Access Control Models For Online Social Networks

Rula Sayaf and Dave Clarke

IBBT-Distrinet

Dept. of Computer Science

Katholieke Universiteit Leuven, Belgium

ABSTRACT

Access control is one of the crucial aspects in information systems security. Authorising access to resources is a fundamental process to limit potential privacy violations and protect users. The nature of personal data in online social networks (OSNs) requires a high-level of security and privacy protection. Recently, OSN-specific access control models (ACMs) have been proposed to address the particular structure, functionality and the underlying privacy issues of OSNs.

In this survey chapter, we introduce the essential aspects of access control and review the fundamental classical ACMs. We highlight the specific OSNs features and review the main categories of OSN-specific ACMs. Within each category, we survey the most prominent ACMs and their underlying mechanisms that contribute enhancing privacy of OSNs. Toward the end, we discuss more advanced issues of access control in OSNs. Throughout the discussion we contrast different models and highlight open problems. Based on these problems, we conclude our chapter by proposing requirements for future ACMs.

INTRODUCTION

Online social networks (OSNs) are social networks that are established through web-based services through which people can foster social relationships. Sites such as LinkedIn, Facebook, Google+, MySpace, etc, are therefore type of OSNs (Hafez Ninggal, Abawajy, 2011), but also blogging services, peer-to-peer, collaborative and content sharing sites such as Youtube and Flickr, and social bookmarking services such as CiteULike are also types of OSNs.

Users of OSNs create their own social spaces and upload different types of personal data such as photos, videos, texts, etc. OSNs facilitate easy social interaction by allowing users to establish relationships and connect to other users, who may be friends in the offline world or strangers.

One of the fundamental features of OSNs is the ability to share personal data with others in a relatively privacy-preserving manner. The recent surge of interest in OSNs has been coupled with serious privacy and security concerns, primarily caused by the lack of proper data protection means (Cuttillo, Molva, & Strufe, 2009). For instance, users' privacy concerns have affected the popularity of MySpace. Studies have showed that due to lack of privacy control on MySpace, users have abandoned this OSN (Baracaldo, López, Anwar, & Lewis, 2011) and have migrated to other OSNs for their better privacy-preserving means.

Access control mechanisms are employed in OSNs to enable users to control the dissemination of their own data and protect their privacy accordingly (Abiteboul et al., 2005). Other approaches are employed to protect rights and ownership of data, such as digital rights management (Rodriguez, Rodriguez, Carreras, & Delgado 2009), which we will review later, and watermarking of individual data (Bedi, Wadhai, Sugandhi, & Mirajkar, 2005). Both these approaches and access control models are intended to improve privacy preservation of OSN users.

However, there are many underlying problems in access control mechanisms used in current OSNs. First, only a small percentage of users change the default access control settings to define

their own access control policies (Gross & Acquisti, 2005). Second, when these access control mechanisms are used they fail to address the required fine-grained control to avoid privacy violations (Masoumzadeh & Joshi, 2010). The sensitive personal data in OSNs requires a high-level of protection by means of appropriate access control (Gates, 2007). An inherent challenge is how to define an appropriate ACM to regulate access to OSNs' users' data. ACMs should offer a fine-grained control that captures the specific structure and features of an OSN. Mostly, data dissemination is based on relationships represented in the OSN. Therefore, simple access control lists (Cankaya, 2011) and even more advanced classical ACMs fail to satisfy access control requirements of OSN, as they are not based on the specific properties of social relationships.

Recently, various ACMs have been specifically proposed to address OSN privacy-protection requirements. In this chapter we focus on OSN-specific problems and requirements and how those are tackled by different ACMs.

BACKGROUND AND PRELIMINARY NOTIONS

Online Social Networks

A *social network* (SN) is a set of people connected to each other by social relationships. *Offline Social Networks* refer to real-world social communities. *Online Social Networks* (OSNs) are web-based services that offer the functionality of creating a personal representation of one's self through which one can socialize with others. A *user* is represented in the OSN via a profile to which personal data can be added. An *owner* is a user who adds her data, referred to as *objects*, and can share them with others.

A main feature of OSNs is the articulation of various types of relationships between profiles to facilitate the social communication with others. The social communication includes various activities such as sharing objects, creating groups, organizing online and offline events, etc.

Users in an OSN and their relationships form a *social graph*. Nodes and links in the graph denote users and relationships, respectively (Carminati, Ferrari, & Perego, 2006b). Each pair of users in the graph is connected via a path of links between them. The distance between two users measures the number of links of the shortest path between the two corresponding nodes. The social graph is commonly utilized as an abstraction of OSNs upon which ACMs are formalized.

Access Control Models

An *access control model* (ACM) is a formalization of how policies are composed based on a specific set of features in the system to regulate and authorise access to data. An *access control policy* defines constraints on whether an access request to an object should be granted or denied. In the context of OSNs, a *requestor* initiates a request asking for a specific permission on a specific object from its owner. The owner regulates access to and dissemination of her objects by means of defined access control policies. Once a request is authorised, the specific set of permissions entailed by the policy will be granted to the requestor, who is then referred to as the *accessor*. *Delegation* is entrusting a user (*delegate*) to act on an object with the authority of the object owner (*delegator*). Delegation of authority is convenient for OSNs where users trust each other to further disseminate their objects over the network.

Access control is a two-fold control, authoritative or prohibitive. Most ACMs formalize authoritative, or positive, policies only by assuming a closed-world model (Samarati & Vimercati, 2001). In the closed-world model a request can only be honored by an existing authoritative policy or else it will be denied. In many cases, conflicting policies and hierarchy-propagated policies (Carminati, Ferrari, Heatherly, Kantarcioglu, & Thuraishingham, 2009) might unexpectedly authorise a request and violate the privacy of the owner. Therefore, prohibitive, or negative, policies are crucial to limit accidental authorisations of positive policies. Positive and negative policies are enforced in access control in a mutual exclusion pattern (Samarati & Vimercati, 2001). This pattern authorises a request if this request is entailed by a positive policy and not

denied by a negative policy. This approach ensures more controlled authorisation, contributing to more protection against imprecisely defined access control policies.

For each ACM there should be a specific *enforcement mechanism* to enforce policies in the system. The enforcement mechanism verifies a request and matches it against defined policies to infer an authorisation decision with the right permission to be granted. In OSNs, either a centralized authority, a reference monitor, decentralized authorities or users themselves, can carry out policies enforcement.

Next, we will review the central classical ACMs to establish a sufficient background, before discussing OSN-specific models.

Classical Access Control Models

Access control mechanisms are used in information systems to mitigate security and privacy risks of unauthorised access to data. Those mechanisms vary depending on the underlying structure of the system and the levels of protection needed. The first abstraction of an access control model is the access control matrix (Lampson, 1974). The matrix model describes the system as a protection state by defining a list of access permissions of each subject. A *reference monitor* guards access to objects based on the protection state of the system. A major drawback of this model is the static nature of defining permissions for all the system's subjects. The matrix model lacks abstraction possibilities for groups of subjects and objects. This entails that for each new subject in the system, new lists should be created to guard access to each existing object; the same also applies for each new object in the system. The overhead of changing the protection state limits the applicability of the matrix in large-scale systems. More advanced models expand upon earlier models with specific enhancements to address requirements, identified weaknesses and limitations in expressiveness. These models are more suited to emerging structure and context changes of systems.

Administrative Access Control Models

ACMs can be categorized into three models based on the administration method (Chinaei, Barker, Frank &, 2009):

1. Mandatory Access Control (MAC) (Bell & LaPadula, 1973) is a central authority system that enforces a lattice-based representation of objects and subjects using specific security or sensitivity levels. System administrators define the security level classifications of subjects and objects to guard access authorisations in the system. A policy constrains access based on the security level of the requestor and the security level of the object to be accessed. MAC models are employed in systems where high security needs to be maintained.
2. Discretionary Access Control (DAC) (United States Department of Defense, 1985), or identity-based access control (IBAC), enables system subjects to decide on how to grant permissions to other subjects in the system without any authority involvement. A subject is entitled to define constraints that should be satisfied by an entity in order to be granted specific access permission. DAC models are employed in systems where subjects are responsible for guarding access to their own objects, e.g., OSNs. Other models such as the model of Carminati, Ferrari, Heatherly, Kantarcioglu, and Thuraisingham (2009) extend the DAC concept by enabling users to also define sets of constraints to filter access requests before granting access.

DAC and MAC are not mutually exclusive and can be jointly applied, as in the Chinese Wall model (Kessler, 1992).

3. Role-based Access Control (RBAC) is an alternative model for systems that define specific roles of subjects. Roles are abstract descriptions of what subjects are entitled to perform in the system. Access to an object is dependent on the role assigned to the requestor and the permissions associated to this role. Roles can have different positive and negative permissions, if the model defines negative policies. When different roles are assigned to one subject then the authorised permissions might result in conflicts. The main issues of concern in RBAC are how to assign roles to subjects statically and/or dynamically, and how to guarantee that no conflicts will arise. F. Chen and Sandhu (1995) addressed the assignment of non-conflicting roles by applying constraints. In their approach, constraints can be used as invariants in the system or preconditions

for an action. For example, mutually exclusive roles can be validated by constraints to check that a user cannot have the two roles assigned at once (F. Chen & Sandhu, 1995). Schaad (2001) argues that the Separation of Duty constraints proposed by F. Chen and Sandhu (1995) could still cause conflicts if users are able to delegate roles. Schaad (2001) proposed a rule-based declarative separation of duty approach to statically and dynamically detect role-assignment constraint conflicts and further prohibit delegation of roles. In principal, separation of roles can be guaranteed (H. Chen & Li, 2006) based on the requirements highlighted in the work of Clark and Wilson (1987).

Attribute-based Access Control Models

Attribute-based Access control (ABAC) is another kind of access control model. ABAC formally describes policies based on attributes of subjects, objects and other environment-specific data. In comparison with RBAC, ABAC is more flexible by facilitating the definition of rich and fine-grained policies.

Attribute based encryption (ABE) is a more secure version of ABAC. In ABE, attributes are encrypted using a public and a secret key and distributed to users to which the composition of attributes applies. Bethencourt, Sahai, and Waters (2007) employ ABE for a group-based access control. In their Ciphertext-Policy Attribute-based Encryption model, private keys are defined by a set of attributes and embodied in the form of ciphertext. The ciphertext is a two-part component: an encrypted object and a set of attributes involved in the access control policy. For a request to be authorised, the attributes of the requestor must comply with the ciphertext's attribute component. The policies can be expressed in a collision-resistant monotonic access tree structure. This structure allows a user to have access to more than one private key without being able to aggregate the keys or attributes to access data.

Classic policy models are not targeted to a specific type of system. In general, those models are too abstract to be employed in collaborative systems such as OSNs. OSNs systems have a particular structure and type of communication that requires flexible and highly expressive ACMs. Classical models fail to fully address the requirements of OSNs. However, we will discuss later in this chapter some classical models that have been adapted to OSNs. The adaptations basically focus on exerting more dynamic policy definition mechanisms using specific OSN features to support high granularity protection (Tolone, Ahn, Pai, & Hong, 2005).

ACCESS CONTROL IN ONLINE SOCIAL NETWORKS

In this section we provide an extensive overview of the main aspects of access control models as solutions to various privacy-related issues in OSNs. We start off by reviewing the main privacy problems reported in OSNs. We then provide the essential requirements proposed for OSN-specific ACMs. Then we survey the most prominent OSN-tailored ACMs. In the description of each model, we highlight the main contribution of the model and contrast different approaches. Towards the end of the chapter, we discuss the points in which ACMs need to be enhanced to address open privacy issues. We conclude our discussion by proposing more extensive requirements to fulfill the discussed issues of current OSN-specific ACMs, and to be considered in future research in this domain.

Privacy Risks in Online Social Networks

OSNs have grown in popularity and become a worldwide phenomenon (A. C. Squicciarini & Sundareswaran, 2009). The main features of fostering relationships and sharing data OSNs attract up to 4 users among each 5 Internet users (The State of Social Media 2011: Social is the new normal, 2012). Nonetheless, those features involve many privacy risks. A risk is defined as the insecurity about a potential negative consequence of a specific action (Havlena & DeSarbo, 1991) that is proportional to the likelihood of the negative consequence (Peter & Tarpey, 1975). Estimating risks is strongly coupled with how users perceive their privacy (Norberg, Horne, & Horne, 2007). The indisputable problem in OSNs is that users fail to correctly estimate privacy risks (Acquisti and Grossklags, 2005) and fail to match them to their actual behaviours in the

OSNs (Spiekermann, Grossklags, & Berendt, 2001); this is due to many reasons as we will discuss here.

