Chapter 9
A Graph-Based Approach to Model Privacy and Security Issues of Online Social Networks

Luca Caviglione
National Research Council of Italy, Italy

Mauro Coccoli
University of Genoa, Italy

Alessio Merlo
University of Genoa, Italy & Università Telematica E-Campus, Italy

ABSTRACT

With millions of users, Online Social Networks (OSNs) are a huge cultural phenomenon. Put briefly, they are characterized by: i) an intrinsic sharing of personal information, ii) a rich set of features to publish, organize and retrieve contents, especially for emphasizing their social organization, iii) the interaction with a heterogeneous set of devices, e.g., ranging from desktops to mobile appliances, and iv) the mix of Web-based paradigms and sophisticated methodologies for processing data. However, if not properly implemented, or without effective security policies, i) – iv) could lead to severe risks in terms both of privacy and security. In this perspective, this chapter analyzes the major peculiarities of OSN platforms, the preferred development methodologies, and usage patterns, also by taking into account how personal information can be exploited to conduct malicious actions. Then, a graph-based modeling approach is introduced to reveal possible attacks, as well as to elaborate the needed countermeasures or (automated) checking procedures.

DOI: 10.4018/978-1-4666-3926-3.ch009
INTRODUCTION

Online Social Networks (OSNs) have changed the way people communicate and share their personal information. Also, they are a key advancement for pursuing the vision of developing an Internet of People (IoP), rather than a straight internetwork of nodes. Even if revolutionary, OSNs are not based on completely novel concepts. Specifically, the World Wide Web Consortium (W3C), when detailing the model at the basis of the Social Web (W3C, 2010), envisaged the introduction of a core set of people-centric services. Nowadays, such functionalities are partially implemented within the most popular OSN platforms, rather than in a unified manner as originally planned by the W3C. As a consequence, the current social vocation of the Web has not been developed according to a precise standard, or under an organic guidance. Rather, it has grown (and continues to evolve) around features introduced by the different OSN providers. As a result, social tools are constrained to provide functionalities for task-specific duties, for instance to share photos in an OSN aiming at entertainment, or to publish resumes or portfolios in platforms designed to support business development. To summarize, the overall OSN geography is substantially split, populated by different frameworks delivering services in a non-uniform, redundant and mostly incompatible manner.

But the evolution of Application Programming Interfaces (APIs), jointly with the availability of agreed data representation models, and the creation of business partnerships, allow cross-platform interaction. Among the others, we mention the OpenGraph (OGP, 2012) template for depicting personal relations, thus enabling developers to handle user identities in a portable way. For the case of OSNs relying upon Web technologies, integration mainly takes benefit from the maturity of the **mash-up** approach, which facilitates the aggregation of different Web service providers to produce brand new contents. Another important factor accounting for the success of OSNs is the support of the **anywhere-anytime** paradigm. Yet, it introduces further heterogeneities, since OSNs are accessed from desktops, home appliances, gaming consoles, and mobile devices, e.g., smartphones and tablets. Moreover, this leads to an additional layer of complexity, since some devices exchange data with the OSN by using Web facades (even if tweaked for reduced screen sizes and resolutions), while others do have ad-hoc client-interfaces. In this case, the use of Web views can reduce the necessity of having different server-side implementations, but many applications do use an additional tier of Web-services and specific data models or protocols. As a result, accessing an OSN from different devices implies the use of several technologies, a broad variety of network requirements, traffic behaviors, and security mechanisms. The exploitation of social interactions over the Internet is done via a complex mix of services, technologies, programming methodologies, protocols, usage patterns, and incoherent designs, especially concerning Graphical User Interfaces (GUIs). Besides, to increase the interactivity of pages composing the OSN and to support real-time communications and feedbacks, the usage of specific programming methods within the users’ browsers reduce the boundaries between the client and the server. We mention, among others, the XMLHttpRequest Javascript object, which enables a constant data movement by using long-held HTTP connections. Thus, the composite nature of the aforementioned scenario has also a huge impact in terms of privacy and security levels offered by OSN applications (Caviglione & Coccoli, 2011). In fact, many providers offer a variety of privacy management policies or security options, leading to possible attacks, misconfigurations or other hazardous conditions. These aspects should be also jointly considered with specific users’ behaviors regarding the disclosure of critical information (e.g., family details reducing the strength of password recovery mechanisms based on secrets), and the pondered reduction of security policies of their accounts (e.g., for accessing to