Privacy Threat Analysis of Mobile Social Network Data Publishing

Jemal H. Abawajy[1(✉)], Mohd Izuan Hafez Ninggal[2], Zaher Al Aghbari[3], Abdul Basit Darem[4], and Asma Alhashmi[4]

[1] School of Information Technology, Deakin University, Victoria, Australia
jemal@deakin.edu.au
[2] Department of Computer Science, Universiti Putra Malaysia, Putrajaya, Malaysia
mohdizuan@upm.edu.my
[3] College of Sciences, University of Sharjah, Sharjah, UAE
zaher@sharjah.ac.ae
[4] Department of Computer Science, University of Mysore, Mysore, India
basit.darem@yahoo.com

Abstract. With mobile phones becoming integral part of modern life, the popularity of mobile social networking has tremendously increased over the past few years, bringing with it many benefits but also new trepidations. In particular, privacy issues in mobile social networking has recently become a significant concern. In this paper we present our study on the privacy vulnerability of the mobile social network data publication with emphases on a re-identification and disclosure attacks. We present a new technique for uniquely identifying a targeted individual in the anonymized social network graph and empirically demonstrate the capability of the proposed approach using a very large social network datasets. The results show that the proposed approach can uniquely re-identify a target on anonymized social network data with high success rate.

Keywords: Mobile social network · Social network data publication
Privacy attack · Re-identification attacks · Disclosure attacks

1 Introduction

With hundreds of millions of avid users worldwide, social networking platforms such as Facebook and Twitter have become part and parcel of modern life. Nowadays social networks are largely used by mobile users [1]. Therefore, mobile social networking has become an indispensable source of information and communication medium for people world over. Mobile social networking provides anytime and anywhere proximity-based platform for mobile users to be connected and instantly interact with each other based on mutual interests and backgrounds. The routinization of mobile social networks has radically transformed the way people communicate, socialise and share information.

As mobile phones become indispensable in society, mobile social networks have evolved dramatically over the last few years. The growing integration of mobile social networks with other mobile services such as location-based services have significantly

X. Lin et al. (Eds.): SecureComm 2017 Workshops, LNICST 239, pp. 60–68, 2018.
https://doi.org/10.1007/978-3-319-78816-6_5

increased the amount of user information being generated and collected by the service providers. Unfortunately, mobile social networks may occasionally leak sensitive information [1] and thus privacy concerns has become a fundamental issue [2]. For example, the location information of mobile social network users can be used to track their whereabouts and it can also be disclosed to external service providers with dire consequences. Therefore, with a growing mobile social network platform users, privacy preservation of social network data has taken a centre stage in both industry and academic fields. Although mobile social network privacy has gained tremendous momentum following the recent widespread drive towards coupling mobile social network with other mobile services such as location-based services, much of the exiting work focuses on protecting the privacy of user trajectory (i.e., the protection of the location movement of a user) [3], location information privacy preservation (i.e., securing user's position as well as the time they were there) and profile matching aspects of mobile social network [5].

In this paper we address the privacy issues associated with mobile social network data publication. Although there is a wide variety of mobile social network data use cases in areas such as business, health, science and security, mobile social network user posts potentially reveal much sensitive information about them [1]. However, there is little research regarding the security and privacy concerns associated with mobile social network data collected, collated and published by service providers to enable social network data analysis. As the publication of social network data reasonably threatens user privacy, the mobile social network service providers face fundamental challenges in how to release the data they collect to the interested third party without violating the confidentiality of social networks users personal information. Currently, a variety of anonymisation techniques are used to protect the privacy of individuals in mobile social network data publishing [4].

In this paper we present our work on the privacy vulnerability of the mobile social network data publication with emphases on a re-identification and disclosure attacks. We present a new technique for uniquely identifying a targeted individual in the anonymized social network graph. The proposed approach specifically exploits neighbourhood structures of the online social networks. As friend relationships information are major privacy concerns for mobile online social networks users [7], the proposed approach specifically explores neighbourhood structures of online social networks to breach privacy of the mobile social network users. Our work complements previous work on the privacy preserving social network data publishing [9] and privacy threat analysis of social network data [12] by focusing on privacy vulnerability analysis of mobile social network data. We also focus on specific aspect of attack vector analysis namely the friendship information as this information is considered to be a serious privacy concerns for mobile online social networks users [7]. The capability of the proposed approach is empirically evaluated using a very large social network dataset. The results show that the proposed approach can uniquely re-identify a target on anonymized social network data.

