Information Sciences 421 (2017) 43–69

Contents lists available at ScienceDirect

Information Sciences

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

Social network security: Issues, challenges, threats, and solutions

Shailendra Rathore[a], Pradip Kumar Sharma[a], Vincenzo Loia[b], Young-Sik Jeong[c], Jong Hyuk Park[a,*]

[a] Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Republic of Korea
[b] Department of Management and Innovation Systems, University of Salerno, Italy
[c] Department of Multimedia Engineering, Dongguk University, Seoul 04620, Republic of Korea

ARTICLE INFO

Article history:
Received 5 April 2017
Revised 17 August 2017
Accepted 19 August 2017
Available online 23 August 2017

Keywords:
Social network service
Security and privacy
Multimedia data
Security threats

ABSTRACT

Social networks are very popular in today's world. Millions of people use various forms of social networks as they allow individuals to connect with friends and family, and share private information. However, issues related to maintaining the privacy and security of a user's information can occur, especially when the user's uploaded content is multimedia, such as photos, videos, and audios. Uploaded multimedia content carries information that can be transmitted virally and almost instantaneously within a social networking site and beyond. In this paper, we present a comprehensive survey of different security and privacy threats that target every user of social networking sites. In addition, we separately focus on various threats that arise due to the sharing of multimedia content within a social networking site. We also discuss current state-of- the-art defense solutions that can protect social network users from these threats. We then present future direction and discuss some easy-to-apply response techniques to achieve the goal of a trustworthy and secure social network ecosystem.

1. Introduction

A Social Network Service (SNS) is a kind of web service for establishing a virtual connection between people with similar interests, backgrounds, and activities. A SNS allows its users to find new friends and expand their circle of friends. Data sharing is another key feature of a SNS where users are able to share their interests, videos, photos, activities, and so on. In recent years, SNS such as Twitter and Facebook have become desired media of communication for billions of online users. These services combine user-created profiles with a communication mechanism that enables users to be connected with their friends, families, and colleagues. The prominence of these services is due to the fact that users can update their personal information, interact with other users, and browse other member's profiles. SNSs can be very beneficial for users because they shrink economic and geographical borders. In addition, they can be utilized for achieving goals related to job searching, entertainment, education. However, the popularity of SNSs creates a high risk for their users. The large amount of personal data that users share on SNSs makes them a desirable target for attackers. Attackers can obtain sensitive personal

* Corresponding author.
E-mail addresses: rathoreshailendra@seoultech.ac.kr (S. Rathore), pradip@seoultech.ac.kr (P.K. Sharma), loia@unisa.it (V. Loia), ysjeong2k@gmail.com (Y.-S. Jeong), jhpark1@seoultech.ac.kr, parkjonghyuk1@hotmail.com (J.H. Park).

http://dx.doi.org/10.1016/j.ins.2017.08.063
0020-0255/

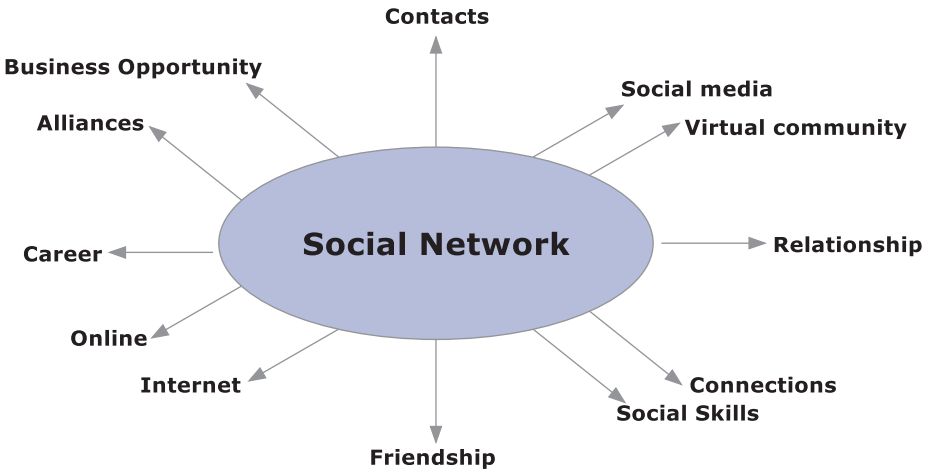

Fig. 1. The fundamental concept of SNSs.

