Towards Provenance and Risk-Awareness in Social Computing

Yuan Cheng[*‡]
ycheng@cs.utsa.edu

Dang Nguyen[*‡]
dnguyen@cs.utsa.edu

Khalid Bijon[*‡]
kbijon@cs.utsa.edu

Ram Krishnan[†‡]
ram.krishnan@utsa.edu

Jaehong Park[‡]
jae.park@utsa.edu

Ravi Sandhu[*‡]
ravi.sandhu@utsa.edu

[*]Department of Computer Science
[†]Department of Electrical and Computer Engineering
[‡]Institute for Cyber Security
University of Texas at San Antonio

ABSTRACT

Although social computing (SC) has been growing phenomenally, it still lacks an appropriate way of protecting the security and privacy of data shared in the system. Current access control mechanisms in the domain of SC mainly rely on pre-defined access control policies to achieve authorization statically, which are intrinsically unsuitable for capturing the dynamic changes in social environment. In this paper, we explore the approach towards a more flexible and adaptive control through the incorporation of risk awareness in SC. In particular, risk values are associated with users and objects; meanwhile, risk thresholds are defined for each of the permissions. Risk values and risk thresholds can be derived from provenance data in a timely manner. Such dynamic computation can be enabled and facilitated with the incorporation of provenance awareness in SC systems.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access controls*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Unauthorized access*

Keywords

Risk, Provenance, Social Computing

1. INTRODUCTION

With the advent of the social computing (SC) era, applications and services that facilitate social behaviors among users and then make use of those behaviors for a multitude of purposes have emerged as the dominating forces on the web. Social computing enables a novel way of creating and sharing information where information is coming through users and is shaped by the social interaction among users. Some of the well-known SC applications, such as Youtube, Flickr, Facebook, Wikipedia, Amazon and eBay's review and recommendation systems, have become a global phenomenon, attracting millions of users actively engaged in.

As social computing has been growing phenomenally, its potential benefits for collaboration and information sharing have been identified [20]. However, data security and privacy has become a pressing problem in the domain of SC, since an increasing amount of user-generated data has been collected and shared in all kinds of SC applications. In SC systems, content is almost entirely contributed by users, so it is users' interest to control their own or related resources. Recently, there have been several access control mechanisms proposed for SC systems, where access control policies are specified by users rather than the system alone. Park et al [23] presented an activity-centric framework to capture various activities that can influence on control decisions and address how these activities can be controlled in SC systems, while many other researchers have focused on providing access control solutions for online social networks [6, 7, 9, 10, 11, 12], which comprise a prominent subset of SC applications. While these recent works deal with access control in SC from various aspects, they are inflexible in coping with the dynamic changes that occur in SC systems, since their authorization decision mainly relies on some static access control policies pre-defined by either individual users or the system. Users usually do not have a complete understanding of the threats to their data security and privacy, thus user-specified access control policies are intrinsically incomplete and imprecise to capture the future needs and user behaviors in such an agile and dynamic environment.

Risk awareness presents a novel form of access control for sharing information in agile and dynamic ways [2, 8, 14]. A risk-aware access control system grants or denies an access request dynamically based on an estimated risk rather than some pre-defined access control policies that always give the same outcomes as we may find in traditional access control systems. To model access control based on risk, such systems require proper means of assessing and managing risk in the context of the application. In a typical SC application, users are able to specify policies about other's access to their resources and the activities to be performed on such

SRAS'12, September 19, Minneapolis, MN, USA

resources; on the other hand, they are also allowed to control how they can perform on resources and other users. To make access control more flexible and adaptive for SC environments, we incorporate a risk-aware approach to access decision process. Essentially, we associate risk values with users and objects in the system. In addition, we incorporate risk thresholds that are set by users (e.g., requesting users or owner of objects) into access control policies and make access decision dynamically based on risk values and risk thresholds.

The first key step to deploy such risk-aware access control mechanism is to estimate the risk of granted access being misused, which depends on the likelihood of misusing permissions by the requesting user as well as the sensitivity of the data being accessed and the action performed on the data. Investigating the likelihood of misusing permissions is especially difficult as it is always hard to predict the future behaviors of the requesting user. As using data provenance for access control has received increasing interest in the security research community, we strongly feel that data provenance can be exploited to derive user trustworthiness and data sensitivity in SC systems as well. Data provenance contains a chain of past processes that have influences on data objects. Some information, including versioning and user's past activities, can be utilized as a basis for risk assessment. This approach provides the needed dynamicity to the process and can be utilized in a variety of ways to enhance the security of the SC platform.