The rest of the paper is structured as follows. In Sect. 2, the models used in the paper are discussed. The proposed attack and its analysis are discussed in Sects. 3 and 4 respectively. The conclusion is given in Sect. 5.

2 Privacy Threat Analysis Framework

Figure 1 shows the online mobile social network (MSN) threat analysis framework with the key actors that include MSN data source (i.e., mobile social media users), MSN data gatherers (i.e., mobile social media service provider), and MSN data explorers (i.e., third party data analysts such as researchers and adversaries).

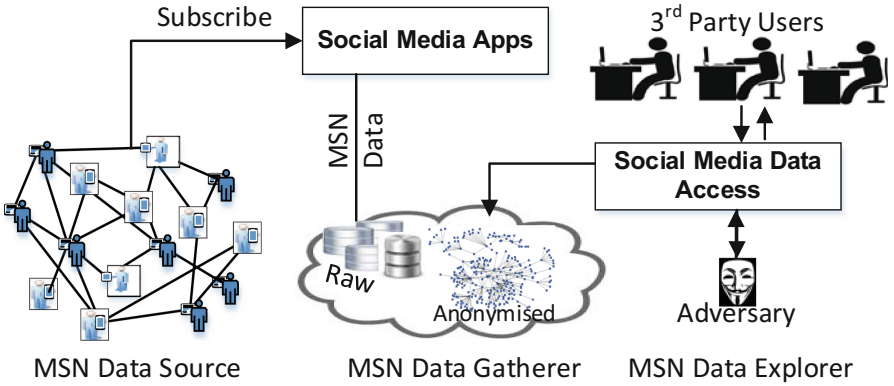

Fig. 1. High level threat analysis framework.

2.1 Mobile Social Networks Data

With the ubiquity of mobile social networks, users of the social network share terabytes of information. The mobile social network users use the social media services primarily to stay connected and interact with family members and friends. They also use the social media to find out the latest information of interest as well as share and contribute to what matters to them using built-in email or instant messaging [2]. The growing integration of mobile social networks with other services such as location-based services have significantly increased the amount of user generated information. As the result, a tremendous amount of user-generated data is collected by social network service providers. In this paper, we use an undirected and unweighted graph $G(V, E)$ to model a social network data, where $V = \{v_1, v_2, \ldots, v_n\}$ is a set of n vertices representing mobile social network users while the social links between the users is captured with a set of edges $E \subseteq V \times V$.

The third party customers have access to the published data for a variety of purposes. Although the user-generated data may include sensitive information such as user shopping habits, the social media data offers many possibilities for data analysis and business intelligence. The information is valuable for third party users such as researchers, business and government agencies to better understand interesting phenomena such as sociological and behavioural aspects of individuals or groups, measure social influence, identify the influential users in mobile social networks, and community structure detection [2]. However, as the collected data often contains sensitive information, network operators may release anonymized and sanitized versions of the complete social network

graph or a subgraph to the third party users such as advertisers, marketers, sociologists, epidemiologists, and healthcare professionals.

*Definition 1 (***Anonymized Graph):** *Let* $G(V, E)$ *be the original social network dataset graph. The graph* $\bar{G}(\bar{V}, \bar{E})$ *is an anonymized version of the original social network graph* $G(V, E)$.

In this paper, we assume that the social network data graph $G(V, E)$ is sanitized into $\bar{G}(\bar{V}, \bar{E})$ before publishing using k-anonymization mechanism with $k = 2$.

2.2 Adversary

An adversary is assumed to have access to the published social networks data. However, unlike the third party consumers, the intent of an adversary is to re-identify certain users in the published social network data. Specifically, an adversary is interested in deriving private information such as the identity of an individual or an attribute value from the anonymized social network graph. The outcome of structural attack depends on the background knowledge that an adversary has. Although existing research with high percentage of successful re-identification commonly assume that the adversary knows large set of structural information regarding the target vertex in the anonymized social network graph, we assume that the adversary knows basic information which is friends and friend of friends.

3 Mobile Social Network Data Vulnerability Analysis

In this section, we examine a class of attack that exploits the friendship information as this information is considered to be a serious privacy concerns for mobile online social networks users [7]. We will first define some background information needed to carry out the attack.

