QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

A Multi Secret Sharing Approach for Vulnerability Identification in Social Media

Dr. Saman Mirza Abdullah
Software Engineering, Koya University - Iraq
saman.mirza@koyauniversity.org
http://sites.koyauniversity.org/saman-mirza/

ARTICLE INFO

Article History:
Received: 19 March 2017
Accepted: 1 April 2017
Published: 10 April 2017
DOI:
10.25212/lfu.qzj.2.2.05

Keywords: *Social Media, OSN, Vulnerability, Shamir Access Sharing.*

ABSTRACT

Online Social Networks (OSN)s become a suitable channel for attackers and threats to break system's security and disclose privacies. In the few years, the demand on keeping OSN users safe from attackers was the trend of researchers. However, it was not a challenge-less process. The most significant challenge was the awareness of the OSN users about their vulnerability level. Works have been achieved to identify relations between OSN user vulnerability and the policies that used by attackers to penetrate systems, and then providing solutions, which were in the form of awareness that difficult for OSN users understand them. Different techniques, such as statistical and datamining tools, have been provided utilized to provide solutions for identifying vulnerabilities, however, target formation was still in primitive stages. This work presents a secrete sharing approach for computing the vulnerability percent of OSN users. The approach computes the rate of the vulnerability of an OSN user based on a polynomial equation.

1. INTRODUCTION

From different countries and having a variety interest and perspective, millions of OSN user are doing huge actives every day. Activities, such as uploading emotional information, downloading applications, and sharing or disclosing private information are attractive to attackers. Such activities make the job of intruders and system breakers very easy to find gaps and vulnerabilities among users and systems. Existing of such types of OSN user activities are changing the trend direction of attackers' policies from misusing the systems' vulnerabilities to misuse user's vulnerabilities. Such attackers' trend encouraged researchers to focus mostly on OSN behaviors and attackers' fingerprint analysis[1].

Most researchers provided security solutions in the form of advice and awareness so that OSN users can follow them for keeping their systems clean. Solutions that presented in the text format are included many security and privacy related terminologies [2-4]. To understand and follow these solutions, readers need to have good knowledge and skills about systems and security issues, which most OSN users are not familiar with them. Moreover, explaining a problem with texts can't give users a measurable indicator for their vulnerability level. Therefore, OSN users need simple and understandable solutions with some measurable indicators about their gaps and vulnerabilities. At the same time, it is necessary to teach OSN

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

users the behaviors that make them disclose to attackers. Also, users should know which misused behaviors they have and at what vulnerability level they are.

This work focusing more on identifying the level and the rate of vulnerability of an OSN user. The rest of the work is going like this. Section-2 provides the some works that achieved in this field to show how researchers provided their solutions to OSN users, and expected gap that not solved yet. Section-3, provides the concept of the secret sharing approach and the point where crosses the concept of OSN vulnerability identification. Section-4 and later show the process of building the model from the scratch, and some results.

2. Literature Review

In the recent years, the use of OSNs has increased dramatically. People find OSNs very attractive as they offer many services, such as virtual relations with persons having similar hobbies and backgrounds. Facebook, for example, currently has more than 1.39 billion active members. Due to the portability of the current devices, location and time limitations are not challenging the OSN users anymore to connect OSN websites. Each user has allowed doing whatever activities he/she likes over there. Moreover, every day OSN websites are providing new services and facilities for their users. With such availability, Internet users can stay connecting OSN website more and more times, and can do wider and wider range of activities. For example, users on FB doing around 3.21 billion activities per day. Of course, not all activities are clean in the viewpoint of security and privacy standards[5].

The variety of users, activities, and even OSN websites facilitate the work of attackers to find a number of gaps to systems and penetrating more number of users and systems. Attackers and intruders now are learned to get a ride over systems through OSN users' vulnerability rather than systems vulnerability. Such trend changed the direction of researching toward analyzing the users' behavior more than operating systems' behavior. In such studies, the aims were not for improving the systems, however, they aimed to improve the users' behaviors. Therefore, most works provided security and privacy solutions to OSN users [6, 7]. However, only a few of OSN users can understand these solutions perfectly.

To simply the solutions for users, most works classified the attacks and threats on OSN users. They even sub-classify them into security related and privacy related works [6, 8-12]. The studies usually provided an overview of the types of OSN attacks. They explained the possibility of those threats to users; furthermore, they provided recommendations and suggestions as solutions for OSN users to protect their privacy and security. A study presented by researchers[7] and they perfectly defined four groups of threats and attacks. In that study, the authors offered many commercial and scientific solutions for OSN users. In other studies [11, 13], privacy, security, and users' behavior were discussed. The works focused on one type of user vulnerability, namely Third Party Applications (TPAs). The authors of both studies highlighted the unique security and privacy design challenges posed by the core functionalities of OSNs, and some opportunities for utilizing social network theory to mitigate these design conflicts and provide possible solutions to limit the information disclosure. For both cases, it is difficult for users to understand and use those models and theories, as they are not sufficiently clear, and users would need plenty of time to learn them.

