

Preface

Richard Chbeir and Bechara Al Bouna

Abstract With the increasing success in social networks, the various facets of our “digital” lives are directly and indirectly accessible on the web with public and private details. To secure our digital footprints and protect our privacy on social networks, dedicated techniques and methods are required. The aim of this book is to assess the current approaches and technologies related to the security and privacy protection of social networks. It provides main concepts, an overview of the state of the art, latest techniques, studies, and approaches as well as future directions in this field, by including a wide range of contributions from various studies and research groups.

1 Introduction

Social networks provide users, within their platforms, powerful ways to interact with other users through different forms and modalities. Consequently, each user can search and check the profiles of her social network members (for various reasons), exchange messages with some of them, publish some videos, and post comments on shared photos, etc. Although such tools are attracting continuously more and more users, several security and privacy problems related to their usage have emerged. For instance, how to provide users with an easy way to protect their shared data? How to protect a data repository (e.g., photo album) while several related information about the same content is already published (by some user

R. Chbeir (✉)

University of Pau and Adour Countries, LIUPPA Laboratory, 64200 Anglet Cedex, France

e-mail: richard.chbeir@univ-pau.fr

B.A. Bouna

UPA University, Ticket Laboratory, Beirut, Lebanon

e-mail: bechara.albouna@upa.edu.lb

friends) on the same or other blog/wiki/social network? etc. Several privacy settings are provided on social networks to help users secure their profiles and data. Those privacy settings are indeed useful for basic cases. However, they become relatively complicated to be correctly tuned by (non-expert) users and also inappropriate for complex cases (particularly when multimedia data come to play). In addition, social networks suffer regularly from security breaches and sometimes leak intentionally or accidentally users' information to unauthorized entities or third parties.

The book explores emerging and new problems that everyone is facing in his/her daily digital life and it contributes to the awareness campaign shedding the light on the risk of publishing private information particularly on social networks. Thus, it is a valuable companion and comprehensive reference for:

- *Social network users* who would like to be aware of the risks and possible (current and future) solutions.
- *Undergraduate and postgraduate students* who are taking a course in security and protection and need to study related current concepts in social networks.
- *Developers* who need to implement advanced security and protection techniques and make benefit of existent technologies.
- *Researchers* who desire to understand exiting approaches, pin down their limits, and identify several future directions.

Why This Book Is Interesting?

As mentioned earlier, the primary target audience for this book includes researchers, scholars, postgraduate students, developers, as well as end users who are interested in social network security and protection. To achieve this:

- The book is organized in self-contained chapters to provide greatest reading flexibility.
- The book covers introductory material suitable for various reader profiles.
- Basic concepts will be explained in simple language with illustrations and examples, which will help readers new to this field understand concepts at play regarding the subject matter.
- There will be plenty of questions in the last chapter, which will be helpful for both lecturers and students to check the understanding of the book concepts.

2 Book Organization

This edited volume of the book aims to gather the latest advances and innovative solutions in security and privacy preserving in social networks. It assesses the current technologies, as well as major challenges and future perspectives in this field. In its current form, this book covers interesting works gathered from experts

working in heterogeneous domains related to security and privacy. It is devoted to help the readers have a glance at the research priorities to be explored in social network throughout a security perspective.

The book contains eleven self-contained chapters organized into four parts as follows:

- Online Social Networks: Analysis, Privacy, and Terrorism
- Access Control, Reputation, and Semantic policies in social networks
- Security and Privacy in Mobile and P2P social networks
- Multimedia-based Authentication and Access Control Models for social networks

The last chapter contains a battery of problems and questions so as to allow the reader to better identify the main concepts in each chapter.

Part I deals with *Online Social Networks Analysis, Privacy, and Terrorism* and consists of three chapters.

In Chap. 1, “*Privacy in Online Social Networks*,” Elie Raad and Richard Chbeir address privacy-related issues by resorting to social network analysis and link mining techniques. They first describe the fundamental of social networks, their common representations, and the main motivations associated with their use. Afterwards, they particularly show how privacy attacks can build on social network analysis and link mining techniques to reveal user-sensitive information. The chapter concludes with a discussion of some open challenges to address in future privacy-related works.