Acquisti and Grossklags (2005) highlight the following reasons that hinder making proper privacy decisions:

- *Incomplete information* about the possible accessors that makes the risks involved indeterministic especially for external parties accessors.
- *Bounded rationality* (Simon, 1982) limits users ability to rationalize about all available data. Even if a user has access to all data about possible accessors and who should not have access due to all the possible risks, the user's mental model would simplify the quantitative facts when making privacy-related decisions. The inferred decisions might be not very accurate for defining certain policies.
- Social preferences and patterns of data disclosure affect users' decisions. Complete information utilization would not prevent privacy-related decisions from deviating from rationality under those effects.
- Failure in predicting the future preferences and the tendency to compromise in the present to get immediate benefits affects the future privacy status of users.

Users lack proper information about how to make informed privacy decisions (Acquisti & Grossklags, 2005). Therefore, the outcome of the decisions they make using the privacy management tools in current OSNs clashes with their expectations. In Facebook, only about 40% of the privacy settings enable access to data as the owner expects (Lipford, Besmer, & Watson, 2008). The rest of the settings enable more users to access than the owner expects. Users contribute to this discrepancy by acting differently to the privacy concerns they express. Norberg, Horne and Horne (2007) coined the term "privacy paradox" to describe the relationship between users' intentions of disclosure and their actual behaviour.

When users grant access to their data, they are concerned about their privacy. However, these concerns are multi-faceted. Users are more concerned about privacy when disclosing to close friends than to strangers (Gross & Acquisti, 2005). This can be explained based on the incomplete information factor about weak ties shared with strangers (Granovetter, 1973). OSNs facilitate the fostering and managing of a large number of weak ties very easily. Reasoning about the incomplete information to estimate privacy risks of weak ties makes those ties one of the main reasons behind the difficulty of managing privacy in OSNs (Donath & Boyd, 2004). In addition, trust plays a significant role in disclosure decisions (Norberg, Horne, & Horne, 2007). Estimating trust for weak ties is a challenge that results in privacy risks.

The patterns of data sharing in OSNs further complicate reasoning about privacy. OSN users aim at expanding their social interactions within the network and sharing their objects on a large scale (A. C. Squicciarini, Shehab, & Wede, 2010). Indeed, OSNs are designed to encourage users to share. For instance, Facebook is designed to encourage disclosure of as much information as possible (Hu, Gail-Joon, & Jan, 2012). Facebook status textbox encourages users to update the status by showing the text "What's on your mind?" in order to encourage users to write what's on their minds as their status. Facebook users reveal significantly more identifying information about themselves than users in other OSNs (Dwyer, Hiltz, & Passerini, 2007), (Gross and Acquisti, 2005). A personal information revelation study states "Participants are happy to disclose as much information as possible to as many people as possible" (Gross and Acquisti, 2005, p. 2). As the social interactions evolve, more privacy threats arise. Social interactions with friends and friends of friends and so on, might lead to inappropriate disclosure of private information. This is often the case when users are not aware of who can access their objects (A. C. Squicciarini, Shehab, & Wede, 2010; Hogben, 2008).

Trying to mitigate privacy risks by limiting interaction on OSNs would not satisfy users needs. ACMs employed in OSNs should facilitate maximal privacy-preservation without hindering interaction. Access control tools in current OSNs are generally simplistic and coarse-grained (A. C. Squicciarini, Shehab, & Wede, 2010; Masoumzadeh & Joshi, 2010), which occasionally contributes to the failure of privacy protection required by users. All the reasons mentioned above contribute to specifically making OSNs users the victims of privacy violations (H. Wang & Sun, 2010).

We will now list the main OSNs challenges and privacy risks reported in the literature:

- Automatic identity theft (Leyla, Thorsten, Davide, & Engin, 2009), where an attacker can fake a profile of a user and establish connections with the victim's friends resulting in accumulating sensitive communication data.
- Economic loss can be caused due to unauthorised access to data of users in OSNs (Tuunainen, Pitkanen, & Hovi, 2009).
- Data aggregation is possible for malicious users and third party applications (Acquisti et al., 2007).
- Reputation jeopardy of users, especially for prospective employer (Rosenblum, 2007).
- Hacking and phishing of personal data by third parties (Debatin, Lovejoy, Horn, & Hughes, 2009).
- OSNs profile pictures can be improperly used. For example, a personal profile photo from Facebook was publicly used to announce the death in the media (ABC Media Watch, Filleting Facebook. Australian Broadcasting Corporation (ABC), 29 October 07, 2007).
- OSNs-targeting worms that turns users machines into zombies on a botnet (New MySpace and Facebook Worm Target Social Networks, 2008).
- Cyberbullying and stalking by acquiring sensitive data about the victim user (Acquisti et al., 2007).
- Unwanted linkability from photos through the tags of other users who are not the owner of the photo (Acquisti et al., 2007).
- Blackmailing users (Gross & Acquisti, 2005).
- Price discrimination (Gross & Acquisti, 2005).
- Selling data to marketing companies (Rosenblum, 2007).
- Sexual predators, especially of kids, through accessing their sensitive data on OSNs (Rosenblum, 2007).
- Face recognition of profile images available on OSNs can result in users being tracked and recognized in other contexts, e.g., traffic cameras (Acquisti et al., 2007).

All of the previously mentioned issues intensify the fundamental necessity of enhancing security and privacy protection mechanisms of OSNs. To address the unforeseen threats, fine-grained ACMs are required to facilitate more control and protection over any type of data disclosed in the OSN (Masoumzadeh & Joshi, 2010). We do not explicitly suggest that access control is a solution to all the above-mentioned threats; however, guarding access to data is the first fundamental step towards privacy protection. Moreover, OSNs providers, such as Facebook and MySpace, support access control models to construct better trust basis with the privacy-concerned users (H. Wang & Sun, 2010).

Access Control Models Requirements for OSNs

OSNs can be viewed as group-like and collaborative systems, where various ACMs can be applicable for such systems. Same models include Task-based access control (Thomas & Sandhu, 1994; Thomas & Sandhu, 1998), Team-based access control (Thomas, 1997), and Context-based ACMs (Covington et al., 2001). These models are appropriate for OSNs more than the previously discussed classical models are.

In order to evaluate whether an ACM fits OSNs, we review the essential ACM requirements to effectively address security and privacy in OSN within Web 2.0 (Gates, 2007). An ACM should fulfill the following requirements:

- Requirement 1: Relation-based access control is a fundamental requirement to capture the main notion of OSNs. A model should distinguish different types of relationships and grant permissions appropriately (Villegas, Ali, & Maheswaran, 2008).
- Requirement 2: Fine granularity is required to control access to every single piece of data disclosed over the OSN.
- Requirement 3: Interoperability of access control policies to enable users to save and refer to their policies on different OSNs.
- Requirement 4: Sticky policies (Mont, Pearson, & Bramhall, 2003) should be enforced to encapsulate an object and its access control policies in one entity. This guarantees that access to an object is regulated according to the owner's specification, regardless of who is delegated to disseminate this object.

The requirements address different access control aspects; requirement 1 and requirement 2 are related to the modeling. Requirement 3 is concerned with linking multiple OSNs frameworks and business models and thus raising issues that are out of access control models scope. The encapsulation of policies with objects in requirement 4 specifies access control enforcement approach that is not a fundamental part of the access control modeling. Therefore, access control models vary in the degree they address these requirements; most of the models are concerned with requirements 1&2. We will notice the variance in adoption of these requirements in the reviewed OSN-specific ACMs. We will refer to which requirements are satisfied by each model.

It is noteworthy that fine granularity contributes to the complexity of an ACM. This complexity negatively affects users and makes the construction of well-specified policies challenging, which results in privacy violations (Villegas, Ali, & Maheswaran, 2008). Finding models that compromise fine granularity and complexity towards user-friendliness with an acceptable level of privacy-preservation and protection is a challenge.

In the subsequent sections we will review the most common ACMs in the domain. The models are separated into sections based on the most prominent feature of the model.

Rule-based Access Control Models

In rule-based models (Didriksen, 1997) policies are based on rules that constrain authorization decisions based on various features. In an early OSN-specific ACM, Carminati, Ferrari, and Perego (2006b) capture relationships in a rule-based model. The work views the OSN as a social graph to capture particular relationship features on which the model is formalized. A directed link in the social graph represents a relationship from the initiator of the relationship to the receiver. The depth of a relationship is the length of the path. The notion of depth is used to distinguish between a direct and indirect relationship when the depth is $= 1$ or > 1 , respectively. Trust is another feature to distinguish relationships. Trust denotes how much the initiator of a relationship and all the users within the same path trust the receiver of the relationship. The model exploits the Web Ontology Language (OWL) (Oasis Committee. XACML 2.0 Specification., 2012) to represent the OSN and relationships features. Typically, a relationship is represented as an attribute of a *User* class ontology. Since in this model a relationship has many features, it cannot be modeled as an attribute. Using REL-X OWL vocabulary (Carminati, Ferrari, & Perego, 2006a), a relationship is represented as class ontology with features as class properties. Representing the relationship as a separate class makes reasoning about specific relationship properties feasible (Carminati, Ferrari, Heatherly, Kantarcioglu, & Thuraishingham, 2009).

An *access control rule* is the composition of antecedent constraints about an access request, including the to-be-accessed object, and the requestor specifications that entail a specific set of access permissions or prohibitions (Carminati, Ferrari, Heatherly, Kantarcioglu, & Thuraishingham, 2009). The relationship-based access control rules constrain access based on relationship features. Rules have the format:

$$Rule = (obj_{id}, Condset): Condset = \{cond_1, \dots, cond_n\},$$

where obj_{id} is the object to be accessed, $cond_i$ is a tuple of a requestor relationship properties specifications, which has the form:

$$Cond = (v, rt, D_{max}, t_{min}),$$

where v is the object's owner node, rt is the relationship type between the requestor and the object owner, D_{max} is the maximum depth, and t_{min} is the minimum trust. When a request is initiated on a specific object, the requestor's has to prove that the relationship features she owns comply with the condition set of the rule defined. The model translates relationships and rules to logical formulas to easily generate and assert proofs. A rule is expressed as follows:

$$hasSubj(?rel, ?x) \wedge hasObj(?rel, v) \wedge hasType(?rel, rt) \wedge hasDepth(?rel, ?D) \wedge \leq (?D, D_{max}) \wedge hasTrust(?rel, ?t) \wedge \geq (?t, t_{min}),$$

where $?x$ is the requestor, $?rel$ is the relationship between the requestor and object owner.

Access control enforcement here is done at the client-side, inspired by the work of Weitzner, Hendler, Berners-Lee, and Connolly (2006). The model extends the distributed architecture of access control enforcement to be semi-decentralized and thereby overcome the burden of managing certificates. Trusted central nodes save users' data and issue certificates of relationships and trust levels. A signed certificate by both users proves the existence of a direct relationship with a specific trust value. An indirect relationship certificate is a chain of certificates of all

relationships in its path; the trust level of this indirect relationship is the accumulated trust value of all sub relationships.

This early work establishes the basis for later OSN-specific access control models. This model conforms to requirements 1 and 2 by utilizing relationships and enriching the fine granularity of policies with various relationship features. Nonetheless, the rules are limited to relationship properties and do not include other aspects of OSNs such as various user, object, permission, and ownership types.