On the other hand, users need to know their vulnerability level while they are active on OSNs. This could be done through studying the policies of the OSN based attacks and the vulnerabilities that opened by OSN users for those attackers. The problem is how to calculate

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

the vulnerabilities so that a model can decide a user is disclosed or not. A linear model has been designed by [5] and attached to Artificial Neural Network to compute the rate of vulnerability. This work presents a Mutli-Secrete Sharing (MSS) approach to reveal the vulnerability level of a user.

3. Shamir's based Identification Model

The concept of vulnerability is disclosing privacy and doing abnormal behaviors by OSN users while they are interacting with systems. Within each disclose and abnormal behavior, a secret will be provided or a channel will be opened for attackers or threats to penetrate systems. The aim that needs to obtain is to compute the overall vulnerability rate for an OSN user based on their disclosing and abnormally behaving rates.

This work uses the Shamir's (n, t) secret-sharing scheme. In this scheme, n shares of original secret are created, and to retrieve or disclose the secret, an attacker needs to have at least t number of these shares, which means any t-1 or fewer number of shares are not allowed the attacker to reconstruct the original secrete. This is called Shamir's Threshold Scheme. For the vulnerability perspective, an OSN user has n level of security (or vulnerability) for a certain type of the abnormally behaviors. An attacker needs to reach a certain level, which should be equal to t to get advantage of the vulnerability for getting-over the system. Only on that level, the disclosed secret or opened vulnerability is useful for the attacker. However, there is not only one secret (vulnerability) or one attack.

An OSN user may not open only a type of vulnerability (secrete), it may open more than one channel. On the other hand, an attacker has a chance to get over a system through the availability of only one from a set of vulnerabilities. Therefore, there is a possibility of existing more than one channel (vulnerability), and only one channel is enough for an attacker to get-over a system. From other side, there is a possibility of using one vulnerability by more than one attack to get systems.

Assume $V = \{v_1, v_2 \dots v_m\}$ is the set of all available vulnerabilities, and the V_a: $V_a \subseteq V$ is the subset of vulnerabilities that a specific attack can misuse one or some of them to overcome a system. For both (V and V_a), the same Shamir's (t, n) threshold should be applied on each v vulnerability. To achieve this aim, this wok proposes a multi-secret sharing approach.

Through the proposed approach of this work, secrete V will be divided over m participants (channels), in which each v is including all types of levels of a vulnerability (a secret) $\{S_1, S_2, \dots . S_l\}c$ that an attacker should find t of them so that it become able to penetrate a system.

3.1. System Model

The proposed model by this work consist of three main parts. The first part is the OSN users whom do normal and abnormal activities and behaviors over OSN platforms. The second part is the type of abnormal activities that considered as vulnerabilities by system. The last part are the threats and attackers that misusing these activities (vulnerabilities) to penetrate systems. Table 1 shows mapping between the required model and the proposed scheme terminologies.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

TABLE 1: Model and Scheme mapping

OSN identification Model	Shamir's Secret Sharing	Defined Symbol
Vulnerability	Original message	V
Types of vulnerability's	Share of message	v
Level of each v	Content of v	n
Attack policies	Number of necessary v	t
Attacker	A set of t number of v	Reconstruct V

The work of these three parts of the OSN user vulnerability identification regarding the Table 1 is going like this. An OSN user has V vulnerability, which is considered as an original message in Shamir's Secret Sharing Scheme. When the user does some activities on OSN platform, some vulnerabilities (v) are disclosed and become public for attackers. The level of publicity of each vulnerability depend on the frequency rate of doing that vulnerability which rates by the users themselves. To reconstruct the original message V by an attacker, a t number of v elements inside the V should be found.

3.2. Model's Algorithm

The process of this work can be illustrating with two different algorithms. The first algorithm is announcing the vulnerabilities by OSN users, and the second algorithm is reconstructing the vulnerabilities by the attacker.

A. Announcement Algorithm

1. The set of all available vulnerabilities V will be initialized.
2. For any v_i inside V, there is a corresponding weigh w_i shows the degree of risks that caused by the v_i.
3. An OSN user dose some activities that announces all or a part of vulnerabilities of the set V, crating V_a.
4. Equation (1) is using to compute the final rate of the vulnerability for an OSN users caused by a V_a number of vulnerabilities.

$$V(v, w) = v_1 w_1 + v_2 w_2^2 + \cdots + v_t w_t^t \qquad (1)$$

B. Collecting Algorithm

1. An attacker tries to scan an OSN user activities to collect the t number of vulnerabilities that needs for attacking or penetrating a system.
2. When the number of vulnerabilities reach to some predefined t number, the system should give an alarm that reaches a predefined level of vulnerability and indicate the attackers that might possible to attack the system.

