MORGAN & CLAYPOOL PUBLISHERS

Security and Trust in Online Social Networks

Barbara Carminati
Elena Ferrari
Marco Viviani

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST

Elisa Bertino & Ravi Sandhu, *Series Editors*

Security and Trust in Online Social Networks

Synthesis Lectures on Information Security, Privacy, & Trust

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Security and Trust in Online Social Networks
Barbara Carminati, Elena Ferrari, and Marco Viviani
2013

Hardware Malware
Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl
2013

Private Information Retrieval
Xun Yi, Russell Paulet, and Elisa Bertino
2013

Privacy for Location-based Services
Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

Security and Trust in Online Social Networks

Barbara Carminati, Elena Ferrari, and Marco Viviani

www.morganclaypool.com

ISBN: 9781627052658 paperback
ISBN: 9781627052665 ebook

DOI 10.2200/S00549ED1V01Y201311SPT008

A Publication in the Morgan & Claypool Publishers series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #8
Series Editors: Elisa Bertino, *Purdue University*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Synthesis Lectures on Information Security, Privacy, & Trust
Print 1945-9742 Electronic 1945-9750

Security and Trust in Online Social Networks

Barbara Carminati, Elena Ferrari, and Marco Viviani
Università degli Studi dell'Insubria — University of Insubria
Varese, Italy

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #8

MORGAN & CLAYPOOL PUBLISHERS

ABSTRACT

The enormous success and diffusion that online social networks (OSNs) are encountering nowadays is vastly apparent. Users' social interactions now occur using online social media as communication channels; personal information and activities are easily exchanged both for recreational and business purposes in order to obtain social or economic advantages.

In this scenario, OSNs are considered critical applications with respect to the security of users and their resources, for their characteristics alone: the large amount of personal information they manage, big economic upturn connected to their commercial use, strict interconnection among users and resources characterizing them, as well as user attitude to easily share private data and activities with strangers.

In this book, we discuss three main research topics connected to security in online social networks: (i) trust management, because trust can be intended as a measure of the perception of security (in terms of risks/benefits) that users in an OSN have with respect to other (unknown/little-known) parties; (ii) controlled information sharing, because in OSNs, where personal information is not only connected to user profiles, but spans across users' social activities and interactions, users must be provided with the possibility to directly control information flows; and (iii) identity management, because OSNs are subjected more and more to malicious attacks that, with respect to traditional ones, have the advantage of being more effective by leveraging the social network as a new medium for reaching victims.

For each of these research topics, in this book we provide both theoretical concepts as well as an overview of the main solutions that commercial/non-commercial actors have proposed over the years. We also discuss some of the most promising research directions in these fields.

KEYWORDS

online social networks, security, trust, controlled information sharing, online identity management

Contents

Acknowledgments

A work of this kind depends on the cooperation of many people, students, colleagues, and researchers who worked or collaborated over the years with our research group on topics related to social networks. Without their efforts and ideas this book would not have been possible.

Barbara Carminati, Elena Ferrari, and Marco Viviani
December 2013

CHAPTER 1

Online Social Networks and Security Issues

1.1 INTRODUCTION

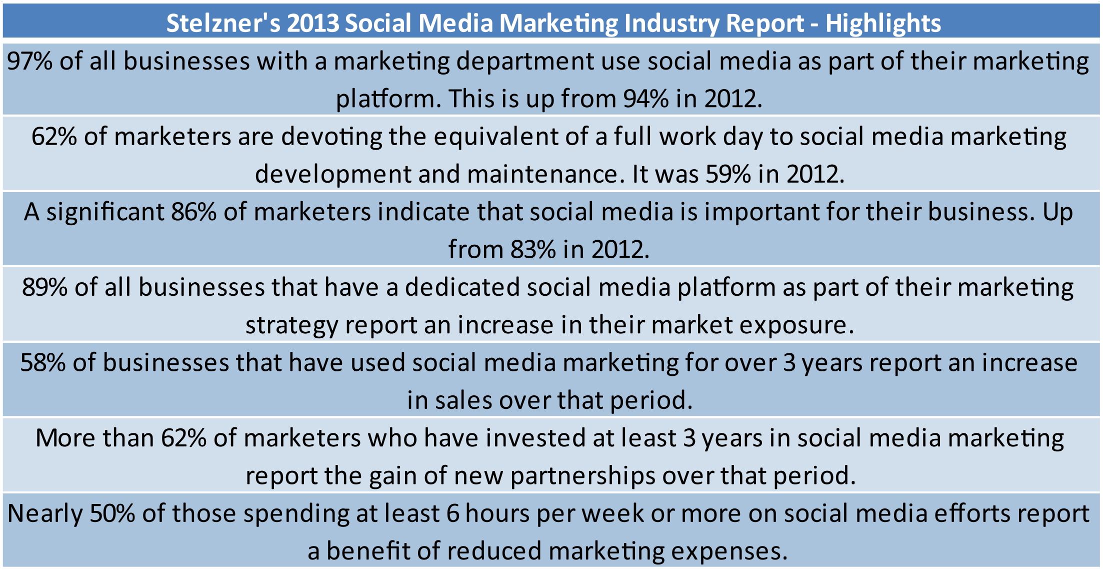
Nowadays, an increasing fraction of social interactions occurs using online *social media* as communication channels. According to Kaplan and Haenlein [162], "social media is a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content."

Social media differentiates from traditional/industrial media in many aspects. The first difference is *quality*: contrary to traditional/industrial media, social media generally exhibits a rich variety of information sources. In addition to the content itself, there is a wide array of "non-content" information available, such as links among items and explicit quality ratings from members of the community [10]. Other comparisons, listed by Morgan et al. [213], include: *reachability*—both traditional/industrial and social media provide scale and enable anyone to reach a global audience; *accessibility*: social media tools are usually available for free or at a very low price, whereas industrial ones are proprietary in most cases; *usability*—the use of traditional/industrial media usually requires particular skills and training, whereas using social media is immediate and approachable by anyone; *immediacy*—the time lag between communications produced by industrial media can be long with respect to social media, i.e., hours, days, and even weeks vs. possible immediate response; and *permanence*—industrial media content usually cannot be altered, unlike what happens in social media via commenting or editing operations.

Social media uses different technologies and can take different forms (e.g., forums, wikis, blogs, podcasts, video, social bookmarking). A classification in six different categories was provided by Kaplan and Haenlein [162], applying a set of theories in the field of media research and social processes. The set of relationships that link people together over the Web via social media technologies is called *Social Web* [14]. These online social interactions form the basis of many online services, including online shopping, e-learning, content-sharing, and social networking.

The growing use of these social media technologies brings with it many positive societal effects. According to Nielsen [2], Internet users continue to spend more time with social media sites than any other type of site. In fact, the total time spent on social media in the U.S. across PC and mobile devices increased by 37%, from 88 billion minutes in July 2011 to 121 billion minutes a year later. The benefits of participating in social media go beyond simple social sharing to build reputation and bring career opportunities and monetary income, as discussed in Tang et al. [261]. In particular, according to Rupert [244], there are five major contributions that social media bring to society: (i) it supports information during crisis or disasters, during which social media provides the only viable venue for communication; (ii) it is a valuable aid in crime-solving; (iii) it can influence political decisions, giving a true voice to the people; (iv) it is, of course, a way to connect people sharing common interests or friends and relatives across vast distances; and finally, (v) it constitutes a revolutionary way to conduct marketing.

Focusing on this last contribution, a BIA/Kelsey report [3] says that social media ad revenue will reach $11 billion by 2017. In addition, from Stelzner's 2013 Social Media Marketing Industry Report [258], we can clearly see how all businesses are counting on social media for their marketing strategies. As an example, some of the results of the Stelzner's Report are illustrated in Figure 1.1.



Stelzner's 2013 Social Media Marketing Industry Report - Highlights
97% of all businesses with a marketing department use social media as part of their marketing platform. This is up from 94% in 2012.
62% of marketers are devoting the equivalent of a full work day to social media marketing development and maintenance. It was 59% in 2012.
A significant 86% of marketers indicate that social media is important for their business. Up from 83% in 2012.
89% of all businesses that have a dedicated social media platform as part of their marketing strategy report an increase in their market exposure.
58% of businesses that have used social media marketing for over 3 years report an increase in sales over that period.
More than 62% of marketers who have invested at least 3 years in social media marketing report the gain of new partnerships over that period.
Nearly 50% of those spending at least 6 hours per week or more on social media efforts report a benefit of reduced marketing expenses.

Figure 1.1: Highlights from the Stelzner's 2013 Social Media Marketing Industry Report [258].

According to Stelzner's statistics for 2013, Facebook, Twitter, LinkedIn, blogging, and YouTube are the top five platforms used by marketers, with Facebook leading the pack. Their global success—not only with respect to social media marketing—is confirmed by statistics provided by Bullas,[1] which, according to Forbes,[2] is one of the major media power influencers in

[1] http://www.jeffbullas.com/2013/05/06/21-awesome-social-media-facts-figures-and-statistics-for-2013/
Retrieved September 1, 2013. For all other website addresses cited in the rest of the book, this has to be considered the date of retrieval.

[2] http://www.forbes.com/sites/haydnshaughnessy/2013/04/17/who-are-the-top-50-social-media-power-influencers-2013/

2013. From its statistics, it's apparent that Facebook continues to grow and make profits via advertisements and mobile users (the number of people accessing the Internet via a mobile phone has increased by 60% in last two years), reaching the number of 1.2 billion active users in 2013. With an increase of 79% of active users, Twitter is the fastest growing social media. It has approximately 290 million active users per month. YouTube, with 1 billion unique monthly visitors, has doubled the hours of video watched in a year, from 3 to 6 billion hours. Also, Google+ is having a fundamental impact in social media: it is, at the time of writing this book, the second largest social network with a growth of 33% in the number of its active users from 2012 to 2013. Similarly, LinkedIn, the largest professional business network currently available, continues to grow at a similar pace to that of Twitter or Google+—it has been estimated that two new users join LinkedIn every second.

The provided statistics show the importance that social media has and will have on society today and in the future. In particular, as can be seen from the rank of the most successful social media sites, these all belong to the category of social network services. For these reasons, and in order to understand how their technologies support the Social Web paradigm, in this chapter we start introducing *sociological aspects* connected to (offline) social networks as a way to build virtual communities (Section 1.2), and we then discuss *technological aspects* connected to (online) social network services (Section 1.3). Once these general concepts are clarified, the reader will be able to better understand which are the *security issues* connected to the use of social network services. We first introduce these issues in Section 1.4 and we discuss them in detail in Chapters 2, 3, and 4. Finally, in Chapter 5, we draw the conclusions and illustrate some of the most promising research directions in the discussed fields.

1.2 SOCIAL NETWORKS

According to the definition provided by Wasserman and Faust in [275], a *social network* is "a social structure made up of a set of *social actors* (such as individuals or organizations) and a complex set of the *dyadic ties* between these actors (such as relationships, connections, or interactions)."

The development of the so-called Web 2.0, and the consequent possibility for users to interact and collaborate with each other in a *virtual community*, has led to some ambiguity in the use of the term "social network" that is, first of all, a real-world social connection. For this reason, the term *offline* social network (or community) is often used to differentiate a real-life social network/community from a web-based one, known as *online* social network (or community).

1.2.1 THE MEANING OF COMMUNITY

First attempts to define the concept of *community* date back to the 19th century, with the studies of the theorists Tönnies and Loomis [263], Toqueville [80], and Durkheim [86]. These theorists follow the desire for a pre-modern society; in this scenario, a community can be described as "a private and intimate place that stands for the basic needs of individuals" (e.g., warmth, shelter, nurture), whereas *society* is seen as a more rational and purposeful place [168].

In current literature, the *existence* and utility of the concept of community is debated. In particular, the *focus* of community varies from domain to domain: it is a cultural construct or social context for sociologists; in psychology, the individual members of a community are emphasized; and anthropologists concentrate on interaction among the members of a community. With such wide-ranging and diverse interpretations, the concept of community is definitely an ambiguous and abstract concept. According to post-modernists, it is only a diluted concept unsuitable to describe current society. Bauman [23], for example, sees community as an extension of the concept of *identity* (see Chapter 4 for a detailed treatment of concepts connected to identity).

Other authors have a different vision. Turner, for example, sees community as an opposition to *structure*, an expression of the *social nature* of society [82]. He calls *liminality* the expression of such a community. Liminal moments refer to life events not subjected to instrumental rationality which create a powerful bonding between members of society. In this vision, one obtains a feeling of belonging and relating to others when not being subjected to rules, laws, norms, etc. Then, when interacting with others, members of the community reveal the community itself [5]. In his hermeneutic approach on community, Cohen defines it in terms of *particular kinds of awareness of reality*. As such, community is a "symbolization of boundaries by which the community differentiates itself from others" [82]. Lyon [193] reviews a plethora of definitions of community, noting that the vast majority enumerates three common qualities: *shared place*, *distinctive social interaction,* and *common ties*. These three qualities are not independent, but mutually reinforcing instead. They are theoretically distinguishable, and capture critical facets of what community is characterized for, as Nisbet observes [226]. Based on Lyon and other researchers' work, Carroll [55] proposes a conceptual model of communities, comprised of *collective identity*, *community engagement*, and *network of social ties*. According to [297], these three elements emphasize different underpinnings of communities: social identities as *psychological foundation*, social engagement as *behavioral manifestation*, and network of social ties as *structural depiction* of communities. Concerning the structural aspects of a community, Granovetters, in his famous paper "The Strength of Weak Ties" [126], affirms that ties connecting people should be measured in terms of *strength*: "the strength of a tie is a combination of the amount of time, the emotional intensity, the intimacy, and the reciprocal services which characterize the tie." A deeper analysis of this concept will be provided in Section 1.3.2.

Following these positive perspectives on communities, it is possible to divide the concept of community into two categories: *community of interest* and *community of place*. Community of place refers to a geographically fixed community. In contrast, a community of interest is based upon a common interest among members. It may be that both communities overlap each other. This indicates us that a community does not need to be anchored in a particular location, but can also exist virtually.

1.2.2 FROM OFFLINE TO ONLINE COMMUNITIES

As it emerges from the previous section, the ways the concept of community has been defined are diverse and, at times, vague. Despite this, the concept of community in the digital era is the basis for describing social interactions in the cyberspace. In this scenario, the absence of a spatial environment has raised issues on how communities in online environments have to be studied, detected, and investigated [296].

For these reasons, the main question we have to address when dealing with the concept of *online community* is about its effective existence (in terms of reality or virtuality) with respect to the "classical" offline community.

Thick and Thin Communities

According to Giddens [113], *virtuality* is a product of modernity that constantly "displaces" individuals from the places and everyday life with which they were familiar: individuals are re-located in different contexts, in which "familiarity and estrangement" are recombined. Similarly, Rheingold [239]—to our knowledge the first author having introduced the concept of *virtual community*—describes this concept connected to the Internet as an alternative reality, with capacities to transform society [82]. When referring to virtual communities, he only considers communities that are exclusively rooted in cyberspace. This means that, for him, virtual communities are "communities on the Net:" they do not have their counterpart in everyday life. Even further, the decline in real-world communities can be compensated by virtual ones [82]. In this vision, if virtuality is the opposite of reality, it follows that a virtual community on the Web cannot be regarded as the same as—or even similar to—a traditional offline community. Because the online environment can only provide the illusion of reality and because a virtual community exists online, thus it cannot be understood or even discussed as a real world community might be.

A different perspective about virtuality and reality is provided by Castells [60], who includes the concept of virtuality as a part of the real world. New communities like virtual ones are built out of networks of social actors (individuals, families, or social groups) [82]. In our global network society, spatial communities are replaced by spaceless ones in the virtual space (i.e., the Web). Castells affirms that "localities become disembodied from their cultural, historical, geographical meaning, and reintegrated into functional networks, or into image collages, inducing a space of flows that substitutes for the space of places." Social relations have not been changed due to the global network society itself; rather, they are modeled by the individualism inherent in society.

To sum up, in both authors" visions, communities can be defined as personalized communities embodied in networks and centered on the individual. But where Rheingolds refers to virtual communities as *thick*, Castells would definitely speak of *thin* communities. With "thin" we refer to a virtual reality that is an addition to the offline reality, whereas "thick" can be seen as an equivalent of the offline reality.

Thick communities are often composed of *strong ties*: frequent contacts between people who personally know each other. In this sense, examples of thick communities are groups of people working together or the components of the same soccer team. *Weak ties* are often related with thin communities: they are online ties between socially and physically distant people, not bound into work structures or circles of friends. Nowadays, thin communities have known an enormous growth since people are involved in the massive use of social network services.

1.3 ONLINE SOCIAL NETWORKS

According to the definition given by boyd and Ellison in [35], a *social network service* is "a web-based service that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from service to service."[3]

From this definition, we can observe that, in general, a social network service is characterized by the following properties:

- it is an *online* service, platform, or site that focuses on facilitating the building of *social networks* or *social relations* among people;
- people can *share* interests, activities, backgrounds, or real-life connections; and
- each user has a *virtual representation*, often a profile, plus his/her social links, and a variety of *additional services*.

Online community services are sometimes considered as social network services, although in a broader sense, social network services usually mean individual-centered service whereas online community services are group-centered. Despite this, in current dynamic digital society, a convergence between mass communication and personal communication is occurring. This convergence has been defined by Castells [61] as *mass self-communication*. As per [232], this concept is described as the composition of two aspects: "[…] on the one hand mass communication because social computing tools can potentially reach a global Internet audience. On the other hand self-communication because the message production is self-generated, the potential receiver(s) definition is self-directed and the message or content retrieval is self-selected." Hence, new social network services and tools for acting "socially" can be seen as an important fraction of mass self-communication. According to [38], social networks can serve multiple "public" purposes: "they can play a civic function, serving to gather people in a democracy. But they can also play a social role, enabling people to make sense of the world around them and understand their relationships to society."

From this moment on, and in the rest of the book, for the sake of simplicity (but not with abuse of terminology) we will refer to both kinds of services using the simple and widespread term of *online social networks* (OSNs).

[3] We replace the term "site," i.e., social network site, with the more generic term "service."

1.3.1 EVOLUTION OF ONLINE SOCIAL NETWORKS

Many early *online services*, including Usenet [136], ARPANET, LISTSERV, and bulletin board services (BBS), made some efforts to support the social network paradigm via *computer-mediated communication* (CMC) [273], at the end of the 1970s. The 1980s were dominated by other online services, such as America Online, Prodigy, and CompuServe, which also included some prototypical features of social networking services [246].

With the development of the World Wide Web in the 1990s, early services based on the social networking paradigm were developed in the form of *generalized online communities*. This was the case for example of theGlobe.com (1995), Geocities.com (1994), and Tripod.com (1995). These early online communities were essentially focused on bringing people together to interact with each other through *chat rooms*. They encouraged users to share personal information and ideas via *personal web pages*, by providing easy-to-use publishing tools and free or inexpensive Web space. Other online communities (e.g., Classmates.com) followed a different approach: they simply allowed people to link each other via *e-mail* addresses. In the late 1990s, thanks to the introduction of the concept of *user profile* as a central feature of social networking services, users started to have the possibility to compile lists of *friends* and search for other users with *similar interests*. By the end of the 1990s, new social networking methods were developed and many sites began to develop more advanced features to find and manage friends [190]. SixDegrees in 1997, followed by Makeoutclub in 2000, Hub Culture and Friendster in 2002 represented the first "new generation" social networking services, and soon became part of the Internet mainstream. Friendster was followed by MySpace and LinkedIn. The rapid increase in social networking sites" popularity was witnessed in 2005, by the fact that MySpace was getting more page views than Google.[4]

Nowadays, in addition to these basic technical features, online social networks are characterized by a variety of other characteristics. Some sites allow users to upload *multimedia content* (e.g., pictures, videos) or modify the look and feel of the profile. Users can participate in chat rooms, create chat rooms, hold private conversations, publicly interact with their friends commenting their *activities*. In addition to this, in certain OSNs, users are allowed to enhance their profile by adding *modules* or *applications*. This is, for example, the case of Facebook which, launched in 2004 and definitely affirmed in 2009, is currently the largest OSN [134]. According to Socialbakers.com, one of the biggest Facebook statistics portals in the world, at the time of writing this book the total number of users is closing in on 1 billion.[5] Hence, more ore less 1 out of 7 people in the world have a Facebook account.

Not only Facebook, but also Twitter, has acquired a large market share nowadays. Even if it is difficult to determine the precise number of users on Twitter, the number of "tweets per day" (TPD) give an indication of the usage of this medium. The average TPD in March 2010 was 50 million according to Twitter statistics. The average TPD in February 2011 was 140 million.

[4] http://www.businessweek.com/stories/2005-07-18/news-corp-dot-s-place-in-myspace/

[5] http://www.socialbakers.com/countries/continents/

In 2012, with over 200 million active users, over 400 millions tweets daily have been generated, handling over 1.6 billion search queries per day.[6] It is uncertain whether this trend will sustain itself over time. In fact, not so long ago other SNS like Friendster and Myspace, were considered as the revelation of 21st century. In May 2011, however, Friendster repositioned itself from a social network service to a social gaming site. Likewise, the number of MySpace users has declined immensely.[7] Like Friendster, Massive Media (the company behind Netlog), acquired by Meetic, has moved its scope to dating.[8] All these "old" social network services failed to compete with Facebook and Twitter. Maybe the future will bring the same destiny for Facebook and Twitter, maybe not.

Google+, the social network service of Google, is a new competitor in the OSN market. With 25 million users in 2011, Google+ has been the fastest website to reach that audience size[9] and it is currently the second largest social networking site in the world, having surpassed Twitter in January 2013.[10] In December 2012, it had a total of 500 million registered users, of whom 235 million are active in a given month. One of its main characteristics is the possibility given to users to create *groups* that share for example common interests or affiliations.

An emerging trend in many online social networks is connected to the concept of *real-time Web*. Real-time Web allows users to contribute contents, which is then broadcast as it is being uploaded (similarly to live radio and television broadcasts). This emerges clearly from Twitter wherein users can broadcast to the world what they are doing, and from Facebook with its "News Feed" and "Live Feed" plugins. News Feed is an aggregated and summarized view of friends" activities; Live Feed is a constantly updating real-time view of what people are doing.

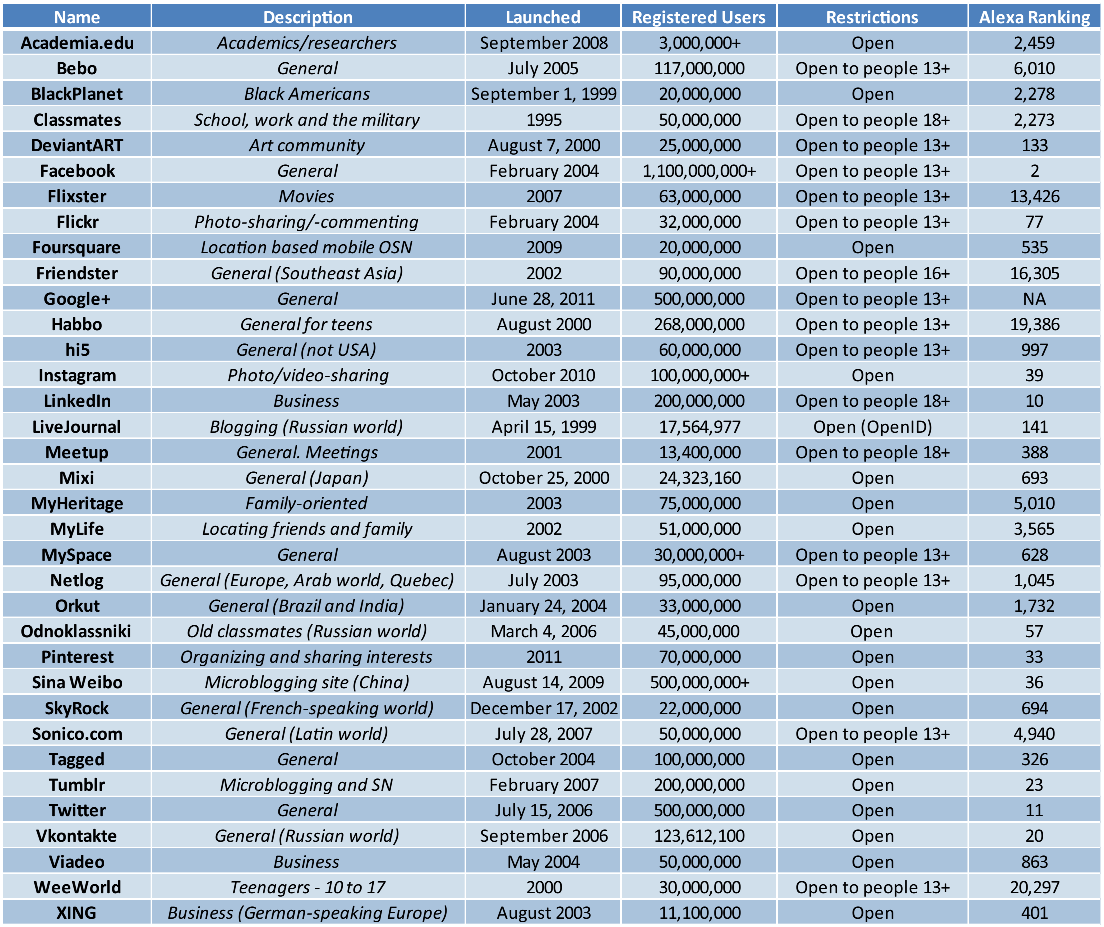
In addition to this "real-time" aspect, also the *location-based* one is receiving today growing attention from OSNs. Geosocial networking co-opts Internet mapping services to organize user participation around geographic features and their attributes. Foursquare gained popularity as it allowed for users to "check-in" to places that they are visiting at that moment. Gowalla is another such service that functions in the same way as Foursquare does, leveraging the phone GPS to create a location-based user experience.

From a business point of view, companies have begun to merge business technologies and solutions with social networking concepts. Instead of connecting individuals based on social interests, companies are developing interactive communities that connect individuals based on shared business needs or experiences. This is, for example, the case of LinkedIn.

Figure 1.2 summarizes some of the major online social networks used nowadays, taking into account (at the time of writing this book) those with a number of users higher than 1 million,

[6] http://www.techvibes.com/blog/twitter-users-tweet-400-million-times-2012-12-17/
[7] Statistics summary for myspace.com
[8] http://pulse2.com/2012/12/23/meetic-acquires-massive-media-for-25-million/
[9] http://in.reuters.com/article/2011/08/03/idINIndia-58589020110803/
[10] http://www.forbes.com/sites/anthonykosner/2013/01/26/watch-out-facebook-with-google-at-2-and-youtube-at-3-google-inc-could-catch-up/

and/or known at a worldwide level, and/or with a good global rank—according to Alexa,[11] a well-known provider of free global Web metrics.[12]



Name	Description	Launched	Registered Users	Restrictions	Alexa Ranking
Academia.edu	*Academics/researchers*	September 2008	3,000,000+	Open	2,459
Bebo	*General*	July 2005	117,000,000	Open to people 13+	6,010
BlackPlanet	*Black Americans*	September 1, 1999	20,000,000	Open	2,278
Classmates	*School, work and the military*	1995	50,000,000	Open to people 18+	2,273
DeviantART	*Art community*	August 7, 2000	25,000,000	Open to people 13+	133
Facebook	*General*	February 2004	1,100,000,000+	Open to people 13+	2
Flixster	*Movies*	2007	63,000,000	Open to people 13+	13,426
Flickr	*Photo-sharing/-commenting*	February 2004	32,000,000	Open to people 13+	77
Foursquare	*Location based mobile OSN*	2009	20,000,000	Open	535
Friendster	*General (Southeast Asia)*	2002	90,000,000	Open to people 16+	16,305
Google+	*General*	June 28, 2011	500,000,000	Open to people 13+	NA
Habbo	*General for teens*	August 2000	268,000,000	Open to people 13+	19,386
hi5	*General (not USA)*	2003	60,000,000	Open to people 13+	997
Instagram	*Photo/video-sharing*	October 2010	100,000,000+	Open	39
LinkedIn	*Business*	May 2003	200,000,000	Open to people 18+	10
LiveJournal	*Blogging (Russian world)*	April 15, 1999	17,564,977	Open (OpenID)	141
Meetup	*General. Meetings*	2001	13,400,000	Open to people 18+	388
Mixi	*General (Japan)*	October 25, 2000	24,323,160	Open	693
MyHeritage	*Family-oriented*	2003	75,000,000	Open	5,010
MyLife	*Locating friends and family*	2002	51,000,000	Open	3,565
MySpace	*General*	August 2003	30,000,000+	Open to people 13+	628
Netlog	*General (Europe, Arab world, Quebec)*	July 2003	95,000,000	Open to people 13+	1,045
Orkut	*General (Brazil and India)*	January 24, 2004	33,000,000	Open	1,732
Odnoklassniki	*Old classmates (Russian world)*	March 4, 2006	45,000,000	Open	57
Pinterest	*Organizing and sharing interests*	2011	70,000,000	Open	33
Sina Weibo	*Microblogging site (China)*	August 14, 2009	500,000,000+	Open	36
SkyRock	*General (French-speaking world)*	December 17, 2002	22,000,000	Open	694
Sonico.com	*General (Latin world)*	July 28, 2007	50,000,000	Open to people 13+	4,940
Tagged	*General*	October 2004	100,000,000	Open	326
Tumblr	*Microblogging and SN*	February 2007	200,000,000	Open	23
Twitter	*General*	July 15, 2006	500,000,000	Open	11
Vkontakte	*General (Russian world)*	September 2006	123,612,100	Open	20
Viadeo	*Business*	May 2004	50,000,000	Open	863
WeeWorld	*Teenagers - 10 to 17*	2000	30,000,000	Open to people 13+	20,297
XING	*Business (German-speaking Europe)*	August 2003	11,100,000	Open	401

Figure 1.2: Thirty five of the most popular social network sites currently.

1.3.2 ANALYSIS AND PROPERTIES

Initially emerging as a key technique in modern sociology, *social network analysis* (SNA) refers to nowadays the methodical analysis of both offline and online social networks. Social network analysis views social relationships in terms of *network theory*, which is based on the concept of

[11] Alexa. The Web Information Company. http://www.alexa.com/

[12] Retrieved September 15, 2013.
The rank is calculated using a combination of average daily visitors to this site and pageviews on this site over the past three months. The site with the highest combination of visitors and pageviews is ranked #1.

nodes (representing individual actors within the network) and *ties* (representing relationships between the individuals, such as friendship, kinship, organizational position, sexual relationships, etc.).

Social network analysis has been originally conducted via mathematical formalisms based on *graph theory* [20], normally used to analyze large real-world graphs such as the World Wide Web. Typically, according to Kumar et al. [173], studies on large graphs address structural properties of the graphs including their size, density, degree distributions, average distance, clustering coefficient, connected components, community structures, etc. Several other studies have also shown that the average diameter of the web is quite small [3, 8]. In the Web 2.0 era, other characteristics must be taken into account to examine network dynamics. For instance, online friendship and email graphs have been studied to explain and demonstrate *homophily* properties [9, 11, 208] of these graphs, and the so-called *small-world phenomenon* [169, 276] characterizing them. A number of papers focus also on the spread of *influence* through friendship networks [13, 164].

Homophily According to [10, 252], *homophily* is the tendency of individuals to choose friends with similar characteristics. This means that people's personal networks tend to be homogeneous with regards to many socio-demographic, behavioral, and intra-personal characteristics. Homophily limits people's social worlds in a way that has powerful implications for the information they receive, the attitudes they form and the interactions they experience. McPherson et al. [206] affirm that homophily implies that distance in terms of social characteristics directly translates into network distance, i.e., the number of relationships through which a piece of information must travel to connect two individuals. It also implies that any social entity that depends to a substantial degree on networks for its transmission will tend to be localized in social space and will obey certain fundamental dynamics as it interacts with other social entities in an ecology of social forms.

Exploiting homophily, Mislove et al. [208] gather fine-grained data (associated with certain users) from two crawled subsets of Facebook (the Rice University Facebook network and the New Orleans Facebook network) and try to infer (other) user profile attributes. They effectively find that users with common attributes are more likely to be friends and often form dense communities. They also show that, with as little as 20% of the users providing attributes, it is often possible to infer the attributes for the remaining users with over 80% accuracy. Similarly, Akcora et al. in [11] describe a technique that facilitates finding user similarity without observing an important fraction of the network. They propose measures for evaluating social network users according to both their connections and profile attributes. Moreover, since user profile data could be missing, they present a technique to infer them from profile items of a user's contacts. For observing how profile and network similarity interact, they first carry out experiments on a DBLP data set[13] enriched with profile data from the ACM digital library.[14] They look into re-

[13] DBLP is a Computer Science bibliography website hosted at Universität Trier, Germany. \http://dblp.uni-trier.de/

[14] The ACM Digital Library is the full-text collection of all articles published by the Association for Computing Machinery in its articles, magazines, and conference proceedings. http://dl.acm.org/

searcher interactions based on their network and profile similarities and, finally, they show how their technique can be used to infer missing profile items performs on Facebook real data.

