TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 2997 - 3003

Risk Measurement of it Privacy and Security Threat in Social Networking Sites on Users Perspective

Balogun Abiodun Kamoru[1], Azmi Jaafar [2], Marzanah A Jabar[3], Masrah Azrifah Azmi Murad[4], Majid Babangida Umar[5]

[1]Dept. Of Software Engineering and Information System, Faculty of Computer Science and Information Technology Universiti Putra Malaysia Serdang Selangor D.E Malaysia.

[2]Dept. Of Software Engineering and Information System, Faculty of Computer Science and Information Technology Universiti Putra Malaysia Serdang, Selangor Malaysia.

[3]Dept. Of Software Engineering and Information System, Faculty of Computer Science and Information Technology Universiti Putra Malaysia Serdang, Selangor Malaysia.

[4]Dept. Of Software Engineering and Information System, Faculty of Computer Science and Information Technology Universiti Putra Malaysia Serdang, Selangor Malaysia.

[5]Dept. Of Software Engineering and Information System, Faculty of Computer Science and Information Technology Universiti Putra Malaysia Serdang, Selangor Malaysia.

E-mail :(balogunabbey@gmail.com)

Article Info
Volume 81
Page Number: 2997 - 3003
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *14 December 2019*

Abstract:

The measurement of privacy and security risks posed to users when using Social Networking Sites (SNS) is considered a challenging task for social networking users. A fundamental aspect associated with the measurement of risks is that a vast amount of data can easily be gathered virtually by any individual. This study presents a Threatware, a tool that can be used for detecting data loss in SNS. This was necessitated by the need for a framework that can identify privacy threats and risks as a way of overcoming the problem of data loss affecting most SNS. We also provided an additional functionality on the software tool that could capture risks based on several ancillary threat models. A critical evaluation of the initial results indicated that an equilibrium existed between the information on privacy threat and its relations that exist among users in SNS. These results rely heavily on users‘ willingness to disclose a significant amount of their settings derived from their friendships on Facebook. The outcome of the study ThreatWare is expected to enhance the detection of data loss as well as provide appropriate actions that can be adopted by users to mitigate privacy and security risks.

Keywords: *Social Networking Sites (SNS), ThreatWare, IT Privacy and Security, Risk Measurement Model*

I. INTRODUCTION

In the last few decades, there has been an increase in the use of Social Networking Sites (SNS) from a global perspective. Statistics provided by Facebook indicate that there are more than 500 million active users and 300 million active users who log on their accounts daily [Facebook Statistic]. The increase in the use of SNS has largely been based on the presence of a huge platform in which users engage with others. However, users have been exposed to numerous privacy and security risks while using SNS. These privacy and security risks are characterized as dynamic, making it difficult to measure the risks posed to users. Within the realms of Information Security, there is a need to prevent data loss fueled by the presence of a vast amount of data in SNS. Measurement of risks within the field of information system is used to estimate the privacy and security risks posed to users while using SNS.

From a global perspective, it is worth noting that the quantification of data loss associated with privacy threats is quite overwhelming. The difficulty in the measurement of risks and its subsequent data loss has largely been attributed to its dynamic nature of the privacy risks posed to users. Therefore, it is essential to estimate the privacy risks in SNS given the extent to which most SNS have exposed users more privacy risks. A study conducted by Facebook (2017) suggested that social media users are very keen not to lose control of their personal information when they disclose it in SNS. To accurately quantify privacy risks posed to social media users, it is essential to identify and measure the various threats and risks.

This paper concentrates on measuring both privacy and security risks that are posed to social media users when using SNS to offer appropriate solutions that can minimize risks. To measure privacy threats posed by SNS, the study proposed a Threatware, a tool that can be used to measure risks within the context of Facebook. This tool is intended to be executed from a user's profile to offer real-time reports and appropriate actions which can mitigate both privacy and security threats. Recent releases of the tool have elaborated the association between privacy and security risks posed to social media users and their friendships on Facebook social network.

Using quantitative research design, the study identified 105 participants who were willing to provide data for the research; however, only 89 research participants were randomly selected to set up the Threatware representing a response rate of 84.7 percent. This was intended to evaluate and measure the risks posed to users on Facebook as one the SNS. In general, the results of the analysis indicated that 58.5 percent of the personal attributes associated with the participants could be derived. Further analysis of the participants' demographics indicates that the research participants represented both men and women who were not married could derive 50 percent of their attributes. Additionally, the study provided participants with user actions which could aid in the mitigation of possible risks. Two critical actions which could be considered by the proposed software tool are possible elimination of risky friend-relations in Facebook and isolation and application of access control mechanisms to offensive friends as a way of classifying them into known groups. For instance, a Facebook user could use access controls as a way of reducing the influence of a certain group of dynamic users. This is based on the concept that the Threatware recommends the adoption of classifying risky users together as opposed to completely deactivating and subsequently deleting their accounts. To offer a list of contact friends, the study relied on the use of a set of heuristics to reduce privacy risk while trying to optimizing friend relationships. These approaches offered considerable improvements as compared to the baseline approaches which adopted the deletion of users pending the fulfillment of both privacy and security. Using the common-friends approach, it was noted that there were 19 less as compared to the baseline approach as a result of remove or group actions.

