Online Social Networks and Media 3–4 (2017) 1–21

Contents lists available at ScienceDirect

Online Social Networks and Media

journal homepage: www.elsevier.com/locate/osnem

Privacy and security in online social networks: A survey

Imrul Kayes[a,*], Adriana Iamnitchi[b]

[a] Sonobi Inc., 444 W New England Ave #215, Winter Park, FL 32789, USA
[b] Computer Science and Engineering, University of South Florida, Tampa, FL, USA

ARTICLE INFO

Article history:
Received 15 May 2017
Revised 10 August 2017
Accepted 18 September 2017

Keywords:
Privacy
Security
Online social networks

ABSTRACT

Online social networks (OSN) are a permanent presence in today's personal and professional lives of a huge segment of the population, with direct consequences to offline activities. Built on a foundation of trust – users connect to other users with common interests or overlapping personal trajectories – online social networks and the associated applications extract an unprecedented volume of personal information. Unsurprisingly, serious privacy and security risks emerged, positioning themselves along two main types of attacks: attacks that exploit the implicit trust embedded in declared social relationships; and attacks that harvest user's personal information for ill-intended use. This article provides an overview of the privacy and security issues that emerged so far in OSNs. We introduce a taxonomy of privacy and security attacks in OSNs, we overview existing solutions to mitigate those attacks, and outline challenges still to overcome.

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. As of 2017, Facebook has 1.94 billion monthly active users and it is the third most visited site on the Internet [1]. Twitter, a social micro-blogging platform, claims over 313 million monthly active users, who send Tweets in more than 40 languages [2].

Perhaps more than previous types of online applications, OSNs are blending in real life: 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 [3]; law enforcement organizations are gleaning evidence from OSNs to solve crimes [4]; activities on online social platforms change political regimes [5] and swing election results [6].

Because users in OSNs are typically connected to friends, family, and acquaintances, a common perception is that OSNs provide a more secure, private and trusted Internet-mediated environment for online interaction [7]. In reality, however, OSNs have raised the stakes for privacy protection because of the availability of an astonishing amount of personal user data which would not have been exposed otherwise. More importantly, OSNs expose now information from multiple social spheres – for example, personal information on Facebook and professional activity on LinkedIn – that, aggregated, leads to uncomfortably detailed profiles [8].

Unwanted disclosure of user information combined with the OSNs-induced blur between the professional and personal aspects of user lives allow for incidents of dire consequences. The news media covered some of these, such as the case of a teacher suspended for posting gun photos [9] or employee fired for commenting on her salary compared with that of her boss [10], both on Facebook. On top of this, social networks themselves intentionally (e.g., Facebook Beacon controversy [11]) or unintentionally (e.g., published anonymized social data used for de-anonymization and inference attacks [12]) are contributing to breaches in user privacy. Moreover, the high volume of personal data, either disclosed by the technologically-challenged average user or due to OSNs' failure to provide sophisticated privacy tools, have attracted a variety of organizations (e.g., GNIP) that aggregate and sell user's social network data. In addition, the trusted nature of OSN relationships has become an effective mechanism for spreading spam, malware and phishing attacks. Malicious entities are launching a wide range of attacks by creating fake profiles, using stolen OSN account credentials sold in the underground market [13] or deploying automated social robots [14].

This article provides a comprehensive review of solutions to privacy and security issues in OSNs. While previous literature reviews on OSN privacy and security are focused on specific topics,

* Corresponding author.
E-mail address: imrulkayes11@gmail.com (I. Kayes).

https://doi.org/10.1016/j.osnem.2017.09.001
2468-6964/

such as privacy preserving social data publishing techniques [15], social graph-based techniques for mitigating Sybil attacks [16], OSN design issues for security and privacy requirements [17], or threats in OSNs [18], we address a larger spectrum of security and privacy problems and solutions. First, we introduce a taxonomy of attacks based on OSNs' stakeholders. We broadly categorize attacks as attacks on users and attacks on the OSN and then refine our taxonomy based on entities that perform the attacks. These entities might be human (e.g., other users), computer programs (e.g., social applications) or organizations (e.g., crawling companies). Second, we present how various attacks are performed, what countermeasures are available, and what are the challenges still to overcome.