In Chap. 2, “*Online Social Networks: Privacy Threats and Defenses*”, Shah Mahmood provides a brief overview of some threats to users’ privacy. He classifies these threats as users’ limitations, design flaws and limitations, implicit flows of information, and clash of incentives. He also discusses two defense mechanisms which deploy usable privacy through a visual and interactive flow of information and a rational privacy vulnerability scanner.

Shah Mahmood in Chap. 3, titled “*Online Social Networks and Terrorism: Threats and Defenses*,” discusses how some users are misusing social networks for terrorism. To do so, he first provides the background, definition, and classification of terrorism. Second, he discusses how some terrorists may be using online social networks to (1) recruit new members to a terrorist organization and maintain the loyalty of their existing sympathizers; (2) plan attacks and share information about them; (3) gather intelligence; (4) train recruits for specific attacks; (5) raise funds for their causes; (6) propagate fear amongst the enemy population; and (7) engage in counterintelligence to uncover undercover agents. Third, he explores several mechanisms to detect terrorists using online social networks, including (1) keyword-based flagging; (2) sentiment analysis; (3) honeypots; (4) social network analysis; (5) facial recognition; and (6) view escalation. He shows that the keyword-only flagging mechanism used by US Department of Homeland Security to detect terrorists is potentially effective but certainly produces a large number of false positives, making it possibly less efficient in practice. Finally, he proposes the use of targeted advertisements to rehabilitate possible radicals using the online social networks.

Part II consists of three chapters and deals with *Access Control, Reputation, and Semantic Policies* in social networks.

In Chap. 4, “*User-Managed Access Control in Web Based Social Networks*,” Gonzalez-Manzano et al. focus on the design and implementation of user-managed access control systems Web Based Social Networks (WBSNs). In this regard, there exists a well-known

set of requirements (relationship-based, fine-grained, interoperability, sticky-policies, and data exposure minimization) that have been identified in order to provide a user-managed access control for WBSNs. These requirements, partially addressed by the works proposed in the literature, represent “building blocks” for a well-defined user-managed access control model. In this chapter, the authors first provide a conceptualization of a WBSN to propose an access control model, called *SoNeUCON_{ABC}*, and a mechanism that implements it. A set of mechanisms among the recently proposed in the literature are selected such that, when deployed over *SoNeUCON_{ABC}*, the whole set of user-managed requirements can be fulfilled.

Chapter 5, “*UPP+: A Flexible User Privacy Policy for Social Networking Services*” by Ramzi A. Haraty and Sally Massalkhy, presents a new privacy policy model, called UPP+, for enhancing privacy and security for ordinary users. To do so, they use the Alloy language to formalize the model and the Alloy analyzer to check for any inconsistencies.

In Chap. 6, “*Social Semantic Network-based Access Control*” by Villata et al., the authors address the privacy problem within the Social Semantic Web umbrella where social networks are integrated and enhanced by the use of semantic conceptual models, e.g., ontologies, where social information and links among users become semantic information and links. In this chapter, the authors discuss the benefits of introducing semantics in social network-based access control. In particular, they analyze and detail two approaches to manage the access rights of the social network users relying on Semantic Web languages only, and they highlight, thanks to these two proposals, what are the pros and cons of adopting semantic models and languages in social networks access control. Finally, they report on the other existing approaches coupling semantics and access control in the context of social networks.

Part III consists of three chapters and focuses on Security and Privacy in *Distributed (Mobile and P2P) social networks*.

In Chap. 7, “*Supporting Data Privacy in P2P Systems*” by Jawad et al., the authors explore large-scale data sharing in Peer-to-Peer (P2P) systems. To provide appropriate access control to sensitive data, they extend Hippocratic DataBases (HDB) approach to provide an effective solution to this problem. In essence, the use of HDB has been restricted to centralized systems. This chapter gives an overview of current solutions for supporting data privacy in P2P systems and develops in more detail a complete solution based on HDB.