This study extends the current functionality of the Threatware by incorporating the ability to estimate as well as report privacy threats affecting users. The remaining section of this paper follows the following format. Section 2 provides a design on the Threatware and the experimental approach that is used for data collection. Section 3 presents extensive details of the results that are obtained subsequently followed by a discussion. Section 4 presents the conclusion, the proposed recommendations and the future direction of the study while Section 5 and 6 contained the acknowledgment and reference sections respectively.

II. PROPOSED DESIGNS AND EXPERIMENT (DATA COLLECTIONS)

Threatware is exclusively built to be executed in open social networks (OSN) and Facebook social platform. Facebook as a social network platform is selected to collect the initial results based on two reasons. First, the presence of a vast amount of data, which is regularly shared with many social media users online. For instance, Facebook is currently registered with more than 500 million active users out of which 60 percent regularly log in and share sensitive information daily. A constant increase in sensitive data offers the threatware an opportunity to un unmaliciously spread using the network to influence control over user-generated content. The second reason is considered more of a benefit in terms of the underlying variations in the policy adopted by OSN and Facebook social platform. In OSN, a third-party agent is permitted to examine the user's data as long as all the parties involved have provided consent and further set up the application [13]. In other words, querying of associate data selected from friends of user A is only possible if user A has initially installed the threatware in the OSN. This is opposed to the use of the Facebook social network, which is not possible to implement this constraint. If a user A could set up the threatware in a Facebook social platform, then it would be conceivable to query the data related to user A’s associates. The variation between OSN and Facebook social platform permits the collection of data and the subsequent examination of users‘ associate information who can set up the threatware. In this study, the threatware was initially built to quantify privacy risks and security threats associated with third-party applications.

Each research participant in the study is requested to provide solutions to a set of inquiries. The participants were provided with privacy and security scores prior to and after they had completed the sets of questions. The was intended to identify the participants‘ perception when exposed to various privacy and security risk.

2.1.1 Inference detection

The identified problem was initially conceptualized as follows. A user T was assumed as the inference target who interacted with direct friends F grouped as t. The inferred problem is provided with the users‘ attributes in F, which is linked to the attributes of t.

2.1.2. Inference calculation

This identified problem epitomizes a set of tangible problems drawn from the real SNS. For instance, the privacy and security consciousness of a user t restricts many private attributes to group-level access. On the other hand, a non-group member could only estimate values associated with group-level attributed to user t's associates. Alternatively, the privacy and security of untrustworthy user who has set up the software tool can be granted access to all attributes emptying particular attributes.

2.1.3. Disambiguation

Several challenges are posed the simplified algorithm illustrated the previous sections. This mainly revolves are the need to establish if any two attributes are equivalent when conceptualized values are symbolized differently. For instance, variables such as "UPM Serdang", "Selangor", and "UPM" are considered as variants within the Universiti Putra Malaysia. Commonly recognized as data disambiguation aspect, it has been associated with both structured and unstructured series of text. To overcome this aspect, the paper adopted various approaches such as the formulation of common differences among universities, political parties, degrees, and employers.

2.1.4. Verification.

The subsequent metrics were employed to measure power in the simplified inference algorithm. This included the inferred attribute which was composed of the threatware. However, the threatware cannot easily infer the attributes related to the number of friends and share common attributes that are below the threshold.

2.1.5. Problem definition

The inferred problem is conceptualized as follows. The study represents user t's using a series of rows f_v; f(type; value; weight)g). In this case, f_v assumes that the values to the associates by the user t. This representation is considered quite beneficial as this permits optimization of the outcomes related to associates with higher social value as indicated in Table 1

III. RESULTS AND DISCUSSION

The outcome from a survey of the participants is presented in Table 1.

Type	Value	Weight
Age	27	1
Employer	Google	0.8
Universiti	Universiti	1
Relationship Status	Single	1

Table 1: Illustration of attributes of an associate.