Role Based Access Control Models

RBAC is applicable in systems in which users can be distinguished and granted access based on different roles. This same distinction of users roles can clearly be realized in OSNs based on the distinction of different relationships users could share with others. Relation Based Access Control (RelBAC) (Giunchiglia, Zhang, & Crispo, 2008) is an RBAC model applicable to OSNs and other applications. RelBAC incorporates relation-based policies as well as role-based policies. This is significant to verify the identity and trust of users as well as relationships for authorisation. RelBAC views relationships differently from other relationship-based models, as we will discuss later. In this model, relations do not denote user-to-user relationships; rather, they denote user-to-object relationships. The user-to-object relationship is established when a user is granted a specific permission over an object. RelBAC is formalized in an *Entity Relationship (ER)* diagram of users, objects and permissions. The ER diagram is translated into a *Description Logic (DL)* representation. DL is a knowledge representation logic that facilitates rich system representation (Baader, Calvanese, McGuinness, Nardi, & Patel-Schneider, 2003). Users and objects are modeled as DL atomic concepts and permissions are modeled of as DL roles. The model captures a dynamic organisation of users in terms of a hierarchy of groups and objects in a hierarchy of classes. Both hierarchies are linked to a permission hierarchy by means of n-ary relations; Users, Objects, and Permission hierarchies are denoted by means of subsumption axioms:

$$X_i \sqsubseteq X_j : X_i^J \sqsubseteq X_j^J,$$

where X_i, X_j are User, Object, or Permission sets. In a hierarchy where *Friend* is a user type that is a generalization of *Closefriend*, the subsumption is expressed as:

$$Closefriend \sqsubseteq Friend.$$

An ontology-based formalization of OSNs (Finin, Ding, Zhou, & Joshi, 2005) lends itself to represent hierarchies using Lightweight Ontologies (Giunchiglia, Marchese, & Zaihrayeu, 2005). The representation captures access control rule instantiations of those permissions/relations. Similarly to the hierarchies, rules are articulated as one the three formulas:

$$C \sqsubseteq P, C \equiv P \text{ or } C \sqsupseteq P,$$

where C is a group of users or a class of objects, P is a class of permissions formulated in DL syntax, $\equiv$ is equality operator and $\sqsubseteq, \sqsupseteq$ are subsumption operators. For example, the following rule states that any user from the *Friend* group is allowed to download all objects of type *Film*:

$$Friend \sqsubseteq \exists Download.Film.$$

The rule above is user-centric. A rule can also be object-centric. For example, the following rule states that all films can be downloaded by some friend:

$$Film \sqsubseteq \exists Download^{-1}.Friend.$$

This formulation of rules allows the system to dynamically evolve the hierarchies without causing conflicts. Moreover, by using the DL atomic negation and complex concept negation, the model formalizes permission negation and denial of permissions, respectively. In addition, RelBAC employs quantificational constructs to represent n-ary relations between objects, users and permissions. This facilitates the expression of policies of an n -owned object by defining permissions of the owners, which we will discuss later in the chapter. Current OSNs and other ACM do not employ quantification constructs. This is advantageous for limiting the number of re-shares and limiting delegation of trust. Such expressiveness satisfies requirement 2 of fine granularity.

Many models extend RBAC for OSNs by preserving authorisation mechanisms and adapting roles to the OSN-specific entities, users or relationships. RBAC captures a social relationship by representing it in terms of the two roles of the users involved in this relationship. For Tang, Mao, Lai, and Zhu (2009), OSN-specific ACM requirements are used to define relationship-based policies and support sharing objects with different users or groups of users. The authors adapted

RBAC to meet those requirements. Their model extends the decentralized management role-based model ARBAC97 (Sandhu, Bhamidipati, & Munawar, 1999) and introduces a server and client to manage roles and permissions, respectively. Upon requesting access to an object, the server managing roles verifies only the roles relevant to the relationship between the requestor and the owner. The owner checks with the client module for the list of permissions that can be granted to a request. A model is required to allow the inherent feature of OSNs users of having multiple relationships and therefore multiple roles. The model reflects this feature by enabling users to have multiple roles assigned to them, one role per relationship. Referring to the relationship path between a requestor and an object's owner implicitly guarantees the separation of roles; yet the authors do not clarify how roles are separated if two users share more than one relationship in different contexts.

Tie-RBAC is another application of RBAC in OSNs (Tapiador, Carrera, & Joaquin, 2011). The notion of tie denotes the composition of a relationship and the two users involved in it. Ties define an automatic system of role-assignment upon establishing a relationship between two users. For instance, when a user establishes a Father-Son relationship with another user, the tie established would assign the roles Father and Son to the initiator and receiver of the relationship, respectively. The access control enforcement in this model is the typical RBAC. Comparably to Tang, Mao, Lai, and Zhu's (2009) model, roles here can be cast on individual users or groups. The model conforms to requirement 1, while the granularity of policies, requirement 2, is rather coarse.

Although RBAC extensions to OSNs are able to conform to requirement 1 and 2, there are other features that can be difficult to explicitly express in such models. Although trust can be implicitly associated with specific roles in a system, it is required to have models where trust can be quantified and used to compose fine-grained policies. Other social graph related aspects, such as a relationship path and distance between users, are not captured in RBAC. Generally, discretionary RBACs are not well suited for OSNs since they burden users with tasks of associating permissions to static roles in different dynamic contexts that are not distinctively separate (Shen & Hong, 2006).

Next, we overview attribute-based models, where a role is decomposed into detailed attributes. These models offer more flexibility in resolving separation of duty constraints.

Attribute-based Access Control Models

The flexibility of Attribute-based Access Control models (ABAC) is employed in OSNs for a higher level of expressiveness and finer granularity. To preserve the privacy and anonymity of OSN users, ABACs usually incorporate encryption techniques. For instance, Persona is a decentralized OSN with an effective and privacy preserving application of ABAC (Baden, Bender, Spring, Bhattacharjee, & Starin, 2009). Access control in Persona is a two-fold mechanism that integrates attribute-based encryption, attribute-based access control and encryption. With this mechanism users are entitled to manage and enforce access control policies without the need to trust a central authority. A user manages access to her objects by distributing public keys to other users entitled to access her objects. The act of exchanging keys implicitly captures the notion of trust over relationships in an OSN by connecting to *a group of potential accessors who can access a set of objects with those keys*. The group encryption protocol is based on generating a group key and encrypting it using each member's public key (Wong, Gouda, & Lam, 1998; D. Naor, Naor, & Lotspiech, 2001). Accessing an object requires the availability of an ABE group key to decrypt a symmetric key with which the object is encrypted. Access permissions and implicit trust can be propagated to indirect relationships such as friend-of-friends via the creation of a group based on another friend's existing group. For instance, if X has defined a group of his 'friends' and Y defines a new group $Y_{X\text{-}friends}$ based on $X_{friends}$ group, then all members of $X_{friends}$ will have access permissions assigned to $Y_{X\text{-}friends}$. The model is not limited to only group-based access, it also facilitates individualistic access control by specifying identity-based access permissions. This multi-faceted accessor specification contributes to the fine granularity of the model, thereby satisfying requirement 2. The downside is that it does not clearly state how group and individual changes can be captured and adapted to in the dynamic environment of OSNs. In case of a group deletion, the ABE key of the group changes for new

encryptions, while previously encrypted objects will still be accessible to the revoked user. Re-encrypting all objects is crucial to overcome this issue and avoid possible privacy threats.

This issue is further addressed in the Encryption-based Access Control in Social Networks with Efficient Revocation (EASiER) (Jahid, Mittal, & Borisov, 2011). EASiER extends ABE and uses a “minimally trusted proxy” to resolve revoked users. The model exploits an effective revocation scheme CP-ABE (Bethencourt, Sahai, & Waters, 2007) to adapt to the dynamic group changes in the OSN. In CP-ABE a ciphertext is a two-part component: encrypted data and components for attributes involved in the ABE key. In order to gain access to an object, a requestor sends part of a ciphertext to the proxy to be decrypted to a form that only an unrevoked user can combine with her attribute keys to decrypt this object. In the revocation scheme of M. Naor and Pinkas (2001), the proxy receives a new key for each revocation without having to commit further changes either to users’ keys or to previously encrypted objects. Attribute-based policies facilitate the incorporation of various OSN-related attributes and features, thereby satisfying requirement 2. The secure proxy-based model is applicable in various OSN structures. The proxy can be a central authority in a centralized OSN, or distributed over the network in a decentralized OSN.

Distinctive authorisation based on the validation of specific attributes facilitates anonymous authentication and preserves requestor’s identity and privacy. A. Squicciarini, Trombetta, Bhargav-Spantzel, and Bertino (2007) propose a k-anonymous (Sweeney, 2002) attribute-based access control model to preserve sensitive information about users’ access history in distributed systems. The proposed model is not specifically tailored for OSNs, yet, it is applicable with OSN-specific attributes. The main contribution of this model is that a requestor can specify k-anonymous credentials to be submitted if there are at least k other undistinguishable sets. The flow of authorisation can be summarized as follows:

- 1- A policy enforcer sends information about attributes to be submitted to the credential submitter (requestor).
- 2- Before sending the k-anonymous attributes, the credential submitter runs a private matching protocol to check for k identical sets or asks the enforcer for more information.
- 3- If the submitter is certain of the existence of k identical sets, then the k-anonymous set is sent to gain access to an object.

The negotiation of the attribute sets facilitates anonymous trust negotiation using a cryptographic based communication in a setting where a submitter cannot be tracked and identified.

It is possible to deploy this model in a decentralized OSN if users are provided with local mechanisms for k-anonymous set generation and for private matching protocols. Despite the privacy preservation of requests and anonymous communication, the model does not explicitly incorporate relationship data of users unless this data is represented in the set of attributes.

In this section we gave an overview of various ABAC models that can be applied in both centralized and decentralized OSNs. The challenge of those models remains in determining which attributes to base policies on.

Trust-based Access Control Models

Golbeck (2009) defines trust as follows: “trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome” (p. 5). Trust plays a key role in relationships between users in OSNs and has a substantial effect on decisions related to authorising access to objects (Golbeck, 2009). In this context, relationships are modeled as edges with a fixed trust value in the social graph (Maheswaran, Tang, & Ghunaim, 2007). As we have seen in the previous sections, many models employ trust as a key constraint in authorising access to objects. Maheswaran, Tang, and Ghunaim (2007) recognize four types of trust modeling:

- Social graph-based trust computation (Xiong & Liu, 2004) similar to trust estimation in the model of Carminati, Ferrari, and Perego (2006b).
- Sensitive trust modeling, where any change in the assessment parameters will be immediately reflected on the trust values.
- Anonymous trust modeling where users anonymously contribute to the ratings of trust (Singh & Liu, 2003).

- Fuzzy trust modeling using fuzzy techniques to combine ratings of users (Aringhieri, Damiani, Di Vimercati, Paraboschi, & Samarati, 2006).

The gravity-based model (Maheswaran, Tang, & Ghunaim, 2007) employs several mechanisms and algorithms for trust computation in OSNs. Trust is established via interactions among users forming positive or negative context-based trust. Independent contexts are modeled in a *Trust Space* where trust calculations are performed in a time-based manner. This trust measure is represented as the distance between two users and can increase or decrease proportionally to the trust value.

Trust-based ACMs are rule-based models that incorporate trust in policy constraints and authorisation decisions. Ali, Villegas, and Maheswaran (2007) introduced Social Access Control (SAC) for OSNs. This multi-level security inspired-model (Benantar, 2006) classifies users and objects in hierarchies based on specific trust values. Each user is assigned an average of trust ratings $r(u)$ by community members (Golbeck, 2006; Levien, 2009). The user can minimally change the rated trust value, by a value λ , to reflect her *operating trust level* τ within a session:

$$\tau = \lambda r(u) \text{ where } 0 \leq \lambda \leq 1.$$

The operating trust level of a user X is cast as the trust level t_o of objects owned by X . The trust level of an object accessed by a user is reflected as an effective trust level of this user. An important contribution of this model is the use of trust to strongly constrain access to objects. While in other models, the trust value of an accessor is independent of the trust level of the owner in the system, this model strongly couples the trust of the accessor with the trust of the owner by allowing users to only access objects within a limited range of their own trust value; otherwise information leakage is reported.

The model employs trusted nodes to encrypt objects based on social encryption schemes (Shamir, 1979). When the trusted node verifies a key, access is granted to the requestor and no delegation of access is allowed.