In this paper, we argue that taking risk awareness into consideration makes access control more flexible and adaptive to the dynamic nature of social computing. We then identify that data provenance can be utilized to derive user trustworthiness and sensitivity of permission, which reflect the likelihood of misusing a permission in the future and the cost of misusing the corresponding permission, respectively. The Open Provenance Model (OPM) [15] is used as the data model for provenance data for our approach of provenance-based risk assessment.

The rest of the paper is organized as follows. We begin in section 2 with an example motivating the need for risk awareness access control for social computing platform, which is later discussed in detail in section 3. Section 4 elaborates the use of provenance data to determine and estimate risk to users and permissions in SC. Section 5 briefs some research works related to access control about risk, provenance and social computing. Section 6 concludes the paper.

2. MOTIVATION

In this section, we illustrate the motivation for the incorporation of risk awareness and provenance awareness to SC system through an example.

2.1 Example Scenario

Our example demonstrates a Facebook-like social environment in the wake of the upcoming presidential campaign. We describe the scenario in details below:

A fan of a presidential candidate might create a **fan page** to show support to the candidate's campaign. To maintain the page, the creator configures a set of rules about how other users can access the resources on the page. For example, anyone in the social network is allowed to join the page by clicking the **like** button. A limited set of actions are then available to those newly joined users, such as **read** and **share** some introductory posts. After one completes a series of reading and sharing to demonstrate his expertise on political affairs and his credibility in online social life, he might acquire read access to some more valuable posts or he might be allowed to **vote** on an already created election **poll**. However, user's credibility might also get degraded if he does not properly or actively involved in participation. Furthermore, the creator of the page might start an **event** to **discuss** on the election outcome, which requires users high trustworthiness to **join**. With more access from highly trustworthy users, the possibility of the resource being misused is being reduced, thus the owner may lower the requirement for user trustworthiness and allow more users to participate in.

In the example, we identify a set of resources, a set of actions that can be allowed on those resources, and a set of users that include the owners of the resources and non-owners.

The set of resources include: an **event**, an election **poll**, and a **fan page**. All of these resources are represented as digital objects, each of which contains additional more minute digital objects: for example, an **event** has a set of discussion posts, a **poll** has a set of votes, and a **fan page** has a set of "fans" users.

The set of actions are: **discuss, join, vote, like,** and **share**. Here we recognize the difference between a specific type of action versus the combination of specific action per object pair, that we label permissions. The set of permissions can be defined as: **(join, event), (discuss, event), (vote, poll), (like, fan page)**, and **(share, fan page)**.

The users in the scenario comprise: a **requesting** user, and an **owner** of the resources (i.e., fan page, poll and event).

2.2 Risk-aware Access Control and Provenance-based Risk Assessment

In a SC environment, the unique aspect, in regard to access control security, is that each owner specifies her own access control policies regarding the possessed resources. The most prevalent approach for modeling access control in online social networking platforms is to specify policies in terms of the existence of relationships among users and resources. However, in some other general SC environments, due to the absence of such relationships, access control policies are usually expressed in terms of some other attributes of users and resources. Typically, these policies are all static by nature, which always give the same outcomes if those specified relationships or attributes do not change. However, users actively perform various activities in SC systems, thus triggering the systems to change relationships or attributes dynamically over time. When policy makers design policies in advance, it is essentially hard for them to foresee the future needs of the system and predict users' future behaviors.

Risk, defined as *the possibility of future loss or damage*, is generally perceived as an ingredient with a "dynamic" flavor to make the traditional access control models more suitable in a dynamically changing environment [2, 8, 14]. In order to achieve more flexible authorization in SC environment, the adaptation of risk awareness in access control is necessary so that authorization can be determined in a timely manner in accordance with the dynamic changes in social computing environments.

Basically, in a risk-aware system, risk values are applied

to requesting users and objects to estimate the probability of granted access being misused. We allow requesting users and resource owners to specify the risk thresholds for the acceptable risk of their own actions and actions performed against their resources respectively. Risk values and risk thresholds can fluctuate over time as a result of user's activities. Users' activities on target resources can be captured in a provenance data store and queried to compute risk values of requesting users and target resources as well as to adjust the risk thresholds users set in accordance with the users' predefined threshold management policies. We further demonstrate the idea of this risk and provenance-aware access control mechanism in the next two sections.

