Retrieving Hidden Friends A Collusion Privacy Attack Against Online Friend Search Engine

Addala saibabu , Dr.I.R.Krishnam Raju , Sri.V.Bhaskara Murthy
MCA Student, Professor, Associate Professor
DEPT OF MCA
B.V.Raju College, Bhimavaram

ABSTRACT

Online Social Networks (OSNs) are providing a variety of applications for human users to interact with families, friends and even strangers. One of such applications, friend search engine, allows the general public to query individual users' friend lists and has been gaining popularity recently. However, without proper design, this application may mistakenly disclose users' private relationship information. Our previous work has proposed a privacy preservation solution that can effectively boost OSNs' sociability while protecting users' friendship privacy against attacks launched by individual malicious requestors. In this paper, we propose an advanced collusion attack, where a victim user's friendship privacy can be compromised through a series of carefully designed queries coordinately launched by multiple malicious requstors. The effect of the proposed collusion attack is validated through synthetic and real-world social network data sets. The in-depth research on the advanced collusion attacks will help us design a more robust and securer friend search engine on OSNs in the near future.

I.INTRODUCTION

Online social networks (OSNs) have become very popular in recent years, such as Facebook and Twitter, which have been part of many people's daily life. The OSNs provide different applications for people to share their information and interact with each other. One of the most popular applications is the friend search engine, which allows users to query friend lists of other users. To increase their sociability and attract more users, OSNs tend to release users' friends as many as possible, as it is believed that the larger number of common friends are displayed, the more likely the requestor and the queried user would connect later.

However, this search engine may expose more friendship information than what a queried user is willing to share, which is considered as a privacy breach. A few researchers have observed such an issue by randomly crawling an OSN through the friend search API [1]. Also, they concluded that without appropriate defenses, one could discover all users' friendships in the OSN without using many queries [2], [3]. If such a privacy breach is not well dealt with, the OSN users may feel panic and hesitate to continue using the OSNs.

In our preliminary work, we designed a privacy-aware friend display scheme in [4], which cannot only successfully preserve users' friendship privacy but also boost the sociability of the OSN. This scheme is one of the most advanced researches on preserving user privacy for friend search engines, which has been verified to successfully prevent attacks from being launched by independent attackers. However, collusion attacks, where multiple malicious requestors share their knowledge and coordinately launch queries, may make the defense scheme ineffective. In this paper, we particularly focus on the design of collusion attacks against users' friendship privacy in

OSNs. The major contributions of this paper are listed as follows.

First, to the best of our knowledge, we are the first researchers studying such advanced privacy attacks as collusion attacks against friend search engine in OSNs. Second, in-depth analysis has been provided on querying a small scale complete graph as well as a general network in various scenarios, which well explains the fundamental reasons of why and how the proposed attack is designed.

In particular, we observe the defense scheme's [4] asymmetric disclosure of users' symmetric friendships. By taking advantage of it, we design an advanced collusion attack, in which multiple malicious requestors closely coordinate with one another to launch their queries on different but related users in well designed orders. The design logic can be generally applied to launch attacks against any friendship privacy preserving solutions that disclose the symmetric friendship in an asymmetric way. Third, the proposed collusion attack is designed to carefully select which users to query, which can significantly reduce the total amount of query effort.

Fourth, to evaluate the effectiveness of our proposed attack strategy, we implement and run it on one synthetic data set and three large scale real-world data sets. Experiment results demonstrate that the proposed attack strategy works efficiently and effectively on large scale data sets. By comparing the proposed collusion attack with a naive direct attack, we find that our strategy performs better in terms of both the success rate and the required number of malicious requestors to compromise a user's friendship privacy. Last but not least, our research on this advanced collusion attack helps us better understand the attack design and shed lights on the design of a securer privacy preserving friend search engine in the future.