data simply by using a SNS and can carry out many kinds of attacks, such as spam, malware, socialbots, and identity theft. Moreover, attackers can find other significant data, such as bank account information, by analyzing the user's personal data and can commit internet crimes, such as bank fraud. According to an analysis by Raggo [82], SNS attacks can range from account hijacking, fraud, and impersonation attacks to malware distribution. A sophisticated attack can compromise the enterprise networks. The fundamental concept of a SNS is shown in Fig. 1.

In many SNSs, such as Facebook, mainly multimedia data is produced and shared. According to a report from Zephoria Digital Marketing (ZDM) [126], approximately 136,000 photos are uploaded every 60 s on Facebook. A set of statistics from SocialMediaToday [50] show that the average viewing and sharing rate of videos on Facebook is increasing day by day. Currently, approximately 8 billion videos per day are viewed on Facebook, which is double the amount viewed in 2015. Due to the vast amount of multimedia data available on Facebook, security risks are also increasing. A malicious user can share malicious information on a SNS by concealing it within multimedia data. Moreover, by doing so, an attacker can easily find the user's important information, such as user identity and location [91].

Some SNSs, like Twitter, do not allow users to disclose significant private information, but attackers can infer the sequence of a user's posted content on a SNS and can reveal their undisclosed private information. In 2005, MySpace was attacked by the Sammy worm, which exploited the vulnerabilities in MySpace and transmitted very quickly. It did not steal users' personal information, but it still had a dangerous effect on MySpace's general operations. In April 2009, Twitter was attacked by the Mikeyy worm, which also did not steal users' personal information, but instead replaced their data with some unusable data. In May 2009, Facebook was attacked by the Koobface worm, which stole significant information, such as a user's password [121].

The Internet Security Threat Report (ISTR) [113] stated that the increasing use of SNSs by hackers cannot be ignored. In 2015, such services turned into a source for spam and malware, and were utilized as a way of making illegal money on the web. Recently, Facebook CEO Mark Zuckerberg's Pinterest and Twitter accounts were hacked, where the hacker used his LinkedIn password of "dadada." [67]. Similarly, attackers infiltrated the SNS accounts of Delta Air Lines Inc. and Newsweek by posting fake messages [2]. After conducting an analysis of the aforementioned attack statistics, we concluded that SNSs are the best way for an attacker to commit cybercrimes.

With the increasing amount of traditional threats and threats due to multimedia data in SNSs, many researchers and security corporations have proposed various solutions to mitigate these threats. Such solutions include watermarking [13], steganalysis [26], and digital oblivion [62] for protecting SNS users against threats due to multimedia data. On the other hand, various solutions, such as spam detection [127] and phishing detection [103], have been proposed to mitigate traditional threats. However, many built-in security solutions, such as authentication mechanisms [78] and privacy settings [54], and commercial solutions, such as minor monitor [43] and social protection application [71], also serve as safeguards against both types of threats in SNSs.

Many security researchers have studied and discussed the security issues in SNSs. Gao et al.'s research [38] categorized major security issues in SNSs into four categories: (a) Privacy issues, (b) Viral marketing, (c) Network structural-based attacks, and (d) Malware attacks. Their research included an in-depth discussion on each issue and the corresponding defense mechanisms. Novak et al. [23] surveyed the major security and privacy issues in SNSs. They discussed the existing techniques that protect SNS users against various entities, such as SNS providers, third party application developers, advertisers, and other users. They also provided a clear overview of the SNS inference of link prediction, location hubs, and user attributes. Jin et al. [66] studied user behavior in SNSs from four viewpoints: (a) malicious behavior, (b) mobile social behavior, (c) traffic activity, and (d) connection and interaction. They discussed the major challenges and motivations of user behaviors and provided a review on existing schemes for SNS security. Fire et al.'s research [74] presented a comprehensive survey of