Name: Esam Alzahrani

Date: 04/25/2012

"Conference and lecture review"

I had a great chance in this semester granted to me by my graduate program director, Ms.Nicole Sealey, to attend an international conference that is related to my field of study, which is computer engineering. International Conference in Data Engineering is a well-known conference among computer discipline community members, in which the most important and up to dated finding and information would be shared. So, I have decided to attend this conference for its an excellent reputation and quality. As a graduate student interested in computer security, I have focused on sessions and workshops that discussed computer security topics. One of them is "Privacy in Social Networks: How Risky is Your Social Graph?", which I will be reviewing in this paper.

Since it is a scientific conference, most audiences were professionals either faculty members, corporations' professionals, or graduate students. The session that I attended was held in room that can take about 50 to 60 attendants. We were approximately 40 individuals in that room. The authors of this paper were three persons, Cuneyt Gurcan Akcora, Barbara Carminati, Elena Ferrari, who are researchers in University of Insubria, Italy. They started by giving an introduction about what have been done to keep privacy level in Online Social Networks (OSNs) secure. But, they highlighted the lack that is of current privacy protection models particularly a risk that could be posed by their weaknesses. They also emphasized some users' attitudes that can lead to privacy violation such making relationship with unknown people whom a user has never met. Therefore, they proposed a risk measure to help users judging new friends and knowing how much they can trust them. They included several risk measure designs, the first one depends on evaluation approach, in which they evaluated users attitudes in different scenarios to measure users' judgments with strangers. Their another risk measure is motivated by social networks users statistics which can help to determine risk level of second level friends based on users prejudgments. Users can predict a risk level, but their risk learning algorithm

will give labels for strangers based on their level of risk. They applied their framework on Facebook environment and they claimed that they have an amazing results. They also stated that they are the first group that proposes framework to estimate the risk of OSNs' users.

In implementing phase, they explained dimensions that they considered to measure a risk. So, they relied on four dimensions, which are providing an appropriate and clear questions to users, considering all questions to be valid on social networks scenarios, classifying unlabeled users to label them precisely, and designing stopping criteria to gain a required accuracy. In their experiment, they applied their framework on Facebook. They also assigned 37 users form different countries in Europe and North America to tag strangers based on their prediction. It took them two months to collect and arrange collected data. They found that there were few strangers were tagged as risky by users. Compared to what their framework tagged and users tagged they found that 80% of results were matched[3].

The proposed framework in this paper is useful in terms of knowing who we can trust in OSNs. Even though, there is no guarantee this will be accurate, it still has reliability by considering old data and statistics. Actually, preventing users privacy relies on many factors by which privacy could be prevented. Users should be protected from companies that checked candidates profiles, hackers blackmailing Social Network Services (SNS) providers, insurances cutting benefits to customers[2]. If we want to consider friendship as the biggest threat for privacy on OSNs, the previous events users has nothing to do with it. A big concern for OSNs' users privacy protection is to prevent them from parties that are considered trusted such as commercial companies and sociologies [1]. “They obtain the data either by crawling the websites through the interfaces provided by the OSN owners, or by requesting to the OSN owners who routinely publish those data” [1]. In addition to that, studies show that the most challenging factor to preserve privacy is to hide users' identities, which is impossible [2]. For example, an adversary can obtained a user's information from different source like a blog, then an adversary can use this information to locate victim's social network profile.

Overall, this study is interesting and a good step toward privacy protection. However, it is too limited to specific factors and scenarios. For, example authors consider Facebook in their example and they emphasize the risk of friendship, but what about other OSNs that have different natures and scenarios such as Twitter. In Twitter, there are followers and your tweets cannot be hided anyone can gain access to your tweets and profiles. Therefore, the generalization that they made by proposing their framework to be valid for all OSNs applications weaken their proposed framework. I wished if they had limited their framework to Facebook environment, that would be more reliable in terms of effectiveness.

References:

[1] Na Li, Nan Zhang, Sajal K. Das. "Relationship Privacy Preservation in Publishing Online Social Networks". 2011. IEEE International Conference on Privacy, Security, Risk, and Trust.

[2] Leucio Antonio Cutillo, Refik Molva, Melek Onen. "Analysis of Privacy in Online Social Networks from the Graph Theory Perspective". 2011. IEEE Globecom.

[3] Cuneyt Gurcan Akcora, Barbara Carminati, Elena Ferrari. "Privacy in Social Networks: How Risky is Your Social Graph?". 2012. IEEE ICDE.