3. RISK-AWARE ACCESS CONTROL FOR SOCIAL COMPUTING

This section discusses the idea of risk-aware access control in SC. We first identify some core components of risk-aware access control in SC, and then explain in details the initial thought of deriving risk values and thresholds from provenance data through the previous motivating example.

3.1 Risk-aware Access Control for Social Computing

Figure 1 presents a conceptual diagram for risk-aware access control in SC environment.

Requesting Users (RU) represent human beings who initiate access attempts for actions against resource objects. **Actions** (A) are abstract functions executed by requesting users against objects. **Objects** (O) represent resource data that are accessed by users. An access **Request** comprises a requesting user, an action instance and one or more objects that are to be accessed.

Each requesting user is associated with a risk value and possesses a set of (outgoing) access control **Policies** that regulate her access against objects. Access control policies attached to each object, on the other hand, define the rules that regulate those (incoming) access against the object. **Risk Value** of a user is an estimate of a requesting user's trustworthiness, denoting the likelihood of misusing permissions granted to her. **Risk Value** of an object represents the likelihood of the object being misused by users.

We define **Permission** as an action per object pair, such as *(join, event), (discuss, event), (vote, poll), (like, fan page)* and *(share, fan page)*. Unlike those security policies commonly seen in online social networks, policies here are not expressed in terms of relationships among users and resources, but rather contain a **Risk Threshold** for each permission that denotes the level of acceptable misuse tolerance. Requesting user and resource owner can then specify the policies deciding how risk value and risk threshold can be used for access decision. Since we recognize the difference between an action and a permission, separate categorization of actions and permissions leads to separate risk assessment for each category. As a result, users are granted more flexibility in policy specification.

Access Evaluation function decides a request by comparing the requesting user's risk value with the risk threshold stated in the policies of the user and the object.

Provenance Data store transactions data that are captured as a result of performed actions by users. The stored information of each transaction consists of two entities and one causality dependency. These dependencies form a directed acyclic graph and such a graph is essential to assess risk values of users and objects and risk thresholds for users actions and permissions, as shown in dotted lines with solid arrows in Figure 1. Please note that though a risk threshold is assigned to a permission, as an object can include different risk thresholds per different actions against the object, the risk threshold in the figure is attached to objects for simplicity.

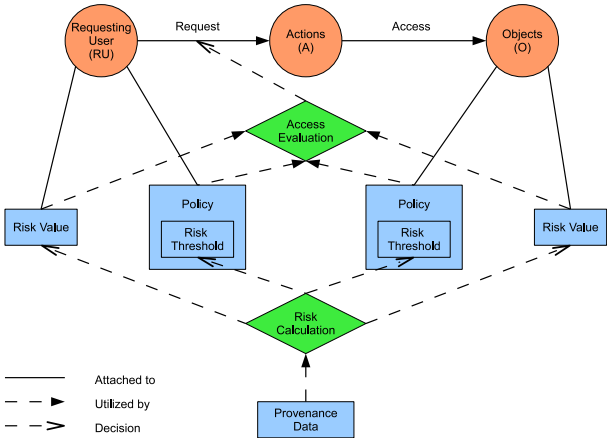

Figure 1: Provenance-based risk assessment for access control

3.2 Provenance-based Risk Assessment

The following example demonstrates how risk values and thresholds can be used for authorization and how these values can be assessed using provenance data.

Consider Alice as a user who is actively involved in the upcoming presidential election on a social network platform. Suppose Alice wants to support candidate X and would like to join an event arranged by the supporter group of X. Under the scenario setting, Alice is required to like the candidate's fan page before she can participate in the mock vote poll, which in turn is a prior requirement for joining the event.

From the page owner's point of view, Alice, the requesting user carries a risk value, which represents the level of misuse granting her access would result in. Each object also possesses a risk value, which denotes the likelihood of the object being misused by others. The risk values of a user and an object are dynamically computed based on the previous activities related to them. The owner also needs to specify a risk threshold for each of the permissions she maintained. This risk threshold represents the level of sensitivity of performing the permission. Based on the threshold, the owner can make policies specifying how the thresholds can be used for access decision. Suppose the owner specifies that the requesting user's risk value has to be lower than the risk threshold for access to be granted. In such case, if Alice has a risk value of 0.5 and the risk threshold is 0.6, then the requested action is granted. Another requestor Bob who has a risk value of 0.7 would be denied his request.

The system allows the owner to efficiently rank the risk value associated with each permission based on the sensitivity of the permission. For example, the risk threshold associated with *(like, fan page)* is considered higher than the risk threshold associated with *(join, event)* because the owner feels there is less potential of misuse for liking a fan

page than joining an event.