II.EXISTING SYSTEM

- Along with defense research, privacy attacks against OSN friendship privacy are also extensively studied in the scientific community. Specifically, such research can be classified into two categories as attacks launched by (1) independent attackers or (2) colluded attackers. There are ample examples of independent attacks. A neighborhood attack defined in [20] studies that an individual attacker with some knowledge of the neighbors of a target node and their relationship information is able to identify the target node from a social network graph where user identifiers are removed. Additionally, a few researchers have observed that by randomly crawling an OSN through the friend search API [1], an individual attacker can glean all friendship connections of users in the OSN without many queries.
- Collusion attacks can be defined as attacks that involve multiple malicious entities aiming at obtaining greater gain than what the entities benefit from individually launched attacks. The multiple entities can be fake accounts created by a single attacker or by different real attackers. Compared to individual attacks, collusion attacks can use more complicated attack strategies and often exploit system vulnerabilities that cannot be discovered by individual attacks.
- There are a few simple collusion attacks researched in the literature. For example, as mentioned in [25], some revoked users can collude with legitimate users to continue accessing the private data. However, less attention has been paid to designing sophisticated collusion attack strategies where

multiple malicious users conduct their behaviors in a highly coordinated way and dynamically adjust their behaviors according to systems' feedback on other colluders' behaviors. To our best knowledge, there is very limited research on designing comprehensive collusion attacks against user friendship privacy in OSNs.

Disadvantages

- There is no filtering system to find Privacy Attack.
- Less security due No URL Based attack Detection.

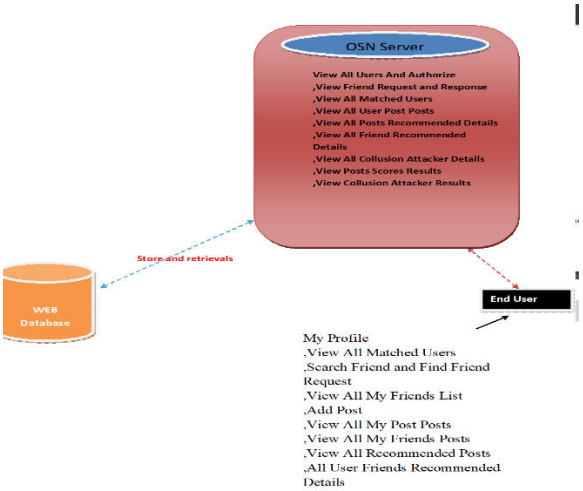
III. PROPOSED SYSTEM

- In the proposed system, First, to the best of our knowledge, the system is the first researchers studying such advanced privacy attacks as collusion attacks against friend search engine in OSNs.
- Second, in-depth analysis has been provided on querying a small scale complete graph as well as a general network in various scenarios, which well explains the fundamental reasons of why and how the proposed attack is designed. In particular, we observe the defense scheme's [4] asymmetric disclosure of users' symmetric friendships. By taking advantage of it, we design an advanced collusion attack, in which multiple malicious requestors closely coordinate with one another to launch their queries on different but related users in well designed orders. The design logic can be generally applied to launch attacks against any friendship privacy preserving solutions that disclose the symmetric friendship in an asymmetric way.
- Third, the proposed collusion attack is designed to carefully select which users to query, which can significantly reduce the total amount of query effort.
- Fourth, to evaluate the effectiveness of our proposed attack strategy, we implement and run it on one synthetic data set and three large scale real-world data sets. Experiment results demonstrate that the proposed attack strategy works efficiently and effectively on large scale data sets. By comparing the proposed collusion attack with a naive direct attack, we find that our strategy performs better in terms of both the success rate and the required number of malicious requestors to compromise a user's friendship privacy.

Advantages

- The system provides the flexibility for individual users to determine the number of friends, say k, to display in response to friend queries.
- Particularly focus on the design of collusion attacks against users' friendship privacy in OSNs.

IV.ARCHITECTURE DIAGRAM



V.IMPLEMENTATION

- **OSN Server**

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as View All Users And Authorize,View Friend Request and Response,View All Matched Users,View All User Post Posts,View All Posts Recommended Details,View All Friend Recommended Details,View All Collusion Attacker Details,View Posts Scores Results ,View Collusion Attacker Results

Friend Request & Response

In this module, the admin can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting.

Social Network Friends

In this module, the admin can see all the friends who are all belongs to the same site. The details such as, Request From, Requested user's site, Request To Name, Request To user's site.

All Recommended Posts

In this module, the admin can see all the posts which are shared among the friends in same and other network sites. The details such as post image, title, description, recommend by name and recommend to name.

- **User**

In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user can perform some operations like My Profile,View All Matched Users ,Search Friend and Find Friend Request,View All My Friends List,Add Post,View All My Post Posts,View All My Friends Posts ,View All Recommended Posts,All User Friends Recommended Details.

Searching Users

In this module, the user searches for users in Same Site and in Different Sites and sends friend requests to them. The user can search for users in other sites to make friends only if they have permission.