*Definition 2 (***Privacy breach):** *Given an anonymized social network data graph* $\bar{G}(\bar{V}, \bar{E})$, *a* privacy breach is said to have taken place when information deemed private and sensitive in the graph is disclosed to unauthorized individuals.

Mobile social network data often contains sensitive information. This data is normally provided to the third party users such as advertisers, marketers, sociologists, epidemiologists, and healthcare researchers. Normally, mobile social network users have strong believe that the mobile social network service providers keep their private information protected [4]. To ensure the privacy of the social network users, the service providers usually anonymize the data prior to publishing it for use by the third party consumers. However, maintaining the privacy of the online mobile social networks users' in published data is an increasingly important challenge facing social network operators [9, 12].

Generally, attacks in this class exploit the neighbourhood structure of a pair of connected vertices in mobile social network. Specifically, the adversary is assumed to have knowledge of neighbourhood structure of a pair of connected vertices as the background knowledge and use this knowledge to carry out the re-identification of targeted

victims in anonymized mobile social network data that has been released by the social network service providers for consumption by interested third party entities.

3.1 Re-identification Attack

We know explain the procedure for the proposed re-identification attack. Let $G(V, E)$ be the social network data graph and $T \in V$ and $u \in V$ be adjacent vertices in G such that $T \neq u$. Let us assume that $T \in V$ represents the target vertex. The aim of the adversary is to re-identify target vertex (i.e., $T \in V$ from the anonymized mobile social network graph by exploiting the friendship (degree) and the neighbor information of vertex $\bar{v} \in \bar{V}$ and $\bar{u} \in \bar{V}$ where $\bar{u}$ is an adjacent vertex of a vertex $\bar{v}$ such that $\bar{v} \neq \bar{u}$. To achieve this goal, the adversary performs the following steps:

(a) Request the anonymised graph data for a vertex with similar node neighborhood information as the target vertex $T \in V$. Assume the query returns a set of vertices $\mathcal{R} \subset V$ that matches the query.
(b) Refine $\mathcal{R}$ further by comparing the link structure among every neighbours of vertices in $\mathcal{R}$. Let the output of this step be $\mathcal{D}$.
(c) Utilize the neighbourhood information of vertex u to determine vertex T in $\mathcal{D}$.

Let us explain the above procedure in detail. When the adversary queries the anonymized graph with neighborhood information as the target vertex $T \in V$, it is assumed that the adversary receives a set of matching vertices $\mathcal{R} \subset V$. It is important to note that the fewer the number of returned vertices the higher the probability that the target victim $T \in V$ could be positively and accurately re-identified. The next step is to further refine the output from the previous step. In order to improve the accuracy of the re-identification of the target vertex, the adversary then compares the link structure among every neighbours of the nodes in $\mathcal{R}$ using his background knowledge. This step is expected to further refine the original query result and produce the set of matching vertices $\mathcal{D}$. Assuming that $\mathcal{D} > 1$, the adversary then uses the background knowledge regarding the neighbourhood information of u to re-identify T in $\mathcal{D}$. The target victim could be definitely re-identified if and only if the cardinality of matching vertices is 1.

We now illustrate the vulnerability anonymized graph $\bar{G}(\bar{V}, \bar{E})$ to the procedure described above. For this we use a sample of an anonymized social network graph shown in Fig. 2. The original mobile social network data is anonymised using the k-anonymity method. Suppose we want to identify 'Ziad' in the anonymized graph which is represented by vertex 4. Note that the anonymization has converted the name of the target 'Ziad' into a number as shown in vertex 4.

In the proposed approach, the adversary exploits the friendship information of vertex $\bar{v} \in \bar{V}$ and $\bar{u} \in \bar{V}$ targeting to identify t in G where $\bar{u}$ is an adjacent vertex of a vertex $\bar{v}$ such that $\bar{v} \neq \bar{u}$. In the case of Fig. 2, when the adversary queries the graph for a vertex with 4 friends, the query matches $R = \{3, 4, 5, 6\}$ vertices in the graph. By just using the friendship information alone, the adversaries only can identify 'Ziad' with probability ¼. The adversary further refines the query using his background knowledge. Specifically, the adversary knows that of the 4 users connected to the target vertex, two of them are also connected to each other. Further, the adversary also knows that one of the neighbours is

