ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW PAPER ON PROFILE CLONE DETECTION IN SOCIAL NETWORKS

Akshay Sharma*, Dr. Sanjeev Dhawan, Dr. Kulvinder Singh
* Department of SE ,University Institute of Engineering and Technology, KUK, Haryana (India)

DOI: 10.5281/zenodo.57976

ABSTRACT

An online social network is used day by day. Social networking is one of the trendiest Internet behaviors, with billions of users from around the humanity. The times use up on public networking sites like facebook, twitter or LinkedIn is frequently increasing at a notable rate. At the similar time, peoples fill their online profile with an overload of information that aims at providing a complete and faultless representation of them. Attackers may duplicate a user's online existence in the same or across dissimilar public networks and, therefore, deceive other users into forming credulous public interaction with the bogus profile.

KEYWORDS: Attack, Detection, Online social networks (OSNs), profile clone, Security.

INTRODUCTION

Social network popularity is growing massively. Billions of community around the humanity is linked to each other by OSN. OSNs like Facebook, MySpace, and Twitter provide the relation between friends, create new relations with people, and reconstruct relation between old friends and share public interest, hobbies in friendship circles. OSN's stores enormous quantity of sensitive plus private information of users and their conversations. As the content of information is increasing, the public network providers and security companies are bound to provide superior safety features in their public network. Several are afford security against hackers, spammers, identity clone, public bots, phishing, and many more threats. But a larger part of online user is not alert with privacy schemes and they frequently disclose an enormous quantity of individual data on their profiles that are able to be seen by anybody in the rest of connections. Attackers could copy a user's online existence in the similar or crosswise dissimilar public networks and, therefore, deceive other users into form credulous public relations with the Profile clone is the perform of construction a profile the same to accessible ones it is usually done to take out in turn from a friend of this profile holder. For example, an attacker is capable to clone the profile of "A" who is B's husband. Then A can send private messages to "B" asking about bank password or because he lost his wallet and mobile phone "A" ask Eve to transfer several cash to his "friend" account. "B" would think that this is her husband and may answer him using the public network or send money. That is why this activity is very dangerous. After the profile clone there will exist two approximately matching user profiles. However, trustful people will normally not confirm that they have two profiles with the similar public information. Profile clone can be done by hand or mechanically. By hand means that someone copies all available information from another profile and then creates a new profile. Mechanically method requires a written script and that the public networking service allows scripts' execution.

TYPES OF PROFILE CLONE

Existing Profile Clone: In existing profile clone, attacker generates a profile of previously-existing users by using their name, own data and then sending buddy requests to friends of that user. This action is thriving since most users admit buddy requests from the person that they previously know without looking through it carefully. Also, it is probable that a person might have multiple accounts. If victims admit the friend requests, then attackers will be capable to contact their data.

Cross-Site Profile Clone: In cross-site profile clone, attacker take user's profile from one public networking site that users register an account, and then generate a new user's profile on a different public networking site that user has not registered on before. After that, attackers apply users make contact with list from the registered public networking site to send a buddy requests to all those contacts in a different public networking site. In this case, it is

further believable than the first case since there is only one account for that particular user. Then, if the contacts accept friend request, attackers can access their profile.

DETECTION OF CLONED PROFILE

Extracting Data from the user's Profile: The User's profile is analyzed to search for rare pieces of data. This data may be specific to a particular user. The user credentials like name of the user, profile photo, Education details, workplace etc. are used to identify the particular user. The data gathered is now used on public network search service provide by the OSN.

Searching for the user's profile on other Public networking sites: In this step to identify the existing profile clone the profiles having same name are identified and user-identifying data is collected from each of these profiles. In case of Facebook this data can be easily extracted by via the Graph functionality. Similarly to identify the cross-site profile clone the profile under consideration is searched on the related OSN by via the user's real name.

Calculating the similarity index to identify the cloned profile: Each Record store is examined in regard to the user's original profile. A comparison is made between the original profile and the searched record and after the comparison a match Index is calculated. Profile photo is having very important role in this method to verify the cloned profile. As cloned profiles may use the victim's photo to look more legitimate. The profile having the maximum match Index may be the cloned profile. The profiles having very low similarity index are declared as bogus profiles. The cloned and bogus profiles are confirmed with the legitimate owners of the respective profile.