Examination of the results indicated that a user assigns a large social value to friends within the family social circle as compared to colleagues. The second tuple corresponds to the attributes related to the user's associate. Each attribute is represented using a set of triple values which include the university, age, and zip code. On a similar note, the value within the context of the triple corresponds to the real values in their respective attributes such as UPM Serdang, 25, 95812. The term weight accepts values from zero to one in line with the confidence interval of the disambiguation process. For instance, the disambiguation process could assign a value of 0.8 to the attribute UPM and a value of one to the attribute UPM Serdang. Based on the inferred algorithm, the weight can be established by computing the occurrence of the attribute values. If UPM attribute represents the university of an associate while UPM Serdang attribute is for a different associate, the weight term can be computed as 0:8 + 1:0 = 1:8 concerning the occurrence of the canonical attribute value as indicated in Table 1.

Table 2 Users‘ responses to Privacy and Security risks in SNS

Questions	Options	Results
To what extent are you familiar with Facebook’s policy on privacy and security concerning third-party applications?	Not Familiar Slightly Familiar Very Familiar	55.3% 51.4% 15.3%
How would rate Facebook setting that is used for privacy and security that protect the information in the user's profile	1,2,3,4,5	3.057
Have you ever utilized any of the privacy and security mechanisms that have been offered by Facebook?	Yes, No	0 %, 100%
From 1 to five, how would you rate the privacy settings related to profile information?	1,2,3,4,5	1.047
Given the risks posed SNS, will you change any of your privacy and security settings?	Yes, No	64.7% 35.3%

Table 2: Reactions to Privacy and Security Threat

	All Users	Men	Women	Married	Not Married	<25	25
Totals	89	47	24	24	40	25	24
Total Friends Contact	12523	6201	5133	2394	6153	5049	2750
Average Friends	134	131	183	99	153	201	114

Table 3: The aggregate and average of the number of associates

	All Users	Men	Women	Married	Not Married	< 25	25
Total people	89	47	24	24	40	25	24
Total social contacts	12,523	6,201	5,133	2,394	6,153	5,049	2,75 0
Average social contacts	134	131	183	99	153	201	114
Total attributes inferred	1,673	933	508	472	726	515	436
Total verifiable inferences	918	508	280	265	402	283	250
Total attributes correctly inferred	546	329	157	141	238	182	131
Percent correctly inferred	59.5	64.8	56.1	53.2	59.2	64.3	52.4

Table 4: Total Inferred attributes

IV. FUTURE WORK AND CONCLUSION

Initially, the paper intended to measure privacy and security risks posed to social media users when using SNS to offer appropriate solutions that can minimize risks. Many social media users have significantly contributed to an increase in the amount of personal data that builds their social graphs. This, in turn, has exposed users to serious consequences unintentionally. Additionally, many users are not aware of the underlying privacy and security risks posed by the SNS.

Using quantitative approaches, the data collected from the participants demonstrated a large bias for users with a huge number of associates. For instance, the participants who had more than 500 active friends needed the removal of a larger number of associates as compared to those users who had less.

It was noted from the study that current releases of the threatware have been able to estimate privacy and security risk posed to social networking users from the perspective of a single threat model using Facebook. Through future releases, this paper adds more threat that can present a holistic evaluation of privacy and security risk in SNS. The paper also compared the implementation of the latest release of the software tool in OSN and facebook social network. This was based on the use of variants that were operating in different networks, providing the ability to compare and contrast privacy and security in each SNS. Subsequently, users were provided with scores that they could use to measure their perception of privacy and security risks.

The threatware was able to portray the loss of data in SNS as well as offer a means of reducing the risks posed to users. Using the current release of the threatware, the results indicated that 58.5 percent of the users‘ attributes were associated with their social contacts. Additionally, the results indicated that different demographics of the users were inferred with a probability of more than 50 percent in most cases. Furthermore, in examining privacy and security risks, the study provided users with appropriate user actions which could assist them to mitigate the risks in SNS. Even though the study relied on small sample size, the outcome is encouraging and could be used as a basis for future research. As a long term strategy, the study intends to develop a system which can effectively measure multiple threat models as well as minimize privacy and security risks.

V. ACKNOWLEDGMENT

We will would like to express appreciation for the support of the sponsors (Geran Putra)[Pusat Kos Number :9596200].

6. REFERENCES

[1] B. M. Rubin. 2018. Social Networking Sites View By Admission Officers Online. Online Source http:// archives.chicagotribune.com/2018/sep/20/local/chi-facebook-college-20-sep2018.

[2] Du. W. 2007. Job Candidates Getting Tripped Up by Facebook. Msnbc.com,August 14. Online Source http://www.msnbc.msb.com/id/20202935

[3] Facebook statistics. [Online].Available://www.facebook.com/press/info.php?statistics (2017).

[4] Korolova, A., Motwani, R., Nabar, S. U., & Xu, Y. 2008. Link privacy in social networks. In *Proceedings of the 17th ACM conference on Information and knowledge management* (pp. 289-298). ACM.

[5] Lucas, M. M., & Borisov, N. 2008. Fly-by-night: mitigating the privacy risks of social networking. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society* (pp. 1-8). ACM.