Small-world Phenomenon The *small-world phenomenon* was originally identified in 1967 by Milgram [207], describing the famous "six degrees of separation" between any two people in the world. In his 2003 work [276], Watts investigates the small-world phenomenon from a computer science point of view, presenting an average length of completed chains of four hops. This vision of our world as a "small world," where everyone is connected to each other with a small chain of average 4/6 people in-between, has been contested by Kleinfeld [169]. According to author, rather than being one highly connected small world, our world consists of many loosely connected and some disconnected small worlds. In her work, she reviews several studies conducted on the small-world phenomenon and its variations. Her study reveals low chain completion rates in almost all of the experiments, suggesting that a vast majority of people in the world are very disconnected, contrary to the believers of "small world." In addition, one recurring conclusion in these studies is that connections are weak outside racial, socio-economic and geographic boundaries. This reinforces the homophilous nature of friendship relationships that allows the creation of these numerous small worlds. Along this line, considering the small world represented by Facebook, Backstrom et al. [17] in 2011 found that its graph is composed of short paths between many pairs of nodes (as effectively happens in small worlds). They also found that the average distance of Facebook is 4.74, that is, 3.74 degrees of separation, and that the spid[15] of Facebook is 0.09, as expected for a social network. Finally, their analysis shows that geographically restricted networks have a smaller average distance, as it happened in Milgram's original experiment.

Influence Summarizing the definitions provided in [10], *influence* refers to the phenomenon that the action of individuals can induce their friends to act in a similar way. This effect is at work in many settings, where new ideas diffuse by word-of-mouth or imitation through a network of people: an example for their friends (as in the case of fashion), informing them about the action (as in the case of viral marketing), or increasing the value of an action for them (as in the case of adoption of a technology).

Research on influence in OSNs has addressed in particular the study of the spread of influence through social network models [65, 164]. For instance, as a problem of influence maximization, it deals with choosing the optimal set of nodes in a social network so as to maximize the resulting spread of a technology (opinion, product-ownership, etc.), given a model of diffusion of influence in a network [32].

1.3.3 MULTIPLE SOCIAL TIES AND SOCIAL CAPITAL

Social network analysis techniques, and in general much of past work on online social networks, have focused only on *single social ties* (e.g., friends or not) characterizing social environments. These binary indicators provide only a coarse indication of the nature of the relationship. Due to

[15] The spid (shortest-paths index of dispersion) is the variance-to-mean ratio of the distance distribution.

the ease of friendship identification in online social networks and the high cost of measuring the variance of interactions in online communities, often social network analysis had not taken into account information differentiating social relationships. In this way, treating all relationships as equal, the models are often characterized by noisy/imprecise results and likely lead to degradation in performance [283].

Multiple Social Ties As stated by Granovetter in [126], social networks contain *multiple* kinds of ties, that he divides into *strong* and *weak ties*. Their importance changes depending on a variety of social phenomena. This concept is now widespread in literature (e.g., in [120, 283]). Technically speaking, the possibility of expressing semantically differentiated social connections among entities has been first addressed by the FOAF (Friend of a Friend) project in the Semantic Web field.[16] The FOAF project is a community driven effort to define an RDF vocabulary for expressing metadata about people, and their interests, relationships and activities. Anyone can use FOAF to describe her- or himself. FOAF allows groups of people to describe social networks without the need for a centralized database. Although it is a relatively simple and standard, FOAF has had limited adoption on the Web. Nowadays, major online social networks such as Facebook, Google+, Myspace, and, in a different way, Twitter, as well as e-commerce websites like Amazon, have developed infrastructures allowing users and their resources of being represented on graphs connecting different entities with multiple kinds of relationships. Technically speaking, Facebook has developed the Open Graph protocol,[17] an RDFa-based protocol enabling any web page to become a rich object in a social graph by adding to it basic RDFa metadata. In the same way, Google+ and Myspace (together with a number of other social networks) follows the OpenSocial public specification.[18] This is instrumental to provide users with the possibility to increase their interactions with other users, as well as resource sharing, in the most possible personalized and semantically meaningful way.

Social Capital The concepts of strong and weak ties described above, and the dynamic interactions happening via these multiple social relationships, bring forward another important concept related to online communities, i.e., *social capital* [22]. In sociology, Bourdieu and Putnam are probably the most prominent authors on this topic. Bourdieu stresses *individual* aspects in his definition of social capital, seen as "the aggregate of the actual or potential resources which are linked to possession of a durable network of more or less institutionalized relationships of mutual acquaintance and recognition" [34]. Putnam defines social capital according to *collective* aspects, as composed of those "features of social organization such as networks, norms and social trust that facilitate coordination and cooperation for mutual benefit" [234]. Broadly speaking, social capital consists of the expected collective or economic benefits derived from the preferential treatment and cooperation between individuals and groups. In the Web 2.0 scenario, it is fostered by the

[16] The Friend of a Friend (FOAF) project. `http://www.foaf-project.org/`
[17] The Open Graph protocol. `http://ogp.me/`
[18] The OpenSocial Foundation. `http://opensocial.org/`

possibility to maintain long-term contacts with people via weak as well strong ties. Which of these ties contribute more to social capital is a debated topic.

Putnam [234] distinguishes between *bonding* and *bridging* social capital. The former is found between individuals connected by strong ties (e.g., emotional support or access to scarce resources). The latter is linked to loose connections between individuals who may provide useful information or new perspectives for one another but typically not emotional support, i.e., the weak ties defined by Granovetter in his paper on the strength of weak ties [126]. In this paper, this latter author states that weak ties are more important in some situations, such as, for instance, looking for a job. Granovetter, after interviewing job seekers, posited that it was because one's close friends tie one back to jobs and job leads that s/he already knew about, whereas weak ties connected one to jobs that s/he had not heard of. He affirms that weak ties are more likely related to sparse networks. Hence, users that are loosely connected within virtual communities can access remote regions and obtain new and non-redundant information. In contrast, dense networks (dominated by strong ties) facilitate frequent, reciprocal, and supportive contact. So, whether or not virtual communities can be labeled as thick or thin, both seem to be important for different reasons.

In his book on virtual communities [239], Rheingold states more or less the same concepts, affirming that: "A social network with a mixture of strong ties, familial ties, lifelong friend ties, marital ties, business partner ties, is important for people to obtain the fundamentals of identity, affection, emotional and material support. But without a network of more superficial relationships, life would be harder and less fun in many ways. Weaker ties multiply people's social capital, useful knowledge, ability to get things done." Following this "optimistic" vision, weak ties in virtual communities enable users to engage and interact with a variety of other users that do not necessarily share the same interests and environments, expanding users' horizon. At the same time, virtuality offers the possibility of bringing offline contacts to online environments, thus extending the possibilities of communications.

Moreover, another author, Calhoun, assigns importance to these mediated relationships, although with a more pessimistic view, stating that we should not exaggerate on these forms [82]. Offline communities are supplemented by virtual ones, rather than substituted. Calhoun has a rather negative view on the capacity of virtual communities to enhance participation, due to compartmentalization in communities: "we are aware of others but not in discourse with them" [46]. This leads to categorization of individuals. This view anticipates the principle of the *filter bubble*, introduced by Pariser [230], which is an effect of the Internet when tailored to the personal identity of the individual, isolating him/her from other perspectives.

Brunie [42] has a more collective perspective with respect to Calhoun. For her, interactions play an important role in defining and measuring social capital. In an online community, social capital refers to "the value derived from the interactions that provide support for bonding between like-minded people." Based on this definition, Sherchan et al. [252] define the social capital of an online community as "the density of interactions that is beneficial to the members of the community."

Independently from the way we consider the effects of social capital, it is a fact that in "real" online social networks such as Facebook, LinkedIn, and Twitter, social capital represents a fundamental reason (among others) behind users' engagement in spreading personal information. First studies from this perspective have been done by Ellison et al. [90] on Facebook, where authors describe social capital as "the resources accumulated through the relationships among people." In the paper, they primarily discuss bonding and bridging social capital. According to their findings, there is a significant connection between how intensely an individual uses a social networking site and her/his perceived bridging and bonding of social capital. In the post "Social Capital and Use of LinkedIn"[19] by Brad Bainum on his blog at the Bowdoin College, the author highlights how joining LinkedIn fulfills the definitions of bonding and bridging social capital. This is due to the site's explicitly defined purposes: the re-discovery of lost relationships with former co-workers and classmates, the acceleration of current job hunting and career prospects through realization of "inside connections," and the answering, by relevant experts, of any questions a user might have (from the LinkedIn Corporation). According to Bainum, LinkedIn and other social network services designed for professional networking, help users in expanding their professional and academic social networks by identifying "latent ties," converting them to weak ones, and growing their bridging social capital in the process. "The more ubiquitous that social networking sites become, the larger the resulting gains in social capital for active users." In their work on Twitter, Recuero et al. [236] explore users' perceptions of the way social capital influences retweet practices. Retweets not only share information with a particular group, but they also allow for other users (those originally posting the information) to become visible to the group where tweet is shared. Therefore, authors highlight that retweets play an important part in gathering social capital not only for individual users, but also from a collective point of view. The motivations for users to select the tweets they will copy, and how they may be modified, can influence how information diffuses and what types of values the social network can have access.

1.4 SECURITY ISSUES IN ONLINE SOCIAL NETWORKS

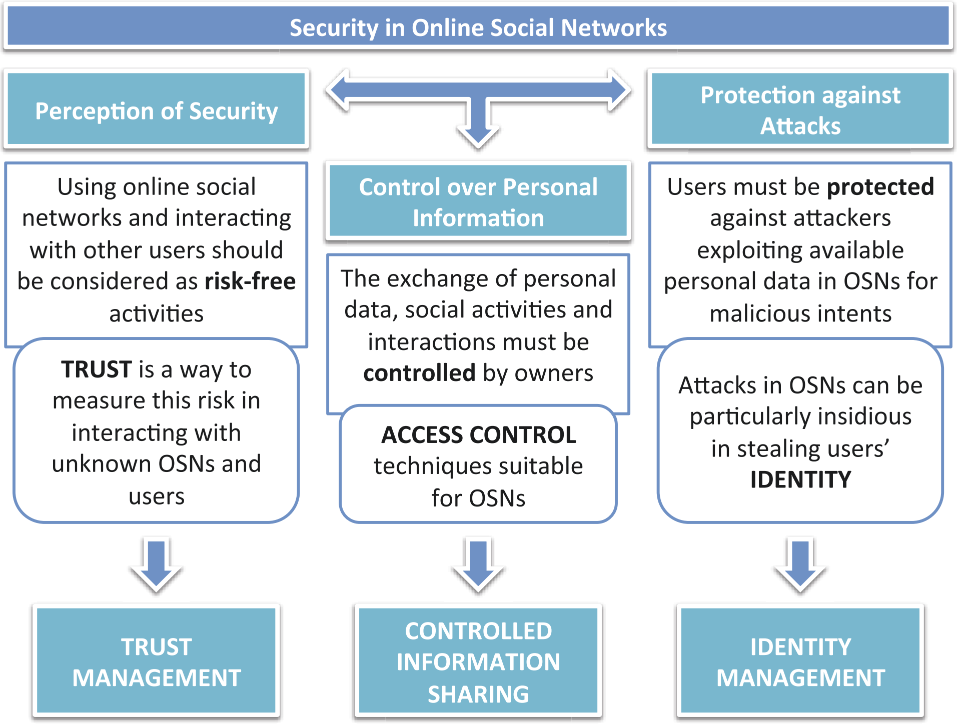
The success of online social networks, the big amount of personal information they manage, the big economic upturn connected to their commercial use, the strict interconnection among users, and resources characterizing OSNs and provided are the main factors making online social networks critical applications with respect to the *security* of their users and resources. In particular, the term "security" in online social networks raises issues with respect to three main aspects, and must provide solutions to the connected users' requirements:

(i) the users' perception of security, defined as the extent to which a user believes that using a OSN application and interacting with other users are risk-free activities (e.g., [110, 240, 253]): How to measure users' safety when interacting with unknown/little-known parties?;

[19] http://learn.bowdoin.edu/courses/sociology-022-fall-2010-bbainum/2010/10/social-capital-and-use-of-linkedin/

(ii) the control over the flow of users generated information, including the transfer and exchange of that information (e.g., [111, 129]): How to protect users' data confidentiality in the OSN scenario where the spread of personal information is at the bases of any social network functioning?; and

(iii) the users' protection with respect to the use of their profiles (in particular personal data) for malicious purposes (e.g., [29, 129]): How to avoid identity theft attacks from malicious entities?


Security in Online Social Networks

Perception of Security

Using online social networks and interacting with other users should be considered as **risk-free** activities

TRUST is a way to measure this risk in interacting with unknown OSNs and users

TRUST MANAGEMENT

Control over Personal Information

The exchange of personal data, social activities and interactions must be **controlled** by owners

ACCESS CONTROL techniques suitable for OSNs

CONTROLLED INFORMATION SHARING

Protection against Attacks

Users must be **protected** against attackers exploiting available personal data in OSNs for malicious intents

Attacks in OSNs can be particularly insidious in stealing users' **IDENTITY**

IDENTITY MANAGEMENT

Figure 1.3: Security aspects in online social networks and solutions of specific issues treated in the book.

These aspects are specifically conjugated, in this book, according to three specific research issues. How they reply to the three security questions connected to aspects (i), (ii), and (iii) is described in detail in the following, and tautly illustrated in Figure 1.3.

- We treat aspect (i) with a focus on users' interactions, in particular when getting into contact with unknown parties. In online social networks, a huge number of interactions are just virtual; people connected in an online community often have never met before establishing a relationship (see [260], for example). However, as discussed along the chapter, users continuously establish virtual relationships with never-met people, accepting associated risks against the possible benefits they are convinced to obtain. In this scenario, correctly understanding the risks/benefits associated with the establishment of new relationships/interactions becomes fundamental for users' personal safety. The well-known, valid, and suitable measure for this is *trust*, whose definition perfectly fits with the OSNs scenario. In fact, according to Mayer et al. [203], trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." We are convinced that, in OSNs, *trust management* represents a crucial dimension in (safely) interacting and developing new relationships with other (possibly unknown) parties.

- In order to reduce the risks connected to the spread of users' personal information, there must be a way for users to have a direct control over how their information flows. This is possible by adopting access control techniques, extensively studied in traditional information systems [98]. With respect to traditional environments, in online social networks personal information is not only connected to user profiles, but spans across users' social activities and interactions. For these reasons, in this book we treat aspect (ii) by focusing on *controlled information sharing*. We have to underline the fact that controlled information sharing is not sufficient to fully protect users' privacy with respect to data inference techniques. Access control should be complemented with privacy preserving techniques specifically tailored to OSNs. These aspects are treated in other Morgan & Claypool books, for example the works of Wong and Fu [281] and Zheleva et al. [301].

- Concerning aspect (iii), the large amount of information published (and often publicly shared) on user profiles is increasingly attracting the attention of attackers. Attacks on social networks are usually variants of traditional security threats (such as malware, worms, spam, and phishing). However, these attacks are carried out in a different context, by leveraging the social network as a new medium to reach the victims, often stealing users' identity. This way, exploiting the trust relationships between "friends" in social networks, adversaries can craft more convincing attacks, by taking advantage of personal information gleaned from victims' pages. In this scenario, a correct *identity management* strategy can protect online social networks from identity theft attacks. In general, the term *identity management* describes the management of *user identities* via "hard security" mechanisms, such as authentication and authorization. However, the spread of Web 2.0 technologies has led to the development of the concept of *online identity management* (OIM), which will be discussed in this book .

1.4.1 TRUST MANAGEMENT IN ONLINE SOCIAL NETWORKS

Past research has dealt with the problem of *trust management* in open and centralized/decentralized systems [63, 118, 139], developing the concept of *Web of trust* [119]. Essentially, in a "Web of trust," each participant is allowed to express the degree of its trustworthiness in others, which helps the community in deciding which participants to be trusted or not trusted, without prior interaction [130].

Most of the current work in the area of trust management connected to online social networks addresses the problem of estimating how much users in an OSN can trust reciprocally, in a scenario where it is extremely unlikely that any two will know one another. Participation in the network, as well as knowing personal information of users, offer one mechanism for estimating *social trust*.

Various techniques have been proposed to compute/manage social trust in OSNs: *structure-based* (in most of the cases based on trust propagation), *interaction-based* (exploiting trust prediction), and *hybrid* techniques.

A survey of these techniques, together with an overview of trust management issues in OSNs, will be detailed in Chapter 2.

1.4.2 CONTROLLED INFORMATION SHARING IN ONLINE SOCIAL NETWORKS

Traditionally, the way to prevent unauthorized operations (such as read and write) on the managed information relies on access control techniques. The Morgan & Claypool book by Ferrari [98] addresses this issue. In the particular case of online social networks, new access control solutions are necessary with respect to what has been proposed so far, due to the several and unique characteristics of OSNs. For instance, according to [66], to prevent users from the spread of confidential contents, an OSN system should implement an access control model that is able to collect users-specified partial policies, along with the system-specified policies and fuse them for the overall control decision.

Nowadays, access to resources in OSNs is typically controlled based on the relationships between the accessing entities (users and resources) and the controlling entity of the target. This type of *relationship-based access control* (ReBAC) [111] takes into account the existence of a particular relationship or a particular sequence of relationships between users and/or resources and expresses access control policies in terms of such *user-to-user* (U2U), *user-to-resource* (U2R), or *resource-to-resource* (R2R) relationships.

Besides the definition of suitable access control models to express the variety of access control requirements that OSN users may have, it is fundamental to define suitable architectures that support proper access control enforcement. Indeed, the traditional centralized way of performing access control does not fit well in the OSN scenario. This is due in particular to the threats to users' confidentiality and privacy that this solution may involve; semi-decentralized/decentralized solutions allow users to have more control over their own data [289].

In Chapter 3, taking into account both commercial and non-commercial proposals, we will discuss in detail the ReBAC paradigm and the importance of relationships and their properties for access control in OSNs.

1.4.3 IDENTITY MANAGEMENT IN ONLINE SOCIAL NETWORKS

The spread of Web 2.0 technologies has lead to the development of the concept of *online identity management* (OIM). OIM can refer to: (i) *online image management*, *online personal branding* or *personal reputation management*—a set of methods for generating a distinguished Web presence of a person on the Internet—and (ii) *identity exposure/disclosure* and *identity theft*: a way to protect the management of digital identities in online social networks [266]. Avoiding identity exposure/disclosure deals mainly with *privacy-preserving social network data mining* [282], whose boundary is essentially constituted by social network analysis. In this book, we are more interested in the treatment of security issues which emerge when users actively exploit social network services. In this sense, we do not treat identity exposure/disclosure (instead, please refer to [281, 301]), but we concentrate on identity theft attacks which can be particularly insidious in OSNs with respect to those committed in other scenarios, just because the social networks themselves are used as a new and "trusted" medium to reach the victims.

In Chapter 4, we will introduce general concepts connected to (online) identity management and we will discuss in detail concerns and solutions connected to online social networks and identity.

CHAPTER 2

Trust Management in Online Social Networks

2.1 INTRODUCTION

Trust has been recognized over the years as a central topic in many aspects of human life [132, 204, 209]. Because trust is considered so important, it has been studied in many disciplines other than Computer Science, including Psychology, e.g., by Rotter [241], Erikson [92], Cook et al. [75]; Sociology, e.g., by Coleman [72], Helbing [138], Molm et al. [212], McKnight et al. [205], Mollering [211]; Economics, e.g., by Zucker [303], Dasgupta [78], Huang [141].

In Psychology, following the definition provided by Rousseau et al. [242], "trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another." This means that an individual, the *trustor*, accepts the *risk* of being vulnerable to another individual, the *trustee*, based on the trustor's expectation that the trustee will not betray her/his risk-assuming behavior [241, 242, 252]. In this field, trust is considered to have three aspects: cognitive, emotive, and behavioral. The cognitive aspect involves a rational decision to place trust in a trustee (based on the trustor's evaluation of the trustee). The emotive aspect involves a non-rational, emotional drive to place trust in a trustee. Finally, the behavioral aspect refers to committing some action that makes the trustor vulnerable to the trustee [26, 250]. The importance of these psychological aspects when dealing with trust management in online social networks will be discussed in Section 2.3.2.

When dealing with Sociology, the position and role of trust are analyzed in the context of *social systems*, where individuals can act singly or within a social context. At the *individual level*, similarly to psychology, the main aspect characterizing trust is the vulnerability of the trustor with respect to the trustee [75, 212, 242]. In particular, it is the contingency of the future creating dependency between social actors (the trustor is dependent on the trustee). According to Mollering [211], trust is one of the possible methods to resolve such a dependency, being an attractive alternative to control. At the *societal level*, trust is considered to be a property of social groups and it is represented by a collective psychological state of the group. Social trust implies that members of a social group act according to the expectation that other members of the group are also trustworthy and, therefore, they expect trust from other group members [252]. As emerges from this brief description, social trust is a main concept in online social networks and will be discussed in detail in Section 2.3.3.

In Economics, trust is treated both as a measure of the difference between actual human behavior and the one individuals keep to maximize utility, and as an economic lubricant, reducing the cost of transactions between parties, enabling new forms of cooperation and generally furthering business activities, employment, and prosperity [214]. When referring to online social networks, both perspectives deal with the concept of *social capital* [211], already discussed in Section 1.3.3, and deeply investigated with reference to trust in Section 2.3.3. Concerning the ways trust is built in economic scenarios, Zucker [303] examined the evolution of the trust mechanism in American economic system, and identified three modes of trust building: *process-based*, in which trust is built on past history of interaction; *characteristic-based*, in which trust is dependent on "social similarity," such as culture, age, and gender; and *institutional-based*, in which trust is built on "formal social structure" comprising of "membership in a subculture" and "intermediary mechanism," such as regulation, legislation, functions of governments, and banks.

In Computer Science, trust has been studied in many different areas, where the term trust has initially been defined by Marsh [200]. In security and access control contexts [154], it has been used connected to authentication, identity, and authorization. In those contexts, trust has often been formalized with logical models [142, 157]. Then, it has been rapidly applied to other areas, such as: electronic commerce [39], reliability in distributed systems and reputation systems [237], game theory [255], multi-agent systems [59, 94], and policies for decision making under uncertainty [254]. The concept of trust in these different disciplines varies in how it is represented, computed, and used. Several definitions have been provided considering trust from different perspectives, and these definitions may not be directly applicable to online social networks. In these environments, trust is, in general, a measure of confidence that an entity or entities will behave in an expected manner. In online social networks, the majority of studies focused on trust use formal methods which are mathematically based techniques for the specification, development, and verification of online systems. The studies are mainly focused on algorithms [121] or frameworks [63] that provide users of online social networks with trust ratings [108].

In this chapter, after having discussed general concepts connected to trust and trust management in Computer Science (Section 2.2), we will focus on online social networks (Section 2.3), providing a complete and detailed view on the techniques that have been proposed to manage trust in this scenario (Section 2.3.4).

2.2 TRUST IN COMPUTER SCIENCE

According to the literature [16, 31, 156, 252], trust in Computer Science can be classified into two general broad categories, depending on whether it refers to *systems* or *users*. The first category consists of security mechanisms involving *policies*, which describe the conditions necessary in a system to obtain trust. The second category is based on trust values (direct or recommendations) gathered and shared by users in a distributed community, via *trust and reputation systems*. In the following sections, this second category will be analyzed in detail compared to the first one, since it is more relevant for the aims of this book.

2.2.1 TRUST AND POLICIES

The standard notion of trust connected to *systems* refers, according to Yao et al. [288], to "the expectation that a device or system will faithfully behave in a particular manner to fulfill its intended purpose." The notion of "system" trust is supported by both software- and hardware-based solutions. These solutions, according to Bonatti et al. [31], follow a "strong and crisp" approach based on *security* mechanisms to create "trusted," or rather, trustworthy, systems that overcome technical failures as well as malicious attacks. In this kind of *policy-based* trust management, we can describe the conditions necessary to obtain trust, and we can also prescribe actions and outcomes if certain conditions are met. Policies frequently involve the exchange or verification of credentials, which are information issued (and sometimes endorsed using a digital signature) by one entity, and may describe qualities or features of another entity [16].

Blaze et al. [30] propose a comprehensive trust management scheme called PolicyMaker and present their trust management policies, which specify the trusted behaviors and trust relationships. Kagal et al. [159] present a security policy responsible for assigning credentials to entities, delegating trust to third parties, and reasoning about users' access rights. The Kerberos system [170] uses a third party to facilitate the exchange of credentials (digital signatures) between a user and a computer. Kerberos does not determine access rights, but instead enables two parties to securely exchange verifiable credentials. In the field of pervasive computing, interesting works are those of Kannadiga et al. [161] (intrusion detection within pervasive computing environments), Weis [277] (security of human–computer interactions), and Yuan et al. [294] (a pervasive computing security system based on human activities analysis). Works based on a public key infrastructure are those of Khalili et al. [165] and Ngai and Lyu [221]. The first one discusses the issues of key distribution in ad hoc networks and proposes a flexible key distribution mechanism using threshold cryptography. The second one provides a public key authentication service based on a trust model to monitor malicious and colluding nodes, allowing mobile nodes to monitor and rate each other with an authentication metric. The trust value can be updated in conjunction with public key certification.

This vision of trust based on traditional policy-based mechanisms has been criticized since security, according to Osterwalder [229], does not necessarily imply trust on its own. Treating all participants as potential attackers and taking corresponding protective measures, can be incorrect and expensive. In their work, Nielsen and Krukow [225], based on the fact that we cannot ever know everything about everyone, determine access control on the basis of a user's level of trust, based on recommendations from others about that user. This work provides a formal policy language in which trust can be proved and takes into account referrals which are at the base of trust and reputation systems, that will be discussed in the next section.

Some argue that security is not even a component of trust. For example, Nissenbaum [227] states that the level of security in a system does not necessarily affect trust. On the other hand, people are certainly more willing to engage in e-commerce if they are assured that their credit card numbers and personal data are cryptographically protected [114].

2.2.2 TRUST AND REPUTATION SYSTEMS

The notion of trust involving *users* is derived from Psychology and Sociology by Marsh [200] and Mui et al. [216], with a standard definition according to which trust is "a subjective expectation an agent has about another's future behavior based on the history of their encounters." This implies that trust is inherently subjective and relational. This is, for instance, confirmed by the probabilistic definition of trust provided by Gambetta [109], and by the cognitive definition of trust provided by Castelfranchi and Falcone [58]. According to the probabilistic one, trust is "the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends." Jøsang et al. [156] refer to this definition as *reliability trust*, since it includes the concept of dependence on the trustee, and the reliability of the trustee, as seen by the trustor. According to the cognitive definition, trust is "a mental state, a complex attitude of an agent x towards another agent y about the behavior/action relevant for the result (goal) g." Both probabilistic and cognitive definitions share that trust is based on a *directed relationship* established from a trustor to a trustee (as in the Rousseau definition [242]). Their *interdependence* is characterized by the fact that: (i) the interests of the two parties are related, and (ii) they cannot be achieved without relying on each other. However, the relationship is not a trust relationship if these two conditions do not exist. So, as two members interact with each other frequently, their relationship strengthens and trust evolves based on their experience. Trust increases between members if the experience is positive and decreases otherwise. According to Nielsen [224], trust can be lost quickly: "[trust] is hard to build and easy to lose: a single violation of trust can destroy years of slowly accumulated credibility." In addition to interdependence, the *risk* aspect connected to interactions among users have to be taken into account. Castelfranchi and Falcone [94] state that "it is possible that the value of the damage per se (in case of failure) is too high to choose a given decision branch, and this independently either from the probability of the failure (even if it is very low) or from the possible payoff (even if it is very high). In other words, that danger might seem to the agent an intolerable risk." From this definition, it emerges that having high (reliability) trust in a person, in general, is not necessarily enough to decide to enter into a situation of dependence on that person. For this reason, in addition to the already discussed concept of reliability trust, Jøsang et al. [156] also introduce the concept of *decision trust* (inspired by McKnight and Chervany [204]), as "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible."

In this field, according to Bonatti et al. [31], trust management follows a "soft and social" approach, based on trust values gathered and shared by a distributed community. In this sense, trust can be *direct* or based on *recommendations*. Direct trust is based on the direct experience of the member with the other party. Recommendation-based trust is connected to *reputation*. Sabater-Mir et al. [245] describe reputation as a social evaluation of a target entity attitude towards socially desirable behavior which circulates in the society (and can be agreed upon or not by each one of the entities in the society). In addition to this, according to Artz and Gil [16], reputation is an assessment based on the history of interactions with, or observations of, an entity, either directly with the evaluator (personal experience) or as reported by others (recommendations or third party verification). Recommendations may be received through a chain of friends network, so the problem for the user is to be able to evaluate various types of trust opinions. *Collaborative filtering* techniques are the most popular methods used in *recommender systems*. The task in collaborative filtering is to predict the utility of items to a particular user based on a database of user rates from a sample or population of other users. Unfortunately, a collaborative filtering system poorly performs when there is insufficient previous available common rating between users; this is commonly known as *cold start* problem [176].

To overcome this problem, the introduction of purely trust-based approaches to recommendation has emerged. These approaches assume a trust network among users and make recommendations based on the ratings of the users that are directly or indirectly trusted by the target user. A general characteristic of *trust systems* is that they can be used to derive local and subjective measures of trust, meaning that different agents can derive different trust in the same entity. On the contrary, *reputation systems* provide global reputation scores, meaning that all the members in a community will see the same reputation score for a particular agent. Another characteristic of trust systems is that they can analyze multiple hops of trust propagation/transitivity, whereas reputation systems normally compute scores based on direct input from members in the community, which is not based on propagation/transitivity [28].

In the literature, there are systems that have characteristics of being both a reputation system and a trust system. In particular, the multi-agent system paradigm and the huge evolution of e-commerce are factors that contributed to the increase of interest on trust and reputation. Theoretically speaking, Marsh was the first in [200] to address the issue of formalizing trust as a computational concept in multi-agent systems, proposing a high-level model based on social and psychological factors. Also, Castelfranchi and Falcone [58] provided a good analysis of what should be taken into consideration to develop trust, how that relates to previous experience, as well as giving descriptions of when trust is rational and irrational. As in Marsh's work, Castelfranchi and Falcone theoretical approach includes many psychological factors in developing a model for trust in multi-agent systems. The more recent and implemented techniques which are at the basis of trust and reputation models can be classified using many different dimensions [156, 191, 233, 252]. Using this classification, we distinguish between *numerical/statistical* and *machine learning* techniques, *heuristical* techniques, and *behavioral* techniques. Numerical/statistical and machine learning techniques focus on providing mathematical models for trust management. Heuristical techniques focus on defining a practical model for implementing robust trust systems. Behavioral models focus on user behavior in the community.

Techniques involving simple summation or average of ratings [238], techniques based on more complex numerical functions [15, 77, 112], Bayesian systems [74, 216], and belief models [155, 291] are the major examples of purely numerical/statistical techniques. In Bayesian systems, binary ratings are used to assess trust by statistically updating the beta probability density functions. Using this approach, Mui et al. [216] propose a computational model based on sociological and biological understanding, able to calculate agent's trust and reputation scores across multiple contexts. In belief models, a consumer's belief regarding the truth of a rating statement is also factored into the trust computation. Various techniques combining beliefs can be adopted. For example, the Dempster-Shafer theory is employed by Yu and Singh in [291]. In their model, the information stored by an agent about direct interactions is a set of values that reflect the quality of these interactions. Only the most recent experiences with each concrete partner are considered for the calculations. When direct information is available, it is considered the only source to determine the trust of the target agent. Subjective logic is used by Jøsang et al. [155]. They argue that subjective logic represents a practical belief calculus which can be used for calculative analysis of trust networks. Solutions based on machine learning typically exploit techniques such as Artificial Neural Networks (ANNs) and Hidden Markov Models (HMMs) for computing and predicting trust. For example, Song et al. (2004) use HMM for evaluating recommender trust, and ElSalamouny et al. (2010) propose a discrete HMM-based trust model.

Heuristics-based solutions, less complex than statistical and machine learning ones, aim to define a practical, robust, and easy to understand and deploy trust management system. Among these solutions, Xiong and Liu propose a decentralized reputation-based trust supporting framework called PeerTrust [285] for P2P environments, whereas Huynh et al. build their FIRE model [143], convinced that most of the trust information source can be categorized into four main sources: direct experience, witness information, role-based rules, and third-party references. FIRE integrates those four sources of information and it is able to provide trust metrics in a wide variety of situations. The reliability value based on the rating reliability and deviation reliability to counteract the uncertainty due to instability of agents.

Behavioral trust is evaluated based on two types of trust: conversation trust and propagation trust. Conversation trust specifies how long and how frequently two members communicate with each other. Longer and more frequent communication indicates more trust between the two parties. Adali et al. [8] present a behavior-based model, where trust is evaluated based on the communication behavior of members in a social network. Propagation trust refers to the propagation of information. Propagating information obtained from one member to various other members indicates that a high degree of trust is being placed on the information and, implicitly, its source. Guha et al. [130] propose a method based on the PageRank algorithm for propagating both trust and distrust. They identify four different methods for propagating the net beliefs values, namely direct propagation, co-citation, transpose, and coupling. The Advogato maximum flow trust metric, proposed by Levien [182], aims at discovering which users are trusted by members of an online community and which are not. Trust is computed through one centralized community server and considered relative to a seed of users enjoying supreme trust. Local group trust metrics compute sets of agents trusted by those being part of the trust seed. Advogato only assigns boolean values indicating presence or absence of trust. It is a global trust algorithm which uses the same trusted nodes to make trust calculation for all users. This makes the algorithm suitable for

P2P networks. As the trust inference algorithm has been released under a free software license, it has become the basis of many research papers. Flow models do not always require the sum of the reputation/trust scores to be constant. One such example is the EigenTrust model [160] which computes agent trust scores in P2P networks through repeated and iterative multiplication and aggregation of trust scores along transitive chains until the trust scores for all agent members of the P2P community converge to stable values.