Adding Posts

In this module, the user adds posts details such as title, description and the image of the post. The post details such as title and description will be encrypted and stores into the database.

VI.CONCLUSION

In this paper, we have proposed an advanced collusion attack strategy where multiple attackers with very limited initial knowledge (i.e. only the victim node) can successfully penetrate the defense and violate victim node's privacy settings on friend search engine. In particular, we start this study with a simple and small social clique model, aiming to deeply understand users' friendship types and reveal the fundamental reasons why collusion attacks can be done successfully. Based on observations made from this model, we further propose to classify social network users into non-popular users and popular users; develop different attack strategies against them; and illustrate the attack effectiveness in a general social network through different scenarios. Experiment results show that our proposed collusion attack strategy has achieved high success rate by using limited number of malicious requestors.

Theoretically, this work has simplified the complex privacy attack problem as a small social clique model, classified users' friendship into three categories, and revealed the fundamental reason of the collusion attack's

success as the defense scheme's asymetric responses on the symmetric friendship. Furthermore, theoretical model analysis has been conducted on the success probability as well as the total number of malicious requestors needed for the proposed collusion attack when a random victim user is chosen. Technically, the observations made from this work also shed light on future design of advanced privacy preserving schemes. Specifically, OSNs may utilize the large-large friendship, so that one friendship can only be released in a symmetric way if both friends are on each other's top k lists. It leads to the intuitive idea as that if a node is not so influential, not releasing its friendship with its top influential friend could help protecting the privacy of both nodes. However, such symmetric design may significantly influence the OSNs' sociability as a node's most influential friends may not be displayed when the node itself is not that influential. In addition, as different nodes may set different k values, it is extremely challenging to always find the symmetric k friends to display for all the nodes. Consequently, advanced design is required to better balance friendship privacy and network sociability.

Practically, for OSNs, as people in reality often ignores that their privacy settings may significantly influence their friends' privacy, it is critical to educate people be aware of not only protecting their own information privacy but also be careful when release their friendship to third parties. In addition, as compromising a non-popular node is much easier than compromising a popular one, an individual node may enhance its privacy by making itself a popular node through connecting with more nodes, contributing more to the OSN, or setting an appropriate k value. Specifically, when the k value is too small, to make itself a popular node, the node has to be ranked in the top k lists of all its top k friends, which is very difficult. As the k value increases, it becomes easier for a node to be in the top k lists. However, a too large k value indicates that the node will release many friends anyway, which also hurts its privacy. Therefore, it could be helpful for an individual node to choose its k value based on its own situations.

REFERENCES

[1] "Friendlist api." [Online]. Available: https://developers.facebook.com/docs/reference/fql/friendlist

[2] J. Bonneau, J. Anderson, F. Stajano, and R. Anderson, "Eight friends are enough: social graph approximation via public listings," in Proceedings of ACM SNS'09, 2009, pp. 13–18.

[3] A. Yamada, T. H.-J. Kim, , and A. Perrig, "Exploiting privacy policy conflicts in online social networks," in Technical report, 2012.

[4] N. Li, "Privacy-aware display strategy in friend search," in Proceedings of IEEE International Conference on Communications (ICC), Communication and Information Systems Security Symposium, 2014, pp. 951–956.

[5] R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," International Journal of Human-Computer Interaction, vol. 31, no. 5, pp. 350–370, 2015.

[6] L. Guo, C. Zhang, and Y. Fang, "A trust-based privacy-preserving friend recommendation scheme for online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 413–427, 2015.

[7] Z. Feng, H. Tan, and H. Shen, “Relationship privacy protection for
mobile social network,” in Advanced Cloud and Big Data (CBD), 2016
International Conference on. IEEE, 2016, pp. 215–220.
[8] N. Li, N. Zhang, and S. Das, “Relationship privacy preservation in
publishing online social networks,” in Proceedings of the Third IEEE
International Conference on Social Computing (SocialCom’11), MIT,
Boston, US, 2011.
[9] B. Zhou and J. Pei, “Preserving privacy in social networks against
neighborhood attacks,” in Proceedings of the 24th IEEE International
Conference on Data Engineering(ICDE’08), 2008, pp. 506–515.
[10] J. Cheng, A. W. Fu, and J. Liu, “K-isomorphism: Privacy preservation
in network publication against structural attack,” in SIGMOD’10, 2010.