RELATED WORK

Profile clone in OSNs

Social Networks are utilized by many people so duplicacy of profile is occurring day by day. Many researcher proposed own method .In 2009 Weimin Luo *et al.* [1] proposed the coercion to public networks and examine the targets what the attackers want and the methods how attackers perform the attacks. The authors had proposed some method to divide public networks into two parts name as user networking site and public networking site. Then introduce the related attacks on public networks after that the contented and manner of coercion to public networks. In the last part authors discussed a security framework of public networks and this makes it clear where and of what we should be aware. In 2011, Bhume Bhumiratana [2] proposed a model to find out duplicate (clone) attacks on OSNs (OSN).In this model to develop OSN pathetic conviction model and maintain authenticity of the bogus online identity established by identity clone attack to harvest more private data and argue regarding how the attack can be dissatisfied and avoid by the users and developers of OSN. Their design was used to develop attack methodology to take advantage of cloned bogus profiles and carry authentic conversation between the exploited users. Author presented a system that Works across different public networking sites, and implement a simple experiment to test and fine tune various aspect of the attack. In addition of profile clone in different public networks Danesh Irani *et al.* [3] proposed a model name as Modeling Unintended Personal-data Leakage. In this model authors was evaluating the attacks like Physical Identification Attack and Password-Recovery Attack by the method of online public footprints and then proposing mechanisms, such as *k*-anonymity and *p*-sensitivities, to model privacy protection in the situation of multiple public profiles. User uses and participate in the public networking sites like twitter, facebook etc. Anil Dhami *et al* [4] analyzed the data revealed in user's profile can show the way the risk like self theft, online irritation, and cyber harassment. The main area was focused impact of privacy, security, and trust on user's enthusiasm to share information within the public networking sites. Moreover, web of trust it mean "TrustBook" public network prototype model was discussed and proposed by Umara *et al.* [5]. In proposed model, the first part was author proposed the experiment to estimate the presentation of our work against well know public networking site. Next Authors used the performance metrics name as applicability, dependability and usability for good resilience against profile clone and other kinds of security attacks.

Detection and preventions process

In 2011, Georgios *et al.* [6] proposed a methodology for detecting public network profile clone. The authors had projected the architectural design and execution details of a prototype system that was able to be engaged by users to explore whether they have fall victims to such an attack. In this design three main components was used name as Information Distiller, Profile Hunter, and Profile Verifier. In execution detail authors had consider two approach