2.3 TRUST IN ONLINE SOCIAL NETWORKS

As introduced in Chapter 1, online social networks constitute nowadays essential services in our life. Their success is certainly due to the fact that, in these environments, users are willing to voluntarily disclose a huge amount of social information, although they are more and more aware of risks and threats associated with their online activities [95, 107]. This phenomenon goes under the name of *privacy paradox* [21], and it is motivated by the fact that users tend to trust other community members with expertise, similar interests, disclosed identity, and in general for the set of social and/or economic "advantages" they can obtain. This shows how social networking takes place within a de facto *context of trust* [125]. In the literature, different are the aspects taken into account when reasoning about trust in OSNs: its *properties*, the *components* whereof trust is made up, the strength of *ties* connecting users, as well as the connection between *social trust* and *social capital*.

2.3.1 TRUST PROPERTIES

In this section, based on the work presented in [69, 118, 120, 194, 252], we detail properties connected to trust in online social networks, briefly discussing basic ones and focusing on those connected to trust transfer.

Basic Properties

In general, trust is *subjective* [118, 120, 252]. An opinion given by a subject can be evaluated differently in terms of trust by other individuals. Due to the entirely personal nature of trust, there is no correct or incorrect value, except when considered from the perspective of a given individual. For this reason, when computing/evaluating trust in social networks, biases and preferences of the trustor have a direct impact on the computed trust value. The subjective nature of trust also plays a crucial role in calculating trust recommendations by affecting the accuracy of a recommendation [120].

Trust is *dynamic*: it increases or decreases with new experiences (interactions and/or observations) [194]. New experiences are usually considered more important than old ones (since old experiences may become obsolete or irrelevant with time). For this reason trust may decay over time.

Trust dynamism is also an effect of the *event-sensitive* property of trust: it takes a long time to be built, but a single high impact event may destroy it completely [219].

Trust is *asymmetric*: when two individuals are involved in a relationship, trust is not necessarily identical in both directions. This is connected to the subjective nature of trust, that is, for each individual built up on personal experiences and psychological backgrounds. Despite this, members usually act positively with other members whom they trust. This way, trust "self-reinforces" attaining a certain level of mutual-trust. If the trust between the members goes under some threshold, it is highly unlikely that they will interact with each other in the future [252]. The asymmetric nature of trust is often difficult to be captured from the undirected social graph which is the basis of pure friendship-oriented networks.

Trust is *context specific*: the context-specific nature of trust has been originally discussed in social and psychological sciences [242]. In computer science, it can be interpreted both as (i) *situation-dependent* [194], which normally refers to the environment in which the trust relationship exists (e.g., an entity would have a higher trust in a system with sophisticated cryptography than in one without cryptography), and (ii) *scope-dependent* [262], influenced by the scope of the interaction (e.g., one can trust another as a mechanic but s/he would probably not address to her/him in the case of a broken leg).

Trust Transfer Properties

Over the years, several studies have addressed the issue of the transfer of trust among users in online social networks [48, 117, 130, 194, 259, 265]. These studies exploit the fact that trust can be passed from one member to another in a social network, creating trust chains, based on its *propagative*, *transitive,* and *composable* nature.

Actually, propagation and transitivity often have been confused in literature [252]. Different authors have debated in particular about transitivity, sometimes reaching different conclusions, even concerning its very existence.

From the perspective of network security (where transitivity would, for example, imply accepting a key with no further verification based on trust) or formal logics (where transitivity would, for example, imply updating a belief store with incorrect, impossible, or inconsistent statements) it may make sense to assume that trust is not transitive [71, 142, 157].

In other fields, some researchers attribute to trust "some degree of transitivity" [127, 130, 157], due in particular to the fact that, in some scenarios, "trust may propagate (with appropriate discounting) through the relationship network" [130]. This has been shown empirically in [117, 130]. Jøsang and Pope [157] define certain semantic constraints under which trust can be considered transitive, and a trust referral system can be used to derive transitive trust. Golbeck and Hendler [120] affirm that trust transitivity can act in two ways, because a person can maintain two types of trust in another person: trust in the person and trust in the person's recommendations of other people. The same is sustained by Ma et al. in [194], where authors talk about "partial transitiveness" associated with direct or indirect trust: direct trust is always earned via individual experience, whereas indirect trust is earned via referrals, opinions, etc. Despite this, the two works differ in the treatment of this dichotomy in social networks. According to [120], it is preferable to let a single trust value (representing both of these ideas) be propagated across people in the network. On the contrary, in [194] the authors affirm that partial transitiveness implies that indirect trust often comes with special constraints (e.g., a maximum referral hop limit) and, for this reason, it is desirable for a trust management scheme to take both direct and indirect trust into consideration, though it may assign different weights to them.

Independently from the chosen solution, it is the fact that trust can be propagated that leads to confusion when discussing the transitive nature of trust that, generally, it is not transitive. In fact, if we consider transitivity in the classical mathematical sense, we cannot say that if Alice trusts Bob and Bob trusts John, this also implies that Alice trusts John [120]. In reality, transitivity implies propagation, but the reverse is not true. A similar concept is expressed in [272], according to which trust transitivity is only a condition for trust propagation. In this sense, when Capkun et al. in [48] assume unconditional transitivity of trust, or when Trifunovic et al. [265] rely on both friend ties and conditional transitivity of trust, or again, according to Swamynathan et al. [259] where transitivity is valid for up to six hops, there is the high probability that they are using the term transitivity with the idea of propagating trust along chains of connections.

Independently from the chosen term, trust remains *composable*. Considering that trust can be propagated along social chains, it follows that participants in an online social network are able to form their trust evaluation on a trustee not directly connected to them, by composing other trustors' evaluation from several social chains. Models that employ propagation feature of trust usually also employ the composition feature [252].

2.3.2 TRUST COMPONENTS

According to [125, 175], trust in online social network services is both a *micro-* and *macro-level* phenomenon, generated by the interplay between the users (the group of micro-level actors) and the network (the macro-level actor). In this vision, the network participants, the social network service itself, and, in general, the Web 2.0 technologies can be considered as *objects of trust* [124]. Both at micro- and macro-level, social components of trust can emerge from the *cognitive*, *emotive*, and *behavioral* aspects of trust discussed at the beginning of the chapter.

At the micro-level, the *interpersonal* one [183], trust can be interpreted both as *dyatic trust* (direct trust between two entities) or *social trust* (a property of social groups), this latter is discussed in the next section. When referring to dyatic trust, the cognitive aspect refers to a rational decision to place trust in a trustee based on *qualitative* characteristics of the trustee her/himself, such as competence, ability, integrity, honesty, benevolence [203] (e.g., a user having received a lot of recommendations or endorsements about his competencies by reputed experts on LinkedIn, a top trending user on Twitter). The emotive aspect involves reciprocal exchanges and mutual empathy: "internalization of the other's preferences, and identification with each other" [125]. We deal in this case with the concept of *identification-based trust* [76]. According to Grabner-Kräuter and Bitter [125], it is "the highest and solid level of trust that may be reached by the parties to the trust relationship." It can be assumed that identification-based trust is more important in friendship-oriented networks (e.g., friends in Facebook) than in other types of OSNs [124]. When considering unknown actors, the emotive aspect refers to the trustor's general tendency to trust others across situations. This *dispositional trust* [204] has a major impact in trusting other parties when the type of relationship and parties are unknown. Concerning the behavioral aspect, trust is based on the observed communication behavior between entities in the OSN. The forms of communication used and their frequency between individuals in a social network are in this sense a good indicator of their social relationships and trust (e.g., the fact of having posted something directly on a user's wall on Facebook instead of just having commented a post left by someone else, the number of times a Twitter user has "retweetted" a specific user's tweets).

At the macro level, the *system* one [183], the emotional component is marginalized and the cognitive and behavioral aspects are connected to *quantitative* characteristics proper of the technical features entering into the picture. In this case, the cognitive aspect is connected to a rational calculation of the costs and benefits in entering into a social network. Trust can, for example, rely on the size of the network, the number of participants, the topics of interest, privacy and security features, the usefulness and ease of use of the network site, etc. An important aspect is also constituted by the individuals' perception of the structures making an environment trustworthy, known as *institution-based trust* [303]. In the case of OSNs, the environment is constituted by the social network itself (or the Web 2.0 technologies associated with it). The behavioral aspect at this level can be observed in the way individuals use the social network and their services (e.g., Facebook is used for staying connected with family, friends, colleagues, and sharing interesting content whereas Google+ is more reputed for the online business applications it supplies).

2.3.3 SOCIAL TRUST AND SOCIAL CAPITAL

In Section 1.3.3 we discussed the concept of *social capital* connected to the richness of interactions between members characterizing online social networks [252]. Although there is much discussion around the concept of social capital, most researchers agree that it refers to investment in personal relationships or social structure that facilitates the achievement of individual or collective goals [115]. In this section, we focus on the relation between trust and the growth and exchange of relationships between individuals. According to Sherchan et al. [252], in the context of social networks, trust is derived from social capital, and takes the name of *social trust*.

Actually, the distinction between social capital and social trust is quite blurred in literature. Certainly, social trust is considered an important aspect of social capital that represents the cooperative infrastructure of a society [72, 234] and social scientists focus on increasing social trust through investment in human capital [141]. According to Putnam's work [234], social trust is an important element of social capital, but they are not the same: "by analogy with notions of physical capital and human capital tools and training that enhance individual productivity, "social capital" refers to features of social organization such as networks, norms, and social trust that facilitate coordination and cooperation for mutual benefit." An interesting contribution to the formalization of the concepts of social capital and social trust has been provided by Huang [141] via the concept of "cooperative tendency." Cooperative tendency is considered to be a component of human capital that is costly to cultivate but yields a stream of returns in the future (especially in increasing social trust). When more people have higher cooperative tendencies in a society, they are more trusting, and hence the social trust of the society is higher. Huang affirms that "social trust in a group is equal to the perceived trustworthiness of a typical member or the average trustworthiness of all members, characterized by the proportion of cooperative players in the group. The level of social trust is determined by the distribution of cooperative tendency in the group and the specific game features, which is why it varies across players and games."

According to [120, 167, 286], social trust is the product of several factors that cannot be easily modeled computationally. Past experiences and perceived trustworthiness can be used to recognize qualitatively social trust, together with other psychological factors such as rumors, influence by others' opinions, and motives to gain something extra by extending trust. Despite this, it is difficult to recognize the different impact of trust relationships in online social networks based on qualitative background knowledge because of the diversity of those relationships. Therefore, it is important to analyze psychological and social information as electronic quantitative information in order to establish a trustworthy relationship model for trust computation in online social networks [167].

2.3.4 TRUST EVALUATION MODELS

Trust evaluation in online social networks is quite a new field of research. According to the literature, [6, 54, 252], research approaches in this field can be essentially classified according to the way they consider the structure of the social network and the interactions among its participants. A first research direction is covered by those works taking into account only the structural properties of the social network and developing *structure-based trust models*. These models usually exploit trust *propagation* techniques. Another direction is taken from those approaches that consider under different perspectives the interactions among users in the social network and that develop *interaction-based trust models*. Trust *prediction* techniques are in most of the cases at the basis of these models. Nowadays, a third direction is covered by those works that tend to take into consideration both aspects and techniques, generating in this way *hybrid trust models*.

Structure-based Trust Evaluation Models

Models that exploit the social network structure in evaluating trust, have been developed based on the concept of "Web of trust" [166], on social networks where trust values are explicitly provided or where they can be inferred. In these models, a trust network is usually created for each member, representing the other members in the person's social network as nodes and the amount of trust s/he has for each of them as edges [252]. Exploiting the propagative nature of trust, various techniques have been studied to traverse the network and determine trust between nodes. Some of them take into account only the concept of trust. Other techniques also consider *distrust* propagation.

Among works considering trust propagation, one of the first studies is the one by Buskens [44]. At the end of the 1990s, Buskens starts from his studies of social network structures and observes that high interconnection between members (i.e., a network with a high density) can yield a high level of trust. Measuring increases in both the in-degree and out-degree of any two members, he obtains the level of trust a member can have in another one. In general, receiving information from members with a higher in-degree increases the level of trust; members with a higher out-degree have higher levels of trust; levels of trust increase if members direct their ties more towards members with higher out-degrees.

More recent popular algorithms for trust propagation include TidalTrust [122], SUNNY [174], the gravity-based model proposed by Maheswaran et al. [197], and Social-Trust [63]. TidalTrust is the trust network inference algorithm proposed by Golbeck in her Ph.D. Thesis [122] for deriving a trust relationship between two people in the social network using the FOAF vocabulary. Using a recursive search with weighted averages, it can take two people in the network and generate a recommendation about how much one person should trust the other, based on the paths that connect them in the network, and the trust ratings on those paths. Her approach is based on the assumption that neighbors with higher trust ratings are likely to agree with each other about the trustworthiness of a third party. In the later work by Golbeck and Kuter [174], authors present SUNNY, a trust inference algorithm that uses a probabilistic sampling technique[1] to estimate the level of confidence in the trust information from some designated sources. More specifically, from the trust network, they obtain a Bayesian network suited for approximate probabilistic reasoning. SUNNY performs a probabilistic logic sampling procedure over the generated Bayesian network. In doing so, it computes estimates of the lower and upper bounds on the confidence values, which are then used as heuristics to generate the most accurate estimates of trust values of the nodes of the Bayesian network. Maheswaran et al. [197] propose a two-stages gravity-based model for estimating trust. First, the strengths of the friendships are recomputed along with the extent of the trusted social neighborhood for each user. This is based on the user's annotations of the connections s/he has with others with trust values or constraints. Second, the social neighborhood is used to compute the effective trust flow for users not in the social neighborhood. The model is based on the presumption that social relationships change over time and social relations may impose constraints on the trust relationships. The model also includes provenance of trust in social networks, where a user can ask questions about the trust value given by the underlying system. Caverlee et al. [63] propose the SocialTrust model that exploits both social relationships and feedback to evaluate trust. Members provide feedback ratings after they have interacted with another member. The trust manager combines these feedback ratings to compute the social trust of the members. A member's feedback is weighted by her/his link-quality (high link-quality indicates more links with members having high trust ratings).

[1] A probability sampling technique is one in which every unit in the population has a chance (greater than zero) of being selected in the sample, and this probability can be accurately determined.

Some works address trust propagation for recommendation, such as the work by Zhang et al. [298], the trust-based recommendation approach by Hang and Singh [135] and the matrix factorization technique proposed by Jamali and Ester [149]. Zhang et al. [298] expand Golbeck's TidalTrust model to include pair-wise trust ratings and reliability factors of the entities in the network, using an edge-weighted graph to calculate trust. First, the similarity of two raters is calculated by comparing the ratings provided by them for the same trustee. It is then employed to decide which neighbor's recommendation to follow. Comparing two recommendations, the recommendation from a rater that is more similar to the trustor will be chosen. Hang and Singh [135] also employ a graph-based approach for measuring trust, with the aim to recommend a node in a social network using the trust network. The model uses the similarity between graphs to make recommendations. The Jamali and Ester's approach [149] makes recommendations for a user based on the ratings of the users that have direct or indirect social relations with the given user, employing matrix factorization techniques. The model also incorporates the mechanism of trust propagation.

When trust and distrust are considered simultaneously, seminal contributions are those by Guha et al. [130], Ziegler [302], Wierzowiecki and Wierzbicki [278], Leskovec et al. [181], DuBois et al. [85], Victor et al. [268], and Verbiest et al. in [267]. Guha et al. [130] develop a formal framework of trust propagation schemes, introducing the formal and computational treatment of distrust propagation. They also develop a treatment of "rounding." In their work, authors show that a small number of expressed trusts per individual allows the system to predict trust between any two people in the system with high accuracy. Ziegler [302] contributes to Semantic Web trust management by introducing a classification scheme for trust metrics along various dimensions and discussing advantages and drawbacks of existing approaches for Semantic Web scenarios. He also describes Appleseed, a proposal for local group trust computation. The proposal is based upon spreading activation models, a concept borrowed from cognitive psychology [73].[2] Appleseed takes into account some clever adaptations in order to handle distrust and sinks such as trust decay and normalization. Wierzowiecki and Wierzbicki in [278] propose a trust/distrust propagation algorithm called CloseLook, which is capable of using the same kinds of trust propagation as the algorithm proposed by Guha et al. With respect to their model, CloseLook has a lower complexity and reduces the amount of consumed computational and network resources by selecting the best paths to propagate trust and by stopping the trust propagation using scope parameters that can limit the number of considered nodes. Also, the approach by Leskovec et al. [181] extends the one by Guha et al., using a machine-learning framework (instead of the propagation algorithms based on an adjacency matrix used in [130]) to enable the evaluation of the most informative structural features for the prediction task of positive/negative links in OSNs. Similarly, DuBois et al. [85] present a method for computing both trust and distrust by combin-

[2] Spreading activation is a method for searching associative networks, neural networks, or semantic networks. The search process is initiated by labeling a set of source nodes (e.g., concepts in a semantic network) with weights or "activation" and then iteratively propagating or "spreading" that activation out to other nodes linked to the source nodes. Spreading activation models are used in cognitive psychology to model the *fan out* effect.

ing an inference algorithm that relies on a probabilistic interpretation of trust based on random graphs with a modified spring-embedding algorithm[3] to classify an edge. Victor et al. [268] build a comprehensive framework that computes trust/distrust estimations for agent pairs in the network using trust metrics: given two agents in the trust network, we can search for a path between them and propagate the trust scores along this path to obtain an estimation. When more than one path is available, we may single out the most relevant ones (selection), and aggregation operators can then be used to combine the propagated trust scores into one final trust score, according with four families of trust score propagation operators. Verbiest et al. [267] address the problem of considering the length of the paths that connect two agents for computing trust-distrust between them, according to the concept of "trust decay." In their paper, they introduce several aggregation strategies for trust scores with variable path lengths, following two general methods. First, they associate weights (computed on the basis of the inverses of the path lengths of the trust scores) with trust scores depending on the number of propagations needed to obtain them. This way, trust scores propagated along longer paths get lower weights. As this approach is sensitive to the number of trust scores that have a given path length, authors have also introduced a method that reserves a total weight for all trust scores with a certain path length, dependent on the number of trust scores of this path length. Secondly, a dynamic horizon search strategy is developed in their approach: trust scores with a certain path length are dismissed whenever there are others available that were propagated along shorter paths. An additional version of this method, the semi-dynamic horizon search strategy, only considers trust scores of higher path lengths if the number of trust scores with shortest path length does not exceed a threshold.

The approaches described in this section evaluate trust based only on structural information of the considered social network, capturing members' relatedness based on their relationships and propagating/composing trust flows according to them. No actual interactions between members are taken into consideration, even if they can represent an important indicator of trust in online social networks, as explained in Section 2.3.3. Trust evaluation models based on users' interactions are described in the following section.

Interaction-based Trust Evaluation Models

Unlike models presented in the previous section, some trust models in literature only use interactions within the network and trust/link prediction [185] to evaluate social trust/distrust.

Models considering only trust (i.e., not distrust) include those by Liu et al. [187], Adali et al. [8], Nepal et al. [220], and Švec and Samek [271]. The work of Liu et al. [187] is based on the observation that a user trusts another user either because of the latter's good reputation or because there have been good personal interactions between the two users. Therefore, authors propose a supervised learning approach for the automatic prediction of trust between a pair of users exploiting evidence derived from (i) *actions* of individual users, as well as from (ii) *interactions*

[3] Spring embedding algorithms also called FDP (Force Directed Placement) can be used to sort randomly placed nodes into a desirable layout that satisfies the aesthetics for visual presentation (symmetry, non-overlapping, etc.) [87].

between pairs of users. Technically speaking, this is obtained by a taxonomy that systematically organizes an extensive set of trust factors into two main categories. The first category, namely *user factors*, refers to features associated with a given user who can be either trustor or trustee. The other category, composed of *interaction factors*, refers to features associated with the interaction that occurs between a pair of users in the trustor-trustee roles. As a case study, authors apply their approach on Epinions,[4] a large product review community supporting various types of interactions. In this scenario, user factors can include, for example, reviews, posted comments, rating, etc., with metrics such as number/frequency of reviews, number/frequency of ratings, and average length/number of comments given to reviews. Interaction factors can be represented, for example, by connections between writers, and raters, writers and writers and raters and raters. Authors state that their taxonomy is general enough to be adopted in other online communities. This work comes to the conclusion that interactions between two users play a more important role than individual user actions in deciding pairwise user trust. Adali et al. [8] aim at quantitatively measuring dyadic trust (trust between two entities) based on observed communication behavior in social networks. They develop statistical measures based on the timing and sequence of communications, not the textual content. They evaluate *behavioral trust* by taking two specific social behaviors into account: *conversations* and *propagation of information* from one person to another. Authors assume that the longer and more balanced a conversation is between two nodes, the more likely it is that they have a trust relationship; in addition, the more conversations there are between such a pair of nodes, the more tightly connected they are. Similarly, propagation of information obtained from one member to other members in the network indicates high degree of trust placed on the information and implicitly on the member that created the information. Authors show that these two types of behavior correlate strongly with each other in terms of the individuals involved and the communities formed. They also show that they correlate with actual forwarding behavior indicative of trust. STrust, the interaction-based social trust model proposed by Nepal et al. [220], aims at augmenting the social capital of a community by encouraging positive interactions among members, building a trust community. In their work, authors separate the interactions derived from social capital into two groups: *popularity* and *engagement*. Popularity-based interactions are, in general, based on the trustworthiness of a member in the community: if a member is trusted by other members in the community, popularity-based interactions of the member will increase. Engagement-based interactions are, in general, based on how much a member trusts other members in the community: if a member trusts other members in the community, engagement-based interactions of the member will increase. The STrust model separates trust values derived from this twofold classification of interactions as *popularity trust* and *engagement trust*. The benefits in separating these two types of trust consist of the possibility to recommend different things. Popularity trust can be used to recommend the leaders in the community, recognizable from metrics such as how many members follow them, the number of positive feedback on their posts, etc. Similarly, engagement trust can be used in friends

[4] Epinions. Unbiased Reviews by Real People. http://www.epinions.com/

recommendation based on metrics such as how frequently members visit the site/network, how many members they follow, how many posts they read and comment on, etc. The combination of popularity trust and engagement trust allows for the determination of the social trust of the community. Švec and Samek [271] aim at creating a model of trust from the point of view of artificial intelligence which would make use of social psychology in social networks. The mathematical core of their model leans on the Marsh theory [200] based on the *contexts of trust* (representing the fields in which we are capable of trusting the entity). In their model, authors take into account the following characteristics to capture different contexts: the interaction time span (the longer the time between the first and the last interaction, the higher trust we are likely to feel), number of interactions, number of characters (i.e., it is possible to study the relation between a number of characters in a message and the credibility of the writer [62]), interaction regularity, photo tagging, group membership, and common interests. The number of friends, a characteristic that could be connected to structural aspects, has not be considered in the final model to the inconsistency in Facebook Graph API, according to authors.

A model taking into account also distrust is the one proposed by Yang et al. [287], focusing on the problem of predicting the "signed social ties" (i.e., positive/negative) out of the unsigned (i.e., acquaintance) relationships in social networks. In the same way that link prediction is used to infer latent relationships that are present but not recorded by explicit links, the sign prediction problem can be used to estimate the sentiment of individuals toward each other, given information about others' sentiments in the network [181]. In this work, authors show that it is possible to infer signed social ties with good accuracy solely based on users' behavior in decision making (or using only a small fraction of supervision information) via unsupervised and semi-supervised algorithms. More specifically, they propose a Behavior Relation Interplay (BRI) model, which is a *latent factor model*[5] that leverages behavioral evidence to infer social interactions and at the same time exploits the learned relations to tie users' behavior. The key idea in BRI is to associate *latent factors* with both users and items and to define coupled models to simultaneously characterize both the *social interactions* and *behavioral evidences*. The aim of this work is to make it possible to turn an unsigned acquaintance network (e.g., Facebook, Myspace) into a signed trust-distrust network (e.g., Epinion, Slashdot).

In this section, we described trust evaluation models considering only members of a community's interactions to compute trust. They deliberately ignore (or take into minimal consideration with respect to interactions) the social network structure. This way, important information about how members in a community are explicitly connected are discarded. Considering this problem, nowadays trust evaluation models taking into account both graph structures and interactions within the social networks are emerging. These hybrid models are described in the next section.

[5] Factor analysis is a statistical method used to describe variability among observed, correlated variables in terms of a potentially lower number of unobserved variables called factors. In other words, it is possible, for example, that variations in three or four observed variables mainly reflect the variations in fewer unobserved variables. Factor analysis searches for such joint variations in response to unobserved latent variables.

Hybrid Trust Evaluation Models

Hybrid trust models use both interactions and social network structure information to compute social trust.

Models focusing on trust include Trifunovic et al. [265], Li and Bonti [184], and Carminati et al. [54]. Trifunovic et al. [265] propose a hybrid model for opportunistic networks.[6] The model supports two complementary approaches for social trust establishment: *explicit* social trust (based on network structure) and *implicit* social trust (based on users' interactions in the network). Explicit social trust relies on consciously established social ties. Each time two users interact, they exchange their friend lists and save them as friendship graphs. Trust is calculated on the friendship graph with direct link/friend having the highest trust value of 1. As the number of links between two users grow, trust decreases proportionately. Implicit trust is based on frequency and duration of contact between two users. It uses two metrics: familiarity and similarity of the nodes. Familiarity describes the length of the interactions/contacts between the two nodes. Similarity describes the degree of coincidence of the two nodes' familiar circles. The drawback of this work is that it considers only the duration and frequency of interactions, while the nature of interactions themselves is an important indicator of trust between two members. The same drawback can be found in the short paper by Li and Bonti [184]. They describe their simple T-OSN model, taking into account both the structural property represented by the number of friends (degree) and the interactional property represented by the contact frequency (contact interval). They assume that if two users have shorter contact interval, they have more contact times and closer relationship. That is to say they have a higher trust relationship. In their model, they firstly use degree centrality to measure whether a friend of a user of OSN can be trusted and they refine this evaluation via contact interval measurement. A work trying to take into account also the nature of the interactions is the one proposed by Carminati et al. [54]. They describe a trust evaluation model based on an "augmented social graph." This graph consists of all the users' relationships, information and resources as well as their interactions with other users and resources, independently from the social web/mobile application we are dealing with and the social network representation. In their approach, authors *dynamically* analyze the augmented social graph (new relationships can be added, modified, or deleted), since it is necessary to evaluate how the interactions of dynamic events affect users/resources relationships in terms of trust. Their *multi-dimensional* and *event-based* approach exploits for trust computation diverse interactions among users in a social scenario. Considering these interactions, together with the structure evolution of the network, a certain trust relationship holds in a certain dimension when an event or some *event patterns*, meaningful for that specific dimension, occur. The selection of meaningful events/event patterns for trust computation can be customized according to given *trust rules*. A possible drawback of this approach is that an in-depth knowledge of the domain is necessary to specify trust rules able to capture significative trust relationships.

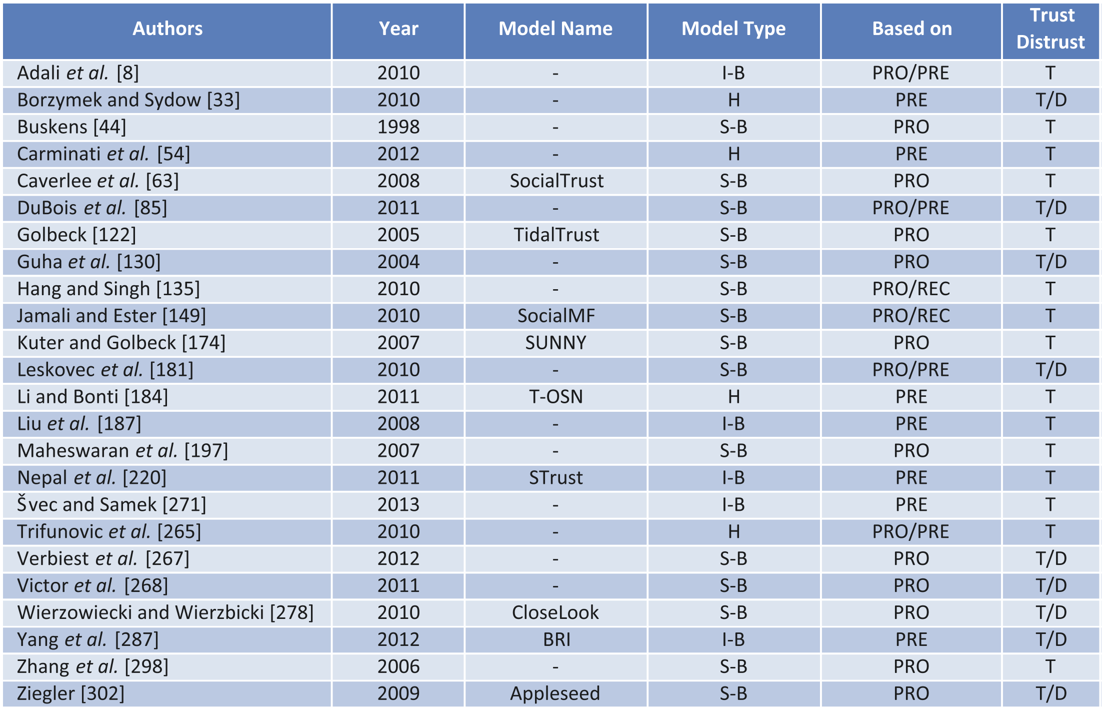
[6] Opportunistic networks enable users to participate in various social interactions with applications such as content distribution and micro-blogs.

The work by Borzymek and Sydow [33] uses both structural-based and interaction-based aspects for predicting trust and distrust in online social networks. Authors experimentally evaluate two groups of attributes: graph-based and those based on user ratings, in prediction of trust and distrust between a pair of users in a social network. To do this, they implement a decision tree algorithm.

Even if, in our opinion, hybrid trust evaluation models are going to represent a promising way to evaluate trust in online social networks, the literature on hybrid approaches is still limited. For this reason, this still represents an interesting area for further research.

Summarization of Approaches

Figure 2.1 provides a graphical summary of the approaches described before, focusing on specific aspects emerging from the above treatment. The different approaches are alphabetically ordered by authors and, where it is possible, we provide the name of the proposed models. For each trust evaluation model, we specify the year of the publication, if it is a structure-based model (S-B), an interaction-based model (I-B) or a hybrid model (H). In addition to this, we specify if it is based on propagation (PRO), recommendation (REC), or prediction (PRE), and if it takes into account trust (T) or also distrust (D).



Authors	Year	Model Name	Model Type	Based on	Trust Distrust
Adali *et al.* [8]	2010	-	I-B	PRO/PRE	T
Borzymek and Sydow [33]	2010	-	H	PRE	T/D
Buskens [44]	1998	-	S-B	PRO	T
Carminati *et al.* [54]	2012	-	H	PRE	T
Caverlee *et al.* [63]	2008	SocialTrust	S-B	PRO	T
DuBois *et al.* [85]	2011	-	S-B	PRO/PRE	T/D
Golbeck [122]	2005	TidalTrust	S-B	PRO	T
Guha *et al.* [130]	2004	-	S-B	PRO	T/D
Hang and Singh [135]	2010	-	S-B	PRO/REC	T
Jamali and Ester [149]	2010	SocialMF	S-B	PRO/REC	T
Kuter and Golbeck [174]	2007	SUNNY	S-B	PRO	T
Leskovec *et al.* [181]	2010	-	S-B	PRO/PRE	T/D
Li and Bonti [184]	2011	T-OSN	H	PRE	T
Liu *et al.* [187]	2008	-	I-B	PRE	T
Maheswaran *et al.* [197]	2007	-	S-B	PRO	T
Nepal *et al.* [220]	2011	STrust	I-B	PRE	T
Švec and Samek [271]	2013	-	I-B	PRE	T
Trifunovic *et al.* [265]	2010	-	H	PRO/PRE	T
Verbiest *et al.* [267]	2012	-	S-B	PRO	T/D
Victor *et al.* [268]	2011	-	S-B	PRO	T/D
Wierzowiecki and Wierzbicki [278]	2010	CloseLook	S-B	PRO	T/D
Yang *et al.* [287]	2012	BRI	I-B	PRE	T/D
Zhang *et al.* [298]	2006	-	S-B	PRO	T
Ziegler [302]	2009	Appleseed	S-B	PRO	T/D

Figure 2.1: Summary of Trust Evaluation Models.

