Social privacy score throhghugh vulnerability contagion process

Aghiles DJOUDI, Guy PUJOLLE
Sorbonne University
4 Place Jussieu, 75005 Paris, France
firstname.lastname@upmc.fr

***Abstract*—The exponential usage of messaging services for communication raises many questions in privacy fields. Privacy issues in such services strongly depend on the graph-theoretical properties of users' interactions representing the real friendships between users. One of the most important issues of privacy is that users may disclose information of other users beyond the scope of the interaction, without realizing that such information could be aggregated to reveal sensitive information. Determining vulnerable interactions from non-vulnerable ones is difficult due to the lack of awareness mechanisms.**

To address this problem, we analyze the topological relationships with the level of trust between users to notify each of them about their vulnerable social interactions. Particularly, we analyze the impact of trusting vulnerable friends in infecting other users' privacy concerns by modeling a new vulnerability contagion process. Simulation results show that over-trusting vulnerable users speeds the vulnerability diffusion process through the network. Furthermore, vulnerable users with high reputation level lead to a high convergence level of infection, this means that the vulnerability contagion process infects the biggest number of users when vulnerable users get a high level of trust from their interlocutors. This work contributes to the development of privacy awareness framework that can alert users of the potential private information leakages in their communications.

I. HGHG GFGF

II. Introduction

With increasing frequency, communication between citizens and institutions occurs via some type of e-mechanisms, such as websites, email, and social media. In particular, email platforms are widely being adopted because of their simplicity of use. Due to the social aspect of these mechanisms, users are continuously infected by their friends' privacy vulnerability. Users can take all the required measures to protect themselves from potential information leakage, but if their friends didn't respect the same measures, this indirectly harms their privacy concerns, especially when they grant a high-level of trust to them.

Currently, available solutions address the privacy issues of users by measuring their vulnerability toward active attackers in low layer protocols (e.g. HTTPS, SSL, PGP, IPsec, etc), or by suggesting new privacy policy settings of their applications. These works are efficient to protect users from external vulnerabilities, but they appear very weak to protect users from (legitimate) information leakage between messaging services users. Many other works [**liu˙framework˙2010**] address this problem by measuring the users privacy vulnerability individually without caring about the social context of the problem. Few works [1] [2] address this problem from a topological view of users' relationships during their social interactions. Our work is motivated by the potential of privacy awareness frameworks to help users being conscious about the trustworthiness of their social interactions.

Trust networks allow users to rate other users, they can put their level of trust in their interlocutors based on their own beliefs such as "Alice trust Bob as 0.8 in [0,1]" [3]. Trust statements can then be aggregated in a single trust network representing the relationships between users [3]. Trust metrics in our work are related to the relation strength between users such as the frequency of interactions, common interests, common friends, etc. Trust metrics can also be related to the relationship closeness such as family, friends, colleagues or just unknown. Based on such metrics and the topology of the interaction network, the system can suggest how much users are trustworthy based on different opinions of interlocutors, this suggestion represents their reputation.

Trust and reputation metrics are used in our work in order to study the relationship between them and users' privacy vulnerability. Reputation concept refers to the extent to which a user is trustworthy. This means that he plays a central role in preserving or revealing sensitive information of his interlocutors. Reputation system collects, distributes and aggregates feedback about participants past behavior to allow users decide whom to trust and with whom to exchange sensitive information, users could then decide to not interact with those who are vulnerable to preserve their own privacy.

Messaging services users often exchange messages with a high number of users without caring about the vulnerability of their social environment. In this paper, we deal with privacy issues by studying the impact of trust in preserving privacy.

The remainder of this paper is organized as follows. Section **??** elucidates summary of related works. In Section **??**, we propose our vulnerability contagion process to reveal the social vulnerability of users. Our experimentation with Enron dataset and our findings are presented in Section **??** and **??** respectively. Finally, conclusion and future works are drawn in Section **??**.

III.

*References

[1] Yongbo Zeng et al. “ Trust-Aware Privacy Evaluation in Online Social Networks ”. In: *Communications (ICC), 2014 IEEE International Conference On*. 00003. IEEE, 2014, pp. 932–938 (p. 1).

[2] Vidyalakshmi B.S., Raymond K. Wong, and Chi-Hung Chi. “ Privacy Preserving Information Dispersal in Social Networks Based on Disposition to Privacy ”. In: 00000. IEEE, Dec. 2015, pp. 372–377 (p. 1).

[3] Paolo Massa and Paolo Avesani. “ Trust-Aware Recommender Systems ”. In: *Proceedings of the 2007 ACM Conference on Recommender Systems*. RecSys ’07. 01500. New York, NY, USA: ACM, 2007, pp. 17–24 (p. 1).