University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Master of Applied Science

of

JIAYI CHEN

BEng (Shangahi Jiao Tong University, 2015)

"Defending Against Inference Attack in Online Social Networks"

Department of Electrical and Computer Engineering

Tuesday, July 11, 2017
10:30 A.M.
Engineering Office Wing
Room 430

Supervisory Committee:
Dr. Lin Cai, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Alex Thomo, Department of Computer Engineering, UVic

Chair of Oral Examination:
Dr. Marjorie MacDonald, School of Nursing, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

The privacy issues in online social networks (OSNs) have been increasingly arousing the public awareness since it is possible for attackers to launch several kinds of attacks to obtain users' sensitive and private information by exploiting the massive data obtained from the networks. Even if users conceal their sensitive information, attackers can infer their secrets by studying the correlations among private and public information with background knowledge. To address these issues, the thesis focuses on the inference attack and its countermeasures.

First, we study how to launch the inference attack to profile OSN users via relationships and network characteristics. Due to both user privacy concerns and unformatted textual information, it is quite difficult to build a completely labeled social network directly. However, both social relations and network characteristics can help attribute inference to profile online social network users. We propose several attribute inference models based on these two factors and implement them with Naïve Bayes, Decision Tree and Logistic Regression. Also, to study network characteristics and evaluate the performance of our proposed models, we use a well-labeled Google employee social network extracted from Google+ to test the proposed models on inferring the social roles of Google employees. The experiment results demonstrate that the proposed models are effective in social role inference with Dyadic Label Model performing the best.

Second, we model the general inference attack and formulate the privacy-preserving data sharing problem to defend against the attack. The optimization problem is to maximize the users' self-disclosure utility while preserving their privacy. We propose two privacy-preserving social network data sharing methods to counter the inference attack. One is the efficient privacy-preserving disclosure algorithm (EPPD) targeting the high utility, and the other is to convert the original problem into a multi-dimensional knapsack problem (d-KP) using greedy heuristics with a low computational complexity. We use real-world social network datasets to evaluate the performance. From the results, the proposed methods achieve a better performance when compared with the existing ones.

Finally, we design a privacy protection authorization framework based on the OAuth 2.0 protocol. Many third-party services and applications have integrated the login services of popular Online Social Networks, such as Facebook and Google+, and acquired user information to enrich their services by requesting user's permission. However, due to the inference attack, it is still possible to infer users' secrets. Therefore, we embed our privacy-preserving data sharing algorithms in the implementation of OAuth 2.0 framework and propose RANPriv-OAuth2 to protect users' privacy from the inference attack.