2.4 CONCLUSIONS

In this chapter, after having introduced trust as a fundamental concept in many aspects of human life, we have first provided general notions and related work concerning trust in Computer Science, in order to better understand our further treatment of the concept of trust applied to online social networks. In these environments, trust is in general a measure of confidence that an entity or entities will behave in an expected manner. Several studies have addressed the issue of evaluating this measure of confidence, taking in particular into account the possibility for trust to be transferred among users in online social networks, creating out-and-out trust chains, based on the propagative and composable nature of trust.

Different are the models that have been proposed over the years. Some of them take into account only the structure of a given social network in order to measure trust propagation among its members. Others predict trust values concentrating only on the interactions among users. Since both structural and interactional aspects are fundamental for measuring trust in a community (as it has been demonstrated not only in Computer Science and not only for online social networks), recently hybrid methods have been proposed to better fulfill this aim. It is our opinion that this represents the most promising research direction in the field of trust evaluation in OSNs.

CHAPTER 3

Controlled Information Sharing in Online Social Networks

3.1 INTRODUCTION

In Chapter 1 we discussed the success of the social network paradigm and its possible use either for social purposes (e.g., find new friends/dates, sharing interests) or enterprise purposes (e.g., facilitate knowledge sharing). Independently of the reason for using online social networks, *information dissemination* is involved: millions of individuals can easily *share* personal and confidential information with an incredible amount of (possible unknown) other users. This poses several *control* issues over the spread of personal data in OSNs.

Traditionally, the way to address this problem and prevent unauthorized operations (such as read and write) has been treated in information systems via *access control* [96] techniques. With respect to online social network services, due to their particular characteristics, it is important to understand that new access control and *controlled information sharing* solutions are necessary with respect to what has been proposed so far in the field of *database management systems* (DBMSs) and *operating systems*. The *discretionary access control* (DAC), *mandatory access control* (MAC), and *role-based access control* (RBAC) paradigms used in traditional systems have been nowadays replaced by the *relationship-based access control* (ReBAC) paradigm in OSNs.[1] DAC is a means of restricting access to objects based on the identity of subjects. In this kind of access control paradigm, a user has complete control over all the programs it owns and executes, and also determines the permissions other users have on her/his data and programs. Conversely, MAC is a type of access control paradigm which is regulated according to security classes associated with subjects and objects. RBAC, sometimes referred to as *role-based security*, is an approach to restricting system access to authorized users based on their role. ReBAC, exploiting the relationship-based nature of OSNs, is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships.

In this chapter, we first provide a brief historical perspective and the basic concepts on access control needed to understand the various access control models and mechanisms in the general field of data protection (Section 3.2). In what follows, we analyze and discuss the main

[1] The ReBAC paradigm is, in particular, an evolution of the DAC paradigm.

access control challenges in online social networks, with particular reference to controlled information sharing in these services (Section 3.3), supported by relevant and recent research proposals (Section 3.3.3).

3.2 ACCESS CONTROL IN DATA MANAGEMENT SYSTEMS

Traditionally, protecting data from unauthorized access requires addressing three main issues.

(i) *Data secrecy or confidentiality*: preventing improper or unauthorized read operations on the managed data; However, it is important to note that protecting privacy requires some additional countermeasures with respect to those employed to ensure data confidentiality. For instance, additional factors must be taken into account, such as the data retention period, the user consent, or the purpose for which data are collected (see Bonchi and Ferrari [2010]; Li [2005] for more details on privacy-preserving data management systems).

(ii) *Data integrity*: protecting data from unauthorized or improper modifications or deletions.

(iii) *Data availability*: preventing and recovering from hardware and software errors and from malicious data denial attacks making the data or some of their portions unavailable to authorized users.

Generally, each of the above security properties is ensured by a *security mechanism* [96], based on different services. The *access control mechanism* is one of the most relevant security services, since it is the basis of enforcing both data confidentiality and integrity. Indeed, whenever a user tries to access a data object, the access control mechanism checks the rights of the subject against the set of specified *authorizations*. The access is granted only if it does not conflict with the stated authorizations. Data confidentiality is also obtained through the use of *encryption techniques*, either applied to the data stored on secondary storage or when data are transmitted on the network, to prevent an intruder from intercepting the data and access their contents. Besides the access control mechanism, data integrity is also ensured by *integrity constraints*, provided by most DMSs. Integrity constraints allow one to express correctness conditions on the stored data, and therefore avoid incorrect data updates and deletions. These constraints are automatically checked by the DMS upon the request for each update operation. Furthermore, digital signature techniques are applied to detect improper data modifications. They are also used to ensure data authenticity. Finally, the recovery subsystem and the concurrency control mechanism ensure that data are available and correct despite hardware and software failures and despite data accesses from concurrent application programs. Data availability, especially for data that are available on the Web, can be further enhanced by the use of techniques avoiding query floods or other Denial-of-Service (DoS) attacks.[2]

[2] Please refer to [98] for further details.

Basic Concepts

- Access control is usually performed against a set of *authorizations* are stated by Security Administrators (SAs) or users according to the *access control policies* of the organization. An access control policy defines the high-level rules according to which access control must be regulated. These may depend on many heterogeneous factors, such as the in-force legislation, the domain in which the owner of the data operates (e.g., business, education, healthcare), local rules, or the specific user requirements. Simple examples of access control policies are: "Psychological evaluations of employees can be seen only by their managers" or "Drugs prescribed to a patient while he/she is in the hospital can be seen only by his/her family doctor once the patient has been discharged." Access control policies can be seen as high-level requirements concerning data protection that, in order to be automatically enforced, should be translated into a set of authorizations. An authorization states which subjects can perform which actions on which objects and, optionally, under which conditions. How to represent and store authorizations depends on the protected resources, but the standard way is to use a uniform representation for authorizations and the managed data. For instance, in a relational DMS, authorizations are usually modeled as tuples stored into system catalogs. In contrast, when resources to be protected are XML data, authorizations are usually encoded using XML itself.

- Authorizations are expressed according to an *access control model*, which provides a formal representation of the authorizations and their enforcement. The formalization allows the proof of a set of properties (e.g., security, complexity) on the corresponding access control system.

- Authorizations are then processed by the *access control mechanism* (or reference monitor) to decide whether each access request can be authorized (totally or partially) or should be denied. The reference monitor is a trusted software module in charge of enforcing access control. It intercepts each access request submitted to the system (for instance, SQL statements in case of relational DBMSs) and, on the basis of the specified authorizations, it determines whether the access can be partially or totally authorized, or it should be denied. The reference monitor should be non-bypassable, that is, it should mediate each access request. Additionally, the hardware and software architecture should ensure that the reference monitor is tamper proof, that is, it cannot be maliciously modified (or at least that any improper modification can be detected).

3.2.1 A BRIEF HISTORICAL PERSPECTIVE

Over the years, much research has been done in the field of access control in information systems. Much of the early work on data protection was on inference control in statistical databases. Then, in the 1970s, as research in relational databases began, attention was directed toward access control. A lot of early work on access control for relational database systems, e.g., [93, 128], was done as part of the research on System R at IBM Almaden Research Center. The developed model strongly influenced most of the subsequent research activities as well as the access control models and mechanisms of current commercial relational DBMSs. At the same time, some early work on mandatory access control for data management systems began, but it was the Airforce Summer Study [248] that started much of the developments in this field. Later, in the mid-1980s, pioneering research was carried out at SRI International and Honeywell Inc. on systems such as SeaView and LOCK Data View [57]. Some of the technologies developed by these research efforts were transferred to commercial products by corporations such as Oracle, Sybase, and Informix. In the 1990s, numerous other developments started, mainly to meet the access control requirements of new applications and environments, such as the World Wide Web, data warehouses and decision support systems, distributed, active, and multimedia DBMSs, workflow management systems, collaborative systems, and, more recently, peer-to-peer systems, geographical information systems, and data stream management systems. This has resulted in several extensions to the basic access control models previously developed, by including, for instance, the support for temporal constraints, derivation rules, positive and negative authorizations, strong and weak authorizations, and content and context-dependent authorizations. Some of these developments have also been partially transferred to commercial DBMSs (e.g., Oracle Virtual Private Database). In the mid-1990s, Role-based Access Control (RBAC) was proposed by Sandhu et al. [247], as a way to simplify authorization management within companies and organizations. Since the beginning of this century, there have been numerous other developments in the field of access control, mainly driven by developments in Web data management. For example, standards such as XML (eXtensible Markup Language), RDF (Resource Description Framework), and all the technologies related to the Semantic Web require proper access control mechanisms [50]. Also, Web Services are becoming extremely popular and therefore research has been carried on to address the related access control issues [100]. Access control has also been investigated for new application areas such as Database as a Service [97] and location-based services [81]. Additionally, privacy is becoming a primary concern and this has been reflected in research work trying to enhance protection mechanisms for DBMSs with the protection of personal data [45, 223].

Concerning recent developments, those connected to the Web 2.0 revolution, they will be described in Section 3.3.3, since they constitute the main topic of the chapter.

3.2.2 ACCESS CONTROL MODELS

Among the approaches proposed in literature, a basic distinction when dealing with access control models is nowadays accepted, according as they follows a *discretionary*, *mandatory*, or *role-based* access control paradigm.

Discretionary Access Control (DAC) governs the access of subjects to objects on the basis of subjects" identity and a set of authorizations that state, for each subject, the set of objects that s/he can access in the system and the allowed access modes. When an access request is submitted to the system, the access control mechanism verifies whether the access can be authorized or not according to the specified authorizations. The system is discretionary in the sense that a subject, by proper configuration of the set of authorizations, is able both to enforce various access control requirements, and to dynamically change them when needed (simply by updating the authorization state).

In contrast, in *Mandatory Access Control* (MAC) the accesses that subjects can exercise on the objects in the system are derived from subjects and objects security classification [99]. The security classification of an object is a measure of the sensitivity of the information it conveys (the higher is the classification, the higher is the protection that must be assured). In contrast, the subject classification is a measure of how much the subject is trustworthy with respect to information released to unauthorized subjects. This type of security has also been referred to as multilevel security, and DBMSs that enforce multilevel access control are called Multilevel Secure Data Management Systems (MLS/DBMSs). When mandatory access control is enforced, authorizations are implicitly derived by subjects and objects security classes. Indeed, the decision as to whether to grant access or not depends on the access mode and the relation existing between the classification of the subject requesting the access and that of the requested object. MAC and DAC policies are not mutually exclusive. If they are jointly applied, then an access is granted only of it is allowed by both MAC and DAC.

In addition to DAC and MAC, *Role-Based Access Control* (RBAC) has been more recently proposed by Sandhu et al. [247], as introduced in a previous section. RBAC is an alternative to DAC and MAC, mainly conceived for regulating accesses within companies and organizations. In RBAC, permissions are associated with roles, instead of with users, and users acquire permissions through their membership to roles. The set of authorizations can be inferred by the sets of user-role and role-permission assignments.

3.3 ACCESS CONTROL IN ONLINE SOCIAL NETWORKS

Access control in online social networks presents several unique characteristics different from access control in traditional data management systems. As introduced before, in mandatory and role-based access control (MAC and RBAC), a system-wide access control policy is typically specified by the security administrator. In discretionary access control (DAC), the resource owner defines access control policy.

Similarly to DAC, in OSN systems, users may want to regulate access to their resources and activities related to themselves, thus access in OSNs should be driven by user-specified policies. Other than the resource owner, some related users (e.g., user tagged in a photo owned by another user, parent of a user) may also expect some control on how the resource or user can be exposed. In addition to this, to prevent users from accessing unwanted or inappropriate contents, user-specified policies that regulate how a user accesses information need to be considered in authorization as well. Thus, the system needs to collect these individualized partial policies, from both the accessing users and the target users, along with the system-specified policies and fuse them for the overall control decision.

To do this, besides the definition of suitable access control models able to express the variety of access control requirements that OSN users may have, a fundamental issue is the definition of suitable architectures on support of access control enforcement. Indeed, as it will be clarified later on, the traditional centralized way of performing access control does not fit well in the OSN scenario. This is due in particular to the threats to users' confidentiality and privacy that this solution may involve. According to Yeung et al. [289], decentralized solutions allow users to have more control over their own data. Privacy of online SNS relationships is therefore a primary need. In this respect, the research has focused on two main issues. The first is the development of privacy-preserving techniques to protect relationship privacy when mining social network data (e.g., data about the topology of the online SNS). Most of the techniques developed so far achieve this goal mainly by producing an anonymized version of the network graph. The second direction, which has been so far less investigated, is how to protect relationship privacy when performing access control.

For this reason, semi-decentralized and fully decentralized solutions have been proposed nowadays for access control over personal information in OSNs (see Section 3.3.3). In most of the cases, the paradigm they implement exploits the relationships between the accessing entity and the controlling entity of the target found in the social graph.

3.3.1 RELATIONSHIP-BASED ACCESS CONTROL

Relationship-Based Access Control (ReBAC) paradigm [111][104] takes into account the existence of a particular relationship or particular path of relationships between social entities (users and/or resources) and expresses access control policies in terms of such relationships.

When considering users, granting access permission to an accessing user is typically subject to the existence of a particular relationship or a particular sequence of relationships between the accessing user and the target user (or resource owner), and access control policies are specified in terms of such *user-to-user* (U2U) relationships [67].

When a user requests access to a resource, current OSNs rely on an implicit relationship, namely *ownership*, between the resource and its owner, hence the authorization of such *user-to-resource* (U2R) access is still based on the underlying U2U relationships. However, due to the various functionalities offered by today's OSNs, there exist several different types of relationships between users and resources in addition to ownership (e.g., *like*, *tag*, *comment*, etc.). OSNs usually allow only the owner Bob to have control on who can view the photo, regardless of whether or not Alice and Carol may wish to release their images. To enable Alice and Carol control capability on the photo, their relationships with the photo, which is not ownership, should be considered for authorization purposes. After the photo has been shared by Bob's friends several times, more and more users from different neighborhoods in the network come to view the photo and comment on it. When Dave reads through all the comments in Bob's photo and becomes curious about another user Eve who has commented recently, he decides to poke her to say hello. In this case, Dave and Eve are connected through the photo, not through another user (such as the owner of the photo Bob). Also, users may share or like the blog posts or videos posted by others, and gain the ability to determine how the shared/liked copy of the original content or the fact of sharing and liking activities can be seen by others. Consider another scenario where Betty finds a weblink originally posted by Ed interesting and then shares it with her friends. From her activity, she acquires the ability to decide how the weblink can be available to others.

As users get increasingly involved in these activities in OSNs, current U2U relationship-based access control mechanism is not able to offer the appropriate control and requires extensions to bring U2R and *resource-to-resource* (R2R) relationships into consideration.

This is witnessed by the fact that, as introduced in Section 1.3.3, various commercial social networks are gradually expanding the set of relationships on which their social graphs are based. Facebook for example, developing Open Graph, has launched new services such as photos and places, including them in the graph over time. Recently, even further extensions to incorporate arbitrary activities and objects are being pushed so as to codify user behaviors effectively.

These recent trends in commercial OSNs strengthen our belief that it is useful to include resources, such as objects and activities, in the social graph [54]. By means of such an extended social graph, users and all of the resources related to users are interconnected through U2U, U2R, and even R2R relationships, allowing stronger expressive power of relationship-based access control policies.

Relationship Characteristics

In order to understand how to take relationships into account in defining suitable relationship-based access control policies, it is necessary, first of all, to analyze the characteristics that relationships in online social networks have.

- They are *not* (always) *mutual* (e.g., the "parent-of" relationship [52]). Thus, rather than a simple graph, we have to consider a directed graph, where the direction of the edges denotes, respectively, which entity has specified the relationship and the entity for whom a relationship has been specified.

- Relationships can be *direct* (e.g., Bob has a direct relationship of type "friend-of" with Alice) or *indirect* (e.g., Eve and Alice are not directly connected, but they are related in that Eve is a friend of Bob, and Bob is a friend of Alice)

- Relationships are *composable*. Given two (binary) relationships $r1$ and $r2$, one may compose the relation $r1 \diamond r2$. This way, complex (binary) relationships can be composed from primitive building blocks. Considering, for example, the relationship *friend-of*, we can derive the *friend-of-a-friend* relationship by the composition *friend-of* $\diamond$ *friend-of*.

- Another property is the *contextual* nature of relationships. A physician who is one's treating physician in one medical case may very well be a consulting expert in a different medical case of his.

- Besides, relation types are often associated with *different levels of information disclosure*. For example, people usually share more private information with close friends than with other types of contact.

- Apart from their type, relationships can be characterized by a *trust level*, and by their *depth* (the length of the shortest among the paths representing all possible in/direct relationships of a type *t* between two users *a* and *b*).

Relationship-Based Access Control Requirements

Based on the above considerations, and according to [53, 252, 264], in this section we summarize the key requirements that a relationship-based access control paradigm for social network services should have. We do this from the *model* point of view and from the *enforcement* point of view, taking into consideration the graph-based, dynamic and decentralized nature of OSNs.

Model Requirements A traditional access control policy basically states who can access what and under which modes. In a traditional scenario, since a user Alice knows a priori her friends, she is able to set up a set of authorizations to properly grant the access only to (a subset of) her friends. In the more general OSNs scenario, this way of specifying policies is not enough. Let us consider, for example, the case of Alice deciding to make available her resources not only to her friends, but also to their friends, the friends of their friends, and so on. The problem is that Alice may not know a priori all her possible indirect friends and, even if it would be the case, she should specify a huge number of policies. Moreover, if we consider that relationships (U2U, U2R, R2R) can change dynamically over time, this solution implies a *complex* policy management. On the contrary, an access control model for OSNs should have the following characteristics.

- Providing a *simple* and *flexible* way of defining access control rules. The growth of online social networks will make it more and more difficult to manage who has access to which online content. An ideal access control scheme must be intuitive and simple to use, matching the way in which people manage their social networks both online and offline.

- Providing a *single* management system able to interact with using *multiple* content sharing sites. The volume of personal content created and shared online has immensely grown, and it will continue to grow. Depending on the type of content, users might prefer using different types of services. An ideal access control scheme must be able to work with all types of content regardless of where they are stored.

- Supporting access control on the basis of users' *relationships*. Access control policies should be defined taking into account the graph-based structure of OSNs, since it is very intuitive for people to use their social relationships to define authorized members for their personal content (e.g., people could restrict the access to their pictures to their "family" or "work colleagues"). This way, one does not need to enumerate people's identities for every piece of data to protect.

- Supporting *customized* relationship, whose names and properties are defined by users. These customizations should be unidirectional and flexible enough to not constrain access control design.

- Allowing the specification and *composition* of complex relationships.

- Tracking *multiple access contexts*. Relationships can be articulated or dissolved separately in each access context. The result is that authorization decisions may be different in each context even though the access request remains the same.

- Taking into account the concepts of *trust* and *depth*. An access control policy for OSNs should make a user able to state which type of relationship should exist between him/her and the requesting user, along with the *maximum depth* and *minimum trust level* of the relationship.

Enforcement Requirements As illustrated in Section 3.2, access control is usually enforced by a software module, called a reference monitor, that intercepts each access request submitted to the system and, on the basis of the specified access control policies, determines whether the access can be partially or totally authorized, or it must be denied. Therefore, the robustness of access control relies on the trustworthiness of the entity implementing the reference monitor, which should correctly enforce all and only the specified access control policies. As a consequence, when designing an access control enforcement mechanism for OSNs, one has to decide *where* the reference monitor has to be placed, that is, which is the trusted entity of the OSN architecture in charge of evaluating access control policies.

A first possibility is to adopt a *centralized access control enforcement*, delegating to the *social network management system* (SNMS) the role of reference monitor. According to this choice, users have to completely delegate the control of their data to the SNMS, by simply stating how data must be released to other network nodes. In this scenario, which we refer to as a centralized access control enforcement, the SNMS stores the access control policies of each user in the network, it processes each access request and evaluates over it OSN members' access control policies.

Even if this kind of solution is largely accepted in other Web-based applications, it is important to understand whether centralized access control is appropriate in OSN scenario. The main reason for this concern is that adopting centralized access control enforcement implies totally delegating to the SNMS the administration of user data. Since access control is enforced by the SNMS, users actually do not know whether access control is correctly enforced. They do not have any assurance about the behavior of SNMSs with respect to their data (for instance, they could maliciously release them to unauthorized users). They have to totally trust SNMSs. Therefore, it is important to carefully evaluate whether this could be easily accepted by OSN members. It is true that, in current OSNs, users are already providing SNMS a huge amount of personal data. But, it is also true that some recent events have made users aware that the SNMS's behavior is not always honest and transparent. Some examples are reported by the EPIC public interest research center.[3] Increasing privacy concerns about how SNMSs manage personal information lead us to believe that a centralized access control solution is not the most appropriate in the OSN scenario.

A possible solution is to give OSN participants the possibility to have more control over their data is to make the network participants themselves able to evaluate their access control policies. In this scenario, which we refer to as (fully) *decentralized access control enforcement*, each participant is in charge of specifying and enforcing his/her access control policies. Each time a user receives an access request, the reference monitor, which is locally hosted by each network node, evaluates it against the specified policies, and decides whether access to the resource can be granted or not.

The main drawback of this solution is that implementing a decentralized access control mechanism implies software and hardware resources more powerful than those typically available to OSN participants. For instance, since access to a resource in an OSN is usually granted on the basis of the direct/indirect relationships the requestor node has with other nodes in the network, answering an access request may require to verify the existence of specific paths within an OSN. This task may be very difficult and time consuming in a fully decentralized solution.

Therefore, a further essential requirement of access control enforcement in OSNs is to devise efficient and scalable implementation strategies.

3.3.2 PRIVACY SETTINGS IN COMMERCIAL ONLINE SOCIAL NETWORKS

Despite the fact that the ReBAC model and its requirements are nowadays rather clearly specified, this paradigm has been applied incompletely or only partially by most of the available commercial SNMSs. Basically, a user is provided with a limited number of options according to which s/he can specify whether a given piece of information (e.g., personal data and resources) must be public, private, or accessible by the users with whom s/he has a direct relationship, or by providing simple variants to these basic settings. The same happens more or less in Google+ with its "circles." The way *privacy settings* are either implemented or used in current OSNs, highly depends on the *type* of the social network we are dealing with. In Section 1.3.1 we illustrated the evolution in social networking and described the major online social networks at present. Clearly defining the type of each social network it is not a simple task, because most OSNs combine different elements of more than one type of network, and may change their focus over time. Despite this, in this section we provide a broad classification of OSNs, and we present security and privacy recommendations valuable for this classification. The same recommendations are applicable, for hybrid types of networks, in a composite form.

Personal networks allow users to create detailed online profiles and connect with other users, and usually emphasize privacy control over social relationships such as friendship. This happens, for example, in Friendster, MySpace, Facebook, and Google+. Facebook, in particular, allows users to manage the privacy settings of uploaded content (photos, videos, statuses, links, and

[3] http://epic.org/privacy/facebook/

notes) using five different granularities: Only Me, Specific People (i.e., explicitly choose friends and/or pre-created friend lists), Friends Only, Friends of Friends, and Everyone. The latter one is the default privacy setting suggested by Facebook for many pieces of contents, meaning users share them with all 1 billion Facebook users. The granularity of privacy settings varies according to content type. Photos are grouped into albums, and privacy settings are specified on an album granularity (i.e., all photos in an album must have the same privacy settings). For the remaining content types, users can specify different privacy settings for each piece of content. In Google+, the way information is shared occurs in two ways: through overall Google+ account privacy settings and through the set-up of "circles" of contacts. With Google+, all of a user's posts will go to either Public (anyone can see) or circles that s/he choose. Organizing contacts into specific circles can be time consuming but allows users to choose the people they want to share contact with. It works in the same way as Facebook lists.

In *status update networks*, designed to mainly allow users to post short status updates in order to communicate with other users quickly, there may be privacy settings to restrict access to status updates. In Twitter, for example, when creating an account, one has to decide if s/he wants to protect her/his tweets or have public tweets. The protected tweet feature means that no one other than the people one allows to follow will see her/his messages. It also means that not authorized users cannot re-tweet her/his messages and share them on their own streams. In a public Twitter feed, anything a user posts can be seen by anyone, even search engines, whether they are following her/his or not.

With the advent of GPS-enabled technologies, *location networks* are growing in popularity. These networks are designed to broadcast one's real-time location, either as public information or as an update viewable to authorized contacts. Foursquare is probably the most well-known location-based network and, together with other location networks is built to interact with other social networks. In addition to this, many OSNs include location-based information (via the "check-in" tools), which is usually protected according to main privacy settings (e.g., allowing users to state if a given piece of location-based information is public or restricted).

When social networks are built around a common interest or geared to a specific group of people, we refer to these as *shared-interest networks*. These networks incorporate features from other types of social networks but are slanted toward a subset of individuals, such as those with similar hobbies, educational backgrounds, political affiliations, ethnic backgrounds, religious views, sexual orientations, or other defined interests. LinkedIn, a social network with business purposes, is based on full and honest disclosure of one's professional information to serve as a profile that can act as an online resume. There are many different settings within LinkedIn to help users to control what information they share publicly and how information is shared in their network. To have the higher level of privacy, a user can choose to display anonymous profile information, or show up as an anonymous LinkedIn member. Otherwise, it is possible to choose intermediate actions: (1) turning on/off the activity broadcasts, to prevent user's connections from seeing when changes are made on her/him profile, followed companies, or recommended connections; (2) selecting who can see the activity feed, choosing who can see the activity section on the user profile; (3) selecting who can see personal connections, by sharing the connections' names with only first-degree connected users, or keeping them private; and (4) choosing who can send invitations, allowing only certain people to send invitations and turning on/off group invitations.

Independently from the specific online social network type, such a simple access control paradigm has usually the advantage of being straightforward and easy to be implemented. Despite this, it suffers from several drawbacks. Over the years, users awareness and use of OSN privacy settings have changed. For example, from early empirical studies, Facebook users in the U.S. had inconsistent behavior with respect to privacy concerns, demonstrating excessive sharing of personal data and rare changes to default privacy settings [129], even users who claimed to be concerned about privacy [7]. Still in 2006–2008, a low percentage of Facebook profiles in the U.S. were restricted to "friends only" [178]. The situation was slightly different in the U.K., where in 2008 the majority of the respondents (57.5%) reported having changed the default privacy settings [152].

Now that more recent studies suggest that users are becoming more privacy concerned and more likely to change their privacy settings [36], some criticalities still remain. In fact, according to [189, 196], users are not completely satisfied about a social network's ability to protect their privacy. The complexity of privacy settings varies greatly across different social network services. In all, according to [196], 48% of social network users still report some level of difficulty in managing the privacy controls on their profile. Few users (2%) describe their experiences as very difficult, whereas 16% say they are somewhat difficult. For instance, social network users who are college graduates are significantly more likely than those with lower levels of education to say that they experience some difficulty in managing the privacy controls on their profiles. In addition to this, according to [189], 36% of the Facebook content still remains shared with the default privacy settings and, overall, privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected.

In general, as emerges from the above analysis, privacy settings of many commercial OSNs have many shortcomings. First of all, it may either grant access to non-authorized users or limit too much information sharing. In addition to this, it may be tedious and time consuming, for example if we think of the process of categorizing friends into lists. Moreover, privacy settings are not flexible enough to express the heterogeneous access control requirements that different OSN users may have, and the different privacy preferences that may vary depending on the piece of information to share. For all these reasons, various research approaches have been proposed to give a response to these open issues.

3.3.3 EXISTING ACCESS CONTROL APPROACHES

Over the years, several approaches have addressed the problem of access control in OSNs. Some of them focus more on describing the access control model properties, and usually implement (explicitly or implicitly) the ReBAC paradigm. Others follow a more or less traditional security-based direction, focusing on crypto-based enforcement techniques taking into account the particular characteristics of OSNs. Obviously, the distinction between approaches that we follow in this section for the sake of simplicity is not always so clear, and both aspects can be found in single approaches.

Approaches focusing on the Access Control Model

Concerning approaches mainly focusing on access control model aspects, the D-FOAF system proposed by Kruk et al. [172] represents a first attempt at taking into account relationships among users. Being one of the first works in this field, it is primarily a Friend of a Friend (FOAF) ontology-based distributed identity management system for social networks, where access rights and trust delegation management are provided as *additional services*. In D-FOAF, relationships are associated with a *trust level*, which denotes the level of friendship existing between the users participating in a given relationship. A first drawback of this work is constituted by the fact that it discusses only a *single generic relationship*, corresponding to the one modeled by the `foaf:knows` RDF property in the FOAF vocabulary. In addition to this, in D-FOAF, both path discovery and access control are enforced by the D-FOAF *centralized* SNMS, hosting the resource owner account. The absence of multiple types of relationships and the centralized nature of the proposed enforcement technique make this model not suitable for the OSN scenario.

In the formal model for access control in Facebook-like systems developed by Fong et al. [105], access control is treated as a two-stage process, namely, reaching the search listing of the resource owner and accessing the resource, respectively. Reachability of the search listings is a necessary condition for access. Although lacking support for directed relationships, multiple relationship types and trust metric of relationships, this model allows expression of arbitrary topology-based properties, such as "*k* common friends" and "*k* clique," which are beyond what Facebook and other commercial OSNs offer today. Fong in his later work [104] proposes an archetypical ReBAC model for social computing applications, i.e., authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the protection system. The model employs a *modal logic language* (extended in [106]) for policy specification and composition and allows *multiple relationship types* and directional relationships. Access is authorized in contexts and is based on U2U relationships between the accessing user and the resource owner. Sharing of relationships among contexts are achieved in a rational manner through a context hierarchy.

Carminati et al. [49, 51, 52, 53] propose a series of access control solutions for OSNs. In [52], *access rules* are specified by the users at their discretion. The access requirements that the accessing user must satisfy are based on enforcement of *access conditions* expressed as constraints like type, depth, and trust level of existing *user-to-user relationships* between the accessing user and the resource owner. Moreover, the flexibility in specifying authorized members is enhanced by *∗-conditions*, that is, the possibility not to limit the required maximum depth and/or minimum trust level in an access condition. Access control is enforced through a *semi-decentralized* client-side approach, according to which the requestor of a resource is in charge of providing the resource owner with a proof showing that s/he satisfies the corresponding access rules. This implies showing that there exists the relationship(s) required by the specified access rule(s), with the required depth and trust level. In order to make a requestor able to generate a proof, each relationship is encoded into a public certificate stored by a Central Node (CN). This solution is semi-decentralized in the sense that members rely on external entities only for certificates management (i.e., retrieval of certificate paths). A member still has the capability to verify whether the certificate paths returned by a CN are correct or not, by simply inquiring other certificate servers. This model has been extended in [53] to make access control decisions using a completely *decentralized* and *collaborative* approach. The final system adopts a distributed trust metrics, in which the trust between the owner and the accessor is obtained by the weighted average of the trust levels between the accessor and the "trustworthy" neighbors of the owner. The issue of *collaborative access control* has been also treated by Carminati et al. [49], introducing a new class of security policies, called *collaborative security policies*, that basically enhance topology-based access control with respect to a set of collaborative users.

Under a different perspective, Squicciarini et al. [257] provide a solution for *collective privacy management* in OSNs. Their work considers access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content. The *Clarke-Tax mechanism* [91] is adopted to enable the *collective enforcement* of policies for shared contents. Game theory was applied to evaluate the scheme. However, a general drawback of their solution is the usability issue, as it could be very hard for ordinary OSN users to comprehend the Clarke-Tax mechanism and specify appropriate bid values for auctions. Also, the auction process adopted in their approach indicates that only the winning bids could determine who can access the data, instead of accommodating all stakeholders' privacy preferences.

With respect to Carminati et al. [49] and Squicciarini et al. [257], the work of Hu et al. [140] proposes a formal model to address the *multiparty access control* (MPAC) issue in OSNs, along with a general *policy specification scheme* and *conflict resolution* mechanism for *collaborative management of shared data* in OSNs. In particular, the model considers the social application as an accessor, the user as a disseminator and the user's friend as the owner of shared profile attributes. Both the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Users can also share their relationships with other members: a user called owner, who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the owner and the stakeholder are considered, in order to avoid the violation of the stakeholder's privacy concerns. Finally, all the users involved in content sharing can specify access control policies to control who can see the shared content.

Still in the field of *collaborative access control* in social computing, Carminati et al. in [51] propose a model offering more complete policy administration by addressing *policy management* and *conflict resolution*. In particular, the model employs Semantic Web technologies, including the Resource Description Framework (RDF) and the Web Ontology Language (OWL), to describe user profiles and relationships among users and among users and resources. Doing so allows authors to see a social network as a knowledge base of *user-to-user* and *user-to-resource* relationships, based on which they define three kinds of access policies: authorization, administration and filtering policies. They are formulated via the Semantic Web Rule Language (SWRL). Semantic Web technologies have been exploited also in [201] so as to propose an access control model enabling users to express more fine-grained access control policies on a social network knowledge base, by also protecting relations. Ontologies are also used in the framework proposed in [202] at the aim of formally analyzing what privacy-sensitive information is protected by the stated policies of a OSN.