Another utilization of trust is found in the ‘Personal Data Access Control’ (PDAC) model, proposed by Villegas, Ali, and Maheswaran (2008) for sharing data in centralized OSNs and other systems. The model aims to be user-friendly so that users are not overburdened with many decisions and access control criteria. To share personal data/objects, the owner is only required to define thresholds of three trust zones: acceptance, attestation and rejection. The owner also specifies attestation nodes and the constraints under which the attesters can undersign a request. PDAC quantifies the trust of a requestor based on the relationship with and the distance from the owner, thereby conforming to requirement 1. Analogously to SAC (Ali, Villegas, & Maheswaran, 2007), the social community contributes to the trust quantification formalism. Initially, a user X and the community mutually perform a trust evaluation of X ’s friends and the zones they belong to from the perspective of X . First, the owner defines the zone her friends belong to, and then the social community contributes to refining the trust and the zones of those friends. The trust degree of a requestor is based on the distance from an owner’s object and past context-dependent access experience. The context-dependent access experience is quantified according to the accesses granted to the requestor by the owner and her social neighborhood community. The requestor is classified based on the estimated trust in one of three zones. In comparison with the k-anonymous model (A. Squicciarini, Trombetta, Bhargav-Spantzel, & Bertino, 2007), although this model does not protect anonymity, it offers more sensitive trust quantification by referring to past access history of a requestor, leading to more accurate authorisation decisions.

Authorisations in the model are automatically dependent on the trust zone. A requestor classified in the acceptance zone can automatically access objects of the owner. A rejected zone requestor will be automatically prohibited from accessing an object. An attestation zone requestor needs to be undersigned by the specific attestation nodes. The incorporation of distance, context, and history of access as well as the trust in a requestor by the community enriches the granularity of this model, thereby conforming to requirement 2. Besides access control, the model implements a tracking mechanism to detect re-sharing of objects and to report data leakage. This mechanism tracks and verifies that the trust constraints of a re-shared object comply with the original owner’s constraints.

The Trust-involved Access Control (TAC) model (H. Wang & Sun, 2010) takes a further step into modeling more complex and fine-grained policies. TAC employs a *trust-involved* and purpose-based model for privacy preservation in OSNs. A purpose defines the reason for accessing a data object (Ni et al., 2010). TAC defines intended purposes P_i over objects to

regulate access. Intended purposes include prohibited intended purposes *PIP* and allowed intended purposes *AIP*. The model defines a hierarchy of purposes with generalization and specialization operations and with precedence of *PIP* over *AIP* for conflict resolution. To access an object, an access purpose P_a should specify the access purposes. The purpose P_a is matched against allowed intended purposes P_{ai} of the same object to check whether *AIP* and *PIP* logically implies P_a .

In contrast to Ali, Villegas, and Maheswaran's (2007) model, this model considers both direct and indirect relationships. Access control policies are composed of trust criteria as well as relationship property criteria, which makes the model more protective if trust is not accurately or easily quantified. A policy is defined as a tuple:

$$(D, S, R, P, D_{max}, T_{min}, O),$$

where D is a data object, S is a subject or a group of subjects requesting access, R is the relationship type between the requestor and the owner, D_{max} is the maximum distance of the relationship path, T_{min} is the minimum trust required, and O is a set of obligations the accessor needs to comply to upon access. For example, the rule “ X allows her friends with minimal T trust to access her object O for P purpose, where an accessor is obliged to notify the owner by email” is formulated as:

$$(O, X, Friends, P, 1, T, Notify(Email)).$$

Based on the notion of purpose introduced, policies are either negative or positive. Positive policies implicitly authorise the requested permissions and all their subclass permissions in the defined hierarchy. The model can be also classified as relationship-based model as it depends on the relationship type and path length of the relationship as well as other features. This model conforms to requirements 1 and 2.

The drawback of trust-based models is usability, if users are required to provide input that contributes to trust assessment, such as defining the trust level of objects and zones of access as well as the trust thresholds. Trust-assessment could be problematic in cases where a new user joins and there is no past experience of OSN interaction with this user to assess the trust level.

Next, we discuss other OSN-specific access control models based on other OSN-related features.

Access Control Models in Semantic-based OSNs

The inclusion of semantic web technologies into frameworks and applications has enhanced data sharing and usage. The semantic web lends itself to OSNs by supporting the fundamental functionality of exchanging and sharing data across the network of users (W3C, 2009). For instance, tagging systems are employed in MySpace (Feigenbaum, Herman, Hongsermeier, Neumann, & Stephens, 2007). Resource Description Framework (RDF) and Web Ontology Language (OWL) have been employed to represent personal information of users in OSNs since the early work on Friend of a Friend (FOAF) (Brickley & Miller, 2007). FOAF describes the relationships of users in RDF annotations as an effort to contextualize the semantic web in social networks. Another example of semantic web extensions in social networks is the “Like” button of Facebook that links data from the web to Facebook using the Open Graph Protocol.

In relation to access control, semantic web technologies enable a standardized and dynamic means to control and track objects an OSN. Using ontology basic representation in OSNs facilitates the composition of a more fine-grained access control policies (Carminati, Ferrari, & Perego, 2006b). On the structural level, ontology-based models emerged to exploit rule-based policies to protect the semantic-rich data.

Kruk, Grzonkowski, Gzella, Woroniecki, and Choi (2006) present a Distributed FOAF Realm of the previous FOAF Realm work on Kruk (2004). D-FOAF is distributed identity management system for OSN that uses structure-based access rights and delegations based on the FOAF notion. The specificity of the system structure they model (W3C information management system as a case study) is that users do not own objects; rather they have access to certain objects and they can extend the accessibility to these objects by delegating it to others. The model is based on friendship relations of users who belong to different/distributed sub-communities. The proposed structure saves information about the relationship between two nodes without further details about type, context or any other relationship feature. This structure of the social network saves access rights in an ACL attached to a resource, which is referred to as the Social Networked Access Control List. This list also defines access rights delegation using two criteria values, namely, a

maximal distance from the user in the networks' graph d_{max} and a minimal friendship level metric $flm_{context_{min}}$, which reflects the strength of the relationship. By exploiting these two criteria, the model employs a rudimentary version of trust-based access control. In contrast to other models such as H. Wang and Sun (2010)'s model, this one does not cover aggregation of policies and how to resolve conflicts of delegations. However, this model conforms to requirement 1 and 2.

Carminati, Ferrari, Heatherly, Kantarcioglu, and Thuraisingham (2009) address privacy issues of OSNs by proposing an enhanced and extensible ACM that exploits OWL to represent the social network in a knowledge base (SNKB). Analogously to Carminati, Ferrari, and Perego's (2006b), relationships are represented as ontology classes compliantly with W3C specification (Consortium., 2009), which enables n-ary relationships. A relationship here denotes a relation between two users as well as a relation between a user and an object, e.g., *ownership* or *tagged in* relationships. The two relationship types support the definition of more fine-grained policies in comparison with only user-user or user-object relationship types seen in RBACs and other models. Similarly to previously discussed RBAC models, objects, relationships and permissions are depicted in hierarchies, which facilitates the propagation of permissions within the hierarchies. The model comprises three types of policies:

- Access control policies: negative and positive relationship-based policies that define conditions over the type, depth and trust value of a relationship to authorise/deny access,
- Filtering policies: define conditions to refine user's access to objects or requests to a user's objects,
- Admin policies: allow the system administrator to specify users or define conditions over users that can define access control and filtering policies.

A security authorisation knowledge base (SAKB) encodes the three types of permissions for the three types of policies, namely access control authorisations, prohibitions and admin authorisations. All are organised by means of ontologies. For policy enforcement, Semantic Web Rule Language (SWRL) first transforms a policy into a rule to be queried by the central authorisation enforcement entity against the SAKB. Finally, this model conforms to requirements 1 and 2.

Ontology modeling of OSNs and ACMs facilitates rich and dynamic representations and flexible control over objects. However, as it is the case in ACMs, there are still specific access control problems that are not addressed. Multiple ownership protection is an important problem that rises in OSNs, yet few of those models address that issue. We will review later in the chapter a model that employs semantic web technologies to extend ontology-based models and addresses this problem.

Relationship-Based Access Control Models

A relationship-based access control model does not base authorisation on users identities. Instead, it only consults the social graph's topological structure to extract relationship-related information between an accessor and an owner of an object to authorise an access request.

Fong (2011) formalizes a general-purpose relationship-based access control model (ReBAC), capturing binary relationships such as Parent-Child. The relationship representation captures direct and indirect relationships, corresponding to requirements stated in Carminati, Ferrari, and Perego (2006b). A relationship X - Y is cast as roles of the users involved in it. The work's novelty is in capturing the context-dependency of relationships. This is a contribution to the extent that relationships are separated by organising contexts into a hierarchical structure, where no two relationships in different contexts can be activated simultaneously. Sharing objects over different contexts is based on this hierarchy structure.

The authors interpret ReBAC as a generalization of RBAC where relationships are represented by roles bound in sessions just as relationships are bound in contexts (Fong, 2011). The context hierarchy is analogous to separation of duties mechanisms in RBAC (F. Chen & Sandhu, 1995).

The model depicts the OSN as "a collection of assertions of relationships between individuals in a given population" (Fong, 2011, p. 1). The social network system is a formalized relational structure in a social graph:

$$\mathcal{G} = \langle V, \{R_i\}_{i \in I} \rangle,$$

where V is the set of users in the network, I is the set of relationships identifiers, and each R_i is a binary relationship between two users.

A *resource* is one or more objects. An access control policy is modeled as a predicate to exclusively capture the relational information between the owner and the accessor:

$$\mathcal{U} \times \mathcal{U} \times \mathcal{G}(\mathcal{U}, \mathcal{I}) \rightarrow \{0,1\},$$

where $\mathcal{U}$ is an owner or an accessor, and $\mathcal{G}(\mathcal{U}, \mathcal{I})$ is the social network, which is a graph of users and relationship identifiers. The predicate takes an owner, an accessor and a social network as parameters and will either authorise or decline the request. The model uses vocabularies defined either by the system and/or the users, such as public, friend-of-friend.

ReBAC exploits modal logic formula to express relationship structure between requestors and owners:

$$\varphi, \psi ::= \top \mid a \mid \neg\varphi \mid \varphi \wedge \psi \mid \langle i \rangle \varphi \mid \langle -i \rangle \varphi.$$

For example an owner a can grant access to *friends or parents* using the formula (Fong, 2011):

$$\langle \text{friend} \rangle a \vee \langle \text{parent} \rangle a.$$

This way of composing policies enables the expression of the strength of a relationship required to gain access to an object, for example $\langle \text{friend} \rangle \langle \text{best_friend} \rangle a$ (Fong, 2011). It also employs composite relations to express trust delegation (Weeks, 2001; N. Li, Mitchell, & Winsborough, 2002), for example granting access to friends-of-friends implicitly delegates authority to friends and their friends.

ReBAC is a formalized as a protection system captured as a tuple:

$$\langle \mathcal{I}, \mathcal{U}, \mathcal{R}, \mathcal{C}, c_0, \text{policy}, \text{owner} \rangle,$$

where $\mathcal{I}$ is a set of relation identifiers, $\mathcal{U}$ is a set of users, $\mathcal{R}$ is a set of protected resources, $\mathcal{C}$ is a set of relationships contexts, c_0 the root context in the context hierarchy, *policy* is a function mapping a policy to resource, *owner* is a function that maps a resource to an owner. The access control protection system evolves based on changes in the context hierarchy by means of *state transitions* that are discussed in (Fong, 2011).

A *protection state* is an instantiation of the protection system tuple for request parameters: owner, requestor, active context relationship and social network. The requestor-owner relationship inherits relationships from ancestor contexts. The authorisation decision depends on consulting the protection state of a request. The model conforms to requirement 1, but it does not incorporate fine-granular policy definition.

A more recent work by Fong and Siahaan (2011) investigates the representational completeness of relational policies in ReBAC. The investigation reveals that there were policies that could not be defined using ReBAC. To address the incompleteness, this work introduces non-idempotent conjunction and vertex identification mechanisms to avoid cycles in the graph. The extended language can express a family of ReBAC policies that are proven to be representationally complete (Fong & Siahaan, 2011). The extended ReBAC model is proven to be complete in binary relationship systems. This would be a potential limitation for applying ReBAC in OSNs where relationships might be of multiple arity, as we will discuss in the next section. To address multiple ownership in ReBAC, the model has to extend the policy predicates to resolve different relationship contexts between a requestor and the multiple owners.