2. A taxonomy of privacy and security problems in online social networks

A social network is an ecosystem consisting of a number of entities. These entities include, but not limited to, users, the OSN service provider, third-party applications, and advertisers. However, the primary stakeholders of this ecosystem are users (who receive various social networking services) and OSN providers (who provide those social networking services). The privacy and security problems bring significant consequences for users and OSN service providers. For users, potential consequences mean inappropriate sharing of personal information, i.e., leakage, and exploitation of personal details using active mining, e.g., information linkage [19]. For OSN services, privacy and security threats disrupt the proper functioning of the service and damage providers' reputation.

We propose a taxonomy of privacy and security problems in online social networks based on the stakeholders of the ecosystem and the axes from which privacy and security risks come. As we have already mentioned, we identify two primary stakeholders in online social networks: the OSN users and the OSN itself.

Users reveal an astonishing amount of personally identifiable information on OSNs, including physical, psychological, cultural and preferential attributes. For example, Gross and Acquisti's study [20] show that 90.8% of Facebook profiles have an image, 87.8% of profiles have posted their birth date, 39.9% have revealed phone number, and 50.8% profiles show their current residence. The study also shows that the majority of users reveal their political views, dating preferences, current relationship status, and various interests (including music, books, and movies).

Due to the diversity and specificity of the personal information shared on OSNs, users put themselves at risk for a variety of cyber and physical attacks. Stalking, for example, is a common risk associated with unprotected location information [21]. Demographic re-identification was shown to be doable: 87% of the US population can be uniquely identified by gender, ZIP code and full date of birth [22]. Moreover, the birth date, hometown, and current residence posted on a user's profile are enough to estimate the user's social security number and thus expose the user to identity theft [20]. Unintended revealing of personal information brings other online risks, including scraping and harvesting [23,24], social phishing [25], and automated social engineering [26].

In the ecosystem of an OSN, users interact with other users (a lot of them are complete strangers), use third-party social applications, and clicks on ads placed by the advertisers. Users' information leakage might happen to all of these entities. Moreover, users' data collected from multiple social networks lead to linkage problems, where a significantly broader profile of the user could be built by linking the user over the social networks.

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. However, attacks such as Sybil, DDoS, spam and malware on OSNs may translate into reputation damage, service disruption, or other consequences with direct effect on the OSN.

We thus classify online social network privacy and security issues into the following categories (summarized in Table 1).

1. Leakages and linkages of user information and content: these issues relate to information disclosure threats. We identify a number of entities who are involved with users' information and their content leakage and linkage.
   (a) Leakages into other users: Users might put themselves at risk by interacting with other users, specially when some of them are strangers or mere acquaintances. Moreover, some of these users may not even be human (e.g., social robots [27]), or may be crowdsourcing workers strolling and interacting with users for mischievous purposes [28]. Therefore, the challenge is to protect users and their information from other users.
   (b) Leakages into social applications: For enhanced functionality, users may interact with various third-party-provided social applications linked to their profiles. To facilitate the interaction between OSN users and these external applications, the OSN provides application developers an interface through which to access user information. Unfortunately, OSNs put users at risk by disclosing more information than necessary to these applications. Malicious applications can collect and use users' private data for undesirable purposes [29].
   (c) Leakages into the OSN: Users' interactions with other users and social applications are facilitated by the OSN services, in exchange for, typically, full control over user's information published on the OSN. While this exchange is explicitly stated in Terms of Service documents that the user must agree with (and supposedly read first), in reality few users understand the extent of this exchange [30] and most users do not have a real choice if they do not agree with the exchange. Consequently, the exploitation by the OSN of user's personal information is seen as a breach of trust, and many solutions have been proposed to hide personal information from the very service that stores it.
   (d) Linkages by aggregators: Large-scale distributed data crawlers from professional data aggregators exploit the OSN-provided APIs or scrape publicly viewable profile pages to build databases from user profiles and social links. Professional data aggregators sale such databases to insurance companies, background-check agencies, credit-ratings agencies, or others [31]. Crawling users' data from multiple sites and multiple domains and further linking them increases profiling accuracy. This profiling might lead to "public surveillance", where an overly curious agency (e.g., government) could monitor individuals in public through a variety of media [32].
2. Attacks on the OSN: these attacks are aimed at the service provider itself, by threatening its core business. OSNs have been targeted by Distributed Denial-of-service (DDoS) attacks; have been used as platforms for propagating malware and social spam. These attacks can be performed by a number of ways. For example, attackers can create a number of Sybil identities and use them for spam content campaign or malware propagation. Attackers can also illegitimately take control of the accounts created by other users, and use those compromised accounts to launch an organized and planned attacks. Note that users of the platforms are