The issue of implementing models taking into account relationships other than user-to-user is addressed in the works of Cheng et al. [66, 67]. In [66] authors propose a *user-to-user relationship-based access control* (UURAC) model and a *regular expression-based policy specification language* which enables fine-grained access control in OSNs. UURAC supports policy individualization, user and resource as a target, distinction of user policies for outgoing and incoming actions, and relationship-based access control. It incorporates in its policy specifications the treatment of inverse relationships. Relationships and authorizations are articulated in access contexts and context hierarchy to support sharing of relationships among contexts. Authors leave the explicit treatment of user-to-resource and resource-to-resource relationships to their later work [67], together with the treatment of *multiple-users access control policies specification* and *conflicts resolution*. Specifically, these policies are specified in terms of relationship path patterns between the accessing user and the target together with hop-count limit of the relationships. The decision modules of the system determine authorizations by retrieving different policies from the accessing session, the target and the system, and then making a collective decision. To address policy conflicts, authors apply conflict resolution policies over relationship precedence.

With respect to these approaches, the work of Shehab et al. [251] presents an access control framework focusing in particular to the management of third party applications. Their framework is based on enabling a user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. Applications are modeled as finite state machines, and use the required user profile attributes as conditions governing the application execution. They formulate the minimal attribute generalization problem and propose a solution that maps the problem to the shortest path problem to find the minimum set of attribute generalization required to access the application services.

Approaches Focusing on Encryption

The first approach we describe is the one of Ali et al. [12]. In their work, authors adopt a *multi-level access control* approach, where the security levels assigned to both users and resources are specified on the basis of the *trust level*. Each user *u* has a security level computed as the average of the trust ratings specified for her/him by other users in the system. Each resource o has associated the security level of the corresponding owner. According to multi-level access control, a user can access only those resources having a security level equal to or less than her/his level. Access control is enforced according to a *challenge-response* based protocol. This implies that, for each resource, the owner generates a secret key K, which is then processed by a (n, K) threshold algorithm, in order to obtain n portions of K. All these portions are then distributed to n trustworthy nodes. Once a requestor wishes to access a resource, the owner sends to her/him the challenge encrypted with the corresponding secret key K. In order to gain the access, the requestor has to retrieve the portions of K from the set of nodes holding them, which in turn release the portion only if the requestor satisfies the trust requirements specified by the resource owner. Once the requestor has reconstructed K, s/he responds to the challenge. The main problem in the mandatory approach proposed by Ali et al. is that, since the security levels are computed on the basis of user trust levels, their management (e.g., computation, update) could be a complex task due to the dynamic nature of OSNs.

In [264], Tootoonchian et al. describe Lockr, a "Social Access Control for Web 2.0." Lockr allows users to express access control policies based on *multiple social relationships* between users. Its aim is the separation between social networking information and the content sharing mechanisms, thereby eliminating the need for users to maintain many site-specific copies of their social networks. The enforcement mechanism provided by Lockr is based on the concepts of *social attestations* and *social access control lists* (ACLs). A social attestation is a piece of data that certifies a social relationship. Two parties could share more than one attestation since two people can have more than one relationship. Via social ACLs, it is possible to have access to others based on their social relationships. The relationship key is a shared key among all parties with the same relationship with the attestation's issuer. Its role is to protect attestations from being revealed to third parties. Whenever the attestation is transmitted to another party, it is first encrypted with the relationship key. This prevents malicious third parties from having access the social information encapsulated in attestations even if they were to intercept their transfers illegitimately. A social ACL contains the owner's public key, the public keys of all people who can access the object (like in traditional ACLs), and a social relationship. To access an object, people must either have their public key listed in the social ACL, or they must present an attestation issued to them by the owner certifying the relationship listed in the ACL. Social ACLs are signed to guarantee their integrity and authenticity. Based on the ACL, the person seeking access determines which attestation to use to obtain access. When the ACL lists a conjunctive relationship, a person might have to send more than one attestation to obtain access. In this case, the attestations are concatenated in one single message. To access an object, a person must either have their public key listed in the ACL or an attestation certifying the social relationship listed in the ACL. An *attestation manager* allows people to exchange attestations, and allows a user's applications to retrieve attestations to gain access to protected content. According to the authors, the attestation manager can be implemented in many different ways, such as a stand-alone desktop application, an extension to an address book or an e-mail client, or even as an application running on a person mobile phone. Based on their preferences, people can use any of such attestation managers in the same way as people use many different e-mail clients or calendars. The main concern with the Lockr extension is the need to rely on a trusted third party storage for the hidden information, instead of trusting the OSN provider.

NOYB (None Of Your Business) is a system proposed by Guha et al. [131] targeted at protecting user privacy on Facebook. It is a general *cipher and encoding scheme* that preserves the semantic properties of data such that it can be processed by the social network provider unaware of encryption. Instead of applying traditional encryption schemes, NOYB divides the personal details of users, such as name and gender, into *atoms*. These atoms are separated and shuffled with atoms of other users, acting as a *random substitution cipher*. For example, the encryption method used by NOYB just replaces the privacy details of user A with those of random users B, C, and D: A's profile ($nameA$, $genderA$, $ageA$, $addressA$) is broken into the three pieces ($nameA$, $genderA$), ($ageA$), and ($addressA$), which are then substituted with ($nameB$, $genderB$), ($ageC$), and ($addressD$) from users B, C, and D, respectively. Only the user her/himself and her/his friends can reverse the process and reconstruct the profile. However, (i) this can only be applied to the personal details on the user's profile, and does not allow encryption of free text entries as frequently found in social networks; (ii) the number of users that use NOYB impacts its effectiveness. The larger the number of users, the better the anonymity; and (iii) NOYB does not allow old friends to get in touch unless they have enough information to recover the profile information of their friends.

These issues have been solved by Luo et al. [192] via FaceCloak: a Firefox extension that uses a *symmetric key* mechanism to encrypt user's information in Facebook. Differently from NOYB, FaceCloak opts to store the encrypted data on a third-party server, with fake data (random text fetched from Wikipedia) stored at the OSN provider. The symmetric keys are shared with the set of users authorized to read the content. The random text acts as an index to the encrypted data on the server. A main drawback of this approach consists in its complicated and inefficient key distribution system [24]. For each piece of content, the user accessing the content has to use an offline channel to retrieve the key.

Another implementation of an OSN-independent Firefox extension is Scrumble by Beato et al. [25]. It allows users to enforce access control over their data. Scramble lets users define *access control lists* (ACL) of authorized users for each piece of data, based on their preferences. The definition of ACL is facilitated through the possibility of dynamically defining contact groups. In turn, the confidentiality and integrity of one data item is enforced using cryptographic techniques. When accessing an OSN that contains data encrypted using Scramble, the plugin transparently decrypts and checks integrity of the encrypted content. With respect to FaceCloak, Scramble uses a simpler and more reliable approach for key distribution. The encryption of the content is done using *public keys*, and thus a user with access rights just needs to use his own secret key for decryption. As a usability compromise, authors restrict the use of PGP's web-of-trust mechanism to power-users and adopt *leap-of-faith authentication* as the default key-distribution paradigm. In their later work, Beato et al. [24] present a system still enabling users to exchange data over any web-based sharing platform, while keeping both the communicated data confidential and hiding from a casual observer that an exchange of confidential data is taking place. Their approach is based on *steganography*, the same technique employed by Luo et al. [192] for FaceCloak and Besenyei et al. [27] in their StegoWeb system. In general, steganography refers to concealing a message or file within another message or file. With respect to other approaches using this technique, in the work of Beato et al. [24] the pointer to the protected data is concealed, not the data itself. This way, their system hides the fact that confidential data are being exchanged. Specifically, the approach replaces the user's real posting on the OSN with fake data that look like another genuine message either automatically or with the user's help. Users real data are encrypted for a user-defined set of recipients and stored in a user-selectable, public storage service which returns a URL to the encrypted content. Next, in order to keep the storage location private, the system applies a pseudo-random function to the posted fake data (the implementation uses a keyed hash function) and computes a lookup-key. In a final step, this lookup-key is then used to store the (encrypted) URL of the encrypted file in another user-selectable, arbitrary URL lookup service (e.g., TinyURL). On the authorized recipients side, the system performs the reverse operations while the user visits the OSN page.

Persona, by Baden et al. [19], is essentially a privacy-enhanced OSN. It proposes the use of *attribute-based encryption* (ABE) to enable fine-grained access control. As Lockr [264] uses ACLs based on social attestations of relationships between users, similarly Persona distributes ABE secret keys (ASKs) corresponding to the set of attributes that defines the groups that friend should be part of. A user can create groups by assigning different attributes and keys to her/him social contacts, and then encrypt data such that only particular users having the desired set of attributes can decrypt it (both Persona and Lockr use XML-based formats to transfer privacy-protecting structures). This mechanism protects information from unauthorized users on the OSN, third-party application developers, and above all the OSN itself. Despite this, it must be taken into consideration that groups are dynamic and therefore user attributes may change over time (e.g., change in location, work environment, the nature or strength of the relationship with a contact, etc.). Persona and similar systems (e.g., Beato et al. [25] and Ali et al. [12] for trust re-computation issues) introduce significant overhead for group membership changes, especially when a contact is removed from a group. In this case, all other members of the group must receive a new key; additionally, all existing data items accessible for that group must be re-encrypted. This does not scale when groups are large and dynamic, and when the volume of past data is high.

Since ABE supports fine-grained policies but it leaves open the challenge of supporting dynamic groups, and in particular, revocation, EASiER solves this issue by introducing a *minimally trusted proxy* implemented by a *centralized* service. Each user's proxy is assigned a secret proxy key with revocation information. A user who revokes a contact or an attribute need not issue new keys to the rest of the group, nor re-encrypt data. Proposed by Jahid et al. [147], EASiER is an architecture that enables users to set fine-grained access control policies based on *multiple types* *of relationships*. In their further prototype DECENT, Jahid et al. [148] propose two extensions to the base EASiER scheme. First, they use *threshold secret sharing* to split the proxy functionality among several randomly selected nodes; since they assume that the majority of nodes are not actively malicious, this will ensure the security of the proxy. Second, they extend EASiER to support *attribute delegation*: if Alice issues a key with a set of attributes to Bob, Bob can delegate a subset of these attributes to Carol. This way, Alice can define a friend-of-a-friend attribute and ask all her contacts to delegate it to all of their contacts.

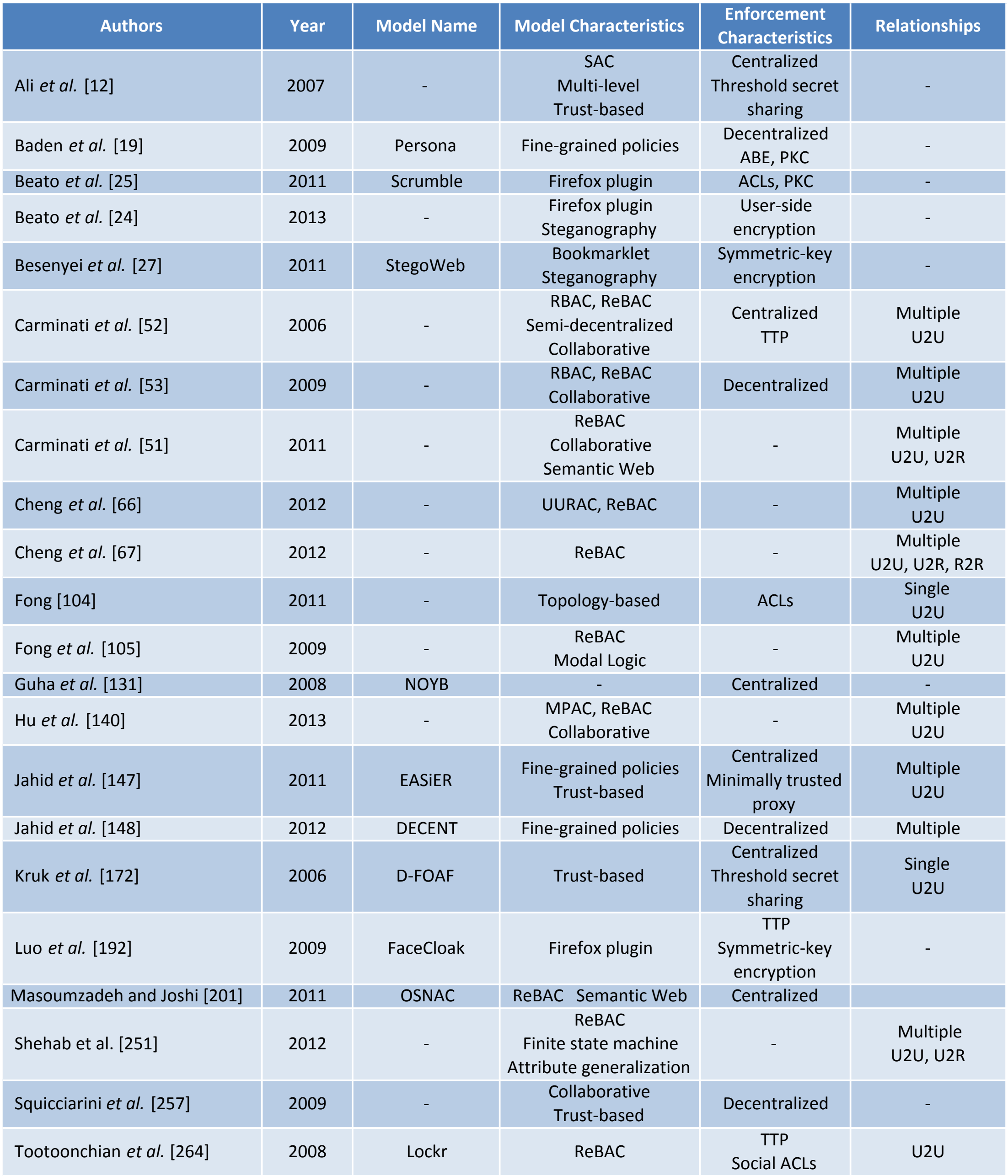
Summary of Approaches

Figure 3.1 summarizes the described approaches, focusing on specific aspects emerging from the above treatment. Different approaches are alphabetically ordered by authors, where it is possible we provide the name of the proposed models. For each access control proposal, we specify the year of the publication, the model characteristics (if applicable) and the enforcement characteristics (if applicable). For those approaches focusing in particular on the model, we analyze which kinds of relationships they take into account: *single* or *multiple*, and, between them, if they are U2U, U2R, R2R.

3.4 CONCLUSIONS

In this chapter we addressed the problem of information dissemination in online social networks. In these environments, millions of individuals share personal and confidential information with an incredible number of (possible unknown) other users. Traditional solutions adopted in conventional data management systems are based on access control techniques. These techniques aim in particular to prevent unauthorized operations (such as read and write) on data.

In the scenario of online social networks, the focus shifts on controlled information sharing of users' personal data. Taking into account the relationship-based nature of OSNs, the ReBAC model for access control has been proposed; it is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships.



Authors	Year	Model Name	Model Characteristics	Enforcement Characteristics	Relationships
Ali *et al.* [12]	2007	-	SAC Multi-level Trust-based	Centralized Threshold secret sharing	-
Baden *et al.* [19]	2009	Persona	Fine-grained policies	Decentralized ABE, PKC	-
Beato *et al.* [25]	2011	Scrumble	Firefox plugin	ACLs, PKC	-
Beato *et al.* [24]	2013	-	Firefox plugin Steganography	User-side encryption	-
Besenyei *et al.* [27]	2011	StegoWeb	Bookmarklet Steganography	Symmetric-key encryption	-
Carminati *et al.* [52]	2006	-	RBAC, ReBAC Semi-decentralized Collaborative	Centralized TTP	Multiple U2U
Carminati *et al.* [53]	2009	-	RBAC, ReBAC Collaborative	Decentralized	Multiple U2U
Carminati *et al.* [51]	2011	-	ReBAC Collaborative Semantic Web	-	Multiple U2U, U2R
Cheng *et al.* [66]	2012	-	UURAC, ReBAC	-	Multiple U2U
Cheng *et al.* [67]	2012	-	ReBAC	-	Multiple U2U, U2R, R2R
Fong [104]	2011	-	Topology-based	ACLs	Single U2U
Fong *et al.* [105]	2009	-	ReBAC Modal Logic	-	Multiple U2U
Guha *et al.* [131]	2008	NOYB	-	Centralized	-
Hu *et al.* [140]	2013	-	MPAC, ReBAC Collaborative	-	Multiple U2U
Jahid *et al.* [147]	2011	EASiER	Fine-grained policies Trust-based	Centralized Minimally trusted proxy	Multiple U2U
Jahid *et al.* [148]	2012	DECENT	Fine-grained policies	Decentralized	Multiple
Kruk *et al.* [172]	2006	D-FOAF	Trust-based	Centralized Threshold secret sharing	Single U2U
Luo *et al.* [192]	2009	FaceCloak	Firefox plugin	TTP Symmetric-key encryption	-
Masoumzadeh and Joshi [201]	2011	OSNAC	ReBAC Semantic Web	Centralized	
Shehab et al. [251]	2012	-	ReBAC Finite state machine Attribute generalization	-	Multiple U2U, U2R
Squicciarini *et al.* [257]	2009	-	Collaborative Trust-based	Decentralized	-
Tootoonchian *et al.* [264]	2008	Lockr	ReBAC	TTP Social ACLs	U2U

Figure 3.1: Summary of Research Access Control Proposals.

CHAPTER 4

Identity Management in Online Social Networks

4.1 INTRODUCTION

Identity management (IdM) generally describes the management of *user identities* and their rights to access resources throughout the identity life cycle, according to users' rights and restrictions associated with the established identities. *Identity management systems* provide services and technologies for controlling user access to critical information. Among these services and technologies, the most well known include Active Directory, Identity Providers, Digital Identities, Password Managers, Single Sign-on, Security Tokens, Security Token Services (STS), OpenID, WS-Security, WS-Trust, SAML 2.0, and OAuth.

The development of Web 2.0 technologies has led to the definition of the concept of *Online Identity Management* (OIM), whose meaning it twofold.

- When it refers to *online image management* or *online personal branding* or *personal reputation management* (PRM), OIM is a set of methods for generating a distinguished Web presence of a person on the Internet. That presence could be reflected in any kind of content that refers to the person, including news, participation in blogs and forums, personal websites [198], social media presence, pictures, videos, etc.

- But online identity management also refers to *identity disclosure* and *identity theft*, and has particularly been developed in the management of online identity in social network services [266].

In OSNs, aspects belonging to both meanings constitute an integral part of the identity construction process on these sites. Due to *impression management* [41], i.e., "the process through which people try to control the impressions other people form of them"—one of whose objectives is in particular to increase the online reputation of the person—users provide a lot of personal information concerning their identities. This identity disclosure brings to mind several *identity attacks* which are particularly insidious in online social networks.

In this chapter, after having briefly introduced the general concepts connected to identity management (Section 4.2), we will discuss in detail the concerns and solutions connected to online identity management, considering the different meanings it has in online social networks (Section 4.3) as introduced before, and focusing in particular on identity protection (Section 4.3.3).

4.2 IDENTITY MANAGEMENT

Traditionally, *identity management* (IdM) refers to the task of controlling information about managed entities on computers. Managed entities typically include users, hardware and network resources, and even applications. Such information includes data that authenticate the identity of an entity, that describes actions the entity is authorized to perform. It also includes the management of descriptive information about the entity and how and by whom that information can be accessed and modified.

The concept of *identity* spans across different fields, from Philosophy, where identity, from Latin *identitas* (sameness), is the relation each thing bears just to itself,[1] to Social Sciences, where identity may be defined as "the distinctive characteristic belonging to any given individual, or shared by all members of a particular social category or group" [243].

4.2.1 DIGITAL IDENTITY

In Computer Science, the term *digital identity* is used to define "the digital representation of the information known about a specific individual or organization, in a specific application domain" [256, 279]. It includes unique descriptive data, allowing a precise identification of an entity among others, as well as other generic information. According to [158], an entity (such as a person or an organization) may have multiple identities, and each identity may consist of multiple characteristics that can be unique or non-unique identifiers.

An *identity domain* is a domain where each identity is unique. For users, derived from psychological concepts summarized by the Future of Identity in the Information Society (FIDIS),[2] a digital identity can be seen as constituted by:

1. a *personal identity*, composed of persistent identity information such as name, date of birth and genealogical relations;

2. a *shared identity*, that is, information which is susceptible to change such as social network of user profile information (shopping list, centers of interest, friends); and

3. an *abstract identity*, consisting of derived or inferred information about the user.

Nowadays, according to Viviani et al. [270], in the context of engineering online systems, the management of digital identities can involve three main research fields.

- The *pure identity* field: issues concerning the creation, management and deletion of digital identities without considering access issues (e.g., anonymization problems).

- The *user access* field: issues concerning user access requirements connected the need to assume a unique digital identity across applications and networked infrastructures.

[1] From the Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/entries/identity
[2] http://www.fidis.net/resources/fidis-deliverables/identity-of-identity/int-d2100/doc/16/

- The *personalized service provision* field: issues concerning the delivery of personalized, role-based, online, on-demand, multimedia (content), presence-based services to users and their devices.

Current identity management systems focusing on the first (pure identity) and the second (user access) field of research constitute *strict identity management* systems. Other systems, addressing also issues connected to the personalized delivering of services, are considered as *extended identity management* systems. Concrete solutions implementing these two kind of systems are described in the following section, where they are further divided according to whether as they belong to Identity 1.0 or Identity 2.0 [88].

4.2.2 IDENTITY MANAGEMENT MODELS: FROM IDENTITY 1.0 TO IDENTITY 2.0

Over the years, from a "directory-centric" approach where authentication means simply that an identity is registered on a service provider's directory (every service provider stores its own copy of each user's identify information), we have shifted towards a "user-centric" environment where an identity can truly be applied to a variety of service providers (each user controls her/his digital identity and credentials and can share them amongst many different sites). This is, according to Dick Hardt's Identity 2.0 Keynote at OSCON 2005,[3] the difference between Identity 1.0 and Identity 2.0.

Traditional Identity 1.0 management systems [89, 158] include *isolated*, *centralized*, and *federated* user identity models. In isolated solutions, service providers are both credential providers and identifier providers for their users. A user gets separate unique identifiers from each service/identifier provider s/he transacts with and has separate credentials (e.g., passwords) associated with each of their identifiers. In centralized models, a single identifier and credentials provider is used by all service providers, either exclusively, or in addition to other identifier and credentials providers. Finally, in federated systems, a set of software components and protocols allows service providers to identify users within a federated domain throughout their identity life cycle. Federating isolated identifier domains gives the client the illusion of being in a single identifier domain. Either centralized or federated models can be implemented in different manners and with different technologies, but both can provide Single Sign-On (SSO) [79] solutions. In a SSO solution, a user only needs to authenticate her/himself (i.e., sign-on) once to access all the services of multiple related, but independent software systems. In this sense, Microsoft .Net Passport (over the years also known as Microsoft Wallet, Microsoft Passport, Microsoft Passport Network, and more recently Windows Live ID) was the first centralized SSO implementation of a large identity management system for e-commerce. Due to the absolute control over the identity information by Microsoft, the .Net Passport has failed to become the Internet identity

[3] http://dickhardt.org/presentations-2/

management tool [89].[4] Federated SSO standards like the Security Assertion Markup Language (SAML)[5] and WS-Federation [123] represent secure mechanisms for passing credentials and related information between different websites that have their own authorization and authentication systems. SAML is an open standard developed by the Organization for the Advancement of Structured Information Standards (OASIS)[6] Security Services Technical Committee, while WS-Federation was developed by a group of companies led by Microsoft and it offers federated SSO functionality equivalent to those provided by standard SAML [4].

Nowadays, that online identity communities place the end-user at the center by relaying all communication between identity providers and service providers through the user's client [40], the Identity 2.0 paradigm takes into account these user-centric aspects while still being compatible (at least) with federated identity management. In this field, the OASIS consortium has proposed its Version 1.0[7] of Identity Metasystem which, according to [47], can be defined as "an interoperable architecture for digital identity enabling people to have and employ a collection of digital identities based on multiple underlying technologies, implementations, and providers." Concrete examples of Identity 2.0 management systems are: OpenID [235], describing how users can be authenticated in a decentralized manner via a third party service. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication; OAuth [144], a service that is complementary to, but distinct from OpenID, providing a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections; Shibboleth,[8] a "single sign-in," or logging-in system for computer networks and the Internet, a project for federated identity-based authentication and authorization infrastructure based on SAML and Information Card.[9] This latter enables people to organize their digital identities and to easily select the one they want to use for any given interaction. The Information Card metaphor is implemented by Identity Selectors like Windows CardSpace [47, 64] and the Higgins project.[10] An Identity Selector system generally provides the user with an interface to create and manage personal information cards. Higgins, in particular, proposes a technique also addressing extended identity management problems. The same happens in G-Profile [270], whose aim is to provide a user-centric, general-purpose and flexible user modeling system via the possibility for user profiles to evolve over the time. This model is based on secure users' information propagation among applications and the possibility for applications to establish partnerships among them. In the field

[4] The evolution of Microsoft .Net Passport is nowadays constituted by Microsoft Account, a single sign-on Web service allowing users to log into many websites using one account via an existing e-mail address or the sign-up for a Microsoft e-mail address. http://account.live.com

[5] Online Community for the Security Assertion Markup Language (SAML) OASIS Standard. http://saml.xml.org/

[6] OASIS. Advancing open standards for the information society. http://www.oasis-open.org/

[7] http://docs.oasis-open.org/imi/identity/v1.0/identity.html

[8] Shibboleth. http://shibboleth.net/

[9] Information Cards. http://informationcard.net

[10] Higging. Personal Data Service. http://www.eclipse.org/higgins/

of cloud computing, SPICE [70] focuses in particular on two problems. On the one hand, it treats unlinkability, ensuring that none of the cloud service providers (CSPs), even if they collude, can link the transactions of the same user. On the other hand, it guarantees that delegatable authentication is unique to the cloud platform: several CSPs may join together to provide a packaged service, with one of them being the source provider which interacts with the clients and performs authentication while the others will be transparent to the clients.

4.3 IDENTITY MANAGEMENT IN ONLINE SOCIAL NETWORKS

As introduced before, Identity 2.0 is a set of methods for *identity verification* on the Internet, using emerging user-centric technologies (e.g., Information Cards, OpenID). Identity 2.0 stems from the Web 2.0 theory of the World Wide Web transition but, as discussed in Section 4.1, the development of Web 2.0 technologies and the Social Web phenomenon have lead to the development of *Online Identity Management* which is, in a sense, a wider concept than Identity 2.0. In fact, Web 2.0 technologies provide the means to identify other people to assess the benefit of engaging with them into a *social exchange* [217]. In this perspective, a main component in online social networks is the support for the definition and the construction, for each entity in the social environment, of a rich *online identity*. An online identity, *internet identity*, or *internet persona* is a social identity that an Internet user establishes in online communities and websites.

In the OIM scenario, as illustrated in the Introduction, the management of an online identity can be considered as (i) an actively constructed *presentation of oneself* or (ii) a way to protect user identities in OSNs. Considering OIM as an activity of identity protection we must take into account that identities in OSNs can be found in a variety of forms and can have different nature. Some people prefer to use their real names online (or they are pushed to explicitly declare their identity due to the social network policy concerning user profiles). Other users prefer (or are requested) to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally identifiable information. Some can even be deceptive about their identity or, again, it can implicitly emerge (tacit identity) via the posted opinions in blogs, the role one fulfill (e.g., in Wikipedia) or reputation indicators [217]. Taking into consideration these different circumstances, two main "security" problems emerge: *identity disclosure* [1] and *identity theft* [171], already studied in "traditional" Identity Management. In OIM and in particular connected to OSNs, they present specific concerns.

In the following sections, taking into account the different aspects connected to OIM, we first briefly analyze issues connected to self-presentation and identity disclosure, leaving to the rest of the chapter a detailed treatment of identity theft attacks and solutions on OSNs.

4.3.1 IDENTITY AS SELF-PRESENTATION

As Goffman originally argued [116], individuals construct their identities in reaction to their cohorts. In the Web 2.0 scenario, we can affirm that individuals express and expose their identities relatively to their networks [198]. In doing this, individuals focus both on strong ties as articulated by Granovetter [126]—close, intimate, high-trust, long-term relations (see Section 1.3.3)—and weak ties, requiring less investment, in terms of emotion, information capital, or time. They can exist along single channels, thus diminishing the "noise" of overlapping identities. If a new identity (or self-presenting strategy) fails, it costs relatively little to cut the tie linked to that particular identity.

The ease and freedom in generating different identities/identity strategies are connected to the concept of *masking identity*. According to Wiszniewski and Coyne [280] (Building Virtual Communities), whenever individuals interact in a social sphere they portray a mask of their identity. The kind of mask one chooses reveals at least something of the subject behind the mask. One might call this the "metaphor" of the mask. The online mask does not reveal the actual identity of a person. Anyway, even if a person chooses to hide behind a totally false identity, this says something about the fear and lack of self-esteem behind the false mask.

In addition to this, the concept of *blended identity* explains that many different aspects or dimensions of self-definition can be salient simultaneously. In other words, it includes the situation where more than one identity simultaneously shapes a person's self-definition in a particular social context. The study of blended identity is controversial, perhaps mainly due to the fact that some critics believe that this theoretical notion can be overstated.

Self-presentation involves, in particular, emotional and psychological fields, for this reason its detailed treatment is out of the scope of this chapter.

4.3.2 IDENTITY DISCLOSURE

In general, information disclosure enables an attacker to gain valuable information about a user (or a system). In online social networks, where identities deal with personal data, disclosure of confidential information Users profiles contains many personal information and many of user's extra information may be recorded by social services without notifying (at least explicitly) users. This represents a risk in terms of exposure of this data and user information/identity abuse. Users can loose control of the extra information, knowing nothing about who can acquire the information, and cannot assure how these indirect receivers will use the information. Avoiding identity disclosure deals mainly with *privacy-preserving social network data mining* [282], whose treatment is out of the scope of this book (instead, please refer to [281, 301]). Despite this, since disclosure is in a sense connected to identity theft, here we provide a brief discussion.

According to [137], disclosure can be connected to (i) explicit data release, also known as *self-disclosure* [180], or (ii) *private information leakage* [186].

Self-disclosure

Concerning the first issue voluntary confidential information disclosure is often concomitant with the online social network use itself. OSNs often encourage registered users to provide as much information as possible. For example, on the marketing front, Google recently patented an algorithm to rate individual's influence within social media. Once publicized, it will likely encourage greater participation by active users in order to boost their influence score. Users are therefore willing to provide self-disclosure to obtain some advantages. The concepts of self-disclosure and self-presentation are in this sense strictly connected [249]. According to the works by Goffman [116], Donath and boyd [83] and boyd and Heer [37], users employ an online social network as a performance of identity. Strategically presenting themselves, through the constructed profiles, users' challenge is to increase their diverse networks of social ties. Similarly, Lampe et al. [177] note that motivations for use and disclosure within an online social network are a function of offline outcomes such as relational formation and deepening. Works by Bumgarner [43] and Joinson [152] illustrate the social motive of online social network use and consequent personal data disclosure: the participants desire to connect and learn about one another. Without significant personal sharing in these sites, these motives of use would not be addressed. For this reason, recent research points out that OSNs seem to require self-disclosure by default [153, 222].

Private Information Leakage

Conversely, private information leakage is related to details about an individual that are not explicitly stated, but, rather, are inferred through other details released and/or relationships to individuals who may express that detail [137]. Over the years, several *inference attacks* and or ways to prevent them have been studied in literature. Some works are based on link-based classification [186, 195] and link prediction [274, 290], while others focus on attribute disclosure [68, 300]. Other works consider attacks over anonymized networks [18, 218] and others several methods to anonymize social networks [188, 299] as a way to prevent users' identification. Naively speaking, in order to preserve node identity in the graph of relationships, synthetic identifiers are introduced to replace names. Naive anonymization represents the easiest solution in online social networks to perform social network analysis in the absence of names and unique identifiers. Even if network anonymization represents a hot topic in the current OSN scenario, in this book we treat security issues emerging when users actively exploit social network services, not during social network analysis activities. For this reason, due to the attention that the latter topic has received in literature, we invite one more time the reader to refer to the works of Wong and Fu [281] and Zheleva et al. [301], already published by Morgan & Claypool.

4.3.3 IDENTITY THEFT

Intuitively speaking, based on their characteristics described all along the book, online social networks have one of the greatest potential for abuse. Over the years it has been demonstrated that identity theft and personal security issues are ever-present concerns associated with information disclosed online (for example in [102, 180, 228, 266]). Dealing with personal information collected by social network services, which often include full names, addresses, birth day and year, contact information, and photos, the risk of seeing one's own identity stolen or used for unwanted/illegal purposes is particularly high. Even a selected few pieces of personal information has possibly the potential to provide identity thieves with the means to acquire "identity-based" information such as social security numbers, credit cards, drivers licenses, etc. In addition to this, apart from concerns regarding the protection of identity, disclosure of personal information (even if limited) can be sufficient, when combined with other Internet based tools (e.g., reverse directory checks), to obtain home phone numbers, full addresses, age and gender and other information that could leave a person vulnerable.[11]

In all these cases, attacks on identity make the theft easier to gain profits from the stolen identity information. Attacks on social networks are usually variants of traditional security threats (such as malware, worms, spam, and phishing) [145]. However, these attacks are carried out in a different context by leveraging the social networks as a new medium to reach the victims. In the following sections, we will provide a description of the main identity theft attacks in online social networks. In February 2008, the Consumer Sentinel, a Federal Trade Commission (TFC) complaint database, gave a statistic of identity theft events in 2007, during which the Consumer Sentinel received over 800,000 consumer fraud and identity theft complaints [4].

