# Online Social Networks and Media

## 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. 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.

## Introduction

In online social networks, privacy and security issues are not separable. In some contexts, privacy and security goals may be the same, but there are other contexts where they may be orthogonal, and there are also contexts where they are in conflict. For example, in an OSN, a user wants privacy when she is communicating with other users though the messaging service. She will expect that non-recipients of the message will not be able to read it. OSN services will ensure this by providing a secure communication channel. In this context, the goals of security and privacy are the same. COSNs 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.

## System Description

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. For OSN services, privacy and security threats disrupt the proper functioning of the service and damage provider’s reputation. Millions of Internet users are using OSNs for communication and collaboration. Many companies rely on OSNs for promoting their products and influencing the market. It becomes harder and harder to imagine life without the use of OSN tools, whether for creating an image of oneself or organization, for selectively following news as filtered by the group of friends, or for keeping in touch. However, the growing reliance on OSNs is impaired by an increasingly more sophisticated range of attacks that undermine the very usefulness of the OSNs. OSNs and social applications are here to stay, and while they mature, new security and privacy attacks will take shape. Technical advances in this area can only be of limited effect if not supported by legislative measures for protecting the user from other users and from the service providers. We have categorized various attacks on OSNs based on social network stakeholders and the forms of attack targeted at them. Specifically, we have categorized those attacks as attacks on users and attacks on the OSN.

| **Users' information and content leakages and linkages** | **Attacks on the OSN** |
|---|---|
| Leakages into other users | Sybil attacks |
| Leakages into social applications | Compromised accounts |
| Leakages into the OSN | Social spam and malware |
| Linkages by aggregators | Distributed Denial-of-service attacks (DDoS) |

## Challenges & Future research directions

As the OSNs are enjoying unprecedented popularity, keeping users engaged with new functionalities, new privacy and security threats are emerging. The dynamic landscape of privacy and security attacks have enabled researchers to continuously looking forward for new threats and provide mitigating techniques. One possible future research direction includes understanding the privacy leakage and associated risks when OSNs work as a Web tracker. OSNs (e.g., Facebook, Twitter) continue to be the login of choice for many websites and applications. As such, OSNs can track their users in third-party websites by placing cookies to users' devices on behalf of those websites. Note that OSNs already know what users do in their platforms. Tracking the users in third-party websites enables them to create a more detailed user profile. As such, OSNs could essentially work as a traditional third-party Web aggregator by offering advertisers targeted advertising in publisher's websites.