Furthermore, the fluctuation of these risk values can serve as basis for the flexible specification of access control policies in a dynamically changing environment. More specifically, the requesting user's risk values may increase or decrease over time as a result of her past activities and behavior in the system. For example, the number of times Alice shares the posts on a candidate's page may reduce her risk value as she has been an active user in the system. Similarly, the risk value of an object can be also changed over time depending on the interactions on the object. For instance, a page that is mainly modified by users with high risk values might consequently have its risk value elevated, since its contents could be less trustworthy. In a more complex scenario, a private discussion event may initially be considered prone to user misuse, hence it is being assigned a high risk value by the system. Its owner also sets a low threshold so that only users with lower risk value can join in. Later on, with more and more access from trustworthy users, it becomes less likely to be misused and may have its risk value descend accordingly. Due to the drop of the risk value, the risk threshold can be adjusted higher in order to allow access from a greater set of users, which may also results in changes of risk value and risk threshold in the future.

In addition, we also consider the policy that is specified by a requesting user herself. Such a policy provides a form of assurance that the requesting user does not unintentionally perform a high risk action against her own desire. In regard to the requesting user's point of view, there is a risk threshold associated with her own actions that can restrict her requests in a system. The user's risk threshold on a particular action and risk value of a target object are evaluated for access decision. In the scenario above, Alice is allowed to and may want to like and share as many fan pages as she wants. However, it is most likely the case that Alice does not want like or share a fan page which has a risk value below a certain threshold as this kind of actions may increase her own risk value. Here we recognize a potential conflict of policies between those the requesting user specify and those specified by the resource owner. We believe this issue can be resolved as of context and poses no significant concern in the discussion of this paper.

4. PROVENANCE AWARENESS IN SOCIAL COMPUTING

As demonstrated in our approach of provenance-based risk assessment, it is essential that provenance awareness is incorporated into a social computing platform.

A request is made for performing an activity in the system. Once the request is granted, a corresponding transaction is executed by the system. Such execution and the relating information is captured as provenance data and stored in a provenance store. Provenance information can then be extracted from this provenance store for the purposes such as dynamic risk assessment and access control.

For provenance to be fully utilized for these purposes, it is essential that an appropriate data model is employed to model provenance information. There are a variety of provenance models in the literature [1, 3, 13], each of which is suitable for specific purposes within the respective application domains. Regardless, the community concurs on the unique characteristic of provenance to form a directed-acyclic graph.

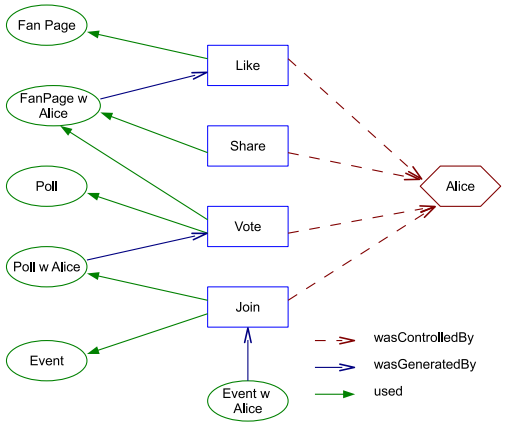

Figure 2: SC Scenario captured in OPM

We utilize the Open Provenance Model (OPM) [15] as the data model for provenance within the SC environment. The OPM model captures the information associated with a transaction and expresses the relations between them in the form of causality dependencies. Specifically, in an OPM graph, three different types of entities serve as the graph nodes and five different types of dependency edges are used to connect specific pairs of node types.

Consider the following scenario, where Alice wants to join a discussion event on a fan page. Before gaining that access, Alice is required to demonstrate her knowledge about the discussion group through actions such as to like and share the fan page, and to take part in a poll. We can capture the event of Alice's request to join an event. More specificallly, Alice's request can be formalized as:

request(Alice, join, accountOf(Alice), event)

Here, **accountOf(Alice)** and **event** are input objects. Once the request is granted, an associating transaction is executed:

(Alice, join, accountOf(Alice), event,
eventWithAccountOfAliceAdded)

Here, **eventWithAccountOfAliceAdded** is the output object as consequence of executing the transaction. The corresponding provenance information is captured in OPM-format in the provenance store as the following triples:

(join, wasControlledBy, Alice)
(join, used, event)
(join, used, accountOf(Alice))
(eventWithAccountOfAliceAdded, wasGeneratedBy, join)

These triples altogether form a DAG. Figure 2 depicts OPM representation of the full usage scenario described in Section 2. Here we only utilize three types of dependency edges. Data objects are represented in ovals, actions in rectangles, and the user in hexagon.