Social Engineering Attacks

First of all, from an attacker's point of view, the access to detailed personal information in social networks is ideal for launching targeted, *social engineering attacks*. A social engineering attack is one in which the intended victim is somehow tricked into doing the attacker's bidding. Most online social engineering attacks rely on some form of "pretexting" [210]: the attacker establishes contact with the target, and sends some initial request to bootstrap the attack. In this sense, this kind of attack can come in many forms—emails that masquerades as breaking news alerts; greeting cards; announcements of bogus lottery winnings—but the most well-known attacks are *spear phishing* [146] and *spam* [29] attacks.

Spear Phishing Attack In general, phishing is the practice of using fraudulent emails to gain access to personal information for the purpose of identity theft. But, whereas single, mass e-mails are sent to a certain number (hundreds of thousand) of people in a phishing attack, *spear phishing attacks* are customized and sent to a single person at a time. The aspect making this attack particularly insidious is that spear phishing exploits personal information extracted by social network services (e.g., a name from Facebook or some tidbit about employment from LinkedIn) in order to let users be lulled into a false sense of security when receiving a (fraudulent) customized email. In [146], authors crawled a number of social networking sites and downloaded publicly available information on users. Then, they manually constructed phishing e-mails that contained some personal information on the victims that they were able to retrieve from the social networking sites.

[11] http://www.pcworld.idg.com.au/article/190913/study_facebook_users_easy_targets_identity_theft/

The results of the study show that victims are more likely to fall for phishing attempts if some information about their friends or about themselves is included in the phishing mail.

In a statement released to Forbes in August 2012,[12] Facebook reported that the company has "discovered a single isolated campaign that was using compromised email accounts to gain information scraped from Friend Lists due to a temporary misconfiguration on our site. We have since enhanced our scraping protections to protect against this and other similar attacks, and will continue to investigate this case further." Even if the company also declared: "to be clear, there was neither a mass compromise of Facebook accounts nor any leak of private information," the number of spammers interested in the vast amount of personal data available on sites like Facebook, Google+, Twitter, and LinkedIn to learn all about users is continuously growing.[13] Facebook recommends that users visit Facebook's security page and read the items "Take Action" and "Threats," and take particular steps to help protect their accounts in the future, e.g., review the security settings and eventually enable login notifications; do not click on strange/unknown links (even if they're from friends), and notify the person in the case of something suspicious happens; do not accept on friend requests from unknown parties; report a scam so that it can be taken down; don't download unknown/suspicious applications; text "otp" to 32665 from a U.S. mobile phone when accessing from public places to receive a one-time password to the personal account. The company also outlined several measures taken to prevent this kind of attack: "to help protect our users, we've built enforcement mechanisms to quickly shut down malicious pages, accounts and applications that attempt to spread spam by deceiving users or by exploiting several well-known browser vulnerabilities. We have also enrolled those impacted by spam through checkpoints so they can remediate their accounts and learn how to better protect themselves while on Facebook. Beyond these protections, we've put in place backend measures to reduce the rate of these attacks and will continue to iterate on our defenses to find new ways to protect people. In addition to the engineering teams that build tools to block spam we also have a dedicated enforcement team that seeks to identify those responsible for spam and works with our legal team to ensure appropriate consequences follow."

Apart from these recommendations and tentative enforcement mechanisms, no particular guarantees are provided nowadays to protect users from a spear phishing attack. Many are the social bloggers suggesting techniques and tricks to prevent this kind of attack, in articles titled in most of the cases, like: "50 ways to protect yourself...," "How to protect your identity...," etc. In general, all these tricks can be summarized affirming that education and vigilance are essentially the keys to stay safe from a spear phishing attack, together with "traditional" ways of protecting ourselves on the Internet (e.g., do not click links in e-mail, pay attention to URLs, install a security suite, choose robust passwords).

[12] http://www.forbes.com/sites/davidewalt/2012/08/29/facebook-spam-email-spear-phishing/

[13] http://marketingland.com/the-rise-of-social-spam-1-5-of-tweets-4-of-facebook-posts-are-spam-2571/\http://louisem.com/3731/social-media-statistics-2013/

Spam Attack The collected personal information is also invaluable for *spam attacks* in social networks, in the form of unsolicited messages. Spammers would (1) have access to e-mail addresses that belong to real people (i.e., one problem spammers face is that they often do not know if the e-mail addresses they collect are indeed being used by real people or they are just secondary addresses that are not regularly read) and (2) have information about the people using these e-mail addresses allowing them to efficiently personalize their marketing activities, tailored according to the knowledge from the targets profile. Also, note that the ability to associate personal information with an e-mail address is important to be able to successfully bypass spam filters [163]. Such filters usually generate a list of "spammy" tokens vs. "good" tokens after training with a large set of previously received e-mails. As a result, e-mails that contain the name of the user receiving the e-mail, or names of people that s/he is acquainted with, tend to receive lower spam ratings than e-mails that are less personal. Therefore, if the spammer is able to include some personal information in the spam that s/he is sending, s/he would be able to improve her/his chances of reaching the targeted user.

In the general field of Social Web, Apple has taken steps to support privacy initiatives that limit the ability of third-parties to collect personal data useful for spamming. For example, in 2012 Apple added support for the do-not-track browser header in OS X Lion.[14] Its Safari browser also defaults to block cookies from third-party websites. Apple has also had its privacy proclivities reinforced as a result of the controversy over its storage of unprotected location data on the iPhone and of iOS developers' use of the UID identifier as the key to data profiles of iPhone users.[15]

On the official Google Online Security Blog a post recently appeared "An update on our war against account hijackers,"[16] explaining how the number of Google Accounts used to send spam has been reduced. Every time a user signs in to Google, the system performs a complex risk analysis to determine how likely it is that the sign-in really comes from that user. If a sign-in is deemed suspicious or risky for some reason (e.g., it's coming from a country oceans away from the last user sign-in), Google asks some simple questions—easy for the real owner but normally hard to solve for a hijacker—about the user account (e.g., the phone number associated with the account, or for the answer to the user security question). According to Google, using these security measures, the number of compromised account has dramatically reduced by 99.7% since 2011.

In the field of online social networks, in the last few years Twitter and Facebook have implemented their plans to weed out spammers. In its 2012 post: "Shutting down spammers,"[17] Twitter affirms in its official blog having taken into account also law to combat spammers: "By shutting down tool providers, we will prevent other spammers from having these services at their disposal.

[14] http://www.apple.com/osx/whats-new/features.html

[15] http://www.informationweek.com/tech-center/gov-cloud/apple-gets-patent-for-polluting-electron/240002423/

[16] http://googleonlinesecurity.blogspot.it/2013/02/an-update-on-our-war-against-account.html

[17] https://blog.twitter.com/2012/shutting-down-spammers/

Further, we hope the suit acts as a deterrent to other spammers, demonstrating the strength of our commitment to keep them off Twitter." Twitter says they have also launched additional efforts to keep users' feeds spam-free, such as new measures aimed to stop spam tied to mentions[18] and tweaks to their link to analyze whether tweeted items are malicious. "We are committed to fighting spam on all fronts, by continuing to grow our anti-spam team and using every tool at our disposal to shut down spammers." Concerning Facebook, "Protecting the people who use Facebook from spam and malicious content is a top priority for us," a Facebook representative told *The Next Web* in a statement. In April 2013, the company announced the charge of a fee for messaging people outside one's friends' circle in the UK. The charges range between 71 pence to 10.68 pounds depending on the person the user wants to contact, be it a celebrity or any other person outside the network of friends. Prior to this, Facebook gave its messaging services for free, and the messages from strangers used to land up in the folder "Others," while the Inbox receives messages only from friends. With the new anti-spam technique based on the charging of a fee to "unknown messages" (messages from unknown senders), the recipient of an unknown message has the possibility to mark it as spam and move it into the folder "Others." If the recipient does not undertake any action, s/he implicitly allows the unknown sender to continue sending unlimited messages for free.

The idea of associating a fee to "unknown messages" is not new in online social networks. LinkedIn already uses this payment model for sending messages to contacts that are not in the sender's professional network, and it is managed through the purchase of a premium account. In addition to this, in the LinkedIn "Protect your Identity" section, some tips are suggested to users to confirm whether a message is really from Linkedin or not. They suggest being very cautious if receiving an email claiming to be from LinkedIn asking for information relating to bank or financial information. In addition to this, valid LinkedIn messages are always addressed to users personally by including their names and current professional headlines in the footer of the message.

Impersonization Attacks

In online social networks, adversaries can take advantage of the trust relationships among "friends" to craft more convincing attacks, by exploiting personal information gleaned from victims' pages. In fact, typically, a prerequisite for being able to access personal information in a social networking service is to have a confirmed personal relationship with the person who is concerned. In Facebook, for example, a user is allowed to have access to her/his friends' personal information (e.g., e-mail address, pictures, etc.). Another example is constituted by LinkedIn, where the contacts of a person can only be accessed if s/he is a confirmed business contact, and therefore s/he has already accepted a request and confirmed the relationship. Previous work has shown that it is possible to raise levels of trust by injecting the attack into existing chat conversations [179]

[18] A mention is any Twitter update that contains `@username` anywhere in the body of the tweet. This means that `@replies` are also considered mentions.

or by impersonating an existing friend of the target (e.g., [29, 146]). This is the case described in [133], where Hamiel and Moyer conduct an impersonation experiment in which a fake profile on LinkedIn is created for their colleague, the security expert Marcus Ranum. The information to create a plausible profile is obtained by manually surfing the Web, visiting Ranum's personal web page, and his entry in Wikipedia. By impersonating a high-profile person, the authors show how effective an *impersonization attack* can be. The forged profile receives many friend requests, even from one of the target's immediate family members. The most well-known attacks based on impersonization are *Sybil* [84, 269] and *identity clone* [29, 151] attacks. These two attacks look somehow similar in appearance since both need to create a number of online identities, and use these identities to compromise the reputation and evaluation mechanisms in OSN systems.

Sybil Attack The normal assumption of an OSN is that every user is represented by exactly one user account (i.e., one identity), and thus each vertex of the social graph is controlled by a distinct user. Typically, this assumption is enforced by imposing terms of use, by CAPTCHA,[19] and by cross-referencing personal data collected from users. There is, however, no "hard" mechanism for strictly enforcing such a policy [103]. This makes it possible to launch a Sybil attack on an OSN system, where an attacker creates multiple fake identities and pretends to be distinct users in the network, using them to gain a disproportionately large influence. This indicates that an adversary needs to have multiple unique usernames or a huge number of e-mail addresses for launching the attack. Thus, the adversary also needs to compromise this restriction in the registration process, in order to create many identities automatically.

To date, in order to defend social networks against Sybil attacks, two main systems have been proposed: SybilGuard [293] and SybilLimit [292]. At a high level, these schemes attempt to isolate Sybils embedded within a social network topology. The key insight used in both approaches is that real-world social networks are fast mixing [101] that aids to distinguish the Sybil nodes from normal nodes. Fast mixing means that subsets of honest nodes have good connectivity to the rest of the social network. Both the schemes declare nodes in the network as either Sybils or non-Sybils from the perspective of a trusted node, effectively partitioning the nodes in the social network into two distinct regions (non-Sybils and Sybils). Hence, each Sybil defense scheme can actually be viewed as a graph partitioning algorithm, where the graph is the social network.

SybilGuard defines a social network as a graph whose vertices represent users, and whose edges represent the human-established trust relations in the real world. The idea is that if an attacker creates too many Sybil nodes and connects them to the network by attack edges, the graph will have a small set of edges whose removal will disconnect a large fraction of the Sybil nodes in the network. Similarly, SybilLimit assumes and shows that social networks are fast mixing. In comparison to SybilGuard, it ensures more optimal and acceptable limits for the number of Sybil nodes in the network.

[19] A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), a trademark of Carnegie Mellon University, is a type of challenge-response test used in computing to determine whether or not the user is human.

Both SybilGuard and SybilLimit are good solutions for detecting Sybil nodes. However, the quality and performance of the algorithms depend on the inputs, namely, the network topology and the trusted node. For these reasons, according to [269], the research community lacks a clear understanding of how these schemes compare against each other, how well they would work on real-world social networks with different structural properties, or whether there exist other (potentially better) ways of Sybil defense. Therefore, Viswanath et al. [269] show the opportunity to take into account prior work on general community detection algorithms in order to defend against Sybils, and demonstrate that networks with well-defined community structure are inherently more vulnerable to Sybil attacks, and that, in such networks, Sybils can carefully target their links in order to make their attacks more effective.

Identity Clone Attack In an *identity clone attack* (also called *profile cloning attack*) [29, 151], an already existing profile in a social network is cloned (the knowledge of a victim is a mandatory requirement in this case) and friend requests are sent to the contacts of the victim. Hence, it is possible to "steal" the contacts of a user by forging her/his identity and creating a second, identical profile in the same social network. Having access to the contacts of a victim, therefore, means that the sensitive personal information provided by these contacts become accessible to the attacker. In [29], the authors demonstrate that a typical user tends to accept a friend request from a forged identity who is actually already a confirmed contact in their friend list. In the same paper, they also describe the concept of *cross-site profile cloning attack*. In this attack, it is possible to automatically identify users who are registered in one social network, but who are not registered in another. The identity of a victim is then cloned in the site where he/she is registered, and forged in a social networking site where he/she is not registered yet. After the forged identity has been successfully created, it is possible to contact his/her friends registered on both social networks so as to rebuild the social networks.

As stated in [151], the identity clone attack in social network services is similar to node replication attack on sensor networks [231]. In this field, some solutions have been proposed (see for instance [231, 295]). However, the detection process in sensor network is different from the detection of faked identities in OSNs. For social network sites, the first step for detecting faked identities is to discover similar identities, while similarity discovering in sensor network may be negligible because the cloned nodes are the same as the victim nodes. On the other hand, the approaches of searching and matching profiles in social networks may be similar with the detection of similar identities on social sites. In this scenario, Bilge et al. [29] present an algorithm for matching individuals across social networks to conduct cross-site identity clone attack, based on attribute similarity, such as the similarities of name and education. Motoyama et al. [215] develop a system for searching and matching users on Facebook and MySpace via a boosting algorithm based on users' attributes. Markines et al. [199] summarize several folksonomy-based similarity measures and evaluate them in finding similar social tags. Xiao et al. [284] propose a positional filtering principle, which exploits the ordering of tokens in a record and leads to upper-bound estimates of similarity scores, to achieve better qualities and improve the runtime efficiency in detecting near duplicate web pages. The method described by Jin et al. [151] is based not only on the similarities of attributes or items in entities but also on the impact of friend network similarity when discovering similar profiles. Moreover, Jin et al. [150] show how the ability of an user to query the list of mutual friends between him and any other user exposes information that could be used for attacks to identify friends and distant neighbors of targeted users.

Concerning tools that online social networks make available to users to protect themselves against an identity clone attack, in most of the cases they consist of procedures to report a fake/cloned account. In all these cases, users are invited to report the abuse. LinkedIn, taking into consideration that members accidentally open a duplicate account for themselves when they accept an invitation to connect while using an email address that is not currently listed on their account, can first of all checking if they have a duplicate account. However, if a user is certain that a specific account with her/his data is not a duplicate account for her/him, s/he can report the profile for further investigation by LinkedIn's Trust & Safety team. Concerning the Twitter Impersonation Policy, accounts with similar usernames or that are similar in appearance (e.g., the same background or avatar image) do not automatically violate the impersonation policy. In order to do impersonation, the account must also portray another person in a misleading or deceptive manner. In this case it can be permanently suspended. An account will not be removed if the user shares the name with another one but it has no other commonalities, or the profile clearly states it is not affiliated with or connected to any similarly-named individuals. In addition to this, Twitter users are allowed to create parody, commentary, or fan accounts. According to the Google+ User Conduct and Content Policy, it is not allowed to use Google products to impersonate others. It is forbidden to create a Google+ profile or page that might deceive users into thinking that it officially represents a person, business, or other organization when it does not. For creating fan commentaries and parodies, Google+ encourages users to make sure they clearly label them as a fan page or parody, or provide other information to clearly distinguish them from the subject of the commentary. Google+ policy also suggests not to use an official logo as a profile picture. If a page or a profile is reported as an impersonation via the Google+ abuse reporting tool, the Company examines the report and lets the possible impersonator know whether or not the page or community violates the Google+ policies. For profiles/pages suspended for impersonation, it is possible to make any changes necessary to conform them to the Google+ guidelines and resubmit them for a further review by the Company.

Under a different perspective, in order to solve the problem of "Little Brothers" (automated programs that monitor people's Internet activities), Apple recently acquired a patent [56] that describes a way to pollute online data to promote privacy exploiting an identity clone approach. The patent suggests that nowadays, resistance to data collection is futile: "if the user engages in any Internet activity, information may be successfully collected about that user." In addition to this, "even the most cautious Internet users are still being profiled over the Internet via dataveillance techniques from automated [Little] Brothers." For these reasons, techniques to pollute electronic profiling represent a way to attack invasive data collection by creating a fake identity, or clone. In particular, the approach works in three ways. First, it creates a fake identity (and, actually, many fake identities) for the user. Second, it takes elements of users' real identities—interests and the like, based on browser history and cookies—and merges those with elements that do not reflect the identity of the user, creating a close-but-not-quote shadow identity. Third, it creates actual network activity based on those false interest areas, spreading them across the network. Acting this way, the patent affirms that "data collection is not prevented; rather, it is intentionally polluted so as to make any data collection about a principal less valuable and less reliable."

Reverse Social Engineering Attacks

In addition to social engineering attacks, also *reverse social engineering* (RSE) *attacks* in social networks should be carefully considered. To our knowledge, RSE attacks have been studied and formalized (connected to OSNs) only by Irani et al. in [145]. In a reverse social engineering attack, the attacker does not initiate contact with the victim. Rather, the victim is tricked into contacting the attacker him/herself. This way, an RSE attack can bypass current behavioral and filter-based detection techniques that aim to prevent wide-spread unsolicited contact. In addition to this, a high degree of trust is established between the victim and the attacker as the victim is the entity that established the relationship. This way, less suspicion is raised and there is a higher probability that a social engineering attack will be successful.

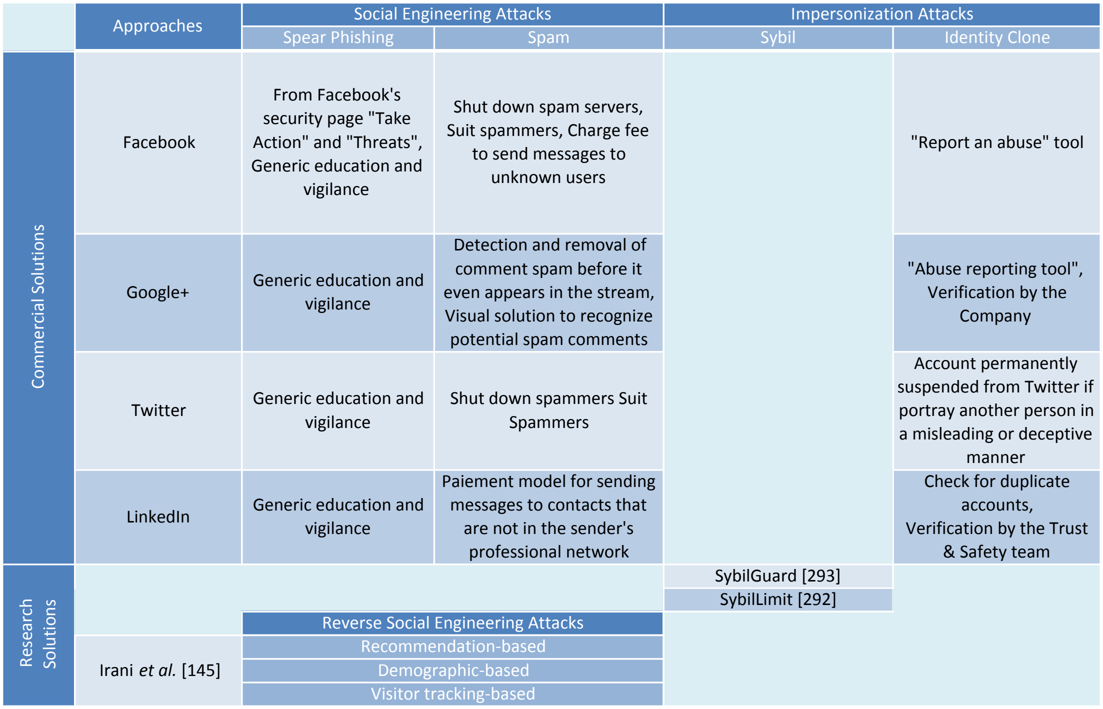
In [145], authors classify RSE attacks based on two characteristics: (i) *targeted/un-targeted* and (ii) *direct/mediated*. Concerning the first characteristic, the attacker focuses/does not focus on a particular user. Considering the second one, the baiting action of the attacker is visible/invisible to the targeted users. In particular, in mediated attacks the baiting is collected by an intermediate agent that is then responsible for propagating it (often in a different form) to the targeted users.

In addition to this, they present three different combinations of RSE attacks within the context of online social networks: (i) *recommendation-based* RSE, (ii) *demographic-based* RSE, and (iii) *visitor tracking-based* RSE. In the first case, if the attacker is able to influence the recommendation system and make the social network issue targeted recommendations, s/he may be able to trick victims into contacting her/him. In the second case, the attacker simply creates a profile (or a number of profiles) that would have a high probability of appealing to certain users, and then waits for victims to initiate contact. Finally, the attack in the third case involves exploiting the user's curiosity by visiting their profile page. The notification that the page has been visited might raise interest, baiting the user to view the attacker's profile and perhaps take some action.

In their work, Irani et al. show that RSE attacks are a feasible threat in real life, and that attackers may be able to attract a large numbers of legitimate users without actively sending any friend request. The experiments that authors have conducted demonstrate that suggestions and friend-finding features (e.g., demographic-based searches) made by social networking sites may provide an incentive for the victims to contact a user if the right setting is created (e.g., an attractive photograph, an attack profile with similar interests, etc.).

Summary of Approaches

As illustrated in the previous section, there are various solutions and intents taken into account by commercial social networks to avoid/limit identity theft attacks. Together with approaches studied by researchers concerning attacks that have been recently formalized (i.e., the reverse social engineering attacks) or which are not taken into account by commercial OSNs, Figure 4.1 summarizes these "tentative solutions."



<table>
<tr><th rowspan="2"></th><th rowspan="2">Approaches</th><th colspan="2">Social Engineering Attacks</th><th colspan="2">Impersonization Attacks</th></tr>
<tr><th>Spear Phishing</th><th>Spam</th><th>Sybil</th><th>Identity Clone</th></tr>
<tr><td rowspan="4">Commercial Solutions</td><td>Facebook</td><td>From Facebook's security page "Take Action" and "Threats", Generic education and vigilance</td><td>Shut down spam servers, Suit spammers, Charge fee to send messages to unknown users</td><td rowspan="4"></td><td>"Report an abuse" tool</td></tr>
<tr><td>Google+</td><td>Generic education and vigilance</td><td>Detection and removal of comment spam before it even appears in the stream, Visual solution to recognize potential spam comments</td><td>"Abuse reporting tool", Verification by the Company</td></tr>
<tr><td>Twitter</td><td>Generic education and vigilance</td><td>Shut down spammers Suit Spammers</td><td>Account permanently suspended from Twitter if portray another person in a misleading or deceptive manner</td></tr>
<tr><td>LinkedIn</td><td>Generic education and vigilance</td><td>Paiement model for sending messages to contacts that are not in the sender's professional network</td><td>Check for duplicate accounts, Verification by the Trust & Safety team</td></tr>
<tr><td rowspan="2">Research Solutions</td><td></td><td colspan="2"></td><td>SybilGuard [293]
SybilLimit [292]</td><td></td></tr>
<tr><td>Irani <i>et al.</i> [145]</td><td colspan="2">Reverse Social Engineering Attacks
Recommendation-based
Demographic-based
Visitor tracking-based</td><td></td><td></td></tr>
</table>

Figure 4.1: Summary of proposals to avoid/limit Identity Theft Attacks.

4.4 CONCLUSIONS

In this chapter, we focused in particular on those issues involving identity theft in online social networks. With respect to traditional environments, attacks performed in OSNs are particularly insidious due to the use of the social networks themselves and their relationship-based structure to reach many potential victims.

Online identity management should provide, in this sense, solutions to protect users against these attacks. Actually, solid research techniques have not been proposed yet in the field of online social networks. For this reason, different are the solutions that have been chosen by commercial OSNs to help users in managing and protecting their identities. In this chapter, we tried to summarize some of these techniques, focusing on the most commonly adopted. It has emerged that, in many cases, the responsibility for identity protection is still on the final users that have to pay attention to their behaviors if they want to avoid such an attack. Despite this, growing attention to these kinds of attacks (even from a legal point of view) and new algorithms to prevent them are constantly emerging.

CHAPTER 5

Conclusions and Further Research Directions

The aim of this book is to give the readers a global view on the topics that, in our opinion and on the basis of our literature review, represent the main security issues in current online social networks.

Due to their characteristics—i.e., the huge amount of personal information they manage, big economic upturn connected to their commercial use, strict interconnection among users and resources characterizing them, user attitude to easily share private data and activities with strangers—online social networks are considered critical applications with respect to the security of users and their resources.

With respect to the traditional meaning, the term "security" in online social networks assumes a different sense depending on the research topic taken into account. In our book, we focused on three main research topics involved in: (i) guaranteeing the users with a given level of perceived security before interacting with others (even strangers); (ii) providing users with control over the flow of their personal information; and (iii) protecting users with respect to the (possible malicious) use of their profiles and identities.

The first research topic is constituted by *trust management*. Trust can be used in online social networks to measure, in terms of risks/benefits, the establishment of new relationships/interactions. The development of suitable trust models/measures become in this sense fundamental for users' personal safety.

The second research topic focuses on *controlled information sharing*. In online social networks, where personal information is not only connected to user profiles but spans across users social activities and interactions, traditional access control techniques must be improved to take these characteristics into account and to be more user-centric as possible.

The last research topic lies on *identity management*. A correct strategy to protect the online identities of users is fundamental especially in the online social network scenario, where traditional attacks (e.g., malware, worms, spam, and phishing) are carried out in a different context, by leveraging the social networks as a new medium to reach the victims. By stealing users' identity, and exploiting this way the trust relationships between "friends," adversaries can craft more convincing attacks.

For each of these research topics, we have first provided theoretical concepts—often borrowed from general Computer Science and Psychology/Sociology/Economics (being those of online social networks a research field involving multiple disciplines)—and later discussed the main solutions that commercial/non-commercial actors have proposed over the years.

Doing this, we have noticed that both commercial and non commercial solutions are converging towards interesting research directions in the three research topics. In the next section, we discuss some of the most promising research directions.

5.1 OPEN SECURITY ISSUES IN ONLINE SOCIAL NETWORKS

Concerning online social networks, in general, we have already discussed throught the book the fact that, over the last few years, the possibility to express semantically differentiated social connections among entities has become a distinctive characteristic of main OSNs. The Open Graph protocol by Facebook and the OpenSocial public specification followed by Google+ and Myspace (together with a number of other social networks) are examples confirming it. This has repercussions on the way new issues emerge and the way they are treated by each of the previous three research fields (by both commercial and non-commercial solutions).

5.1.1 TRUST MANAGEMENT

As illustrated in Chapter 2, several methods have been proposed to measure trust among users in online social networks. From trust evaluation methods based on the analysis of the *structure* of (often purely friendship-oriented) social networks, the interest has rapidly shifted to methods taking into consideration *interactions* among users in OSNs. In the first case, an analysis is done on the graph representing the (explicit) relationships forming the network. In the second case, a virtual graph representing the way users interact on the network is exploited. Both approaches allow extracting useful trust measurements based on different premises. Thus, the use of *hybrid* approaches, based on the dynamism of both relationships and interactions, seems to be the promising solution in the trust management field connected to online social networks.

In addition to a more extensive investigation of these emerging approaches, it will be necessary, in our opinion, a major study aiming at identifying the main aspects influencing trust among users in an online social network, even with respect to social capital. Not all relationships among users are (semantically) equivalent in term of trust: the addition/deletion of a (type of) relationship can influence more trust with respect to the same action executed on another (type of) relationship. This not only connects directly to the execution of a given action on a relationship with respect to the users and their resources, but considering the propagative nature of trust, also connects to other users related to them. The same is valid concerning interactions.

Another interesting aspect to evaluate would be the perception of trust that users have not only with respect to other participants of the social network, but with respect to the social network itself. A further research direction is studying the interplay among trust, privacy/confidentiality, and risk, as well as discovering relevant trust patterns in the network to be used for access control purposes.

5.1.2 CONTROLLED INFORMATION SHARING

With the development of the ReBAC paradigm, the relationship-based nature of OSNs has been exploited for access control purposes. This paradigm is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships.

Current access control mechanisms for commercial OSNs implementing the ReBAC paradigm, as well as many research proposals that have appeared so far, are based on a fully centralized solution to enforce access control. However, a semi-decentralized/fully decentralized architecture in support of access control enforcement is best suited for the OSN environment. This is because in OSNs the "user-centric" aspect is fundamental, and decentralized solutions allow users to have more *control* over their own data by, at the same time, putting less trust in the OSN provider. However, no widely accepted decentralized solution for enforcing ReBAC in OSNs has appeared so far, due to the many issues that need to be solved to make this possible. The main drawback of decentralization is that it increases the overhead of the access control service since it requires decentralized path discovery. It also requires the management of off-line nodes during path discovery. It is therefore necessary to develop a solution able to trade-off between security and efficiency.

In addition to the above-mentioned issues, since traditional user-to-user (U2U) relationship-based access control mechanisms are not able to offer the appropriate control in a scenario where user-to-resource (U2R) and resource-to-resource (R2R) relationships are entering into the picture, recent trends in controlled information sharing in OSNs are based more and more on all these three kinds of relationships, allowing stronger expressive powers of relationship-based access control policies. A unified model and related access control mechanism is therefore needed.

Concerning commercial solutions, they only partially implement the ReBAC protocol. Most of the available commercial social network management systems only allow users to specify, via *privacy settings*, whether a given piece of information (e.g., personal data and resources) must be public, private, or accessible by the users with whom s/he has a direct relationship, or by providing simple variants to these basic settings. Even if it is easy to implement, the use of this simple access control paradigm presents several drawbacks (e.g., time-consuming, not sufficiently flexible, unsuitable in the case of heterogeneous access control requirements that different OSN users may have, etc.). For these reasons, further developments in this field are necessary. An important issue is increasing the expressivity of the supported access control model by, at the same time, developing techniques and tools to make OSN privacy settings easier to be customized. This is crucial, since average OSN users are much less skilled than users of traditional data management systems w.r.t. access control policy specification.

5.1.3 IDENTITY MANAGEMENT

Connected to the controlled information sharing problem, there has always been the issue of where to store personal data, and how to protect users' identities from malicious attacks.

From early identity management systems, which keep personal data in one central location under the control of one large corporate provider, current identity management solutions tend to leave to users the possibility of storing their personal data where they prefer. This represents a positive development both in terms of security and scalability, and reduces the user perception of such systems as "big brothers."

Despite this, it seems that current online social networks have not faced this issue yet, at least not completely. Rather, the social networking's business model is still primarily based on the ability to leverage large warehouses of personal information under OSN providing main control. Nevertheless, in order to increase interoperability and to give users the possibility and the sensation of being more "owners of their data," multiple initiatives have been (and are going to be) undertaken to provide, for instance, portable APIs. This way, third parties are allowed to integrate a user's social network profile into external Web applications. Along this line, the OpenSocial public specification defines a component hosting environment (container) and a set of common application programming interfaces for Web-based applications. OpenSocial is currently used as a runtime environment allowing untrusted and partially trusted components from third parties to run into an existing Web application.

In addition to this, in order to increase the possibility for users to better manage their personal data and, at the same time, prevent identity theft attacks, more or less all OSNs implement solutions that, in most of the cases, are variants of classical behaviors for protecting ourselves on the Net (e.g., the choice of strong passwords, pay attention to the address bar, avoid to reveal sensitive information, etc.), or simple procedures for reporting fake/compromised identities. A major effort is necessary in this field to provide users with more consolidated solutions with which to protect themselves.

