Chapter 10
Security and Privacy Issues in Social Networks

Sepideh Deliri and Massimiliano Albanese

10.1 Introduction

In recent years, online social networks (OSNs) like Facebook, LinkedIn, and Twitter have turned out to be fundamental parts of our online lives, and their popularity is increasing at a surprising rate each and every day. According to a survey conducted by the Pew Research Center’s Internet & American Life Project, almost 72% of online US adults are members of online social network sites, compared to only 8% in 2005 and 67% in late 2012 [3]. Among the social networking sites, Facebook—with nearly 1.28 billion users worldwide as of the first quarter of 2014—has been one of the most successful ones in recent years [14]. Users employ OSNs as a tool to connect with family, friends, colleagues, associates, or people with the same interests for different purposes such as professional networking, advertising their brands and businesses, job searches, making profit, or entertainment.

Besides the revolution that OSNs have generated in social networking, they have introduced new threats to their users due to their attractiveness, the ever-increasing number of users, and the massive amount of personal information they share. Being a part of users’ daily lives, online social networks introduce new security concerns especially because of the potential exposure of huge amounts of personal information. Some examples of threats to OSNs include stealing the identities or credentials of users and social networking risks like phishing, social engineering and reverse social engineering, spoofing, fiscal fraud, malware, and spam. As a result, maintaining security and privacy of OSN users has become a major challenge in recent years.
In this chapter, we discuss the main classes of security and privacy attacks to online social networks and the countermeasures that can be used to protect the privacy of OSN users and keep shared data secure against different types of attacks. Additionally, we propose a set of guidelines for OSN users to protect themselves against different types of attacks. Finally, we examine existing laws and regulations introduced to combat online social network attacks and prosecute illegal activities by cyber criminals.

10.2 Overview of Online Social Networks

Online social networks have seen a rapid increase in the number of users, especially in the last few years [8]. Being a strong communication channel, online social media has become a popular tool to comment on worldwide events, improve information discovery, and facilitate social interaction. In addition, OSNs are powerful tools to not only stay connected with friends and family members but also to connect with professional groups. Additionally, they can be used for marketing and advertising purposes and for enhancing business reputation.

People join OSNs, create their own profiles, and connect to other members of the network with the main purpose of keeping in touch with them and sharing common interests. Most online social network sites share some common features. One of the fundamental properties of OSNs is that they allow their users to create their own profiles. Using this feature, OSN members can represent themselves with the purpose of connecting to other users in the network. Users can post contents like pictures, videos, and personal blogs in their profiles, which can be seen by all or only selected members of the network. Another common feature of OSNs is the ability to create links with other members of the network. If a link exists between two members, they are supposed to be neighbors. Neighboring users usually have common interests, and a higher degree of trust exists among them. Users can trace a specific OSN member by following the links connecting OSN users in order to reach his online profile. Finally, unlike other online sites that are usually content based, OSNs are mainly organized around their users. In other words, two major components of OSNs are user accounts and the links between users [12].

Although a social networking site can be a good way of connecting to people with similar interests, the ever-increasing number of OSN users leads to a growing amount of available data related to social relations. The availability of massive amount of personal information has attracted the attention of malicious users and motivated them to initiate attacks against OSNs by gaining access to the information shared by the users. Therefore, the privacy of OSN users can be at risk. Indeed, OSNs can become a tool that opens up new ways for criminals and hackers to perform undesired or fraudulent activities such as spamming, attacking through viruses, phishing, etc., which often results in information and identity theft.