3.3. Dataset

This work is evaluating the OSN user behaviors. To start with, the work needs a set of dataset that collecting the user behaviors. This process needs to distribute a questionnaire sheets among OSN users and ask them about their activities they do. This work depends on a dataset that used by [5]. The set covered 18 attack types distributed over 32 policies and vulnerabilities. The type of attacks that covered by that are Spams, XXS and CSRF attacks,

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Phishing, Internet Fraud, Clickjacking, De-anonymous, Face Recognize, SocialBot, Identity Clone, Inference Attack, Information Leakage, Location Leakage, Socware, Online Predators, and Cyberbullying. There are many behaviors that bring risks to users beside systems, such behaviors called Risky Behaviors. With all these attacks and risks, there are many unwanted software called malicious software (malwares). Possibility of becoming vulnerable to malwares increases with increase of doing many risky behaviors and activities. The dataset has built a nice relation between each type of attack and the vulnerabilities of the OSN users. Table 2 explains that each attack is associating with at least more than five vulnerabilities. The table shows the maximum number of vulnerability that an attack can associate with them is 17.

TABLE 2: Permeance Evaluation

Attacks	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
Number of Vulnerabilities	9	6	12	11	11	7	12	6	6	12	11	25	17	5	5	7	11	7

There are five levels (from 1 to 5) of the risk that a threat may attack or penetrate a system. A user at level 1 to 2 in not considered as vulnerability. However, users with levels of 3 to 5 degree are considered as vulnerable. The dataset consists of 705 observations collected in two different countries.

4. Scheme Analysis

The proposed scheme should show a good permeance, and this section analysis this performance in the viewpoint of the responding of the scheme to cases that given in the used dataset. To analysis the scheme, this work will consider a case from the dataset as example of evaluation OSN user behaviors. Table 3 shows the situation of a user. The table shows that the behavior of this user is open for 16 vulnerabilities. For example, v_1, v_2 are considered as vulnerable, while v_3 is not considered as risky.

TABLE 3: An OSN user case

v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	v_{16}	v_{17}	v_{18}	v_{19}	v_{20}	v_{21}	v_{22}	v_{23}	v_{24}	v_{25}	v_{26}	v_{27}	v_{28}	v_{29}	v_{30}
3	4	2	3	2	3	3	3	1	2	2	4	1	2	3	5	4	2	2	1	3	5	3	2	5	2	3	3	3	1

Through both parts of the algorithm, it could be easy to identify which vulnerability(s) a user may have, and what is the rate, and finally awareness is already exist for those vulnerabilities. Table 4 shows the main differences between the performance if this work with two other recent works.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

TABLE 3: Permeance Evaluation

Schemes and approaches	Awareness	Rate of Vulnerability	Revealing Type of attacks	Calculation of vulnerability
[5]	No	Yes	No	Linearly
[4]	Yes	No	No	NA
This work	Yes	Yes	Yes	Polynomial

5. CONCLUSION

OSN user vulnerability becomes a direct target for attackers to penetrate system rather than system's vulnerability. Attackers may get advantage for more than one vulnerability to get over the control of a system. Studies showed that three measures are important for an OSN user; (1) awareness (2) rate of vulnerability of a user (3) type of attack that brings threats for a use. The out performance of this work is showing that no work can include all these three measures in one work. Moreover, the linearity of computing the rate of the work is primitive, because an impact of single vulnerability on the risk degree should be increase nonlinearly (not linearly) if second vulnerability is found be a threat.

6. ACKNOWLEDGEMENTS

This work wants to thank both researchers of the work [5] to provide the dataset of that collected by them to be used by this work.

7. REFERENCES

1. Contributors:, et al. *Security Issues and Recommendations for Online Social Networks*. 2007. **1**, 36.

2. Franchi, E., A. Poggi, and M. Tomaiuolo, *Information and password attacks on social networks: An argument for cryptography*. Journal of Information Technology Research (JITR), 2015. **8**(1): p. 25-42.

3. Savage, D., et al., *Anomaly detection in online social networks.* Social Networks, 2014. **39**: p. 62-70.

4. Hassanzadeh, R., *Anomaly detection in online social networks: using data-mining techniques and fuzzy logic.* 2014.

5. Abubaker, F.R. and P.S. Boluk. *An Intelligent Model for Vulnerability Analysis of Social Media User*. in *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on*. 2016. IEEE.

6. Sadeghian, A., M. Zamani, and B. Shanmugam. *Security threats in online social networks*. in *Informatics and Creative Multimedia (ICICM), 2013 International Conference on*. 2013. IEEE.

7. Fire, M., R. Goldschmidt, and Y. Elovici, *Online Social Networks: Threats and Solutions.* 2013.

8. Fire, M., R. Goldschmidt, and Y. Elovici, *Online Social Networks: Threats and Solutions.* Communications Surveys & Tutorials, IEEE, 2014. **16**(4): p. 2019-2036.

9. Gao, H., et al., *Security issues in online social networks.* Internet Computing, IEEE, 2011. **15**(4): p. 56-63.

10. Daniel, W., et al., *PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS: USER BEHAVIORS AND THIRD-PARTY APPLICATIONS.* 2014.

11. Zhang, C., et al., *Privacy and security for online social networks: challenges and opportunities.* Network, IEEE, 2010. **24**(4): p. 13-18.

12. Guha, S., K. Tang, and P. Francis. *NOYB: Privacy in online social networks*. in *Proceedings of the first workshop on Online social networks*. 2008. ACM.

13. Daniel, W., et al., *PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS: USER BEHAVIORS AND THIRD-PARTY APPLICATIONS.*