Bibliography

[1] Identity disclosure. In Liu, Ling, Özsu, and M. Tamer, editors, *Encyclopedia of Database Systems*, pages 1342–1342. Springer US, 2009. 63

[2] State of the Media: The Social Media Report. Technical report, The Nielsen Company, April 2012. http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html. 1

[3] U.S. Social Ad Revenues to Reach $11B in 2017. Technical report, BIA/Kelsey, April 2013. 2, 10

[4] AA.VV. Federated SSO Authentication Service. Technical report, Cisco Systems, 2009. 62, 66

[5] AA.VV. SPION - D2.1 - State of the Art. Technical Report WP2 - D2.1, SBO Security and Privacy for Online Social Networks, September 2011. S. Gürses and K. U. Leuven Eds. 4

[6] T. Abdessalem, B. Cautis, and A. Souhli. Trust Management in Social Networks. Technical Report ANR-08-CORD-011-05, Télécom ParisTech, LTCI, UMR CNRS 5141, 2010. 29

[7] A. Acquisti and R. Gross. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, volume 4258 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2006. 50

[8] S. Adali, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, W. A. Wallace, and G. Williams. Measuring behavioral trust in social networks. In *Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on*, pages 150–152, 2010. DOI: 10.1109/ISI.2010.5484757. 10, 24, 32, 33

[9] L. A. Adamic and E. Adar. How to search a social network. *Social Networks*, 27(3):187–203, 2005. DOI: 10.1016/j.socnet.2005.01.007. 10

[10] E. Agichtein, C. Castillo, D. Donato, A. Gionis, and G. Mishne. Finding high-quality content in social media. In *Proceedings of the 2008 International Conference on Web Search and Data Mining*, WSDM '08, pages 183–194, New York, NY, USA, 2008. ACM. DOI: 10.1145/1341531.1341557. 1, 10, 11

[11] C. G. Akcora, B. Carminati, and E. Ferrari. Network and profile based measures for user similarities on social networks. In *Proceedings of the IEEE International Conference on Information Reuse and Integration, IRI 2011, 3-5 August 2011, Las Vegas, Nevada, USA*, pages 292–298. IEEE Systems, Man, and Cybernetics Society, 2011. DOI: 10.1007/s13278-012-0090-8. 10

[12] B. Ali, W. Villegas, and M. Maheswaran. A Trust Based Approach for Protecting User Data in Social Networks. In *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, CASCON '07, pages 288–293, Riverton, NJ, USA, 2007. IBM Corp. DOI: 10.1145/1321211.1321251. 53, 56

[13] A. Anagnostopoulos, R. Kumar, and M. Mahdian. Influence and correlation in social networks. In *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '08, pages 7–15, New York, NY, USA, 2008. ACM. DOI: 10.1145/1401890.1401897. 10

[14] D. Appelquist, D. Brickley, M. Carvalho, R. Iannella, A. Passant, C. Perey, and H. Story. A Standards-based, Open and Privacy-aware Social Web. Technical report, W3C, December 2010. `http://www.w3.org/2005/Incubator/socialweb/XGR-socialweb-20101206`. 1

[15] R. Aringhieri, E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems. *Journal of the American Society for Information Science and Technology*, 57(4):528–537, 2006. DOI: 10.1002/asi.20307. 23

[16] D. Artz and Y. Gil. A Survey of Trust in Computer Science and the Semantic Web. *Journal of Web Semantics*, 5(2):58–71, June 2007. DOI: 10.1016/j.websem.2007.03.002. 20, 21, 22

[17] L. Backstrom, P. Boldi, M. Rosa, J. Ugander, and S. Vigna. Four degrees of separation. *CoRR*, abs/1111.4570, 2011. DOI: 10.1145/2380718.2380723. 11

[18] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *Proceedings of the 16th international conference on World Wide Web*, WWW '07, pages 181–190, New York, NY, USA, 2007. ACM. DOI: 10.1145/1242572.1242598. 65

[19] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: an Online Social Network with User-Defined Privacy. *ACM SIGCOMM Computer Communication Review*, 39(4):135–146, August, 2009. DOI: 10.1145/1594977.1592585. 56

[20] R. Balakrishnan and K. Ranganathan. *A Textbook of Graph Theory*. Springer New York, 2012. DOI: 10.1007/978-1-4614-4529-6. 10

[21] S. B. Barnes. A privacy paradox: Social networking in the United States. *First Monday*, 11, 2006. DOI: 10.5210/fm.v11i9.1394. 25

[22] F. Baum and A. M. Ziersch. Social capital. *Journal Epidemial Community Health*, 57(5):320–323, 2003. DOI: 10.1136/jech.57.5.320. 12

[23] Z. Bauman. Identity in the globalizing world. *Social Anthropology*, 9(2):121–129, 2001. DOI: 10.1017/S096402820100009X. 4

[24] F. Beato, I. Ion, S. Čapkun, B. Preneel, and M. Langheinrich. For some eyes only: Protecting online information sharing. In *Proceedings of the third ACM conference on Data and application security and privacy*, CODASPY '13, pages 1–12, New York, NY, USA, 2013. ACM. DOI: 10.1145/2435349.2435351. 55, 56

[25] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In *Proceedings of the 11th international conference on Privacy enhancing technologies*, PETS'11, pages 211–225, Berlin, Heidelberg, 2011. Springer-Verlag. DOI: 10.1007/978-3-642-22263-4_12. 55, 56

[26] P. Beatty, I. Reay, S. Dick, and J. Miller. Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys*, 43(3):14:1–14:46, April, 2011. DOI: 10.1145/1922649.1922651. 19

[27] T. Besenyei, A. M. Foldes, G. G. Gulyas, and S. Imre. StegoWeb: Towards the ideal private web content publishing tool. In *Proceedings of SECURWARE 2011*, pages 109–114, August 2011. 56

[28] T. Bhuiyan, A. Josang, and Y. Xu. Managing Trust in Online Social Networks. In B. Furht, editor, *Handbook of Social Network Technologies and Applications*, pages 471–496. Springer US, 2010. DOI: 10.1007/978-1-4419-7142-5. 23

[29] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 551–560, New York, NY, USA, 2009. ACM. DOI: 10.1145/1526709.1526784. 15, 66, 70, 71

[30] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, SP '96, pages 164–, Washington, DC, USA, 1996. IEEE Computer Society. DOI: 10.1109/SECPRI.1996.502679. 21

[31] P. A. Bonatti, C. Duma, D. Olmedilla, and N. Shahmehri. An Integration of Reputation-based and Policy-based Trust Management. In *Proceedings of Semantic Web Policy Workshop, Galway, Ireland (7th November 2005)*, 2005. 20, 21, 22

[32] A. Borodin, Y. Filmus, and J. Oren. Threshold models for competitive influence in social networks. In A. Saberi, editor, *Internet and Network Economics*, volume 6484 of *Lecture Notes in Computer Science*, pages 539–550. Springer Berlin Heidelberg, 2010. DOI: 10.1007/978-3-642-17572-5. 11

[33] P. Borzymek and M. Sydow. Trust and distrust prediction in social network with combined graphical and review-based attributes. In *Proceedings of the 4th KES international conference on Agent and multi-agent systems: technologies and applications, Part I*, KES-AMSTA'10, pages 122–131, Berlin, Heidelberg, 2010. Springer-Verlag. DOI: 10.1007/978-3-642-13480-7_14. 36

[34] P. Bourdieu. The Forms of Capital. In J. G. Richardson, editor, *Handbook of Theory and Research for the Sociology of Education*, pages 241–258. New York: Greenwood Press, 1986. 12

[35] d. boyd and N. B. Ellison. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1-2), 2007. DOI: 10.1111/j.1083-6101.2007.00393.x. 6

[36] d. boyd and E. Hargittai. Facebook privacy settings: Who cares? *First Monday*, 15(8), 2010. DOI: 10.5210/fm.v15i8.3086. 50

[37] d. boyd and J. Heer. Profiles as Conversation: Networked Identity Performance on Friendster. In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 3, pages 59c–59c, 2006. DOI: 10.1109/HICSS.2006.394. 65

[38] d. boyd and A. E. Marwick. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. In *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011*, 2011. 6

[39] S. Brainov and T. Sandholm. Contracting with uncertain level of trust. In *Proceedings of the 1st ACM conference on Electronic commerce*, EC '99, pages 15–21, New York, NY, USA, 1999. ACM. DOI: 10.1145/336992.336998. 20

[40] P. Bramhall, M. Hansen, K. Rannenberg, and T. Roessler. User-centric identity management: New trends in standardization and regulation. *Security Privacy, IEEE*, 5(4):84–87, 2007. DOI: 10.1109/MSP.2007.99. 62

[41] N. Brody, D. C. Davis, B. E. Drushel, S. Green-Hamann, J. A. Hall, A. Johnson, B. Johnson, J. H. Kuznekoff, M. B. Lippman, C. J. Liberman, B. McEwan, J. J. Mease, T. W. Morris, K. Nuitjen, J. Pea, N. Pennington, J. Rosenbaum, J. C. Sherblom, P. Stepman, B. Sundararajan, M. Sundararajan, C. Toma, J. A. Tougas, and C. Cunningham. *Social Networking and Impression Management: Self-Presentation in the Digital Age*. Lexington Books, 1st edition, 2012. 59

[42] A. Brunie. Meaningful distinctions within a concept: relational, collective, and generalized social capital. *Social Science Research*, 38(2):251–265, 2009. DOI: 10.1016/j.ssresearch.2009.01.005. 13

[43] B. Bumgarner. You have been poked: Exploring the uses and gratifications of Facebook among emerging adults. *First Monday*, 12(11), 2007. DOI: 10.5210/fm.v12i11.2026. 65

[44] V. Buskens. The social structure of trust. *Social Networks*, 20(3):265–289, 1998. DOI: 10.1016/S0378-8733(98)00005-7. 30

[45] J.-W. Byun and N. Li. Purpose based access control for privacy protection in relational database systems. *The VLDB Journal*, 17(4):603–619, July 2008. DOI: 10.1007/s00778-006-0023-0. 42

[46] G. Calhoun. Community without propinquity revisited: communications technology and the transformation of the urban public sphere. *Sociological Inquiry*, 68(3):373–397, 1998. DOI: 10.1111/j.1475-682X.1998.tb00474.x. 13

[47] K. Cameron. Laws of identity. Technical report, Microsoft Corporation, 2005. 62

[48] S. Capkun, J.-P. Hubaux, and L. Buttyan. Mobility helps peer-to-peer security. *IEEE Transactions on Mobile Computing*, 5(1):43–51, 2006. DOI: 10.1109/TMC.2006.12. 26, 27

[49] B. Carminati and E. Ferrari. Collaborative Access Control in On-line Social Networks. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*, pages 231–240, 2011. 51, 52

[50] B. Carminati, E. Ferrari, and E. Bertino. Securing XML data in third-party distribution systems. In *Proceedings of the 14th ACM international conference on Information and knowledge management*, CIKM '05, pages 99–106, New York, NY, USA, 2005. ACM. DOI: 10.1145/1099554.1099575. 42

[51] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Semantic Web-based Social Network Access Control. *Computers & Security*, 30(2-3):108 – 115, 2011. Special Issue on Access Control Methods and Technologies. DOI: 10.1016/j.cose.2010.08.003. 51, 52

[52] B. Carminati, E. Ferrari, and A. Perego. Rule-Based Access Control for Social Networks. In R. Meersman, Z. Tari, and P. Herrero, editors, *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, volume 4278 of *Lecture Notes in Computer Science*, pages 1734–1744. Springer Berlin Heidelberg, 2006. DOI: 10.1007/11915034. 45, 51

[53] B. Carminati, E. Ferrari, and A. Perego. Enforcing Access Control in Web-based Social Networks. *ACM Trans. Inf. Syst. Secur.*, 13(1):6:1–6:38, November, 2009. DOI: 10.1145/1609956.1609962. 46, 51, 52

[54] B. Carminati, E. Ferrari, and M. Viviani. A Multi-dimensional and Event-Based Model for Trust Computation in the Social Web. In K. Aberer, A. Flache, W. Jager, L. Liu, J. Tang, and C. Gueret, editors, *Social Informatics*, volume 7710 of *Lecture Notes in Computer Science*, pages 323–336. Springer Berlin Heidelberg, 2012. DOI: 10.1007/978-3-642-35386-4. 29, 35, 45

[55] J. M. Carroll. *The Neighborhood and the Internet: Design Research Projects in Community Informatics*. Routledge, 2011. 4

[56] S. R. Carter. Techniques to pollute electronic profiling. Patent Application, April 2007. US 2007/0094738 A1. 72

[57] S. Castano, M. G. Fugini, G. Martella, and P. Samarati. *Database Security*. Addison-Wesley, 1995. 42

[58] C. Castelfranchi and R. Falcone. Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification. In *Proceedings of the 3rd International Conference on Multi Agent Systems*, ICMAS '98, pages 72–, Washington, DC, USA, 1998. IEEE Computer Society. DOI: 10.1109/ICMAS.1998.699034. 22, 23

[59] C. Castelfranchi, R. Falcone, and F. Marzo. Being trusted in a social network: Trust as relational capital. In K. Stølen, W. H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management*, volume 3986 of *Lecture Notes in Computer Science*, pages 19–32. Springer Berlin Heidelberg, 2006. DOI: 10.1007/11755593. 20

[60] M. Castells. *The Rise of the Network Society*. Oxford: Blackwell, 1996. 5

[61] M. Castells. *Communication Power*. Oxford University Press, 2009. 6

[62] C. Castillo, M. Mendoza, and B. Poblete. Information Credibility on Twitter. In *Proceedings of the 20th international conference on World wide web*, WWW '11, pages 675–684, New York, NY, USA, 2011. ACM. DOI: 10.1145/1963405.1963500. 34

[63] J. Caverlee, L. Liu, and S. Webb. Socialtrust: tamper-resilient trust establishment in online communities. In *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*, JCDL '08, pages 104–114, New York, NY, USA, 2008. ACM. DOI: 10.1145/1378889.1378908. 16, 20, 30

[64] D. Chappell. Introducing windows cardspace. Technical report, Chappell & Associates, 2006. 62

[65] N. Chen. On the Approximability of Influence in Social Networks. *SIAM Journal on Discrete Mathematics*, 23(3):1400–1415, 2009. DOI: 10.1137/08073617X. 11

[66] Y. Cheng, J. Park, and R. Sandhu. A User-to-User Relationship-Based Access Control Model for Online Social Networks. In N. Cuppens-Boulahia, F. Cuppens, and J. Garcia-Alfaro, editors, *Data and Applications Security and Privacy XXVI*, volume 7371 of *Lecture Notes in Computer Science*, pages 8–24. Springer Berlin Heidelberg, 2012. DOI: 10.1007/978-3-642-31540-4. 17, 53

[67] Y. Cheng, J. Park, and R. Sandhu. Relationship-Based Access Control for Online Social Networks: Beyond User-to-User Relationships. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom)*, pages 646–655, 2012. DOI: 10.1109/SocialCom-PASSAT.2012.57. 44, 53

[68] S. Chester and G. Srivastava. Social network privacy for attribute disclosure attacks. In *Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on*, pages 445–449, 2011. DOI: 10.1109/ASONAM.2011.105. 65

[69] J.-H. Cho, A. Swami, and I.-R. Chen. Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, volume 2, pages 641–650, 2009. DOI: 10.1109/CSE.2009.68. 25

[70] S. S. M. Chow, Y.-J. He, L. C. K. Hui, and S. M. Yiu. SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment. In F. Bao, P. Samarati, and J. Zhou, editors, *Applied Cryptography and Network Security*, volume 7341 of *Lecture Notes in Computer Science*, pages 526–543. Springer Berlin Heidelberg, 2012. 63

[71] B. Christianson and W. S. Harbison. Why isn't trust transitive? In M. Lomas, editor, *Security Protocols*, volume 1189 of *Lecture Notes in Computer Science*, pages 171–176. Springer Berlin Heidelberg, 1997. DOI: 10.1007/3-540-62494-5. 26

[72] J. Coleman. *Foundations of Social Theory*. Belknap Press of Harvard University Press, 1990. 19, 28

[73] A. M. Collins and E. F. Loftus. A Spreading Activation Theory of Semantic Processing. *Psychological Review*, 82(6):407–428, 1975. DOI: 10.1037/0033-295X.82.6.407. 31

[74] B. E. Commerce, A. Jøsang, and R. Ismail. The Beta Reputation System. In *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002. 23

[75] K. S. Cook, T. Yamagishi, C. Cheshire, R. Cooper, M. Matsuda, and R. Mashima. Trust Building via Risk Taking: A Cross-Societal Experiment. *Social Psychology Quarterly*, 68:121–142, 2005. DOI: 10.1177/019027250506800202. 19

[76] C. L. Corritore, B. Kracher, and S. Wiedenbeck. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6):737 – 758, 2003. DOI: 10.1016/S1071-5819(03)00041-7. 27

[77] E. Damiani and M. Viviani. Trading anonymity for influence in open communities voting schemata. In *Proceedings of the 2009 International Workshop on Social Informatics*, SOCINFO '09, pages 63–67, Washington, DC, USA, 2009. IEEE Computer Society. DOI: 10.1109/SocInfo.2009.10. 23

[78] P. Dasgupta. Trust as a commodity. In D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, pages 49–72. Department of Sociology, University Oxford, 2000. 19

[79] J. De Clercq. Single Sign-On Architectures. In G. Davida, Y. Frankel, and O. Rees, editors, *Infrastructure Security*, volume 2437 of *Lecture Notes in Computer Science*, pages 40–58. Springer Berlin Heidelberg, 2002. DOI: 10.1007/3-540-45831-X. 61

[80] A. de Tocqueville. *Democracy in America (De la démocratie en Amérique)*. Garden City, New York, 1969 [1835-1840]. 3

[81] M. Decker. Requirements for a location-based access control model. In *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*, MoMM '08, pages 346–349, New York, NY, USA, 2008. ACM. DOI: 10.1145/1497185.1497259. 42

[82] G. Delanty. *Community*. Routledge, 2003. 4, 5, 13

[83] J. Donath and d. boyd. Public Displays of Connection. *BT Technology Journal*, 22(4):71–82, October, 2004. DOI: 10.1023/B:BTTJ.0000047585.06264.cc. 65

[84] J. R. Douceur. The sybil attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems*, volume 2429 of *Lecture Notes in Computer Science*, pages 251–260. Springer Berlin Heidelberg, 2002. 70

[85] T. DuBois, J. Golbeck, and A. Srinivasan. Predicting trust and distrust in social networks. In *SocialCom/PASSAT'11*, pages 418–424, 2011. DOI: 10.1109/PASSAT. 31

[86] E. Durkheim. *Suicide: A Study in Sociology (Le suicide. Étude de sociologie)*. New York: The Free Press, 1951 [1897]. 3

[87] P. Eades. A Heuristic for Graph Drawing. *Congressus Numerantium*, 42:149–160, 1984. 32

[88] T. El Maliki and J. M. Seigneur. A survey of user-centric identity management technologies. In *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on*, pages 12–17, 2007. DOI: 10.1109/SECUREWARE.2007.4385303. 61

[89] T. El Maliki and J.-M. Seigneur. Chapter 17 - Identity Management. In J. R. Vacca, editor, *Computer and Information Security Handbook*, pages 269 – 292. Morgan Kaufmann, Boston, 2009. 61, 62

[90] N. B. Ellison, C. Steinfield, and C. Lampe. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, 12(4):1143–1168, July 2007. DOI: 10.1111/j.1083-6101.2007.00367.x. 14

[91] E. Ephrati and J. S. Rosenschein. Distributed consensus mechanisms for self-interested heterogeneous agents. In *Intelligent and Cooperative Information Systems, Proceedings of International Conference on*, pages 71–79, 1993. DOI: 10.1109/ICICIS.1993.291768. 52

[92] E. H. Erikson. *Identity: Youth and Crisis*. New York, W. W. Norton, 1968. 19

[93] R. Fagin. On an authorization mechanism. *ACM Transactions on Database Systems*, 3(3):310–319, September, 1978. DOI: 10.1145/320263.320288. 41

[94] R. Falcone and C. Castelfranchi. Social trust: a cognitive approach. In C. Castelfranchi and Y.-H. Tan, editors, *Trust and Deception in Virtual Societies*, pages 55–90. Kluwer Academic Publishers, Norwell, MA, USA, 2001. DOI: 10.1007/978-94-017-3614-5. 20, 22

[95] L. Fang, H. Kim, K. LeFevre, and A. Tami. A privacy recommendation wizard for users of social networking sites. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 630–632, New York, NY, USA, 2010. ACM. DOI: 10.1145/1866307.1866378. 25

[96] E. Ferrari. Access control. In L. Liu and M. T. Özsu, editors, *Encyclopedia of Database Systems*, pages 7–11. Springer US, 2009. 39, 40

[97] E. Ferrari. Database as a service: Challenges and solutions for privacy and security. In *Services Computing Conference, 2009. APSCC 2009. IEEE Asia-Pacific*, pages 46–51, 2009. DOI: 10.1109/APSCC.2009.5394141. 42

[98] E. Ferrari. *Access Control in Data Management Systems*. Synthesis Lectures on Data Management. Morgan & Claypool Publishers, 2010. DOI: 10.2200/S00281ED1V01Y201005DTM004. 16, 17, 40

[99] E. Ferrari and B. Thuraisingham. Secure database systems. In O. Diaz and M. Piattini, editors, *Advanced Databases: Technology and Design*. Artech House, 2000. 43

[100] E. Ferrari and B. Thuraisingham. Security and Privacy for Web Databases and Services. In E. Bertino, S. Christodoulakis, D. Plexousakis, V. Christophides, M. Koubarakis, K. Böhm, and E. Ferrari, editors, *Advances in Database Technology - EDBT 2004*, volume 2992 of *Lecture Notes in Computer Science*, pages 17–28. Springer Berlin Heidelberg, 2004. DOI: 10.1007/b95855. 42

[101] A. D. Flaxman. Expansion and lack thereof in randomly perturbed graphs. In W. Aiello, A. Broder, J. Janssen, and E. Milios, editors, *Algorithms and Models for the Web-Graph*, volume 4936 of *Lecture Notes in Computer Science*, pages 24–35. Springer Berlin Heidelberg, 2008. DOI: 10.1007/978-3-540-78808-9. 70

[102] J. Fogel and E. Nehmad. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1):153 – 160, 2009. DOI: 10.1016/j.chb.2008.08.006. 66

[103] P. W. L. Fong. Preventing sybil attacks by privilege attenuation: A design principle for social network systems. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP '11, pages 263–278, Washington, DC, USA, 2011. IEEE Computer Society. DOI: 10.1109/SP.2011.16. 70

[104] P. W. L. Fong. Relationship-based Access Control: Protection Model and Policy Language. In *Proceedings of the first ACM conference on Data and application security and privacy*, CODASPY '11, pages 191–202, New York, NY, USA, 2011. ACM. DOI: 10.1145/1943513.1943539. 44, 51

[105] P. W. L. Fong, M. Anwar, and Z. Zhao. A Privacy Preservation Model for Facebook-Style Social Network Systems. In M. Backes and P. Ning, editors, *Computer Security – ESORICS 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 303–320. Springer Berlin Heidelberg, 2009. DOI: 10.1007/978-3-642-04444-1. 51

[106] P. W. L. Fong and I. Siahaan. Relationship-based access control policies and their policy languages. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, SACMAT '11, pages 51–60, New York, NY, USA, 2011. ACM. DOI: 10.1145/1998441.1998450. 51

[107] N. E. Frye and M. M. Dornisch. When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior*, 26(5):1120 – 1127, 2010. DOI: 10.1016/j.chb.2010.03.016. 25

[108] S. J. Fusco, R. Abbas, K. Michael, and A. Aloudat. Location-based social networking: Impact on trust in relationships. *Technology and Society Magazine, IEEE*, 31(2):39–50, 2012. DOI: 10.1109/MTS.2012.2196340. 20

[109] D. Gambetta. *Trust: Making and Breaking Cooperative Relations*. Blackwell Publishers, 1990. 22

[110] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. Security issues in online social networks. *Internet Computing, IEEE*, 15(4):56–63, 2011. DOI: 10.1109/MIC.2011.50. 14

[111] C. E. Gates. Access control requirements for web 2.0 security and privacy. In *Proceedings of Workshop on Web 2.0 Security & Privacy (W2SP 2007*, 2007. 15, 17, 44

[112] R. Ghiselli Ricci and M. Viviani. Asymptotically idempotent aggregation operators for trust management in multi-agent systems. In *Proceedings of IPMU 2008: Information Processing and Management of Uncertainty in knowledge systems - 12th international conference, june 22-27, Malaga, Spain*, pages 129 – 137, 2008. DOI: 10.1142/S0218488509006170. 23

[113] A. Giddens. *The consequences of modernity*. Cambridge: Polity, 1990. 5

[114] S. Giff. The Influence of Metaphor, Smart Cards and Interface Dialogue on Trust in eCommerce. MSc project, University College London, 2000. 21

[115] J. L. Glanville and E. J. Bienenstock. A Typology for Understanding the Connections Among Different Forms of Social Capital. *American Behavioral Scientist*, 52(11):1507–1530, 2009. DOI: 10.1177/0002764209331524. 28

[116] E. Goffman. *The Presentation of Self in Everyday Life*. Anchor, 1 edition, June 1959. 64, 65

[117] J. Golbeck. Combining provenance with trust in social networks for semantic web content filtering. In *Proceedings of the 2006 international conference on Provenance and Annotation of Data*, IPAW'06, pages 101–108, Berlin, Heidelberg, 2006. Springer-Verlag. DOI: 10.1007/11890850_12. 26

[118] J. Golbeck. Trust on the World Wide Web: A survey. *Foundations and Trends in Web Science*, 1(2):131–197, January, 2006. DOI: 10.1561/1800000006. 16, 25

[119] J. Golbeck. Weaving a Web of Trust. *Science*, 321(5896):1640–1641, 2008. DOI: 10.1126/science.1163357. 16

[120] J. Golbeck and J. Hendler. Inferring binary trust relationships in Web-based social networks. *ACM Transactions on Internet Technology*, 6(4):497–529, November, 2006. DOI: 10.1145/1183463.1183470. 12, 25, 26, 27, 29

[121] J. Golbeck and U. Kuter. The ripple effect: Change in trust and its impact over a social network. In J. Golbeck, editor, *Computing with Social Trust*, Human-Computer Interaction Series, pages 169–181. Springer London, 2009. DOI: 10.1007/978-1-84800-356-9. 20

[122] J. A. Golbeck. *Computing and applying trust in web-based social networks*. PhD thesis, University of Maryland at College Park, College Park, MD, USA, 2005. AAI3178583. 30

[123] M. Goodner, M. Hondo, A. Nadalin, M. McIntosh, and D. Schmidt. Understanding ws-federation. Technical report, International Business Machines Corporation and Microsoft Corporation, 2007. 62

[124] S. Grabner-Kräuter. Web 2.0 social networks: The role of trust. *Journal of Business Ethics*, 90(4):505–522, 2009. DOI: 10.1007/s10551-010-0603-1. 27, 28

[125] S. Grabner-Kräuter and S. Bitter. Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, 2013. DOI: 10.1080/07360932.2013.781517. 25, 27

[126] M. Granovetter. The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory*, 1:201–233, 1983. DOI: 10.2307/202051. 4, 12, 13, 64

[127] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen. Trust Propagation in Small Worlds. In P. Nixon and S. Terzis, editors, *Trust Management*, volume 2692 of *Lecture Notes in Computer Science*, pages 239–254. Springer Berlin Heidelberg, 2003. DOI: 10.1007/3-540-44875-6. 26

[128] P. P. Griffiths and B. W. Wade. An authorization mechanism for a relational database system. *ACM Transactions on Database Systems*, 1(3):242–255, September, 1976. DOI: 10.1145/320473.320482. 41

[129] R. Gross and A. Acquisti. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM. DOI: 10.1145/1102199.1102214. 15, 50

[130] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *Proceedings of the 13th international conference on World Wide Web*, WWW '04, pages 403–412, New York, NY, USA, 2004. ACM. DOI: 10.1145/988672.988727. 17, 24, 26, 31

[131] S. Guha, K. Tang, and P. Francis. Noyb: Privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, WOSN '08, pages 49–54, New York, NY, USA, 2008. ACM. DOI: 10.1145/1397735.1397747. 55

[132] M. A. Hall. The Importance of Trust for Ethics, Law, and Public Policy. *Cambridge Quarterly of Healthcare Ethics*, 14:156–167, 4 2005. DOI: 10.1017/S096318010505019X. 19

[133] N. Hamiel and S. Moyer. Satan is on my Friend List. Attacking Social Networks, May 2008. 70

[134] K. Hampton, L. S. Goulet, L. Rainie, and K. Purcell. Social networking sites and our lives. Technical report, June 2011. Available from: http://www.pewinternet.org/Reports/2011/Technology-and-social-networks.aspx. 7

[135] C.-W. Hang and M. P. Singh. Trust-based recommendation based on graph similarity. In *in AAMAS Workshop on Trust in Agent Societies (Trust)*, 2010. 31

[136] M. Hauben and R. Hauben. *Netizens: on the history and impact of Usenet and the Internet*. IEEE Computer Society Press, Los Alamitos, CA, USA, 1997. 7

[137] R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Preventing private information inference attacks on social networks. *IEEE Transactions on Knowledge and Data Engineering*, 25(8):1849–1862, 2013. DOI: 10.1109/TKDE.2012.120. 64, 65

[138] D. Helbing. A mathematical model for the behavior of individuals in a social field. *Journal of Mathematical Sociology*, 19(3):189–219, 1994. DOI: 10.1080/0022250X.1994.9990143. 19

[139] D. Hong and V. Shen. Setting Access Permission through Transitive Relationship in Web-based Social Networks. In I. King and R. Baeza-Yates, editors, *Weaving Services and People on the World Wide Web*, pages 229–253. Springer Berlin Heidelberg, 2009. DOI: 10.1007/978-3-642-00570-1. 16

[140] H. Hu, G.-J. Ahn, and J. Jorgensen. Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 25(7):1614–1627, 2013. DOI: 10.1109/TKDE.2012.97. 52

[141] F. Huang. Building Social Trust: A Human-Capital Approach. *Journal of Institutional and Theoretical Economics (JITE)*, 163(4):552–573, 2007. DOI: 10.1628/093245607783242981. 19, 28

[142] J. Huang and M. S. Fox. An ontology of trust: formal semantics and transitivity. In *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, ICEC '06, pages 259–270, New York, NY, USA, 2006. ACM. DOI: 10.1145/1151454.1151499. 20, 26

[143] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt. Certified reputation: how an agent can trust a stranger. In *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*, AAMAS '06, pages 1217–1224, New York, NY, USA, 2006. ACM. DOI: 10.1145/1160633.1160854. 24

[144] Internet Engineering Task Force (IETF). The OAuth 2.0 Authorization Framework. Technical report, Microsoft Corporation, 2012. 62

[145] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. In *Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment*, DIMVA'11, pages 55–74, Berlin, Heidelberg, 2011. Springer-Verlag. DOI: 10.1007/978-3-642-22424-9_4. 66, 73

[146] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, October, 2007. DOI: 10.1145/1290958.1290968. 66, 70

[147] S. Jahid, P. Mittal, and N. Borisov. EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 411–415, New York, NY, USA, 2011. ACM. DOI: 10.1145/1966913.1966970. 56

[148] S. Jahid, S. Nilizadeh, P. Mittal, N. Borisov, and A. Kapadia. DECENT: A Decentralized Architecture for Enforcing Privacy in Online Social Networks. In *PerCom Workshops*, pages 326–332. IEEE, 2012. DOI: 10.1109/PerComW.2012.6197504. 57

[149] M. Jamali and M. Ester. A matrix factorization technique with trust propagation for recommendation in social networks. In *Proceedings of the fourth ACM conference on Recommender systems*, RecSys '10, pages 135–142, New York, NY, USA, 2010. ACM. DOI: 10.1145/1864708.1864736. 31

[150] L. Jin, J. B. D. Joshi, and M. Anwar. Mutual-friend based attacks in social network systems. *Computers & Security*, 37:15–30, 2013. DOI: 10.1016/j.cose.2013.04.003. 72

[151] L. Jin, H. Takabi, and J. B. Joshi. Towards active detection of identity clone attacks on online social networks. In *Proceedings of the first ACM conference on Data and application security and privacy*, CODASPY '11, pages 27–38, New York, NY, USA, 2011. ACM. DOI: 10.1145/1943513.1943520. 70, 71, 72

[152] A. N. Joinson. Looking at, looking up or keeping up with people?: Motives and use of Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1027–1036, New York, NY, USA, 2008. ACM. DOI: 10.1145/1357054.1357213. 50, 65

[153] A. N. Joinson, D. J. Houghton, A. Vasalou, and B. L. Marder. Digital Crowding: Privacy, Self-Disclosure, and Technology. In S. Trepte and L. Reinecke, editors, *Privacy Online*, pages 33–45. Springer Berlin Heidelberg, 2011. DOI: 10.1007/978-3-642-21521-6. 65

[154] A. Jøsang. The right type of trust for distributed systems. In *Proceedings of the 1996 workshop on New security paradigms*, NSPW '96, pages 119–131, New York, NY, USA, 1996. ACM. DOI: 10.1145/304851.304877. 20

[155] A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference - Volume 48*, ACSC '06, pages 85–94, Darlinghurst, Australia, Australia, 2006. Australian Computer Society, Inc. DOI: 10.1145/1151699.1151710. 23, 24

[156] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618 – 644, 2007. DOI: 10.1016/j.dss.2005.05.019. 20, 22, 23

[157] A. Jøsang and S. Pope. Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling - Volume 43*, APCCM '05, pages 59–68, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc. 20, 26

