Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 82 (2016) 20 – 27

Procedia Computer Science

Symposium on Data Mining Applications, SDMA2016, 30 March 2016, Riyadh, Saudi Arabia

Protecting online social networks profiles by hiding sensitive data attributes

Hatem AbdulKader[a], Emad ElAbd[b], Waleed Ead[c]*

[a,b]*Faculty of computers and information, Menoufia University, EGYPT*
[c] Faculty of computers and Information, Beni-suef University, EGYPT

Abstract

Online Social Networks (OSNs) have become a mainstream cultural phenomenon for millions of Internet users. More importantly, OSNs expose now information from multiple social spheres e.g. personal information or professional activity. We identify two stakeholders in online social networks: the OSN users and the OSN itself. On one hand, OSN users share an astonishing amount of information ranging from personal to professional. On the other hand, OSN services handle users' information and manage all users' activities in the network, being responsible for the correct functioning of its services and maintaining a profitable business model. Indirectly, this translates into ensuring that their users continue to happily use their services without becoming victims of malicious actions. We thus classify online social networks privacy and security issues into two categories of attacks on users and OSN. In this paper we propose a utility based association rule hiding algorithm for privacy preserving user profiles data against attacks from OSN users or even OSN applications. Experimental has been conducted on samples of real datasets. Experimental has been showed less attribute modification in the released user's profiles datasets.

Peer-review under responsibility of the Organizing Committee of SDMA2016

Keywords: online social networks; user's profiles; privacy preserving; profiles attacks.

1. Introduction

Online Social Networks (OSNs) have become a mainstream cultural phenomenon for millions of Internet users. Combining user-constructed profiles with communication mechanisms that enable users to be pseudo-permanently "in touch", OSNs leverage users' real-world social relationships and blend even more our online and offline lives. Facebook in 2015 had more than 1.5 billion monthly active users and it was the second most visited site on the Internet [1]. Twitter, a social micro-blogging platform, claims over 500 million users. In addition, the social networking will be the fourth most popular online activity [2].

* Corresponding author.
E-mail address: waleedead@hotmail.com

Peer-review under responsibility of the Organizing Committee of SDMA2016
doi:10.1016/j.procs.2016.04.004

Companies are mining trends on Facebook and Twitter to create viral content for shares and likes. Employers are checking Facebook, LinkedIn and Twitter profiles of job candidates. Law enforcement organizations are gleaning evidence from OSNs to solve crimes. Activities on online social platforms change political regimes [2]and swing election results.

More importantly, OSNs expose now information from multiple social spheres. For example, personal information on Facebook and professional activity on LinkedIn that is aggregated leads to uncomfortably detailed profiles [3].

1.1. Privacy Attacks in Online Social Networks

Privacy attacks in online social networks can be classified based on the stakeholders of the OSN and the forms of attack targeted at the stakeholders. We identify two stakeholders in online social networks: the OSN users and the OSN itself.

On one hand, OSN users share an astonishing amount of information ranging from personal to professional. The misuse of this information can have significant consequences. On the other hand, OSN services handle users' information and manage all users' activities in the network, being responsible for the correct functioning of its services and maintaining a profitable business model. Indirectly, this translates into ensuring that their users continue to happily use their services without becoming victims of malicious actions.

We classify online social network privacy and security issues into the following attacks categories (Fig. 1).

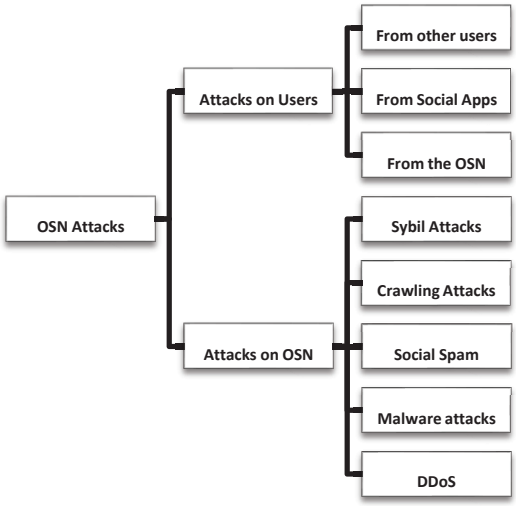

Fig. 1: OSN attacks categories

(1) **Attacks on Users**: these attacks are isolated, targeting a small population of random or specific users. There are several types of attacks based on the attacker: (a) *Attacks from other users*[1, 2]. (b) *Attacks from social applications* [3]. (c) *Attacks from the OSN* [4]. (d) *De-anonymization* and *inference attacks*. OSN services publish social data for others (e.g., researchers, advertisers) to analyze and use for other purposes.

(2) **Attacks on the OSN**: these attacks are aimed at the service provider itself, by threatening its core business. Such as *Sybil Attacks* [5-7], *Crawling attacks [8]*, *Social Spam[9]*, *Distributed Denial*-of-*service attacks* (DDoS) and *Malware Attacks* [10].

OSN users are facing multiple risks while using social applications. First, an application might be malicious; it could collect a high volume of user data for unwanted usage. For example, to show this vulnerability, BBC News developed a malicious application that could collect large amounts of user data in only three hours [11]. Second, application developers can violate developer policies to control user data. Application developers are supposed to abide by a set of rules set by the OSNs, called "developer policies". Developer polices are intended to prohibit application developers from misusing personal information or forwarding it to other parties. However, reported incidents[11] show that applications violate these developer policies. For example, a Facebook application, "Top Friends" enabled everyone to view the birthday, gender and relationship status of all Top Friends users, even though