Note that our OPM capture of provenance information is simplified to capture only essential components. Typically, provenance information can contain additional information such as time, location, platform, etc. However, those present additional complexities that can be addressed in the future work on our approach.

We believe incorporating provenance awareness through the use of OPM for capturing and representation of provenance information provides a solid first step in our approach toward a model for provenance-based risk assessment for access control.

5. RELATED WORKS

Provenance is the full documentation of all processes that influence and lead to the current state of a data object. Major researches have been done on provenance in many different fields of computer science, including databases, workflows, and semantic webs, etc. [1, 3, 13]. Provenance awareness in those subfields provides many additional utilities and enhances the underlying computing platforms. In this paper, we aim to utilize provenance information for risk assessments in social computing environments.

As the role and importance of provenance information increase, so do the community's recognition and focus on security aspects of provenance information [4, 5, 16, 18]. Towards this end, the research community has spent efforts on securing provenance data as well as utilizing the provenance data as a mechanism for securing other data. In this paper, we utilize provenance data as a basis for risk assessment toward securing social computing platforms. The results of assessment can be utilized for access control purpose. Provenance data can also directly serve as a basis for access control mechanisms, as published in various works [16, 22].

In our proposed approach, we use the Open Provenance Model to represent captured provenance data within the system. In a similar approach, Park et al [21] uses OPM to capture the provenance of data objects within a group-centric collaboration. Within the underlying distributed systems, they also proposes methods for integrating provenance data for access control purposes [17].

Several works have been proposed for utilizing risk theme in different access control systems. Kandala et al [14] provide a model that identifies different risk components for a dynamic access control environment. They claim those components are essential elements for developing a risk-adaptive access control system. Jason Report [19] proposes three core principles for a risk-aware access control system: measuring risk, identifying tolerance levels of risk and controlling information sharing within that levels. Cheng et al [8] give a model to quantify risk for access control and provide an example of this for information sharing in multilevel system. Bijon et al [2] propose risk aware RBAC [24] session that dynamically decides privilege of a user in a session based on the involved risk in current situation. Their main idea is to set a risk-threshold for every session that limits the maximum access capability of the user on that particular session. They also categorize the session risk-threshold in three different ways, i.e., static, dynamic and adaptive, based on the time and functionality of the risk computation. They also propose a framework for different role activation-deactivation models in such risk restricted session.

There has been significant research on access control for online social networks [6, 7, 9, 10, 11, 12]. Most of these works attempt a relationship-based approach for modeling access control, since it is intuitive to take the advantage of the existing social graph topology for authorization purpose. The basic idea of such relationship-based access control mechanisms is to decide distinctly privileged user groups by tracking the existence of relationship of particular type and/or depth between the access requester and the target resource or its owner. In particular, Carminati et al [7] identified aggregated trust value to denote the level of relationship between users, and utilized trust metric along with relationship type and depth on a path between users as decisive factors for access control. [9, 10, 12] delved to improve the expressiveness and flexibility of policy specification for access control in terms of multiple relationship types and directions. However, not every social computing application has a social graph, relationship-based approach cannot be universally applied to the general SC environment. Park et al [23] proposed an activity-centric access control framework that is independent of social graphs and deals with fundamental aspects of access control in SC. The major difference between this paper and these works is that, by incorporating risk awareness, access control decision does not statically rely on the pre-defined policies, but becomes adaptive to the dynamic changes in the system.

6. CONCLUSION

In this work, we identified the necessity of incorporating risk awareness, and hence provenance awareness, for access control in social computing. We showed the core components of risk-aware access control in SC, and demonstrated the idea of assessing risk values and risk thresholds, based on provenance data, for access control decisions. We used the Open Provenance Model as the data model for provenance information, and elaborated our provenance-based risk assessment approach through a social network example scenario. In the future, we plan to develop this initial idea into a more concrete risk-aware provenance-based access control model for social computing.

Acknowledgments

This work was partially supported by grants the US National Science Foundation CNS 1111925 and AFOSR MURI.

7. REFERENCES

[1] O. Benjelloun, A. Das Sarma, A. Halevy, M. Theobald, and J. Widom. Databases with uncertainty and lineage. *The VLDB Journal*, 17(2):243–264, Mar. 2008.