names as Automated Profile Clone Attacks and Detecting Forged Profiles. In similar way Lei Jin *et al.* [7] proposed a detection framework that was focused on discovering suspicious identities and then validating them. Towards detecting doubtful identities, was proposing two approaches based on attribute similarity and similarity of friend networks. The first approach addresses a simpler situation where a common friend in friend networks was considered; and the second one captures the scenario where a similar friend identity was involved. In last part authors discussed various realistic Solutions to authorize doubtful identities. In addition of bogus profile detection method Mauro Conti *et al* [8] proposed a public network graph from a active point of view within the situation of confidentiality threats. Authors had discussed about Dataset, development more time of the number of friends, genuine life public network based verification, OSN graph structure for bogus profile detection all of these mechanism help to detect bogus profile in OSNs.Futhermore, Mohammad and Fatemeh [9] proposed a loom for detect profile clone in OSNs. In this loom authors had discussed about attribute similarity and friend network similarity by using this loom clone profiles can be detected more exact.Zifei *et al.* [10] proposed an approach for detecting profile clone in OSNs name as Content-free Detecting Approach and the second was Content-related Detecting Approach. In addition of detection process profile will be confined and prevent the data leakage in public network then Raymond *et al.* [11] discussed the how to start supposition attacks using unconfined public networking data to predict private information. Then plan three possible refinement techniques that could be used in different situation In addition, they explore the outcome of removing facts and links in preventing susceptible data outflow. In the process, they exposed situation in which shared inferencing do not develop on using a simple local classification method to identify nodes. At last author had combined the consequences from the collective inference implications with the individual results; they start to see that remove details and familiarity links equally was the best way to decrease classifier accuracy.Detecting Clone Attack in Public Networks Using Classification and Clustering Techniques was proposed by Kiruthiga *et al.* [12] .The first part author had discussed the clone attack detection based on user action time period and users click pattern to find the similarity between the cloned profile and real one in facebook. The second part author had discussed the users profile information every user's information is stored. Using Naïve Bayes Classifier classify the details for every user information. K-Means clustering is to group the same Network. Clone Spotter is to detect the clone in facebook. In last authors was considering the Cosine similarity and Jaccard similarity to find the similarity for improving the performance. Moreover Morteza and Fatemeh [13] proposed the detection approach was organized by six methods that was Discovering community the public network graph, Extraction user's attribute, Search in community, Selecting profile, Computing strength of relationship, Decision making all these methods to identify and detect profile clone. In addition of profile clone and detection method Fatemeh *et al*. [14] proposed a techniques to finding cloned profile .Firstly, define the profile clone attack and cross site clone attack after that the next step was Profile Clone Detection in this six main method was proposed Collecting Suspicious Profiles, Profile Evaluation, Attribute Similarity Measure, Strength of relationship measure, Discovering communities in public network, Evaluation and detection. Through experiments, it was shown that the presented approach was very effective and it can discover clone identity more accurate.Similary, Dipali Suhalal Patil [15] proposed techniques to detect profile clone in online public networking sites Firstly, she discussed the type of profile clone name as profile clone and cross site profile clone and check the profile victim after that she discussed the CLONE IDENTITY COMPONENT in this she define Attribute similarity, Friend Network similarity, Basic Profile Similarity (BPS) ,Multiple-Bogusd Identities Profile Similarity (MFIPS).In last she define Clone Detection Process mainly three component was used name as Information Distillery, Profile Hunter, Profile Verifier. Furthermore, Piotr *et al.* [16] proposed a Profile Clone finding in public Networks. The author was discussed two methods to detect profile clone the first method was based on the connection of attributes from both profiles and the second method was based on the connection of relationship networks. The methods are further evaluated with experiments and the results clearly describes that the proposed methods was functional and capable compared to existing methods.Similary, Devmane and Rana [17] discussed finding and preclusion of profile clone in OSNs The first part authors had discussed type of profile clone name as similar site profile clone and cross site profile clone. Next discussed the detecting technique of cloned profile and bogus profile, the technique was Extracting Information from the user's Profile, Searching for the User's Profile on other Public networking Sites, Calculating the similarity index to identify the cloned profile, Discussion about the results shown in the tables. At last part author had discussed about prevention methods which was proactively manage your profiles privacy settings, Accept friend requests from known people only, Perform the checking of existing friend list and many more. Ali *et al*. [18] proposed a model for detect clone attacks in OSNs based on a novel public graph topology. The first part was that author had introduce a hypothetical structure which depends on a novel topology of a public graph called Trusted social Graph (TSG) which was used to image trust instance of public communications between OSN users.A different role was

proposed discovery model that based on TSG topology as well as two techniques; DFA and Regular Expression. The proposed detection model decides whether these public announcements or societal performance from authenticated and trusted profiles or from bogus and unauthenticated profiles. Ameena and Reeba [19] proposed the Classification techniques for detection of bogus profiles in public networks. There was three classification techniques was proposed name as Naive Bayes Classification, Decision Tree Classification, Support vector Machine. For classifying profiles was proposed and this be able to be used as a structure with which automatic detection of bogus profiles was possible with a very high efficiency as high as around 95%. Prevention of bogus profile explosion in OSNs was discussed and analyzed by S.Priyanga *et al*. [20] firstly, the author had discussed about attack known as identify clone attacks (ICAs),after that the two similarity determine was used for calculating the similarity of two profiles name as attribute similarity and friend network similarity. These two similarity author was discussed about the detection process and prevent them.

Hence the different techniques proposed by researchers are studied mainly two concepts were there, profile clone and detection methods. Many techniques are used for detecting profile clone .Each one has its own advantages as well as drawbacks. But there is a large amount added improvement is needed in the existing techniques

CONCLUSION & FUTURE WORK

This paper presents a concise knowledge about the attacks and defense mechanisms which are prominent on OSNs. It also explains the work which had been performed in the field of detecting clone profiles and cross site clones on OSNs.In this paper defines approaches for detecting public network profile clone using a different techniques .In future, a new propose a enhance algorithm using naïve Bayes classification and Enhanced clone spotter to find the similarity and dissimilarity between two users.