N-owned object Protection / Relational Data Protection

An *n*-owned object is an object that is owned by and linked to more than one user. Relational data is the data about and generated by an existing relationship between two users, and therefore is owned by the two users. *N*-owned data protection is a fundamental aspect of multi-user systems such as OSNs (Hu, Gail-Joon, & Jan, 2012). In these systems, sharing is not only uni- or bi-directional, it is mostly *n*-ary directional, causing ownership to become of *n*-ary as well. A photo owner can share a photo in her OSN with *n*-users tagged in it, thereby expanding the unary ownership to be *n*-ary ownership. The original owner should not control such *n*-owned object without involving the other *n* owners in access control decisions (A. C. Squicciarini, Shehab, & Wede, 2010).

Almost all models reviewed earlier in this chapter do not address this issue. A challenge is how to aggregate the owners' preferences and compose their policies defined over one object. Bonatti, De Capitani Di Vimercati, and Samarati (2002) employ an algebra for security policies composition. The algebra implementation is based on translating policies of multiple owners to equivalent logic.

In relationship-based models, the policy composition mechanism of n -owners policies has to preserve the original owners' relationship-based constraints. A policy is monotonic if access is never denied upon adding an edge to the social graph and is never granted upon deletion of an edge. On the other hand, anti-monotonic policies do not allow access if the social graph structure is changed. The policy combinators introduced in (Anwar & Fong, 2010) combine primitive policies to represent complex policies, while preserving monotonic and anti-monotonic policies. More policy composing mechanisms are surveyed in (De Capitani Di Vimercati, Foresti, Jajodia, & Samarati, 2007).

Another challenge is how to detect the existence of relational data and that an object is n -owned. Masoumzadeh and Joshi (2010) employ semantic web technologies and the richness of ontology-based models to define a flexible and fine-grained model to address this challenge. The proposed Ontology-Based Access Control Model for Social Networking Systems (OSNAC) extends many notions of the previously discussed model of Carminati, Ferrari, Heatherly, Kantarcioglu, and Thuraisingham (2009). The main contributions of OSNAC are, the formalization of multiple authorities in OSNs, and, the enforcement mechanism of combined policies of multiple owners. The model extends the OSN knowledge base using a sublanguage of OWL to represent rich RDF graphs representation. The access control policies are queried on the knowledge base via SWRL. The model defines the concept of type "*Annotation*" to represent a relation between more objects; e.g., a comment annotates an object with a note or a tag annotates a photo with a person.

The model defines an access control ontology (ACO) to represent user-object relations as *reified* properties, permissions, and permission authorisations to specific users.

The model formalizes policies for administrators and uses authorisations. These can be either basic or advanced. A basic policy rule defines access authorisations granted by a user or the system to a requestor. Advanced policies define various types of delegation rules based on complex composition of authorisations. This is extended in a formalization of *dependent authorisations*, where an authorisation can be inferred based on another authorisation. The main core contribution of this model is the *multiple-authority specification* that enables disjunctive or conjunctive forms of multi-authority to authorise permissions for n -owned objects.

An access request is a tuple $\langle s, rsc, p \rangle$, where s is the requesting subject, rsc is an instance of a reified property to be accessed, and p is the requested permission. A request is authorised if there exists an instance of permission p in the access control ontology for s on rsc . Negative policies are not explicitly captured in the model, however, the closed-world assumption here guarantees that if an authorisation cannot be inferred by a defined rule then the negation cannot be inferred either. This assumption constrains unintended authorisation from being granted; consequently prohibited permissions are not required to be explicitly defined by users. This model conforms to requirements 1 and 2.

Next we discuss another type of access control model that follows a different approach in addressing some of the issues discussed before.

Voting-based models

Users vary in their privacy preferences. When defining access control policies over n -owned objects it is a challenging task to satisfy all owners' preferences. A. C. Squicciarini, Shehab, and Wede (2010) state that this process should be fair to all owners of an object. Their proposed model is focused on how to reflect co-owners policy specifications onto one policy that maximizes the satisfaction of co-owners privacy preferences. In other word, this model focuses on the conjunctive multi-authority introduced in OSNAC. This work is based on the Clark-Tax voting protocol (E. H. Clarke, 1971) as it provides a simple mechanism that does not allow users to manipulate their voting. This mechanism aggregates owners' access control policies and promotes truthfulness of users. In this mechanism, an ownership right is granted based on an assessment of the user's truthfulness. To make the process less burdensome, the mechanism learns about the users privacy preferences in order to estimate preferences of new objects. If the new object is not similar to any existing object then the mechanism cannot predict the privacy preferences.

Aggregation of policies is modeled as a Nash equilibrium problem (Mas-Colell, Whinston, & Green, 1995) wherein users are rewarded with incentives for truthfulness based on the VCG

payment model (Groves, 1973). The incentive-based systems simply rewards a user i proportionally to the number of n -owned object with n -co-owners:

$$c = m_i + (\beta \times m_i) \times n,$$

where m_i is the credit value assigned to i , $\beta \times m_i$ is the credit assigned to users who accept co-ownership, with $\beta \in [0,1]$. Each co-owner quantifies the benefit value she gets from sharing an object and associates it to her privacy preference g . A collective function outputs the value that maximizes the social values of co-owners:

$$g^* = \arg \max \sum_{i=1}^n v_i(g),$$

where $v_i(g)$ is the benefit value a user i gets.

The mechanism can be applied on different types of policies where attributes are based on the social graph, such as distance-based, geographical locations or common user groups (A. C. Squicciarini, Shehab, & Wede, 2010). This model does not conform with ACMs requirements because it addresses a specific problem; but it can be integrated with other models.

Web Traveler

Although ACMs enable owners to control access to their objects, this control is limited to the user's own space in the OSN. The lack of proper accountability and audit tools enable users to re-share an object and unlawfully gain ownership, thereby depriving the original owner from access control. The difference with the previously discussed n -owned object problem is that the set of owners of one object keeps on expanding over time. As a result, the previously discussed models are unable to directly address this problem.

Rodriguez, Rodriguez, Carreras, and Delgado (2009) address this issue by using Digital Rights Management in OSNs. In their work, users can control access to data by defining flexible conditions in a Right Expression License. Authorisations are granted based on decentralized verification of the license the requestor owns against the requested permissions.

A. C. Squicciarini and Sundareswaran (2009) propose Web-traveler, a model to preserve the owners original access control policies over any access to her objects within the OSN, thereby conforming to requirement 4. In their model they focus on photos, which are shared in vast amounts in OSNs; 3 billion photos are uploaded on facebook each month (Facebook Stat Page, 2011). Web-traveler is an image-centric ACM where policies are always linked to images defining who can access, download and upload them. The policy language XACML-like rules (Oasis Committee. XACML 2.0 Specification, 2012), defines five actions/permission over images, view, upload, download, tag, and comment, organised into a hierarchy. Policies are relationship and attribute-based, and can only be defined for an added image if the image does not exist in the system before (Chang, Li, Wang, Mork, & Wiederhold, 1999). If the new image already exists in the system then the original owner's policies are enforced.

The model utilises positive and negative policies to limit granted authorisations, and it also prohibits delegation of authority unless the user explicitly allows it. Moreover, the model can be generalized over different data types, given appropriate matching mechanisms. Consequently, the model provides a strict privacy protection of users and their data through all out the OSN.

DISTRIBUTED ACCESS CONTROL FOR OSNS

In centralized OSNs, a central authority is responsible for providing the functionality of managing users' data and enforcing access control. In a decentralized or distributed OSN system, trust in a central authority is not required; rather data management and access control enforcement are distributed and carried out by users themselves, or by parties they trust. Distributed access control enables users to manage their local social networks themselves, and is therefore considered to offer more privacy protection for users.

Ahmad and Whitworth (2011) summarize the social and technical requirements of access control:

- Protect ownership of data
- Discretionary roles by users
- Objects classification by users
- Delegation of access rights.

The authors argue that distributed access control will satisfy these requirements and they develop a mathematical model accordingly.

We add to these requirements that a model should properly represent the social graph information within the decentralized OSN structure. The previously discussed models: Carminati, Ferrari, and Perego's (2006b) model, Tang, Mao, Lai, and Zhu's (2009) model, Baden, Bender, Spring, Bhattacharjee, and Starin's (2009) model, Jahid, Mittal, and Borisov's (2011) model, Kruk, Grzonkowski, Gzella, Woroniecki, and Choi's (2006) model are all applicable in decentralized OSNs as we have noted earlier.

ACCESS CONTROL MODELS FOR EXISTING OSNS

Next, we will overview formalized models of some of the current OSNs to understand the underlying mechanisms behind their access control models and how they can be extended to address related access control and privacy concerns issues.

Facebook-Style Access Control Model

Facebook (Facebook, 2011) is the most wide-spread OSNs in the world and has the largest number of registered users (Facebook Stat Page, 2011). Many researchers have been studying different aspects of this OSN and analyzing its privacy issues and threats (Gross & Acquisti, 2005; Cain, Scott, & Akers, 2009).

In order to better understand the privacy policies and points where refinement is needed, it is essential to refer to the formalization of Facebook access control model by Anwar and Fong (2010). The model formalizes the specific two-phase capability-based (Miller, Yee, & Shapiro, 2011; Dennis & Van Horn, 1966) authorisation process in Facebook. To access a specific user's profile or one of her objects, the first phase involves having the capability to access or reach a *search listing* of this user. Facebook provides two means to access a search listing by global name search or by traversing the social graph. Once the search listing is reached and the user's node in the graph is located, the second phase involves the actual access request to this user's profile or object. The second authorisation phase is based on consulting access policies. This model formalizes the communication history and relationship topology for authorisation decisions. Communication history is captured by means of a *communication automaton*:

$$M = \langle \Sigma, \Gamma, \gamma_0, \delta \rangle,$$

where Σ is a finite set of possible communication primitives defined in Facebook, e.g., initiate relationship or accept a relationship, Γ is a finite set of communication states, $\gamma_0 \in \Gamma$ is an initial state, and δ is the transition function, which given a communication state, maps the current system state into a next state. An *adjacency predicate* translates a communication state between two users into an acquaintance relationship. The model defines the *global communication state* as the mapping of each pair of users to their current communication state. The two-phase authorisations are queried against the system's global communication state and the list of policies defined. An authorisation decision is based on the social graph and the communication state between an owner and a requestor. The model formalizes four types of policies a user u can define:

- Search policies, which define who is authorised to produce a search listing of u .
- Traversal policies, which define who is authorised to traverse links of u .
- Communication policies, which define who is authorised to communicate via the system defined primitives with u .
- Access policies, which define who is authorised to access objects.

Anwar and Fong (2010) state that the model instantiated for Facebook does not capture some aspects of Facebook, such as groups and networks, poking and messaging communication, and the open-world assumption. Rather, the authors instantiate their model to support more policies than the Facebook model does, such as celebrity, clique, stranger, bad company and trusted referral (Anwar & Fong, 2010). However, the n -owned object problem is not covered by the extended family of access control model proposed in this work.

Google+ Access Control Model

Google+ (The Google+ Project, 2011) is a more recent OSN. The most prominent feature of Google+ is the notion of circles, which are used by users to define groups of their friends and assign access control policies accordingly. A circle is a set of friends and an extended circle denotes all the members of a user's circles and all the members in their circles, which is analogous to the notion of FOAF. The utilization of circles in Google+, as well as friendlists in Facebook, adds the possibility to specifically select the desired audience allowed to access a specific object. Studies showed that users' mental models about their privacy involve subgroups and communities of their friends (Alessandra, Kristen, & Eytan, Last Updated April 2011.). Correspondingly, circles assist users in comprehending the targeted audience of a disclosed object and to then take an informed decision about the target disclosure audience.

Hu, Gail-Joon, and Jan (2012) formalised a model based on Google+ notion of circles and extended it to address the n -owned object or multiparty ownership. In the Circle-based multiparty access control (CMAC) friends can be assigned a certain trust level and then grouped into circles. The model classifies owners in four types of controllers:

- *Owner*: a user who posted an object in her space,
- *Contributor*: a user who posted an object in someone else's space,
- *Stakeholder*: a user who shares partial ownership in an object of another owner or contributor, e.g., a user tagged in a photo,
- *Disseminator*: a user who discloses data not owned by herself.