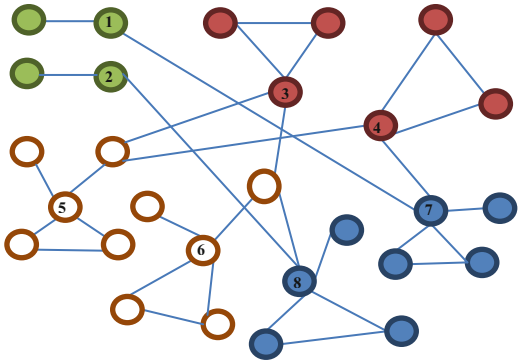

Fig. 2. A sample of anonymized mobile social network graph

connected to five users where two of them known each other. Therefore, the adversary uniquely re-identified 'Ziad' from the anonymized graph as a vertex 4.

4 Performance Analysis

In order to analyses the proposed approach's capability in terms of success rate regarding target re-identification in anonymized social network graph, we performed experimental analysis using real datasets. In this section, we analyses the performance of the proposed attack and compare it with two baseline approaches [9, 11].

4.1 Experimental Setup

We carried out the experiment using MATLAB on Pentium Dual-Core 2.50 GHz machine with 3 GB of RAM running with Windows 7 Enterprise. We used two different datasets (i.e., PolBooks, and Small-World):

- The PolBooks dataset is a network of books sold by an online store where the edges between books represent the purchase frequency of the same buyers.
- The Small-World dataset is a type of graph in which most vertices can be reached from every other vertex by a small number of hops.

The same datasets have been used in previous studies [4, 6, 8].

4.2 Result Analysis

In this section, we discuss the performance results of the proposed approach as compared to the baseline approaches. In the experiments, we used accuracy rate as the performance metric which is defined as a re-identification rate of the three approaches. The percentage represents the amount of vertex that is the dataset that are exposed to re-identification attack using the three types of graph structural information. The graph in Fig. 3 compares

the accuracy rate as a function of the various datasets. Note that the three approaches use different types of social network data structural information to re-identify the target.