REFERENCES

[1] Weimin, Jingbo , Jing and Chengyu , “An study of security in public networks”, 978-0-7695-3929-4/09, 2009, IEEE, pp.648-651
[2] Bhume Bhumiratana, “A Model for Automating unrelenting Identity Clone in OSNs”, 978-0-7695-4600-1/11, 2011, IEEE, pp.681-686
[3] Danesh Irani, Steve Webb, Calton Pu and Kang Li, “Modeling unintended personal-data leakage from multiple OSNs”, 1089-7801/11, 2011, IEEE, pp.13-19
[4] Anil Dhami, Neha Agarwal, Tamal Kanti Chakraborty, Brijendra Pratap Singh and Jasmine Minj, “Impact of trust, security and privacy concerns in public networking: An investigative study to Understand the pattern of information revelation in Facebook”, 978-1-4673-4529-3/12, 2012, IEEE, pp.465-469
[5] Umara Noor, Zahid Anwar, Yasir Mehmood and Waseem Aslam, “TrustBook: Web of trust based relationship establishment in OSNs”, 978-1-4799-2293-2/13, 2013, IEEE pp.223-228
[6] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos,“Detecting Public network Profile clone”, 978-1-61284-937-9/11,2011,IEEE,pp.295-300
[7] Lei Jin, Hassan Takabi and James B.D. Joshi, “Towards active detection of identity clone attacks on OSNs”, February 21–23, 2011, San Antonio, Texas, USA.Copyright 2011, pp.27-38
[8] Mauro Conti, Radha Poovendran and Marco Secchiero, “Bogusbook: Detecting bogus profiles in OSNs”, 978-0-7695-4799-2/12, 2012, IEEE, pp.1071-1078
[9] Mohammad Reza Khayyambashi and Fatemeh Salehi Rizi, “An approach for detect profile clone in OSNs”, 978-1-4799-0393-1/13, 2013, IEEE, pp.1-12
[10] Zifei Shan, Haowen Cao, Jason Lv, Cong Yan and Annie Liu, “Enhancing and Identifying Clone Attacks in OSNs”, Kota Kinabalu, Malaysia.,2013 ,pp:1-6
[11] Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, “Preventing private data inference Attacks on public networks”, 1041-4347/13, 2013, IEEE, pp.1849-1862
[12] Kiruthiga. S, Kola Sujatha. P and Kannan. A, “Detecting Clone Attack in Public networks Using Classification and Clustering Techniques”, 978-1-4799-4989-2/14, 2014, IEEE, pp.1-6
[13] Morteza and Fatemeh, “An IAC approach for detecting profile clone in OSNs”, Vol.6, No.1, January 2014, pp.1-6.
[14] Fatemeh Salehi Rizi, Mohammad Reza Khayyambashi, and Morteza Yousefi Kharaji, “A new approach for finding cloned profiles in OSNs”, Int. J. of Network Security, Vol. 6, and April 2014, pp.25-37

[15] Dipali Suhalal Patil, "An approach to detect profile clone in online public networking sites", ISSUE 3 VOL 3 JUNE-JULY ICMSET, 2014,pp.1-4
[16] Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile Clone Detection in Public networks", 978-1-4799-69, 2014, IEEE, pp.63-68
[17] M.A. Devmane and Dr. N.K.Rana, "Detection and Prevention of Profile Clone in Online Public network", 978-1-4799-4040-0/14, 2014, IEEE, pp.1-5
[18] Ali M. Meligy, Hani M. Ibrahim and Mohamed F. Torky, "A framework for detecting clone attacks in OSN based on a novel publicgraph topology", I.J. Intelligent Systems and Applications, 2015, pp.13-20
[19] Ameena A and Reeba R, "Survey on different classification techniques for detection of bogus profiles in public networks", International Journal of Science, Technology & Management Volume No 04, Special Issue No. 01,March 2015,pp.1525-1530.
[20] S.Priyanga,V.M.Priyadharshini and N.Hariharan"Prevention of Bogus Profile Proliferation in OSNs", Copyright to IJIRSET, Vol. 4, Special Issue 6, May 2015, pp.25-32