A positive or negative policy is a tuple:

$$\langle O, OT, A, D, E \rangle,$$

where O is an owner or a controller of an object, OT is the controller type, A is set of targeted audience defined in terms of circle/extended circles or everyone, D is a data object to be accessed, E effect of enforcing the policy by either denying or permitting access. In the model, a permitted access might cause more privacy violations than a denied access. Furthermore, conflicting policies are resolved based on the higher precedence of denied access over permitted access.

Similarly to the voting-based model (A. C. Squicciarini, Shehab, & Wede, 2010), CMAC enables owners to express their preferences and then implement a preferences balancing mechanism. Whereas in the model of A. C. Squicciarini, Shehab, and Wede, (2010) the objective is to reward users who share, CMAC facilitates the expression of willingness to disclose. The conflict resolution mechanism estimates a *Privacy Risk* counter-proportionally to:

- The trust level of a requestor t_r
- The number of controllers allowing an access
- The privacy concerns of controllers estimated from the default privacy setting pc_o
- The sensitivity of a denied-access-to object s_o

The privacy risk of a requestor r :

$$Pr(r) = (1 - t_r) \times \sum_{o \in \text{controllers}_d} pc_o \times s_o.$$

To balance disclosing intentions of all controllers, the model utilizes a *sharing loss* estimation function using the same four factors utilized for estimating privacy risk from the controllers who permit an access request:

$$Sl(r) = t_r \times \sum_{o \in \text{controllers}_a} (1 - pc_o) \times (1 - s_o).$$

Authorisation is a decision based on a trade off (Brickell & Shmatikov, 2008; T. Li & Li, 2009) between $Sl(r)$ and $Pr(r)$:

$$AD = \begin{cases} \text{Permit} : \alpha Sl(r) \geq \beta Pr(r) \\ \text{Deny} : \alpha Sl(r) < \beta Pr(r) \end{cases},$$

where $0 \leq \alpha, \beta \leq 1$ are preference of privacy risk and sharing loss, such that $\alpha + \beta = 1$.

Given all the n -owned models discussed earlier, the contribution of this model lies in its empowering owners to express their disclosure intentions flexibly based on different factors including the history of their privacy preferences. On the other hand, it does not propose a representation of the n -owned relational data, in contrast with the work of Masoumzadeh and Joshi (2010). Moreover, defining sensitivity of objects might cause problems if an owner is not aware of how other owners model their sensitivity scale.

OPEN PROBLEMS AND FUTURE RESEARCH DIRECTIONS

OSNs are dynamically changing environments with various types of interactions and relationships. The continuous change and evolution makes it look as if any access control model will be insufficient due to the rapid changes in those environments. Context-dependency is a fundamental aspect of the specific nature of interactions in OSNs. Users tend to rely on contexts of data objects to base their disclosure decisions (Majeski, Johnson, & Bellovin, 2011). Amongst all changing aspects of OSNs, context-dependency contributes to making access control models more dynamic and adaptive given the evolution of contexts in the OSNs. Context-dependent access control models (Covington et al., 2001) are not strongly employed in the literature. In many models though, context-dependency is exploited to varying degrees. In the gravity-based model contexts represent trust spaces (Maheswaran, Tang, & Ghunaim, 2007). While in Ali, Villegas, and Maheswaran (2007)'s model, history of access is context-dependent and plays a role in authorisation decisions. In the relationship-based ACM of Fong (2011) relationships are context-dependent. Despite the richness of employing such context-dependent aspects, none of those models formalize context-dependency in all relevant aspects of the ACM. In general, type of users, relationships, history of access, objects, permissions and communication are all aspects that can be context-dependent, which when employed in ACMs would yield a more natural depiction of how users actually think of their social spaces (Majeski, Johnson, & Bellovin, 2011).

Protecting contexts that dynamically change in OSNs is a further complicated issue. Access control models offer protection by means of policies defined with no possibility to dynamically adapt the policies to the changes in the OSN. One work that proposes a privacy-preserving approach through guarding access policies over time is the evolving access control model proposed by Crescenzo and Lipton, (2009). The model implements an extra layer in the ACM to guard privacy settings of users over time. The objective is to maximize the ability to share objects between users while preserving their privacy. An automatic manipulation module manages the visibility settings of objects and maintains the privacy of a user. A data object is not considered to be sensitive on its own, rather an aggregation of user's objects can become at a specific point in time of a sensitive nature depending on changes in relationships, contexts of interaction in the OSN, etc. The model protects sensitive objects and the users' privacy by protecting at least one of the sensitive subset objects by setting it to *private*, thereby mitigating possible privacy violations. The contribution of automatic guarding and changing of policies is novel and promises assistance for users in maintaining a certain level of privacy. For a better employment of this approach, users should be able to specify object's sensitivity criteria in a context-dependent manner. For instance a group of objects is sensitive when disclosed to *friends from work* might be different from the group of objects that are sensitive to be disclosed to *close friends*.

Finally, across the wide spectrum of access control models we can still find gaps in matching users' expectations and requirements for online interaction protection. One of the main issues of why access control models fail is the existence of both offline and online social networks, both of which users rely on to construct their relationships. In specific cases online relationships can complement offline interaction needs. Through facilitating easy communication, online relationships involve more data disclosure when offline social network contact is missing (Dwyer, Hiltz, & Passerini, 2007). Detecting the offline-online SN dependence pattern would enhance users' experience in OSNs and access control privacy protection.

Next, we summarise the requirements we elicited from the review of access control models literature to provide guidelines for future research.

Requirements of Access Control Models for OSNs

Through our review we have discussed open issues that need to be addressed in future work of ACMs. For this reason we propose specific requirements to address those issues of access control models.

We first propose requirements to address general aspects of access control to enhance the overall functionality and efficiency:

- A model should formalize policies, type of users, relationships, history of access, objects, permissions and communication in a context-dependent manner to enable dynamic adaptation of access control policies when contexts change.

- A model should facilitate potential accessor visibility. When a user composes a policy and verifies it against the possible accessors, this contributes to addressing any inconsistency between whom users think will be accessing their objects and the actual accessors. Such functionality will enable users to make informed decisions about the policies they make.
- A model should be able to learn about users' privacy preferences and adapt the defined policies over time according to the learned preferences.
- A model should be able to suggest appropriate policies (Majeski, Johnson, & Bellovin, 2011) for new objects or users added to a user's social space to reduce complexity of composing policies for each update in the OSN.
- A model should facilitate different fine granularity levels of policy definitions. A user should be able to define policies based on specific sets of features.
- A model should be able to maintain the same permissions for the policy targeted-users over time. Normally, a user defines a policy with an intention to allow/prohibit access of a specific set of users, on which the policy criterion applies. This user might require that the policy will always allow/prohibit access to the same set of users over time. Given the changes in the OSN, e.g., relationships, a user who was at a certain point in time prohibited to access some data might gain access. This might happen without the knowledge of the data owner and hence violates his privacy because the user expects that all users who can/cannot access will always have the same permissions. By definition of access control enforcement, a policy criterion will always be consulted to honor or deny a request without any static allocation who is allowed or not allowed to access. This requirement conflicts with the concept of *dynamic* access control enforcement, yet it has to be possible for a user to opt in for such access control enforcement.
- A model should enable control over third party application permissions. In OSNs, users exchange data and communicate over the network. This functionality is not existent with third party applications. Thus permissions of OSN users should be different from permissions of third party applications.
- A model should adapt to offline-online social networks dependencies.

Hereafter, we propose requirement to address specific issues of ACMs. Based on the type of the OSN, an access control model should satisfy some or all of the following requirements:

- Trust based access control models should assess trust precisely without burdening the user with input that has to be provided for this assessment. In some models users are required to assign trust values for their objects and for friends or other users. While this is an important aspect to capture the user's mental model about trust values of her objects and friends, the model should incorporate as much information as possible from the OSN and the interactions between users to assess trust from. Moreover, the model should provide a normalization approach for the trust values of different users.
- A model should enhance control over delegation of authority. Many models utilize the notion of delegation through composite relations (Blaze, Feigenbaum, & Lacy, 1996; D. Clarke et al., 2002; N. Li, Grosz, & Feigenbaum, 2003). The downside is that such models do not incorporate fine-grained control to constrain this delegation. For instance, it should be possible to limit how far the delegation of friends-of-friends in the OSN can be propagated. We propose one solution for this challenge by using certificates of delegation proposed in the work of Abadi, Burrows, Lampson, and Plotkin (1993). A certificate proves an authorisation of the holder and indicates constraints about how this delegation can be further extended.
- A model should define negative and positive policies or else explicitly assume a closed-world model (Samarati & Vimercati, 2001). This is required to guarantee that unintended authorisations are never granted.
- A model should properly represent and protect *n*-owned objects.
- A model should represent any hierarchies of objects, relationships or permissions to the user. This is required to enable the user to comprehend the consequences of propagated permissions from a higher level to a lower level in the hierarchy. This is essential to mitigate implicit permission casting that a user is not aware of, causing privacy vulnerabilities.
- A model should offer specific control over location-based information. In Facebook for instance, location information is added as complementary data to an object. We state that a user should be able to protect this data separately from the object it is attached to.

CONCLUSION

In this chapter we have reviewed the fundamental aspects of access control and the basic essential classical ACMS. We have discussed privacy problems in OSNs and the ACMS requirements to address these problems. We have surveyed the most prominent ACMS and highlighted the main contribution of each model. Through out the review of ACMS, we indicated the aspects that could be extended. The discussion included models in centralized and decentralized OSNs. Finally, we proposed requirements to address the open problems in current ACMS in order to facilitate fine-grained access control and better privacy preservation in OSNs.

REFERENCES

- Abadi, M., Burrows, M., Lampson, B., & Plotkin, G. (1993). A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4), 706–734.
- ABC media watch, filleting facebook. *Australian broadcasting corporation (ABC)*, 29 October 07. (2007) . Retrieved March, 2012, from <http://www.abc.net.au/mediawatch/transcripts/s2074079.htm>.
- Abiteboul, S., Agrawal, R., Bernstein, P., Carey, M., Ceri, S., Croft, B., et al. (2005, May). The Lowell database research self-assessment. *Commun. ACM*, 48(5), 111–118.
- Acquisti, A., Carrara, E., Stutzman, F., Callas, J., Schimmer, K., Nadjm, M., et al. (2007). *Security issues and recommendations for online social networks*. ENISA.
- Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision-making. *IEEE Security and Privacy*, 3(1), 26–33.
- Ahmad, A., & Whitworth, B. (2011). Distributed access control for social networks. *Information assurance and security (IAS)*, (p. 68 -73). IEEE.
- Alessandra, M., Kristen, L., & Eytan, A. (Last Updated April 2011.). The PVIZ comprehension tool for social network privacy settings. *UM Tech Report #CSE-TR-570-11*.
- Ali, B., Villegas, W., & Maheswaran, M. (2007). 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* (pp. 288–293). New York, NY, USA: ACM.
- Anwar, M., & Fong, P. W. L. (2010). *An access control model for Facebook-style social network systems* (Tech. Rep. No. 2010-959-08). Department of Computer Science, University of Calgary, Calgary, Alberta, Canada.
- Aringhieri, R., Damiani, E., Di Vimercati, S. D. C., Paraboschi, S., & Samarati, P. (2006, February). Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems: Special topic section on soft approaches to information retrieval and information access on the web. *J. Am. Soc. Inf. Sci. Technol.*, 57(4), 528–537.
- Ashley, P. (2003). Enterprise Privacy Authorisation Language (EPAL 1.1). *W3C Working Group*. Retrieved March, 2012, from <http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/>.
- Baader, F., Calvanese, D., McGuinness, D., Nardi, D., & Patel-Schneider, P. (2003). *The description logic handbook: Theory, implementation and applications*. Cambridge University Press.