[2] K. Bijon, R. Krishnan, and R. Sandhu. Risk-Aware RBAC Sessions. In *8th International Conference on Information Systems Security*, dec. 2012.

[3] P. Buneman, A. Chapman, and J. Cheney. Provenance management in curated databases. In *Proceedings of the international conference on Management of data*, SIGMOD, pages 539–550. ACM, 2006.

[4] T. Cadenhead, V. Khadilkar, M. Kantarcioglu, and B. Thuraisingham. A language for provenance access control. In *Proceedings of the first ACM conference on Data and application security and privacy*, pages 133–144. ACM, 2011.

[5] T. Cadenhead, V. Khadilkar, M. Kantarcioglu, and B. Thuraisingham. Transforming provenance using redaction. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, pages 93–102. ACM, 2011.

[6] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic

web based framework for social network access control. In *Proceedings of the 14th ACM symposium on Access control models and technologies*, SACMAT '09, pages 177–186. ACM, 2009.

[7] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. *ACM Trans. Inf. Syst. Secur.*, 13(1):1–38, 2009.

[8] P.-C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Security and Privacy, 2007.*, pages 222 –230, may 2007.

[9] Y. Cheng, J. Park, and R. Sandhu. Relationship-based access control for online social networks: Beyond user-to-user relationships. In *Proceddings of the 4th IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*, 2012.

[10] Y. Cheng, J. Park, and R. Sandhu. A user-to-user relationship-based access control model for online social networks. In *Proceedings of the 26th IFIP Annual WG 11.3 Conference on Data and Application Security and Privacy (DBSec '12)*, 2012.

[11] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for Facebook-style social network systems. In *Proceedings of 14th European Symposium on Research in Computer Security (ESORICS)*, page 303. Springer, 2009.

[12] P. W. Fong. Relationship-based access control: protection model and policy language. In *Proceedings of the first ACM conference on Data and application security and privacy*, CODASPY '11, pages 191–202. ACM, 2011.

[13] T. Heinis and G. Alonso. Efficient lineage tracking for scientific workflows. In *Proceedings of the ACM international conference on Management of data*, SIGMOD '08, pages 1007–1018. ACM, 2008.

[14] S. Kandala, R. Sandhu, and V. Bhamidipati. An attribute based framework for risk-adaptive access control models. In *Proceedings 6th International Conference on Availability, Reliability and Security (ARES)*, pages 236 –241, aug. 2011.

[15] L. Moreau, B. Clifford, J. Freire, J. Futrelle, Y. Gil, P. Groth, N. Kwasnikowska, S. Miles, P. Missier, J. Myers, B. Plale, Y. Simmhan, E. Stephan, and J. V. den Bussche. The open provenance model core specification (v1.1). *Future Generation Computer Systems*, 27(6):743 – 756, 2011.

[16] D. Nguyen, J. Park, and R. Sandhu. Dependency path patterns as the foundation of access control in provenance-aware systems. In *4th USENIX Workshop on the Theory and Practice of Provenance*, TaPP'12. USENIX Association, Jun. 2012.

[17] D. Nguyen, J. Park, and R. Sandhu. Integrated data provenance for access control in group-centric collaboration. In *13th IEEE Conference on Information Reuse and Integration*. IEEE, Aug. 2012.

[18] Q. Ni, S. Xu, E. Bertino, R. Sandhu, and W. Han. An access control language for a general provenance model. In *Proceedings of the 6th VLDB Workshop on Secure Data Management*, SDM '09, pages 68–88. Springer-Verlag, 2009.

[19] M. C. J. P. Office. Horizontal integration: Broader access models for realizing information dominance. In *MITRE Corporation, Tech. Rep. JSR- 04-132*, 2004.

[20] M. Parameswaran and A. B. Whinston. Research issues in social computing. *Journal of the Association for Information Systems*, 8(6):336–350, 2007.

[21] J. Park, D. Nguyen, and R. Sandhu. On data provenance in group-centric secure collaboration. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 7th International Conference on*, pages 221 –230, oct. 2011.

[22] J. Park, D. Nguyen, and R. Sandhu. A provenance-based access control model. In *10th Annual Conference on Privacy, Security and Trust*, PST 2012. IEEE, Jul. 2012.

[23] J. Park, R. Sandhu, and Y. Cheng. Acon: Activity-centric access control for social computing. In *Proceedings 6th International Conference on Availability, Reliability and Security (ARES)*, 2011.

[24] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *Computer*, 29(2):38 –47, feb 1996.