Access Control Taxonomy for Social Networks

Adnan Ahmad, Brian Whitworth
Institute of Information and Mathematical Sciences
Massey University
Auckland, New Zealand
[A.Ahmad, B.Whitworth]@massey.ac.nz

***Abstract*—Social networks are online platforms where users form relationships with others by sharing resources. Access control for these social networks is different from other systems as it fulfills the social requirements of community as well as the technical requirements of the system. This paper presents a classification of access control models for social networks based on lattice taxonomy where axes represent the properties of the models. The proposed taxonomy has eight axes representing: requestor identity, mapping authority, resource control, relationship management, credential distribution, access control decisions, rights delegation and transparency. Analysis of existing models using this taxonomy highlights the tradeoffs between user control, state distribution and social needs. The taxonomy reveals that various interesting features of social networks have not been implemented yet and there is a gap between the social requirements and access control features of social networks.**

Keywords-Access Control; Social networks; Taxonomy;

I. INTRODUCTION

Social networks are systems built around the social requirements of community. This special type of software provides online platform where users establish relationships with each other and share resources. Access to these resources is managed by an access control system that decides which users should be allowed to perform certain action. There are few access control models for social networks which address the social and technical requirements in different ways leading to a trade-off between user control, performance, social needs and state distribution. The goal of this paper is to contribute to the understanding of these tradeoffs.

Access control systems are commonly classified by policy design, such as user-based, role-based or mandatory access control, or by an implementation mechanism such as access control lists or capabilities [2]. These classifications do not differentiate between centralized and distributed state, user and system control, and do not offer insight on the properties of social networks. This paper presents a classification and analysis based on identification of properties of access control system for social networks and constructing lattice taxonomy, similar to [2]. Each axis on the lattice represents a property and the points on the axis are current possible values of the property. The systems analyzed are: Rule-based access control [3], Trust based approach [4], Role based access control [5], Fong-Anwar-Zhao [6], Distributed access control [7] and Tie-RBAC [8].

The lattice classifies access control models by assigning a value on each of the axes. The current taxonomy has eight axes representing: requestor identity, mapping authority, resource control, relationship management, credential distribution, access control decisions, rights delegation and transparency. Each of these properties impacts the social requirements of community to use a social network. The current set of axes is useful for the analysis of current designs, and provides suggestions for new access control models for social having other interesting properties, which have not yet been implemented.

The rest of the paper is organized as follows. Section II discusses other classification efforts for different types of systems, section III presents the classification axes along with the various design options, section IV classifies existing models on the lattice, while section V evaluates the results.

II. RELATED WORK

Some recent criteria have been developed to classify access control models other than policy design and implementation mechanisms. Among them, simulatability is used to compare the expressiveness of access control models [9], to show relative relationship between them. Another approach [10] formulates a logical framework for comparing the access control expressiveness for database management system, where the classification of various models is done in terms of structural equivalence, state reachability and consistency. In [2], the authors argued that the implementation of access control for distributed systems does not faithfully conform to the access control scheme. Their comparison addresses the fidelity of implementations of various access control models for distributed systems

However, the comparisons of expressiveness do not address centralized and distributed implementations or user and system control. Also, as social networks are built around the social requirements of the community, comparing social and technical features of access control models and analyzing whether they are fulfilling those requirements is both interesting and challenging.

III. CLASSIFICATION AXES

This research now presents the lattice with identified axes for access control models for social networks. The axes are identified by formulating access control as a workflow, and then extracting properties for each step. The workflow formulation has the steps: (1) identity resolution, (2)

resource control, (3) relationships management, and (4) credential distribution. Other social requirements of online communities like delegation and transparency are also taken into account.

A. Requestor Identity

Requestor identity addresses how friends are identified in social networks and can be compared with other mechanisms like access control list and capabilities. This axis supports the formation of privacy policy and the traversal of relationship graphs. It has the following points in increasing order of availability.

1) Listing

Resource owner explicitly adds other members of the social network to allow access to his resources. It is the most common type of requestor identity currently present in social networks.

2) Certificate

An identity certificate attests the relation of the requestor with the resource owner. The certificate can be centralized, where it adds the testimony of authority, or decentralized where the owner maintains the proof of non-forgery.

3) Trust

Some approaches use trust between resource owner and the requestor to grant access to users in social networks. The owner specifies the trust level that should be present in order to gain access to his resource.

B. Mapping Authority

In social networks, users are mapped in relationship with the resource owner before they can access resources. Mapping authority differentiates who decides this mapping. The axis has the following points in decreasing order of owner control over his relationship mappings.

1) Owner

The requestor mapping is under the control of the resource owner, who either defines the list of users who can access his resource or provides them certificates.

2) System

Resource owner and system both define their own set of rules where mapping is done only if requestor follows both sets. The owner has limited control as he only decides who cannot be mapped but in order to ensure the mapping, the requestor needs to follow the system rules as well.

3) Community

The community defines some rules and the owner only changes the variables. The owner does not mention who can be mapped rather the decision is done by the community.

C. Resource Control

Control over resources ensures that users can contribute their personal stuff on social networks without the concern about its unauthorized disclosure. This axis defines who decides the access rules for resources in order to take the access decision. The identified points on this axis, ordered by decreasing amount of owner control are:

1) Full Control

Owners can decide precisely who can access their resources. It is the most dynamic type of resource control where each individual can be dealt with different types of access control policies.