- Baden, R., Bender, A., Spring, N., Bhattacharjee, B., & Starin, D. (2009). Persona: an online social network with user-defined privacy. In *Proceedings of the ACM SIGCOMM 2009 conference on data communication* (pp. 135–146). New York, NY, USA, ACM.
- Baracaldo, N., López, C., Anwar, M. and Lewis, M. (2011). Simulating the effect of privacy concerns in online social networks (pp. 519-524). *Information Reuse and Integration (IRI)*, IEEE International Conference.
- Bauer, L., Ligatti, J., & Walker, D. (2005, June). Composing security policies with Polymer. *SIGPLAN Not.*, 40, 305–314.
- Bedi, R. Wadhai, VM Sugandhi, R. & Mirajkar, A.(2005). Watermarking Social Networking Relational Data using Non-numeric Attribute. *International Journal of Computer Science* 9.
- Bell, D. E., & LaPadula, L. J. (1973). *Secure Computer Systems: Volume I – Mathematical Foundations, Volume II – A Mathematical Model, Volume III – A Refinement of the Mathematical Model* (No. MTR-2547).
- Benantar, M. (2006). *Access Control Systems: Security, Identity Management and Trust Models* (M. Benantar, Ed.). Springer.
- Berendt, B., Gunther, O., & Spiekermann, S. (2005, April). Privacy in e-commerce: stated preferences vs. actual behavior. *Commun. ACM*, 48, 101–106.
- Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *IEEE symposium on security and privacy* (p. 321-334). IEEE Computer Society.
- Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. In *Proceedings of the 1996 IEEE symposium on security and privacy* (pp. 164–173). Washington, DC, USA: IEEE Computer Society.
- Bonatti, P., De Capitani Di Vimercati, S., & Samarati, P. (2002). An algebra for composing access control policies. *ACM Transactions on Information and System Security*, 5(1), 1–35.
- Brickell, J., & Shmatikov, V. (2008). The cost of privacy: destruction of data-mining utility in anonymized data publishing. In Y. Li, B. Liu, & S. Sarawagi (Eds.), *KDD* (p. 70-78). ACM.
- Brickley, D., & Miller, L. (2007). FOAF Vocabulary Specification 0.91, Retrieved March, 2012, from <http://xmlns.com/foaf/spec/20071002.html> (Computer software manual No. November).
- Brickley, D., & Miller, L. (2010, January). FOAF Vocabulary Specification 0.97 (Namespace document). Retrieved March, 2012, from <http://xmlns.com/foaf/spec/20100101.html>
- Cain, J., Scott, D. R., & Akers, P. (2009, October). Pharmacy students' Facebook activity and opinions regarding accountability and e-professionalism. *American journal of pharmaceutical education*, 73(6), 104.
- Cankaya, H. C. (2011). Access control lists. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security (2nd ed.)* (p. 9-12). Springer.
- Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2009). A semantic web based framework for social network access control. In *Proceedings of the 14th ACM symposium on access control models and technologies* (pp. 177–186). New York, NY, USA: ACM.

- Carminati, B., Ferrari, E., & Perego, A. (2006a). The REL-X vocabulary. *OWL Vocabulary*. Retrieved March, 2012, from <http://www.dicom.uninsubria.it/andrea.perego/vocs/relx.owl>.
- Carminati, B., Ferrari, E., & Perego, A. (2006b). Rule-based access control for social networks. In *On the Move to Meaningful Internet Systems 2006: OTM Workshops (2)*, (pp. 1734–1744). Springer.
- Castrucci, A., Martinelli, F., Mori, P., & Roperti, F. (2008). Enhancing Java-ME security support with resource usage monitoring. In *Proceedings of the 10th international conference on information and communications security, 5308* (pp. 256–266). Berlin, Heidelberg: Springer-Verlag.
- Chang, E., Li, C., Wang, J., Mork, P., & Wiederhold, G. (1999). Searching near-replicas of images via clustering. In *Proc. SPIE symposium of voice, video, and data communications* (pp. 281–292).
- Chen, F., & Sandhu, R. (1995). Constraints for RBAC. In *1st ACM workshop on role-based access control* (pp. 39–46). ACM.
- Chen, H., & Li, N. (2006). Constraint generation for separation of duty. In *Proceedings of the eleventh ACM symposium on access control models and technologies* (pp. 130–138). New York, NY, USA: ACM.
- Chinaei, A. H., Barker, K. & Tompa, K. (2009). Comparison of Access Control Administration Models. *Ubiquitous Communication and Computing Journal (UBICC)*, 4(3).
- Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. In *Proc. Symposium on Security and Privacy 1987* (IEEE Press), 184–193.
- Clarke, D., Elien, J.-E., Ellison, C., Fredette, M., Morcos, A., & Rivest, R. L. (2002, February). Certificate chain discovery in SPKI/SDSI. *J. Comput. Secur.*, 9(4), 285–322.
- Clarke, E. H. (1971). Multipart pricing of public goods. *Star*, 11(1), 17–33.
- Consortium., W. W. W. (2009). *Status for resource description framework (RDF) model and syntax specification*. Retrieved March, 2012, from <http://www.w3.org/1999/status/PR-rdf-syntax-19990105/status>.
- Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M., & Abowd, G. D. (2001). Securing context-aware applications using environment roles. In *SACMAT '01: Proceedings of the sixth ACM symposium on access control models and technologies* (pp. 10–20). New York, NY, USA: ACM Press.
- Crescenzo, G., & Lipton, R. J. (2009). Social network privacy via evolving access control. In *Proceedings of the 4th international conference on wireless algorithms, systems, and applications* (pp. 551–560). Berlin, Heidelberg: Springer-Verlag.
- Cuttillo, L., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE*, 47(12), 94–101.
- United States Department of Defense. (1983). *Trusted Computer System Evaluation Criteria (Orange Book)*. D. of Defense.
- De Capitani Di Vimercati, S., Foresti, S., Jajodia, S., & Samarati, P. (2007). Access Control Policies and Languages in Open Environments. *Secure Data Management in Decentralized Systems*, 21–58. Springer.

- Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Computer-Mediated Communication*, 15(1), 83-108.
- Dennis, J. B., & Van Horn, E. C. (1966). Programming semantics for multi-programmed computations. *Commun. ACM*, 9(3), 143-155.
- Didriksen, T. (1997). Rule based database access control: a practical approach. In *Proceedings of the second ACM workshop on role-based access control* (pp. 143-151). New York, NY, USA: ACM.
- Donath, J., & Boyd, D. (2004). Public displays of connection. *BT Technology Journal*, 22, 71-82.
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and Myspace. In J. A. Hoxmeier & S. Hayne (Eds.), *AMCIS* (p. 339). Association for Information Systems.
- Erlingsson, U., & Irm, F. B. S. (2000). IRM Enforcement of Java Stack Inspection. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, 246-255. IEEE.
- Facebook. (2011). Retrieved March, 2012, from <http://www.facebook.com>.
- Facebook stat. page. (2011). Retrieved March, 2012, from <http://www.socialtechnologyreview.com/articles/50-facebook-stats-every-marketer-should-know>.
- Feigenbaum, L., Herman, I., Hongsermeier, T., Neumann, E., & Stephens, S. (2007, December). The semantic web in action. *Scientific American*, 297, 90-97.
- Finin, T., Ding, L., Zhou, L., & Joshi, A. (2005). Social networking on the semantic web. *The Learning Organization*, 12(5).
- Fong, P. W. L., & Siahaan, I. (2011). Relationship-based access control policies and their policy languages. In *Proceedings of the 16th ACM symposium on access control models and technologies* (pp. 51-60). New York, NY, USA: ACM.
- Fong, P. W. L. (2011). Relationship-based access control: protection model and policy language. In *Proceedings of the first ACM conference on data and application security and privacy* (pp. 191-202). New York, NY, USA: ACM.
- Gates, C. (2007). Access control requirements for Web 2.0 Security and Privacy. *IEEE Web*, 2, 2-4.
- Giunchiglia, F., Marchese, M., & Zaihrayeu, I. (2005). *Towards a theory of formal classification* (Tech. Rep.). University of Trento.
- Giunchiglia, F., Zhang, R., & Crispo, B. (2008). RELBAC: Relation based access control. In *Proceedings of the 2008 fourth international conference on semantics, knowledge and grid* (pp. 3-11). Washington, DC, USA: IEEE Computer Society.
- Golbeck, J. (2006). Combining provenance with trust in social networks for semantic web content filtering. In *IPAW'06* (p. 101-108). Springer.
- Golbeck, J. (2009). Trust and nuanced profile similarity in online social networks. *TWEB*, 3(4). ACM.

- The Google+ project. (2011). Retrieved March, 2012, from <https://plus.google.com>
- Granovetter, M. S. (1973, January). The strength of weak ties. *The American Journal of Sociology* 78(6), (pp. 1360-1380). JSTOR.
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71–80). New York, NY, USA: ACM.
- Groves, T. (1973). Incentives in teams. *Econometrica: Journal of the Econometric Society*, 41, 617–631.
- Hafez Ninggal, M.I.; Abawajy, J. (2011). Attack Vector Analysis and Privacy-Preserving Social Network Data Publishing. *Trust, Security and Privacy in Computing and Communications (TrustCom)* pp.847-852. IEEE.
- Hamlen, K. W., Morrisett, G., & Schneider, F. B. (2006). Computability classes for enforcement mechanisms. *ACM Transactions on Programming Languages and Systems*, 28(1), 175–205.
- Havlena, W. J., & DeSarbo, W. S. (1991). On the measurement of perceived consumer risk. *Decision Sciences*, 22(4), 927–939.
- Hogben, G. (2008). *Security issues and recommendations for online social networks* (Tech. Rep.). European Network and Information Security Agency.
- Hu, H., Gail-Joon, A., & Jan, J. (2012). *Enabling collaborative data sharing in Google+* (Tech. Rep.). Arizona State University.
- Jahid, S., Mittal, P., & Borisov, N. (2011). EASiER: encryption-based access control in social networks with efficient revocation. In *Proceedings of the 6th ACM symposium on information, computer and communications security* (pp. 411–415). ACM.
- Kessler, V. (1992). On the Chinese wall model. In *Proceedings of the second european symposium on research in computer security* (pp. 41–54). London, UK: Springer-Verlag.
- Kruk, S. (2004). FOAF-realm-control your friends' access to the resource. *FOAF Workshop proceedings 186*. Retrieved March, 2012, from http://www.w3.org/2001/sw/Europe/events/foaf-galway/papers/fp/foaf_realm/.
- Kruk, S., Grzonkowski, S., Gzella, A., Woroniecki, T., & Choi, H. (2006). D-FOAF: Distributed identity management with access rights delegation. *The Semantic Web—ASWC 2006*(4), 140–154.
- Lampson, B. (1974). Protection. *ACM SIGOPS Operating Systems Review*, 8(1), 18-24. ACM.
- Levien, R. (2009). Attack-resistant trust metrics. In *Computing with social trust* (pp. 121–132). Springer.
- Leyla, B., Thorsten, S., Davide, B., & Engin, K. (2009, April). All your contacts are belong to us: Automated identity theft attacks on social networks. In *18th international world wide web conference*. ACM.
- Li, N., Grosz, B. N., & Feigenbaum, J. (2003, February). Delegation logic: A logic-based approach to distributed authorisation. *ACM Trans. Inf. Syst. Secur.*, 6(1), 128–171.
- Li, N., Mitchell, J. C., & Winsborough, W. H. (2002). Design of a role-based trust-management framework. In *Proceedings of the 2002 IEEE symposium on security and privacy* (pp. 114–130). Washington, DC, USA: IEEE Computer Society.

