for those. For example, from our search we found many pages for one university. Facebook may request a formal paper from the famous company or people or university to reserve the name.

IV. Literature Review

In this study, researchers made a system called it CLONE PROFILES DETECTOR CPD which contains three levels that are : check IP address, similarity measure and behavioral model to find profile cloning, the system just tested on 500 online facebook accounts and gives promising results, the system takes time up to 14 days.[1]

A framework to detect suspect profiles on social media sites, using similarity and friend network similarity attributes, then measure and compute the similarity to decide which profile is genuine, according to measure the cloned profile can be detected more accurate in this approach. [2]

An approach for detecting clone attack based on user action time period and users click pattern, by using cosine similarity and Jaccard index, Naïve Bayesian classification used to identify which network the person using, K-Means clustering used to group place of including users action, time period and users clicking pattern, in order to improve the performance of the similarity. The Cosine Similarity proves that it has the best measure to find the similarity between clone profile and original one. [3]

A prototype system of a tool which can be used by user's discus if they have fallen victims in an attack, the main idea of the tool is to identify unique information that identify a user profile, the authors try the tool on 7% LinkedIn online profiles, they discover a duplicate profiles in the social network. [4]

In this study, a survey was performed on social media sites, facebook, LinkedIn and Google+, 62 friend requests was sent, 91.93% were accepted, 51.61% of them were accepted entirely unknown people, the survey was in one of engineering colleges, the questionnaire was to know the security and privacy awareness of users, the result was cleared that users doesn't care about security and privacy. The authors design a mechanism to detect profile cloning in the same Online Social Networks and some other networks, the mechanism successfully detect Cloned profiles. [5]

The authors proposed a security solution which is when someone make a friend request he has to record a voice message and answer some questions then send it, the other user listen to the voice message, then decide to accept or not.[6]

Using similarity in two ways, one for similarity of attributes from both profiles, the other similarity of relationship networks to find the fake accounts, the results describes that the proposed methods gives better and efficient results compared to existing methods. [7]

ISSN 2319-7595

International Journal of Information Systems and Computer Sciences, Vol.7. No.1, Pages : 46-49 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJISCS/static/pdf/Issue/icsic2017sp21.pdf

Researchers in this study, propose a methodology for detecting Facebook fake profiles, they identify some attributes which are: number of friends, uploaded-photos, tagged-photos, real-profile-photos and wall activity, then assign a score to each attribute to see if the score fall in a specific range, if overall scored more than 60, then the profile is valid. Results in an improved estimation of validity. [13]

V. Proposed Methodology

If someone tries to create a profile or a page of an X person, first we check if the name of X matches a reserved name. If yes we tell the user to change the name because it's reserved. If the name is not reserved, we check the names that match X, if there is a match, we check the profile to see if there is a match, if so, tell the user to change the name and image because they are already used for someone else. Someone may create a new account and put any name and any picture, Facebook will allow him to do so, but after a while he can change the name or the picture, we can use the same method if any one tries to change the name or the profile picture.

We suggest two ways for image matching, the first one when the profile has the person's image and may have many images to the same person in many albums. We can use face recognition algorithm to check all profile pictures to increase the accuracy. The second method comes when a profile has no image for the holder, so we can use the image matching algorithm.

Pseudo code for algorithm:

1- The user ask to create a profile X.
2- Check X in name column *// matching the name, take into consideration normalization.*
3- If (X is a reserved name) then // *we consider that there are reserved names.*
4- Break; *// Tell the user to change the name.*
5- Else if (X match N names) then
   a. Match the profile image of A with the profile images in N // *matching the images.*
   b. If there is a match between a profile image with any name in N.
   c. Break; // *Tell the user to change the name and the picture.*
6- Else create the new profile successfully;

VI. Dataset and results

We collect a dataset that contains about 114 Facebook profiles (pictures and names). We have used 26 profiles as a training set. We built a tool to check the efficiency of normalization and image matching of the tool. The results that came out of this tool were very good; the accuracy percentage was about 84%.

VII. Conclusion and Future work

Facebook is widely used around the globe. However, many people don't know how to change settings in security and privacy, while many others don't care. Every day, companies are developing security measures. Even though, we repeatedly find many incidents of people who are trying relentlessly to overcome these security measures. Accordingly, it seems crucial for researchers to continue working in escalating the level of security and privacy in general terms, and particularly for social media usage. In this paper we suggest a new methodology to try to reduce profile cloning in Facebook, before the user create the profile, using name matching and image matching, so that we can increase the level of security and privacy.

In the future, we are looking to extend our methodology to combine between our suggested proposals and a new algorithm that can examine the previously cloned accounts using different attributes like IP address, device type and time, or we will search for efficient attributes that helps find the cloning profiles, and we will test in other social media sites like Twitter and LinkedIn.

References

1. Sadia, Rauf A., Khusro S., Mahfooz S., Ahmad R., "A ROBUST SYSTEM DETECTOR FOR CLONE ATTACKS ON FACEBOOK PLATFORM", NED UNIVERSITY JOURNAL OF RESEARCH - APPLIED SCIENCES, VOL XIII, NO. 4, 2016.
2. *Khayyambashi M., Rizi F.,* "An approach for detecting profile cloning in online social networks", 978-1-4799-0393-1/13/$31.00 ©IEEE 2013.
3. Kiruthiga. S, Kola Sujatha. P, Kannan. A, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques", International Conference on Recent Trends in Information Technology, 2014.
4. Kontaxis G., Polakis, I., Polakis S., Markatos E., "Detecting Social Network Profile Cloning", 978-1-61284-937-9/11/$26.00 ©IEEE, 2011.
5. Devmane M., Rana N., "Detection and Prevention of Profile Cloning in Online Social Networks", IEEE, 2014.
6. Fayed M., " SNKnock: A free security tool for Facebook users".
7. Sobas P., Johnson H., "Profile Cloning Detection in Social Networks", European Network Intelligence Conference, 2014.

ISSN 2319-7595

International Journal of Information Systems and Computer Sciences, Vol.7. No.1, Pages : 46-49 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJISCS/static/pdf/Issue/icsic2017sp21.pdf

8. Erlandsson F., Boldt M., Johnson H., “Privacy Threats Related to User Profiling in Online Social Networks”, 10.1109/SocialCom-PASSAT.2012.
9. Michalski R., Jankowski J., Kazienko P., “Negative Effects of Incentivised Viral Campaigns for Activity in Social Networks”, IEEE Computer Society, , pp. 391-398, 2012.
10. Elsayed H., Elghazaly T., “A Named Entities Recognition System for Modern Standard Arabic using Rule-Based Approach”, 978-1-4673-9155-9/15 $31.00 © IEEE, 2015.
11. Jabeen S., Shah S., Latif A., “Named Entity Recognition and Normalization in Tweets towards Text Summarization”, 978-1-4799-0615-4/13/$31.00 ©IEEE, 2013.
12. Jijkoun V., Khalid M., Marx M., Rijke M., “Named Entity Normalization in User Generated Content”, 10.1145/1390749.1390755, 2008.
13. Siddiqui H., Brill C., Davis Z., Olmsted A., “Friend or Faux”, 978-1-908320/61/2/$31.00 © IEEE, 2016.
14. Huber M., Mulazzani M., Kitzler G., Goluch S., Weippl E., “Friend-in-the-Middle Attacks”, 1089-7801/11/$26.00 ©IEEE, 2011.