[158] A. Jøsang and S. Pope. User-centric identity management. In A. Clark, editor, *Proceedings of AusCERT 2005*, Brisbane, Australia, May 2005. 60, 61

[159] L. Kagal, T. Finin, and A. Joshi. Trust-Based Security in Pervasive Computing Environments. *Computer*, 34(12):154–157, December, 2001. DOI: 10.1109/2.970591. 21

[160] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The EigenTrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th international conference on World Wide Web*, WWW '03, pages 640–651, New York, NY, USA, 2003. ACM. DOI: 10.1145/775152.775242. 25

[161] P. Kannadiga, M. Zulkernine, and S. I. Ahamed. Towards an Intrusion Detection System for Pervasive Computing Environments. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II - Volume 02*, ITCC '05, pages 277–282, Washington, DC, USA, 2005. IEEE Computer Society. DOI: 10.1109/ITCC.2005.279. 21

[162] A. M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1):59 – 68, 2010. DOI: 10.1016/j.bushor.2009.09.003. 1

[163] C. Karlberger, G. Bayler, C. Kruegel, and E. Kirda. Exploiting redundancy in natural language to penetrate bayesian spam filters. In *Proceedings of the first USENIX workshop on Offensive Technologies*, WOOT '07, pages 9:1–9:7, Berkeley, CA, USA, 2007. USENIX Association. 68

[164] D. Kempe, J. Kleinberg, and E. Tardos. Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '03, pages 137–146, New York, NY, USA, 2003. ACM. DOI: 10.1145/956750.956769. 10, 11

[165] A. Khalili, J. Katz, and W. A. Arbaugh. Toward Secure Key Distribution in Truly Ad-Hoc Networks. In *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, SAINT-W '03, pages 342–, Washington, DC, USA, 2003. IEEE Computer Society. DOI: 10.1109/SAINTW.2003.1210183. 21

[166] R. Khare and A. Rifkin. Weaving a Web of Trust. *World Wide Web Journal*, 2(3):77–112, June 1997. 29

[167] M. Kim, J. Seo, S. Noh, and S. Han. Identity management-based social trust model for mediating information sharing and privacy enhancement. *Security and Communication Networks*, 5(8):887–897, 2012. DOI: 10.1002/sec.379. 29

[168] P. Kivisto. *Key ideas in sociocology*. Pine forest Press, 2003. 3

[169] J. S. Kleinfeld. The small world problem. *Society*, 39(2):61–66, 2002. DOI: 10.1007/BF02717530. 10, 11

[170] J. Kohl and C. Neuman. The Kerberos Network Authentication Service (V5), 1993. 21

[171] B.-J. Koops and R. Leenes. Identity theft, identity fraud and/or identity-related crime. *Datenschutz und Datensicherheit - DuD*, 30(9):553–556, 2006. DOI: 10.1007/s11623-006-0141-2. 63

[172] S. R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H.-C. Choi. D-FOAF: Distributed Identity Management with Access Rights Delegation. In R. Mizoguchi, Z. Shi, and F. Giunchiglia, editors, *The Semantic Web – ASWC 2006*, volume 4185 of *Lecture Notes in Computer Science*, pages 140–154. Springer Berlin Heidelberg, 2006. DOI: 10.1007/11836025. 51

[173] R. Kumar, J. Novak, and A. Tomkins. Structure and evolution of online social networks. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '06, pages 611–617, New York, NY, USA, 2006. ACM. DOI: 10.1145/1150402.1150476. 10

[174] U. Kuter and J. Golbeck. SUNNY: A New Algorithm for Trust Inference in Social Networks Using Probabilistic Confidence Models. In *Proceedings of the Twenty-Second AAAI Conference on Artificial Intelligence, July 22-26, 2007, Vancouver, British Columbia, Canada*, pages 1377–1382. AAAI Press, 2007. 30

[175] L. S. L. Lai and E. Turban. Groups formation and operations in the web 2.0 environment and social networks. *Group Decision and Negotiation*, 17(5):387–402, 2008. DOI: 10.1007/s10726-008-9113-2. 27

[176] X. N. Lam, T. Vu, T. D. Le, and A. D. Duong. Addressing cold-start problem in recommendation systems. In *Proceedings of the 2nd international conference on Ubiquitous information management and communication*, ICUIMC '08, pages 208–211, New York, NY, USA, 2008. ACM. DOI: 10.1145/1352793.1352837. 23

[177] C. Lampe, N. Ellison, and C. Steinfield. A Face(book) in the Crowd: Social Searching vs. Social Browsing. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, CSCW '06, pages 167–170, New York, NY, USA, 2006. ACM. DOI: 10.1145/1180875.1180901. 65

[178] C. Lampe, N. B. Ellison, and C. Steinfield. Changes in use and perception of Facebook. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, CSCW '08, pages 721–730, New York, NY, USA, 2008. ACM. DOI: 10.1145/1460563.1460675. 50

[179] T. Lauinger, V. Pankakoski, D. Balzarotti, and E. Kirda. Honeybot, your man in the middle for automated social engineering. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'10, pages 11–11, Berkeley, CA, USA, 2010. USENIX Association. 69

[180] D.-H. Lee, S. Im, and C. R. Taylor. Voluntary self-disclosure of information on the Internet: A multimethod study of the motivations and consequences of disclosing information on blogs. *Psychology and Marketing*, 25(7):692–710, 2008. DOI: 10.1002/mar.20232. 64, 66

[181] J. Leskovec, D. Huttenlocher, and J. Kleinberg. Predicting Positive and Negative Links in Online Social Networks. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 641–650, New York, NY, USA, 2010. ACM. DOI: 10.1145/1772690.1772756. 31, 34

[182] R. Levien. Attack-Resistant Trust Metrics. In J. Golbeck, editor, *Computing with Social Trust*, Human-Computer Interaction Series, pages 121–132. Springer London, 2009. DOI: 10.1007/978-1-84800-356-9. 24

[183] J. D. Lewis. Trust as a social reality. *Social Forces*, 63(4):967–985, 1985. DOI: 10.1093/sf/63.4.967. 27, 28

[184] M. Li and A. Bonti. T-OSN: A Trust Evaluation Model in Online Social Networks. In *Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on*, pages 469–473, 2011. DOI: 10.1109/EUC.2011.73. 35

[185] D. Liben-Nowell and J. Kleinberg. The link prediction problem for social networks. In *Proceedings of the twelfth international conference on Information and knowledge management*, CIKM '03, pages 556–559, New York, NY, USA, 2003. ACM. DOI: 10.1145/956863.956972. 32

[186] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Inferring private information using social network data. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 1145–1146, New York, NY, USA, 2009. ACM. DOI: 10.1145/1526709.1526899. 64, 65

[187] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim. Predicting trusts among users of online communities: An Epinions case study. In *Proceedings of the 9th ACM conference on Electronic commerce*, EC '08, pages 310–319, New York, NY, USA, 2008. ACM. DOI: 10.1145/1386790.1386838. 32

[188] K. Liu and E. Terzi. Towards identity anonymization on graphs. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, SIGMOD '08, pages 93–106, New York, NY, USA, 2008. ACM. DOI: 10.1145/1376616.1376629. 65

[189] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, pages 61–70, New York, NY, USA, 2011. ACM. DOI: 10.1145/2068816.2068823. 50

[190] C. R. Livermore and K. Setzekorn. *Social Networking Communities and E-Dating Services: Concepts and Implications*. IGI Global, 2009. 7

[191] G. Lu, J. Lu, S. Yao, and Y. J. Yip. A Review on Computational Trust Models for Multi-agent Systems. *The Open Information Science Journal*, 2:18–25, 2009. DOI: 10.2174/1874947X00902020018. 23

[192] W. Luo, Q. Xie, and U. Hengartner. Facecloak: An architecture for user privacy on social networking sites. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, volume 3, pages 26–33, 2009. DOI: 10.1109/CSE.2009.387. 55, 56

[193] L. Lyon. *The Community in Urban Society*. Waveland Press, 1986. 4

[194] S. Ma, O. Wolfson, and J. Lin. A survey on trust management for intelligent transportation system. In *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science*, CTS '11, pages 18–23, New York, NY, USA, 2011. ACM. DOI: 10.1145/2068984.2068988. 25, 26, 27

[195] S. A. Macskassy and F. Provost. Classification in networked data: A toolkit and a univariate case study. *Journal of Machine Learning Research*, 8:935–983, 2007. 65

[196] M. Madden. Privacy management on social media sites. Technical report, Pew Research Center, February 2012. Available from: `http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx`. 50

[197] M. Maheswaran, H. C. Tang, and A. Ghunaim. Towards a gravity-based trust model for social networking systems. In *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops*, ICDCSW '07, pages 24–, Washington, DC, USA, 2007. IEEE Computer Society. DOI: 10.1109/ICDCSW.2007.82. 30

[198] B. Marcus, F. Machilek, and A. Schütz. Personality in cyberspace: Personal web sites as media for personality expressions and impressions. *Journal of Personality and Social Psychology*, 90(6):1014–1031, June 2006. DOI: 10.1037/0022-3514.90.6.1014. 59, 64

[199] B. Markines, C. Cattuto, F. Menczer, D. Benz, A. Hotho, and G. Stumme. Evaluating similarity measures for emergent semantics of social tagging. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 641–650, New York, NY, USA, 2009. ACM. DOI: 10.1145/1526709.1526796. 71

[200] S. P. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, April 1994. 20, 22, 23, 34

[201] A. Masoumzadeh and J. Joshi. Ontology-based access control for social network systems. *International Journal Information Privacy, Security and Integrity,*, 1(1):59–78, 2011. DOI: 10.1504/IJIPSI.2011.043731. 53

[202] A. Masoumzadeh and J. Joshi. Privacy settings in social networking systems: What you cannot control. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 149–154, New York, NY, USA, 2013. ACM. DOI: 10.1145/2484313.2484331. 53

[203] R. C. Mayer, J. H. Davis, and F. D. Schoorman. An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3):709–734, 1995. DOI: 10.5465/AMR.1995.9508080335. 16, 27

[204] D. H. Mcknight and N. L. Chervany. The meanings of trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Research Center, 1996. 19, 22, 28

[205] D. H. McKnight and N. L. Chervany. Trust and distrust definitions: One bite at a time. In *Proceedings of the workshop on Deception, Fraud, and Trust in Agent Societies held during the Autonomous Agents Conference: Trust in Cyber-societies, Integrating the Human and Artificial Perspectives*, pages 27–54, London, UK, 2001. Springer-Verlag. DOI: 10.1007/3-540-45547-7_3. 19

[206] M. McPherson, L. S. Lovin, and J. M. Cook. Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*, 27(1):415–444, 2001. DOI: 10.1146/annurev.soc.27.1.415. 10

[207] S. Milgram. The small world problem. *Psychology Today*, 1(1):61–67, 1967. 11

[208] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel. You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining*, WSDM '10, pages 251–260, New York, NY, USA, 2010. ACM. DOI: 10.1145/1718487.1718519. 10

[209] B. Misztal. *Trust in Modern Societies: The Search for the Bases of Social Order*. Polity, 1996. 19

[210] K. D. Mitnick and W. L. Simon. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2002. 66

[211] G. Möllering. The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension. *Sociology*, 35(2):403–420, 2001. DOI: 10.1177/S0038038501000190. 19, 20

[212] L. D. Molm, N. Takahashi, and G. Peterson. Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology*, 105:1396–1427, 2000. DOI: 10.1086/210434. 19

[213] N. Morgan, G. Jones, and A. Hodges. *Social Media. The Complete Guide to Social Media From The Social Media Guys*. 2011. 1

[214] R. M. Morgan and S. D. Hunt. The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, 58(3):20–38, 1994. DOI: 10.2307/1252308. 20

[215] M. Motoyama and G. Varghese. I seek you: searching and matching individuals in social networks. In *Proceedings of the eleventh international workshop on Web information and data management*, WIDM '09, pages 67–75, New York, NY, USA, 2009. ACM. DOI: 10.1145/1651587.1651604. 71

[216] L. Mui, M. Mohtashemi, and A. Halberstadt. A Computational Model of Trust and Reputation for E-businesses. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02) - Volume 7*, HICSS '02, pages 188–, Washington, DC, USA, 2002. IEEE Computer Society. DOI: 10.1109/HICSS.2002.994181. 22, 23, 24

[217] T. Nabeth. Social web and identity: a likely encounter. *Identity in the Information Society*, 2(1):1–5, 2009. DOI: 10.1007/s12394-009-0029-z. 63

[218] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 173–187, 2009. DOI: 10.1109/SP.2009.22. 65

[219] S. Nepal, W. Sherchan, and A. Bouguettaya. A behaviour-based trust model for service web. In *Service-Oriented Computing and Applications (SOCA), 2010 IEEE International Conference on*, pages 1–4, 2010. DOI: 10.1109/SOCA.2010.5707183. 25

[220] S. Nepal, W. Sherchan, and C. Paris. STrust: A Trust Model for Social Networks. In *Proceedings of the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, TRUSTCOM '11, pages 841–846, Washington, DC, USA, 2011. IEEE Computer Society. DOI: 10.1109/TrustCom.2011.112. 32, 33

[221] E. C. H. Ngai and M. R. Lyu. An Authentication Service Based on Trust and Clustering in Wireless Ad Hoc Networks: Description and Security Evaluation. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing -Vol 1 (SUTC'06) - Volume 01*, SUTC '06, pages 94–103, Washington, DC, USA, 2006. IEEE Computer Society. DOI: 10.1109/SUTC.2006.1636164. 21

[222] M. Nguyen, Y. S. Bin, and A. Campbell. Comparing Online and Offline Self-Disclosure: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, 15(2):103–111, 2012. DOI: 10.1089/cyber.2011.0277. 65

[223] Q. Ni, E. Bertino, J. Lobo, and S. Calo. Privacy-aware role-based access control. *Security Privacy, IEEE*, 7(4):35–43, 2009. DOI: 10.1109/MSP.2009.102. 42

[224] J. Nielsen. Trust or Bust: Communicating Trustworthiness in Web Design. Technical report, March 1999. `http://www.nngroup.com/articles/trust-or-bust-communicating-trustworthiness-in-web-design/`. 22

[225] M. Nielsen and K. Krukow. Towards a formal notion of trust. In *Proceedings of the 5th ACM SIGPLAN international conference on Principles and practice of declaritive programming*, PPDP '03, pages 4–7, New York, NY, USA, 2003. ACM. DOI: 10.1145/888251.888253. 21

[226] R. Nisbet. *The Quest for Community*. New York: Free Press, 1976. 4

[227] H. Nissenbaum. Can Trust be Secured Online? A theoretical Perspective. *Etica e Politica*, 1(2), December, 1999. 21

[228] A. Nosko, E. Wood, and S. Molema. All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior*, 26(3):406 – 418, 2010. DOI: 10.1016/j.chb.2009.11.012. 66

[229] D. Osterwalder. Trust through evaluation and certification? *Social Science Computer Review*, 19(1):32–46, 2001. DOI: 10.1177/089443930101900104. 21

[230] E. Pariser. *The Filter Bubble: What The Internet Is Hiding From You*. New York: The Penguin Press, 2011. 13

[231] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Security and Privacy, 2005 IEEE Symposium on*, pages 49–63, 2005. DOI: 10.1109/SP.2005.8. 71

[232] J. Pierson and R. Heyman. Social media and cookies: challenges for online privacy. *Emerald Journal*, 13(6):30–42, 2011. DOI: 10.1108/14636691111174243. 6

[233] I. Pinyol and J. Sabater-Mir. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, 40(1):1–25, 2013. DOI: 10.1007/s10462-011-9277-z. 23

[234] R. D. Putnam. Bowling alone: America's declining social capital. *Journal of Democracy*, 6:65–78, 1995. DOI: 10.1353/jod.1995.0002. 12, 13, 28

[235] D. Recordon and D. Reed. OpenID 2.0: A platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, DIM '06, pages 11–16, New York, NY, USA, 2006. ACM. DOI: 10.1145/1179529.1179532. 62

[236] R. Recuero, R. Araujo, and G. Zago. How does social capital affect retweets? In L. A. Adamic, R. A. Baeza-Yates, and S. Counts, editors, *International AAAI Conference on Weblogs and Social Media, Proceedings*. The AAAI Press, 2011. 14

[237] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Communications of the ACM*, 43(12):45–48, December, 2000. DOI: 10.1145/355112.355122. 20

[238] P. Resnick and R. Zeckhauser. Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In M. R. Baye, editor, *The Economics of the Internet and E-Commerce*, pages 127–157. Elsevier Science, November, 2002. 23

[239] H. Rheingold. *The virtual community: homesteading on the electric frontier*. USA: MIT Press, 2000. 5, 13

[240] J. C. Roca, J. J. García, and J. J. de la Vega. The importance of perceived trust, security and privacy in online trading systems. *Inf. Manag. Comput. Security*, 17(2):96–113, 2009. DOI: 10.1108/09685220910963983. 14

[241] J. B. Rotter. A new scale for the measurement of interpersonal trust1. *Journal of Personality*, 35(4):651–665, 1967. DOI: 10.1111/j.1467-6494.1967.tb01454.x. 19

[242] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3):393–404, 1998. DOI: 10.5465/AMR.1998.926617. 19, 22, 26

[243] J. W. A. Rummens. *Personal Identity and Social Structure in Sint Maarten/Saint Martin: A Plural Identities Approach*. PhD thesis, York University, 1993. 60

[244] S. Rupert. Social Media's Top 5 Contributions to Society. Blog, Socialmedia Today, April 2013. http://socialmediatoday.com/slrupert/1393636/social-media-top-5-contributions-society. 2

[245] J. Sabater-Mir, M. Paolucci, and R. Conte. Repage: Reputation and image among limited autonomous partners. *JASSS - Journal of Artificial Societies and Social Simulation*, 9(2), 2006. 22

[246] P. H. Salus. *Casting the Net: From ARPANET to Internet and Beyond...* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1995. 7

[247] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-Based Access Control Models. *Computer*, 29(2):38–47, February, 1996. DOI: 10.1109/2.485845. 42, 43

[248] M. Schaefer. Multilevel Data Management Security. Technical report, National Research Council (U.S.). Committee on Multilevel Data Management Security, 1983. 42

[249] H. J. Schau and M. C. Gilly. We Are What We Post? Self-Presentation in Personal Web Space. *The Journal of Consumer Research*, 30(3):385–404, 2003. 65

[250] B. R. Schlenker, B. Helm, and Tedeschi. The Effects of Personality and Situational Variables on Behavioral Trust. *Journal of Personality and Social*, 25(3):419–427, 1973. DOI: 10.1037/h0034088. 19

[251] M. Shehab, A. Squicciarini, G.-J. Ahn, and I. Kokkinou. Access control for online social networks third party applications. *Computers & Security*, 31(8):897 – 911, 2012. DOI: 10.1016/j.cose.2012.07.008. 53

[252] W. Sherchan, S. Nepal, and C. Paris. A Survey of Trust in Social Networks. *ACM Computing Surveys*, 45(4):47:1–47:33, August, 2013. DOI: 10.1145/2501654.2501661. 10, 13, 19, 20, 23, 25, 26, 27, 28, 29, 46

[253] D.-H. Shin. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.*, 22(5):428–438, September, 2010. DOI: 10.1016/j.intcom.2010.05.001. 14

[254] P. Slovic. Perceived risk, trust, and democracy. *Risk Analysis*, 13(6):675–682, 1993. DOI: 10.1111/j.1539-6924.1993.tb01329.x. 20

[255] C. C. P. Snijders and G. Keren. Do you trust? whom do you trust? when do you trust? In S. R. Thye, E. J. Lawler, M. W. Macy, and H. A. Walker, editors, *Advances in group processes, volume 18*, pages 129 – 160. JAI, Elsevier Science, Amsterdam, 2001. 20

[256] A. Squicciarini, A. Bhargav-Spantzel, A. Czeskis, and E. Bertino. Traceable and automatic compliance of privacy policies in federated digital identity management. In G. Danezis and P. Golle, editors, *Privacy Enhancing Technologies*, volume 4258 of *Lecture Notes in Computer Science*, pages 78–98. Springer Berlin Heidelberg, 2006. DOI: 10.1007/11767831. 60

[257] A. C. Squicciarini, M. Shehab, and J. Wede. Privacy policies for shared content in social network sites. *The VLDB Journal*, 19(6):777–796, December, 2010. DOI: 10.1007/s00778-010-0193-7. 52

[258] M. A. Stelzner. 2013 Social Media Marketing Industry Report. Technical report, Social Media Examiner, May 2013. http://www.socialmediaexaminer.com/SocialMediaMarketingIndustryReport2013.pdf. 2

[259] G. Swamynathan, C. Wilson, B. Boe, K. Almeroth, and B. Y. Zhao. Do social networks improve e-commerce?: a study on social marketplaces. In *Proceedings of the first workshop on Online social networks*, WOSN '08, pages 1–6, New York, NY, USA, 2008. ACM. DOI: 10.1145/1397735.1397737. 26, 27

[260] M. Sweney. Average teenager has never met quarter of Facebook friends. Technical report, The Guardian, November 2013. http://www.theguardian.com/media/2012/oct/23/teenage-girls-send-220-texts-week. 15

[261] Q. Tang, B. Gu, and A. Whinston. Content Contribution for Revenue Sharing and Reputation in Social Media: A Dynamic Structural Model. *Journal of Management Information Systems*, 29(2):41–76, 2012. DOI: 10.2753/MIS0742-1222290203. 2

[262] K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth. Some Trust Issues in Social Networks and Sensor Networks. In *Collaborative Technologies and Systems (CTS), 2010 International Symposium on*, pages 573–580, 2010. DOI: 10.1109/CTS.2010.5478462. 26

[263] F. Tönnies and C. P. Loomis. *Community & Society (Gemeinschaft und Gesellschaft)*. Michigan State University Press, 1957 [1887]. 3

[264] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman. Lockr: Social Access Control for Web 2.0. In *Proceedings of the first workshop on Online social networks*, WOSN '08, pages 43–48, New York, NY, USA, 2008. ACM. DOI: 10.1145/1397735.1397746. 46, 54, 56

[265] S. Trifunovic, F. Legendre, and C. Anastasiades. Social Trust in Opportunistic Networks. In *INFOCOM IEEE Conference on Computer Communications Workshops , 2010*, pages 1–6, 2010. DOI: 10.1109/INFCOMW.2010.5466696. 26, 27, 35

[266] Z. Tufekci. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008. DOI: 10.1177/0270467607311484. 18, 59, 66

[267] N. Verbiest, C. Cornelis, P. Victor, and E. Herrera-Viedma. Trust and distrust aggregation enhanced with path length incorporation. *Fuzzy Sets and Systems*, 202(0):61 – 74, 2012. DOI: 10.1016/j.fss.2012.02.007. 31, 32

[268] P. Victor, C. Cornelis, M. De Cock, and E. Herrera-Viedma. Practical aggregation operators for gradual trust and distrust. *Fuzzy Sets and Systems*, 184(1):126–147, December, 2011. DOI: 10.1016/j.fss.2010.10.015. 31, 32

[269] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social network-based Sybil defenses. *ACM SIGCOMM Computer Communication Review*, 41(4):363–374, August, 2010. DOI: 10.1145/1851275.1851226. 70, 71

[270] M. Viviani, N. Bennani, and E. Egyed-Zsigmond. G-profile: A hybrid solution for extended identity management in the field of personalized service provision. *Information Resources Management Journal*, 25(3):61–77, 2012. DOI: 10.4018/irmj.2012070103. 60, 62

[271] T. Švec and J. Samek. Trust evaluation on Facebook using multiple contexts. In *3rd Workshop on Trust, Reputation and User Modeling (TRUM'13), Proceedings*, 2013. To appear. 32, 34

[272] F. E. Walter, S. Battiston, and F. Schweitzer. A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems*, 16(1):57–74, 2008. DOI: 10.1007/s10458-007-9021-x. 27

[273] J. B. Walther. Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction. *Communication Research*, 23(1):3–43, 1996. DOI: 10.1177/009365096023001001. 7

[274] D. Wang, D. Pedreschi, C. Song, F. Giannotti, and A.-L. Barabasi. Human mobility, social ties, and link prediction. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '11, pages 1100–1108, New York, NY, USA, 2011. ACM. DOI: 10.1145/2020408.2020581. 65

[275] S. Wasserman and K. Faust. *Social Network Analysis*. Cambridge University Press, 1994. DOI: 10.1017/CBO9780511815478. 3

[276] D. J. Watts. *Six Degrees: The Science of a Connected Age*. W. W. Norton & Company, 1st edition, 2003. 10, 11

[277] S. A. Weis. Security Parallels between People and Pervasive Devices. In *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops*, PERCOMW '05, pages 105–109, Washington, DC, USA, 2005. IEEE Computer Society. DOI: 10.1109/PERCOMW.2005.72. 21

[278] G. Wierzowiecki and A. Wierzbicki. Efficient and Correct Trust Propagation Using CloseLook. In *Proceedings of the 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology - Volume 01*, WI-IAT '10, pages 676–681, Washington, DC, USA, 2010. IEEE Computer Society. DOI: 10.1109/WI-IAT.2010.129. 31

[279] P. Windley. *Digital Identity*. O'Reilly Media, Inc., 2005. 60

[280] D. Wiszniewski and R. Coyne. Mask and Identity: The Hermeneutics of Self-Construction in the Information Age. In A. K. Renninger and W. Shumar, editors, *Building Virtual Communities - Learning and Change in Cyberspace*, pages 191–214. Cambridge University Press, Cambridge, 2002. DOI: 10.1017/CBO9780511606373. 64

[281] R. C.-W. Wong and A. W.-C. Fu. *Privacy-Preserving Data Publishing: An Overview*. Synthesis Lectures on Data Management. Morgan & Claypool Publishers, 2010. 16, 18, 64, 65

[282] X. Wu, X. Ying, K. Liu, and L. Chen. A Survey of Privacy-Preservation of Graphs and Social Networks. In C. C. Aggarwal and H. Wang, editors, *Managing and Mining Graph Data*, volume 40 of *Advances in Database Systems*, pages 421–453. Springer US, 2010. DOI: 10.1007/978-1-4419-6045-0. 18, 64

[283] R. Xiang, J. Neville, and M. Rogati. Modeling relationship strength in online social networks. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 981–990, New York, NY, USA, 2010. ACM. DOI: 10.1145/1772690.1772790. 12

[284] C. Xiao, W. Wang, X. Lin, and J. X. Yu. Efficient similarity joins for near duplicate detection. In *Proceedings of the 17th international conference on World Wide Web*, WWW '08, pages 131–140, New York, NY, USA, 2008. ACM. DOI: 10.1145/1367497.1367516. 71

[285] L. Xiong and L. Liu. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843–857, 2004. DOI: 10.1109/TKDE.2004.1318566. 24

[286] Z. Yan and S. Holtmanns. Trust Modeling and Management. In R. Subramanian, editor, *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, pages 290–323. Hershey: IGI Global, 2008. DOI: 10.4018/978-1-59904-804-8. 29

[287] S.-H. Yang, A. J. Smola, B. Long, H. Zha, and Y. Chang. Friend or Frenemy? Predicting Signed Ties in Social Networks. In *Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval*, SIGIR '12, pages 555–564, New York, NY, USA, 2012. ACM. DOI: 10.1145/2348283.2348359. 34

[288] J. Yao, S. Chen, S. Nepal, D. Levy, and J. Zic. Truststore: Making amazon s3 trustworthy with services composition. In *Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, CCGRID '10, pages 600–605, Washington, DC, USA, 2010. IEEE Computer Society. DOI: 10.1109/CCGRID.2010.17. 21

[289] C. A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-Lee. Decentralization: The Future of Online Social Networking. In *W3C Workshop on the Future of Social Networking Position Papers*, 2009. 17, 44

[290] X. Ying and X. Wu. On Link Privacy in Randomizing Social Networks. *Knowledge and Information Systems*, 28(3):645–663, 2011. DOI: 10.1007/s10115-010-0353-5. 65

[291] B. Yu and M. P. Singh. An evidential model of distributed reputation management. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, AAMAS '02, pages 294–301, New York, NY, USA, 2002. ACM. DOI: 10.1145/544741.544809. 23, 24

[292] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 3–17, 2008. DOI: 10.1109/SP.2008.13. 70

[293] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman. SybilGuard: Defending Against Sybil Attacks via Social Networks. *IEEE/ACM Transactions on Networking*, 16(3):576–589, 2008. DOI: 10.1109/TNET.2008.923723. 70

[294] Y. Yuan, Z. Miao, and S. Hu. A pervasive computing security system based on human activities analysis. In *TENCON 2006. 2006 IEEE Region 10 Conference*, pages 1–4, 2006. DOI: 10.1109/TENCON.2006.343850. 21

[295] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie. Random-walk based approach to detect clone attacks in wireless sensor networks. *IEEE J.Sel. A. Commun.*, 28(5):677–691, June 2010. DOI: 10.1109/JSAC.2010.100606. 71

[296] G. Zhang and E. K. Jacob. Community: Issues, Definitions, and Operationalization on the Web. In *Proceedings of the 21st international conference companion on World Wide Web*, WWW '12 Companion, pages 1121–1130, New York, NY, USA, 2012. ACM. DOI: 10.1145/2187980.2188250. 5

[297] S. Zhang, H. Jiang, and J. M. Carroll. Integrating online and offline community through Facebook. In *Collaboration Technologies and Systems (CTS), 2011 International Conference on*, pages 569–578, 2011. DOI: 10.1109/CTS.2011.5928738. 4

[298] Y. Zhang, H. Chen, and Z. Wu. A social network-based trust model for the semantic web. In L. Yang, H. Jin, J. Ma, and T. Ungerer, editors, *Autonomic and Trusted Computing*, volume 4158 of *Lecture Notes in Computer Science*, pages 183–192. Springer Berlin Heidelberg, 2006. DOI: 10.1007/11839569. 31

[299] E. Zheleva and L. Getoor. Preserving the privacy of sensitive relationships in graph data. In *Proceedings of the 1st ACM SIGKDD international conference on Privacy, security, and trust in KDD*, PinKDD'07, pages 153–171, Berlin, Heidelberg, 2008. Springer-Verlag. DOI: 10.1007/978-3-540-78478-4_9. 65

[300] E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 531–540, New York, NY, USA, 2009. ACM. DOI: 10.1145/1526709.1526781. 65

[301] E. Zheleva, E. Terzi, and L. Getoor. *Privacy in Social Networks*. Synthesis Lectures on Data Mining and Knowledge Discovery. Morgan & Claypool Publishers, 2012. 16, 18, 64, 65

[302] C.-N. Ziegler. On propagating interpersonal trust in social networks. In J. Golbeck, editor, *Computing with Social Trust*, Human-Computer Interaction Series, pages 133–168. Springer London, 2009. DOI: 10.1007/978-1-84800-356-9. 31

[303] L. G. Zucker. Production of trust: institutional sources of economic structure. In B. M. Staw and L. L. Cummings, editors, *Research in organizational behavior*, pages 53–111. JAI Press, 1986. 19, 20, 28

Authors' Biography

BARBARA CARMINATI

Barbara Carminati is an assistant professor in Computer Science at the University of Insubria, Italy. She has visited several foreign universities as a visiting researcher, including: National University of Singapore, University of Texas at Dallas, Aristotle University of Thessaloniki, and Tsinghua University, Beijng. Her main research interests are related to security and privacy for innovative applications, like semantic web, data outsourcing, web services, data streams, and online social networks. On these topics Barbara has published more than 60 publications in international journals and conference proceedings, and has been involved in several research projects. She is currently the principal investigator of a project funded by the European Office of Aerospace Research and Development (EOARD). Barbara is the Editor-in-Chief of the *Computer Standards & Interfaces* journal from Elsevier Press, and has been involved in the organization of several international conferences as a program committee member, as well as program and general chair.

ELENA FERRARI

Elena Ferrari is a full professor of Computer Science at the University of Insubria, Italy, where she leads the STRICT SociaLab and is scientific director of the K&SM Research Center. Her research interests are related to various aspects of data management and analysis, including social networks and the social web, access control, privacy, trust, and cloud computing. She received the IEEE Computer Society's prestigious 2009 Technical Achievement Award for "outstanding and innovative contributions to secure data management." In 2011, she received a Google research award for her research on social network privacy. Prof. Ferrari is on the Editorial Board of the *IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Services Computing, Transactions on Data Privacy*, and *International Journal of Information Technology (IJIT)*. She is an IEEE Fellow and a distinguished member of the ACM.

MARCO VIVIANI

Marco Viviani is currently a postdoctoral researcher at the University of Insubria, Italy, on topics connected to Trust Management in the Social Web. He acquired a Ph.D. in Informatics from the Università degli Studi di Milano (University of Milan, Italy) in February 2008. In 2009, he obtained a one-year postoctoral research fellow at the Université de Bourgogne/Le2i (Dijon, France). In 2010, he obtained a two-year postoctoral research fellow at the Institut National des Sciences Appliquées/Liris (Lyon, France). Marco Viviani has been involved in several research projects. His main topics of interest include Trust Management, Trust and Reputation Systems, Social Network Analysis, User Modeling, Knowledge Extraction and Management, Distributed Systems, and Fuzzy Logic. On these topics he has written several international publications.