Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 108C (2017) 28–37

Procedia Computer Science

International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland

Impact of Neighbors on the Privacy of Individuals in Online Social Networks

Livio Bioglio and Ruggero G. Pensa

University of Turin - Dept. of Computer Science, Turin, Italy
{livio.bioglio,ruggero.pensa}@unito.it

Abstract

The problem of user privacy enforcement in online social networks (OSN) cannot be ignored and, in recent years, Facebook and other providers have improved considerably their privacy protection tools. However, in OSN's the most powerful data protection "weapons" are the users themselves. The behavior of an individual acting in an OSN highly depends on her level of privacy attitude: an aware user tends not to share her private information, or the private information of her friends, while an unaware user could not recognize some information as private, and could share it without care to her contacts. In this paper, we experimentally study the role of the attitude on privacy of an individual and her friends on information propagation in social networks. We model information diffusion by means of an extension of the Susceptible-Infectious-Recovered (SIR) epidemic model that takes into account the privacy attitude of users. We employ this diffusion model in stochastic simulations on a synthetic social network, designed for miming the characteristics of the Facebook social graph.

Keywords: complex networks, modeling, information diffusion, privacy

1 Introduction

The problem of user privacy in the so-called "Big Data Era" cannot be ignored and many companies are realizing the necessity to consider it at every stage of their business. In practice, they have been turning to the principle of *Privacy by Design* [6] by integrating privacy requirements into their business model. Online social network (OSN) providers are embracing this model as well. In recent years, Facebook has improved considerably the privacy protection tools provided within its Web and mobile products, and periodically suggests its users to review their privacy settings using a simplified but still flexible interface. However, differently from other Web, mobile and IoT services where data protection mostly involves access control rules, data anonymization techniques and other centralized or decentralized precautions that are invisible to the users, in OSN's the most powerful data protection "weapons" are the users themselves. In fact, social media (e.g., Facebook, Instagram, Twitter) are essentially human-generated logs

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the International Conference on Computational Science
10.1016/j.procs.2017.05.030

that can be used to reconstruct life events and private facts of those users that carelessly disclose their personal information. As shown by the research project myPersonality [13] carried out at the University of Cambridge, by leveraging Facebook user's activity (such as "Likes" to posts or fan pages) it is possible to "guess" some very private traits of the user's personality. To alleviate this issue, social media usually provide advanced tools for controlling the privacy settings of the user's profile [22], but it has been shown that yet a large part of Facebook content is shared with the default privacy settings and exposed to more users than expected [15]. Moreover, even though OSN users can specify which of their contacts are allowed to see their notifications, they do not have any control on how these contacts will use their information: friends could spread the rumor through other social networks, blogs, websites, medias or simply with face-to-face communication.

The behavior of an individual in these situations highly depends on her level of privacy awareness: an aware user tends not to share her private information, or the private information of her friends, while an unaware user could not recognize some information as private, and could share it without care to her contacts, even to untrusted ones, putting her privacy or the privacy of her friends at risk. Users' privacy awareness then turns into the so-called "privacy attitude", i.e., the users' willingness to disclose their own personal data to other users, that can be measured by leveraging the way users customize their privacy settings in social networking platforms [14, 21].

A new question may arise now: how safe is the privacy of a social network user who is mostly surrounded by friends with a good privacy attitude? The question is not trivial, since the way most people set their privacy settings is based on the notion of closeness: close friends are usually allowed to see all user's updates, while acquaintances can only see "public" or less sensitive updates[1]. The common assumption is that closed friends are trusted ones and thus will not disclose friends' posts to other friends. In this paper, we model the effects of privacy attitude on information propagation in social networks with the aim of studying what happens to information diffused to friends with different levels of privacy awareness. We employ a model, proposed by us in [5] and inspired by the classic Susceptible-Infectious-Recovered (SIR) epidemic model [11], for representing privacy attitude of individuals by means of parametric values. By tuning the values of parameters, we model the attitude on privacy of single users, from more to less aware on privacy. Our objective is to investigate the role of privacy attitudes of the initial spreader, of her neighbors and of the whole population of the social network on the diffusion of information into a Facebook-like social network. We analyze, by means of stochastic simulations, the spreading of information in a Facebook-like network starting from a unique initial spreader. We assign to each user of the network a privacy class, representing its attitude on privacy: in order to study the role of privacy awareness of the whole population, we simulate information spreading on different assignment distributions of privacy classes of the nodes, from safer (where the majority of users has a high awareness on privacy) to unsafer ones (where the majority of users has a low level of attention on privacy issues). With the goal of studying the role of the neighborhood of a user in information diffusion, we set all the nodes directly linked with the initial spreader to the same privacy class, repeating the assignment for all privacy classes. Finally, we repeat the simulations choosing a node in every privacy class as initial diffuser to analyze the role of the privacy attitude of the initial spreader.

[1] Facebook, for instance, allows its users to distinguish between friends, close friends and acquaintances during any posting action.