- Li, T., & Li, N. (2009). On the tradeoff between privacy and utility in data publishing. In J. F. Elder IV, F. Fogelman-Soulie, P. A. Flach, & M. Zaki (Eds.), *KDD* (p. 517-526). ACM.
- Ligatti, J., Bauer, L., & Walker, D. (2005). Enforcing Non-safety Security Policies with Program Monitors. *Computer Security ESORICS 2005*, 3679, 355–373.
- Lipford, H. R., Besmer, A., & Watson, J. (2008). Understanding privacy settings in Facebook with an audience view. In *Proceedings of the 1st conference on usability, psychology, and security* (pp. 2:1–2:8). Berkeley, CA, USA: USENIX Association.
- Maheswaran, M., Tang, H. C., & Ghunaim, A. (2007). Towards a gravity- based trust model for social networking systems. In *Proceedings of the 27th international conference on distributed computing systems workshops* (pp. 24–24). Washington, DC, USA: IEEE Computer Society.
- Majeski, M., Johnson, M., & Bellovin, S. M. (2011). *The Failure of Online Social Network Privacy Settings* (Tech. Rep. No. CUCS-010-11). Department of Computer Science, Columbia University.
- Mas-Colell, A., Whinston, M. D., & Green, J. R. (1995). *Microeconomic theory - chapter 23*. Oxford University Press. Hardcover.
- Masoumzadeh, A., & Joshi, J. (2010). OSNAC: An ontology-based access control model for social networking systems. In *Proceedings of the 2010 IEEE second international conference on social computing* (pp. 751–759). Washington, DC, USA: IEEE Computer Society.
- Mika, P. (2005). Ontologies are us: A unified model of social networks and semantics. In Y. Gil, E. Motta, V. R. Benjamins, & M. A. Musen (Eds.), *The Semantic Web - ISWC 2005*, (pp. 522-536). Springer.
- Miller, M. S., Yee, K.-P., & Shapiro, J. (2011). *Capability myths demolished* (Tech. Rep.). Systems Research Laboratory, Johns Hopkins University. Retrieved March, 2012, from <http://srl.cs.jhu.edu/pubs/SRL2003-02.pdf>.
- Mont, M. C., Pearson, S., & Bramhall, P. (2003). Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. *14th International Workshop on Database and Expert Systems Applications (DEXA'03), September 1-5, 2003, Prague, Czech Republic*, (pp. 377-382). IEEE Computer Society.
- Naor, D., Naor, M., & Lotspiech, J. B. (2001). Revocation and tracing schemes for stateless receivers. *Advances in Cryptology—CRYPTO 2001* (pp. 41–62). Springer.
- Naor, M., & Pinkas, B. (2001). Efficient trace and revoke schemes. In *Proceedings of the 4th international conference on Financial Cryptography*, 9(6), 1–20. London, UK, UK: Springer-Verlag.
- New Myspace and Facebook worms target social networks.* (2008). Retrieved March, 2012, from <http://www.darknet.org.uk/2008/08/new-myspace-and-facebook-worm-target-social-networks/>.
- Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., et al. (2010, July). Privacy-aware role-based access control. *ACM Trans. Inf. Syst. Secur.*, 13(3), 24:1–24:31.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126.
- Oasis committee. XACML 2.0 specification.* (2012). Retrieved March, 2012, from <http://www.oasisopen.org/committees/tchome.php?wgabbrev=xacmlXACML20>.

- Peter, J. P., & Tarpey, S., Lawrence X. (1975, June). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research*, 2(1), 29-37.
- Rodriguez, E., Rodriguez, V., Carreras, A., & Delgado, J. (2009). A Digital Rights Management approach to privacy in online social networks. In *Workshop on privacy and protection in web-based social networks (within ICAIL '09), Barcelona, Spain, 2009*. IDT Series, vol. 3, ISSN 2013-5017.
- Rosenblum, D. (2007, may-june). What anyone can know: The privacy risks of social networking sites. *Security Privacy, IEEE*, 5(3), 40-49.
- Samarati, P., & Vimercati, S. D. C. D. (2000). Access control: Policies, models, and mechanisms. In R. Focardi & R. Gorrieri (Eds.), *FOSAD* (LNCS Vol. 2171, p. 137-196). Springer.
- Samarati, P., & Vimercati, S. D. C. D. (2001). Access control: Policies, models, and mechanisms. In *Revised versions of lectures given during the IFIP WG 1.7 international school on foundations of security analysis and design on foundations of security analysis and design: Tutorial lectures*, 2171, (pp. 137– 196). London, UK: Springer-Verlag.
- Sandhu, R., Bhamidipati, V., & Munawar, Q. (1999). The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security*, 2(1), 105–135.
- Schaad, A. (2001). Detecting conflicts in a role-based delegation model. *Seventeenth Annual Computer Security Applications Conference*, 117–126. IEEE Comput. Soc.
- Shamir, A. (1979, November). How to share a secret. *Commun. ACM*, 22(11), 612–613.
- Shen, H.-b., & Hong, F. (2006). An attribute-based access control model for web services. In *Proceedings of the seventh international conference on parallel and distributed computing, applications and technologies* (pp. 74–79). Washington, DC, USA: IEEE Computer Society.
- Simon, H. A. (1982). Models of bounded rationality.. Trustme: Anonymous management of trust relationships in decentralized P2P systems. In N. Shahmehri, R. L. Graham, & G. Caronni (Eds.), *Peer-to-peer computing* (p. 142-149). IEEE Computer Society.
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. *World Wide Web Internet And Web Information Systems*, 38–47.
- Squicciarini, A., Trombetta, A., Bhargav-Spantzel, A., & Bertino, E. (2007). K-anonymous Attribute-Based Access Control. *E. International Conference on Information and Computer Security (ICICS'07)*.
- Squicciarini, A. C., Shehab, M., & Wede, J. (2010, June). Privacy policies for shared content in social network sites. *The VLDB Journal*, 19(6), 777–796.
- Squicciarini, A. C., & Sundareswaran, S. (2009, December). Web-traveler policies for images on social networks. *World Wide Web*, 12, 461–484.
- The state of social media 2011: Social is the new normal*. (2012). Retrieved March, 2012, from <http://www.briansolis.com/2011/10/> <http://www.briansolis.com/2011/10/state-of-social-media-2011/>.
- Sweeney, L. (2002, October). K-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10, 557–570.

- Tang, Y., Mao, C., Lai, H., & Zhu, J. (2009, December). Role Based Access Control for social network sites. *2009 Joint Conferences on Pervasive Computing (JCPC)*, 389–394.
- Tapiador, A., Carrera, D., & Joaquin, S. (2011). Tie-RBAC: an application of RBAC to social networks. *Web 2.0 Security and Privacy*. Oakland, California.
- Thomas, R. K. (1997). Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. In *Second ACM workshop on role-based access control* (pp. 13–19). ACM.
- Thomas, R. K., & Sandhu, R. S. (1994). Conceptual Foundations for a Model of Task-based Authorisations. In *7th IEEE computer security foundations workshop* (pp. 66–79). IEEE Computer Society Press.
- Thomas, R. K., & Sandhu, R. S. (1998). Task-based authorisation controls (TBAC): A family of models for active and enterprise-oriented authorisation management. In *Proceedings of the IFIP TC11 WG11.3 eleventh international conference on database security xi: Status and prospects* (pp. 166–181). London, UK, UK: Chapman & Hall, Ltd.
- Tolone, W., Ahn, G.-J., Pai, T., & Hong, S.-P. (2005). Access control in collaborative systems. *ACM Computing Surveys*, 37(1), 29–41.
- Tuunainen, V. K., Pitkanen, O., & Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking sites - Case Facebook. *22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety*, Bled, Slovenia.
- Verhanneman, T., Piessens, F., De Win, B., & Joosen, W. (2005). Uniform application-level access control enforcement of organization wide policies. In *Proceedings of the 21st annual computer security applications conference* (pp. 431–440). Washington, DC, USA: IEEE Computer Society.
- Villegas, W., Ali, B., & Maheswaran, M. (2008). An access control scheme for protecting personal data. In *Proceedings of the 2008 sixth annual conference on privacy, security and trust* (pp. 24–35). Washington, DC, USA: IEEE Computer Society.
- W3C. (2009). *W3C semantic web activity*. Retrieved March, 2012, from <http://www.w3.org/2001/sw/>.
- Wang, C., & Leung, H.-f. (2004). A secure and private Clarke tax voting protocol without trusted authorities. In *Proceedings of the 6th international conference on electronic commerce* (pp. 556–565). New York, NY, USA: ACM.
- Wang, H., & Sun, L. (2010). Trust-involved access control in collaborative open social networks. In *Proceedings of the 2010 fourth international conference on network and system security* (pp. 239–246). Washington, DC, USA: IEEE Computer Society.
- Weeks, S. (2001). Understanding trust management systems. In *Proceedings of the 2001 IEEE symposium on security and privacy* (pp. 94–105). Washington, DC, USA: IEEE Computer Society.
- Weitzner, D. J. , Hendler, J., Berners-Lee, T., & Connolly, D. (2006). Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web. In E. Ferrari & B. Thuraisingham (Eds.), *Web and information security* (pp. 1–31). Idea Group Inc.
- Wong, C. K., Gouda, M. G., & Lam, S. S. (1998). *Secure group communications using key graphs*. ACM SIGCOMM Computer Communication Review 28(4), 68-79. ACM.

Xiong, L., & Liu, L. (2004, July 8.–10.) Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7), 843–857.

ADDITIONAL READING SECTION

Abdessalem, T., & Dhia, I. B. (2011). A reachability-based access control model for online social networks. In *Databases and social networks* (pp.31–36). New York, NY, USA: ACM.

Beato, F., Kohlweiss, M., & Wouters, K. (2009). Enforcing access control in social network sites. *Hot Topics in Privacy Enhancing Technologies (HotPETS)*, 1–11.

Carminati B And Ferrari, E. (2008). Access control and privacy in web-based social networks. *Access control and privacy in Web-based social networks*, 4(4), 395–415. Emerald Group Publishing Limited.

Carreras, A., Rodriguez, E., & Delgado, J. (2009). Using XACML for access control in Social Networks. In *W3C workshop on access control application scenarios*.

Chong, C., Corin, R., Doumen, J., & Etalle, S. (2006). License script: A logical language for digital rights management. *Annals of Telecommunications*, 61(3), 284–331.

Danezis, G. (2009). Inferring privacy policies for social networking services. In *Proceedings of the 2nd ACM workshop on security and artificial intelligence* (pp. 5–10). New York, NY, USA: ACM.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Computer-Mediated Communication*, 15(1), 83-108.

Erlingsson, U., & Schneider, F. B. (2000). SASI enforcement of security policies: a retrospective. In *Proceedings of the 1999 workshop on new security paradigms* (pp. 87–95). New York, NY, USA: ACM.

Fernandez, E. B., Marin, C., & Petrie, M. M. L. (2010). Handbook of Social Network Technologies and Applications. *Social Networks*, 569–582.

Giunchiglia, F., Zhang, R., & Crispo, B. (2009). Ontology Driven Community Access Control. In *1st workshop on trust and privacy on the social and semantic Web Spot2009*. Citeseer.

Joshi, J. B. D., Bertino, E., Latif, U. ,& Ghafoor, A. (2005). A generalized temporal role-based access control model. *IEEE Trans. on Knowl. and Data Eng.*, 17, 4–23.

Lazarsfeld, P. F., & Merton, R. K. (1954). Friendship as a social process: A substantive and methodological analysis. In M. Berger, T. Abel, & C. Page (Eds.), *Freedom and control in modern society* (pp. 18–66). New York: Van Nostrand.

Ligatti, J., Bauer, L., & Walker, D. (2005). Enforcing Non-safety Security Policies with Program Monitors. *Computer Security ESORICS 2005, LNCS 3679*, 355–373.

Nasirifard, P. (2007). Context-Aware Access Control for Collaborative Working Environments Based on Semantic Social Networks. In *Proceedings of the Doctorial Consortium Workshop at Sixth International and Interdisciplinary Conference on Modeling and Using Context (Context'07)*, Roskilde, Denmark, 2007.

Palen, L., & Dourish, P. (2003). Unpacking “privacy” for a networked world. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 129–136). New York, NY, USA: ACM.

Park, J., Sandhu, R., & Cheng, Y. (2011). User-Activity Centric Framework for Access Control in Online Social Networks. *IEEE Internet Computing*, 1–9.

Squicciarini, A., Paci, F., & Sundareswaran, S. (2010). PriMa: An effective privacy protection mechanism for social networks. In *Proceedings of the 5th ACM symposium on information, computer and communications security* (pp. 320–323). ACM.

KEY TERMS AND DEFINITIONS

Social network (SN): a set of people connected to each other by social relationships.

Offline Social Networks: real-world social communities.

Online Social Networks (OSNs): web-based services that offer the functionality of creating a personal representation of one's self through which one can socialize with others.

User: any agent that uses the OSN and is represented via a profile of personal data.

Owner: a user who adds her data, referred to as objects, and can share them with others.

Access control model (ACM): a formalization of how policies are composed based on a specific set of features in the system to regulate and authorise access to data.

Access control policy: constraints on whether an access request to an object should be granted or denied.

Requestor: a user who initiates a request to be granted a specific permission on a specific object from its owner.

Accessor: an authorised requestor that has been granted the specific set of permissions entailed by the policy.

Delegation: entrustment in a user (delegate) to act on an object in a certain way with the authority from the object owner (delegator).