Preface

Online Social Network (OSN) applications are nowadays accessed by about a billion of users, thus they can be considered a real cultural phenomenon, and one of the most innovative component of the Web 2.0. As a consequence, they have relevant impacts on the society, the economy and the technological pool of the Internet. OSN platforms are not only used for content sharing purposes. Rather, they have demonstrated their effectiveness to support the development of new services or applications, and also to provide a suitable playground for real-time user-to-user interactions. To be effective, the engineering and creation of new frameworks require a capillary research activity, both by the Academia and the Industrial world. In fact, advancements in the field of OSN impose the understanding of new users’ behaviors, the development of innovative Web-based interaction paradigms, the modeling of application-specific traffic patterns and network requirements, the creation of highly scalable architectural blueprints, the definition of novel Quality of Service (QoS) and Quality of Experience (QoE) guarantees, and, definitely, a thorough understanding of security hazards. To this aim, it must be considered that OSNs store, deliver and manage personal data, and they are tightly coupled with identities of individuals. It must be also underlined that their specificities make the constant cross-pollination between digital and real life a tangible and actual danger, thus making an intimate understanding of privacy issues an unavoidable task. Accordingly, the word “secure” must be considered with the acception of a hyponym embracing security and privacy risks at different levels, i.e., physical, digital, and social. Unfortunately, this requires a highly multidisciplinary effort, ranging from social sciences, to software engineering.

In this perspective, this book entitled Social Network Engineering for Secure Web Data and Services tries to capture the state-of-the-art of engineering, development and research, applied to OSNs, having the secure qualification as the founding principle. Its main goal is to consider issues and solutions to prevent security threats, and introduce proper countermeasures to attacks at every level during the design and development of OSN applications (or while relying upon such frameworks). Due to the multidisciplinary nature of the topic, Social Network Engineering for Secure Web Data and Services has been architected to be useful to a mixed audience. Specifically, it is intended for professionals and researchers in the area of OSN, software engineering, network and software security specialists, as well as professionals in charge of investigating computer frauds, and behavioral aspects of platforms delivering social network services in a broad sense. To increase its accessibility, the book covers aspects both from the theoretical and practical points of view, without neglecting the vision from social sciences, e.g., in the field of communication, education, and sociality.
To support such vision, our work is composed by 12 chapters written by experts in the relevant field, which have been double blindly reviewed by authoritative peers. When receiving submissions, we decided to discard works not clearly focusing on relevant topics, or not giving real benefits to perspective readers. To better organize the contributions, also making the book accessible to readers with a different understanding on the topic, we grouped the chapters into three sections. Namely: (1) Fundamentals, (2) Applications, and (3) Security.

The first section starts with the chapter “On Social Network Engineering for Secure Web Data and Services” introducing the state-of-the-art in the engineering of OSNs infrastructures, the impact of OSN-based services over the Internet, and a possible research roadmap. Then, “Identity, Credibility and Trust in Social Networking Sites. Old Issues, new Mechanisms and Current Challenges for Privacy and Security” provides a wide overview of the current literature on identity, credibility and trust, and their implications for privacy and security, from the perspective of social and behavioral sciences. To complete such an introductory path, the work “Access Control Models for Online Social Networks” showcases the essential aspects of access control and reviews the classical Access Control Models (ACMs) with emphasis on how they can contribute to enhance privacy of OSNs, and by clearly indicating core requirements for future implementations.

In the second section, the chapter “Social Interactions and Automated Detection Tools in Cyberbullying” introduces to Cyberbullies, which are individuals abusing digital media (such as websites, social networking services, blogging, email, instant messaging, chat rooms, and cell phones) to attack victims. This work reviews the state-of-the-art research in automated tools to detect cyberbullying, as well as future perspective for its automated detection. The second contribution is “Social Networks and Collective Intelligence: A Return to the Agora,” where authors answer the following questions: “How can information quality be reliably assessed?” “How can sources credibility be fairly assessed?” “How can gatekeeping processes be found trustworthy when filtering out news and deciding ranking and priorities of traditional media?” The answers they provide are enclosed in Polidoxa (from Greek poly – πολύ, meaning “many” or “several” and doxa – δόξα, meaning “common belief” or “popular opinion”) offering a trust-based search engine, a social network and a holonic system for bottom-up self-protection and social privacy. Then, “Distributed Social Platforms for Confidentiality and Resilience” rethinks the current approach of building social networking systems by using a huge centralized entity owned by a single company. In this vein, authors do propose a solid distributed social networking platform consisting in a novel peer-to-peer blueprint that leverages existing, widespread and stable technologies such as Distributed Hash Tables (DHTs) and BitTorrent. To conclude, “Retrieval of Personal Public Data on Social Networks. The Risks for Privacy” analyzes the risks for privacy coming from the distribution of user data over several social networks. Besides, the work concentrates on hazards introduced by the aggregation of user data discovered on different sources into a single more complete profile, which makes possible to infer other information (possibly private).

The third section focuses on security aspects. The chapter “Privacy Issues in Social Networks” defines concepts belonging to privacy in social networks, and demonstrates how it can be violated. Also, authors discuss various countermeasures, as well as future research directions in the field of competence. The work “A Graph-Based Approach to Model Privacy and Security Issues of Online Social Networks” analyzes how personal information can be exploited to conduct malicious actions, with the aim of introducing a graph-based modeling methodology to elaborate countermeasures or automated checking procedures. The third contribution is “Security and Privacy of Online Social Network Applications”
where authors point out that basic mechanisms for isolating applications are well understood, but when applied to social-enabled applications will fall short. Then, they identify and discuss the current security and privacy problems related to social applications and their platforms, also by making proposals on how to address such problems. The work entitled “On the Use of Formal Methods to Enforce Privacy-Aware Social-Networking” examines the use of formal techniques and verification tools to ensure privacy-aware social networking, where users can predict the consequences of updating their privacy settings. To achieve this goal, they propose a tool called Poporo. The book concludes with “Web Malware That Targets Web Applications” investigating the most severe threats affecting Web applications such as the Structure Query Language Injection Attack (SQLIA) and the Zeus threat.