In Chap. 8, “*Privacy Preserving Reputation Management in Social Networks*” by Omar Hasan and Lionel Brunie, the authors address the reputation management to help establish the trustworthiness of users in social networks to enforce various security requirements. For example, a reputation system can help filter fake user profiles. However, a major challenge in developing reputation systems for social networks is that users often hesitate to publicly rate fellow users or friends due to the fear of retaliation. This trend prevents a reputation system from accurately computing reputation scores. Privacy preserving reputation systems hide the individual ratings of users about others and only reveal the aggregated community reputation score thus allowing users to rate without the fear of retaliation. In this chapter, the authors describe privacy preserving reputation management in social networks and the associated challenges. In particular, they look at privacy preserving reputation management in decentralized social networks, where there is no central authority or trusted third parties, thus making the task of preserving privacy particularly challenging.

In Chap. 9, “*Security and Privacy Issues in Mobile Social Networks*,” Teles et al. present an interesting chapter related to Mobile Social Networks (MSNs), since the use of contextual information gathered from mobile devices sensors, which in many cases occurs without the user’s awareness, leads to new privacy issues. Here, the authors give a general overview on

the challenges and the main concepts that affect privacy and security of MSNs. They show how privacy problems migrate from social networks to MSNs and provide some eventual solutions.

Part IV consists of two chapters and explores in a nice way *Multimedia-based Authentication and Access Control Models* for social networks.

Chapter 10, “*Avatar Facial Biometric Authentication Using Wavelet Local Binary Patterns*” by Abdallah A. Mohamed and Roman V. Yampolskiy, focuses on virtual worlds (e.g., Second Life) since they are populated by different types of people, businesses, and organizations. Users of virtual worlds, either individuals or organizations, might abuse the flexibility and adaptability offered by virtual environment by engaging in criminal activities. Even terrorist organizations have been active in virtual worlds. These organizations recently have used the virtual worlds for recruitment and to train their new members in an environment that is very similar to the real one. Since avatars are not just virtual creations as they have a great social and psychological correspondence with their creators, applying biometric techniques on avatars can give the law enforcement agencies and security experts the ability to identify who the actual users behind these avatars are. There is a mounting pressure to have techniques for verifying the real identities of the inhabitants of virtual worlds to secure cyberworld from incessant criminal activities (e.g., verbal harassment, fraud, money laundering, data or identity theft). In order to reduce the gap between our ability to recognizing human faces and avatar faces and to develop reliable tools for protecting virtual environments, the authors discuss in this chapter how one can use different versions of Local Binary Pattern (LBP) operators (traditional LBP, Multi-scale LBP, and Hierarchical multi-scale LBP) to recognize avatar faces from two different virtual worlds (Second Life and Entropia Universe). This chapter includes a definition of discrete wavelet transform from a face recognition research perspective, a summary of previous work done on this topic, characteristics of the data sets used in the experiments, as well as some suggestions for future work.

In Chap. 11, “*A Flexible Image-Based Access Control Model for Social Networks*,” Al Bouna et al. tackle the problems of publishing images and photos. It is true that social networks are tremendously spreading their tentacles over the web community providing appropriate and well-adapted tools for sharing images and photos. A fundamental glitch to consider is their ability to provide suitable techniques to preserve individuals’ privacy. Indeed, there is an urgent need to guarantee privacy by making available to end users tools to enforce their privacy constraints. This cannot be done over images as simple as it has been designed so far for textual data. In fact, images, as all other multimedia objects, are of complex structure due to the gap between their raw data and their actual semantic descriptions. Without these descriptions, protecting their content is a difficult matter. In this chapter, the authors present a novel security model for image content protection. In the proposed model, the authors provide dynamic security rules based on first-order logic to express constraints that can be applied to contextual information as well as low-level features of images. They finally discuss a set of experiments and studies carried out to evaluate the proposed approach.

Security and Privacy Preserving in Social Networks

Chbeir, R.; Al Bouna, B. (Eds.)

2013, XVI, 367 p. 107 illus., 66 illus. in color., Hardcover

ISBN: 978-3-7091-0893-2