Privacy-Preserved Network Data Publishing

Lei Chen

Hong Kong University of Science and Technology
leichen@cse.ust.hk

Nowadays, more and more people join multiple social networks on the Web, such as Facebook, Linkedin, and Livespace, to share their own information and at the same time to monitor or participate in different activities. Meanwhile, the information stored in the social networks are under high risk of attack by various malicious users, in other words, peoples privacy could be easily breached via some domain knowledge. Thus, as a service provider, such as Facebook and Linkedin, it is essential to protect users privacy and at the same time provide useful data. Simply removing all identifiable personal information (such as names and social security number) before releasing the data is insufficient. It is easy for an attacker to identify the target by performing different structural queries.

In this talk, I will briefly review the current work on protecting the privacy of published social networks including clustering-based approaches and graph editing methods. Then, I will present a recent work, called k-automorphism, to protect against multiple structural attacks, following by a framework which provides privacy preserving services based on the users personal privacy requests. In the end, I would like to highlight some future work related to this topic.

J. Xu et al. (Eds.): DASFAA Workshops 2011, LNCS 6637, p. 1, 2011.