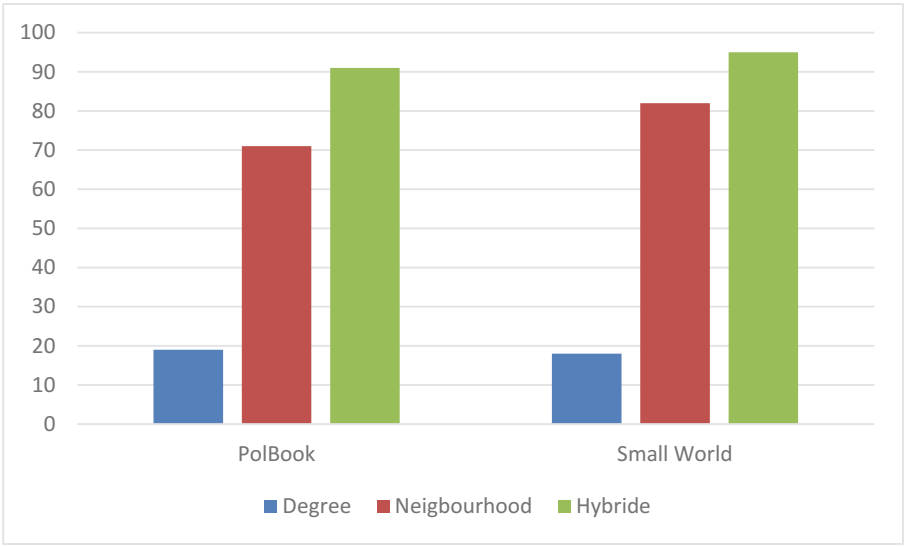

Fig. 3. The re-identification rate comparison graph

The results of the graph shown in Fig. 3 attests to the fact that the re-identification rate of the proposed approach is much higher than the baseline approaches. We note that the result shown in Fig. 3 includes only unique matching vertices based on the specific structural queries performed on the anonymized datasets. This results presented in Fig. 3 only shows the rate of vertices that definitely re-identified. From the graph shown in Fig. 3, we can see that the approach proposed in [9] has 20–30% success rate of definitely re-identifying targets in the anonymized graph datasets. In contrast, the approach proposed in [12] has higher re-deification rate as compared to the approach proposed in [9]. The experiment result shows that the approach proposed in [12] can definitely re-identified in excess of 60% of the social network users from the anonymised datasets doubling the rate of re-identification of the approach proposed in [8]. The proposed approach outperforms substantially both baseline approaches. The proposed approach can definitely re-identified in excess of 89% of the social network users from the anonymised datasets. The reason for the performance differences of the three approaches can be attributed to the structural background knowledge used by the adversary. Undeniably, the 20–30% re-identification rate is already quite in terms of the number of users who are at risk using limited background knowledge. With additional neighbourhood structural information, the approach proposed in [12] substantially increased the risk of re-identification rate to above 60%. The approach we proposed exploits both information proposed in [9, 12] and further refines them to zoom on the targeted vertices in the anonymized graph dataset. Thus combining known information and refining them can be lethal in attacking the privacy of the social network users.

5 Conclusion

There is no doubt that much of the data collected and collated by the social media service providers could assist groups working for the public interest such as sociologists and epidemiologists with new insights and possibilities for action. However, the collected data often contains sensitive information and thus must be made available to external interested parties in a responsible manner. Currently, social network operators release anonymized and sanitized versions of the complete social network graph for use by the third party users. Unfortunately, the approaches used by the social network platform providers to anonymise the data is insufficient to protect the privacy of the individuals as demonstrated in this work. In this paper we investigated the privacy vulnerability of the anonymised social network data with emphases on a re-identification and disclosure attacks. We presented three different approaches that use different background knowledge to uniquely identify a target in the anonymised social network graphs. We have shown empirically that using a variety of structural information that are readily available, the adversary can successfully re-identify targeted victim with high accuracy. Therefore, publishing social network data still raises serious concerns for individual privacy. In future work, we plan to develop privacy preserving mechanisms to safeguard the anonymised social network data publication is not vulnerable to a wide variety of re-identification and disclosure attacks.

Acknowledgement. The help of Maliha Omar is greatly appreciated. Without her support this paper will not come to its present state.

References

1. Teles, A.S., da Silva e Silva, F.J., Endler, M.: Situation-based privacy autonomous management for mobile social networks. Comput. Commun. **107**, 75–92 (2017)
2. Abawajy, J.H., Ninggal, M.I.H., Herawan, T.: Privacy preserving social network data publication. IEEE Commun. Surv. Tutor. **18**(3), 1974–1997
3. Zhang, S., Wang, G., Liu, Q., Abawajy, J.H.: A trajectory privacy-preserving scheme based on query exchange in mobile social networks. Soft Comput. 1–13 (2016)
4. Ninggal, M.I.H., Abawajy, J.H.: Utility-aware social network graph anonymization. J. Netw. Comput. Appl. **56**, 137–148 (2015)
5. Luo, E., Liu, Q., Abawajy, J.H., Wang, G.: Privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks. Future Gener. Comput. Syst. **68**, 222–233 (2017)
6. Abawajy, J.H., Ninggal, M.I.H., Herawan, T.: Vertex re-identification attack using neighbourhood-pair properties. Concurr. Comput. Pract. Exp. **28**(10), 2906–2919 (2016)
7. Xiao, X., Chen, C., Sangaiah, A.K., Hu, G., Ye, R., Jiang, Y.: CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks. Future Gener. Comput. Syst. (2017). https://doi.org/10.1016/j.future.2017.01.035
8. Ninggal, M.I.H., Abawajy, J.H.: Preserving utility in social network graph anonymization. In: The Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2013), Melbourne, Australia, 16–18 July 2013, pp. 226–232. IEEE Computer Society (2013). ISBN 978-0-7695-5022-0

9. Liu, K., Terzi, E.: Towards identity anonymization on graphs. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, pp. 93–106. Vancouver, Canada (2008)
10. Ninggal, M.I.H., Abawajy, J.H.: Attack vector analysis and privacy-preserving social network data publishing. In: The Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011), Changsha, China, 16–18 November 2011, pp. 847-852. IEEE Computer Society (2013). ISBN 978-1-4577-2135-9
11. Zhou, B., Pei, J.: The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowl. Inf. Syst. **28**(1), 47–77 (2011)
12. Ninggal, M.I.H., Abawajy, J.: Privacy threat analysis of social network data. In: Xiang, Y., Cuzzocrea, A., Hobbs, M., Zhou, W. (eds.) ICA3PP 2011. LNCS, vol. 7017, pp. 165–174. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24669-2_16