2) Partial Control

Resource owner defines the rules but their enforcement is done by the system. This type provides some flexibility to owner but the policy needs to be the same for every requestor.

3) No Control

Resource owner does not take part in policy generation rather system has same predefined rules for every user. Any requestor fulfilling those rules can have access to resources.

D. Relationship Management

Relationship management measures how precisely a model allows its users to specify their relationships. It provides universal relationships, same policy circles and fine grained circles. The axis has the following points in decreasing order of available user control.

1) Fine Grained Levels

Fine grained levels of relationship provide the flexibility to the resource owner to distinguish among friends, family and colleagues, and manage access more precisely. It also offers the flexible access as one can give access to any arbitrary user other than his social circle.

2) Social Circle

Social circle allows the resource owners to create authorization circle of their friends to manage potential requestors. It is coarse in nature as it makes no difference within the social circle and treats all friends with the same policy.

3) Shared Secret

In some systems, shared secret is distributed among the friends and they later use it as a proof of relationship with the owner. The distribution does not generate authorization circles and provides flexibility to the owner to manage access of different users over different resources.

E. Credentials Distribution

An access control credential is a record used in access control decisions. This axis shows how much information about access control credentials is held by users and system. The following points are explored on this axis, listed in decreasing amount of authorization state stored at user.

1) Decentralized

All the access control credentials are store on the user side and the access decision requires the cooperation of the resource owner. This type of distribution requires no central repository and does not expose single point of failure.

2) Equal Sharing

The system and the user each maintain part of the access control related state, which may be different as it can be more system-oriented or user-oriented.

3) Centralized

The system maintains complete set of access control credentials related to every user. These credentials are stored at a centralized repository and every request needs to access them on the server.

F. Access Control Decisions

The scalability of access control decisions affects by who takes decisions about allowing access over resources. The credential distribution affects the nature of access control decision as well. The various points on this axis, in decreasing distributed order are:

1) Local

In this type, the access control decisions are made locally at the client side without the interaction of the server. For an access decision to be local, the access control credentials must also be stored locally. Local implementations are fastest and most scalable among others on this axis.

2) Partial

The access decision is made by the client (or server), but it collects information from the other component to take the well informed decision.

3) Server based

Access control decisions are taken by the server as it has the best possible knowledge of the access control credentials.

G. Delegation

The holder of an access control credential may able to share that credential with other users [12, 13]. In social networks, delegations are mostly recorded and can be revocable based on the violation of the stated rules. The identified points on delegation axis, ordered by decreasing amount of community control are:

1) User Control

The user can delegate credentials at will to any other user and the passed credential can works as the actual one, which may or may not be further delegated depending on the owner's policy.

2) N-Model Delegation

The access control credentials are delegated to the users, who can further delegate it to others. The delegation can be further passed on till it reaches N levels.

3) System Control

Credentials are not delegate-able by users at all. The requestor receives the credential from owner or system on one to one correspondence between credentials and requestor.

H. Transparency

Transparency refers to the amount of information available to the user [14, 15] about the access control state. It not only includes the conditions under which the requestor is not allowed to access resources but also to provide them guidance on what they can do. The points on this axis, in decreasing order of transparency are:

1) Public

Owners know the state of the system related to them and when should a particular request be allowed or denied. The requestor also knows the complete state of the request, and the outcome with possible errors and reasons.

2) Partial

In partial transparency, only owner (or requestor) knows the rules and state of the system but not both.

3) System Oriented

In system oriented transparency, no one is aware of the access control state. The owner only knows about his rules and requestor only aware of the outcome of access decision.

The various axes of access control lattice for social networks are shown in Fig. 1.

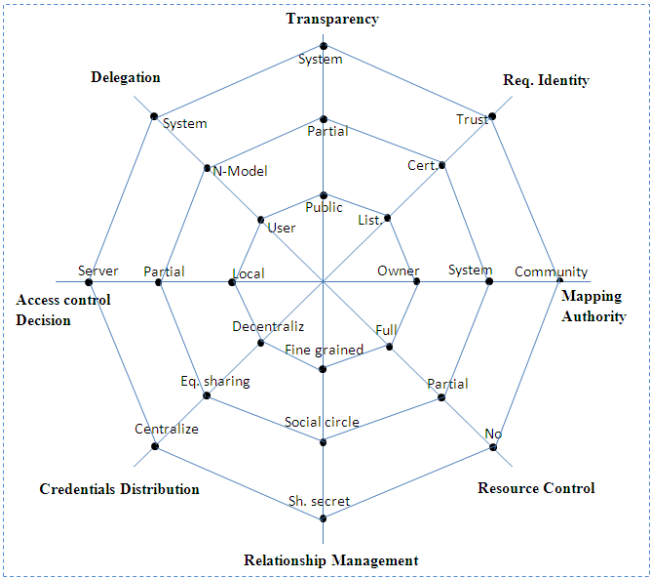

Figure 1. Various axes of access control lattice for social networks

IV. EXAMPLE SYSTEM

The following access control models for social networks are explored for this research.

A. Rule based Access control

A semi-decentralized access control model for sharing information on social networks is presented in [3]. The model allows the owner to specify the access rules and authorized users in terms of relationship type, depth, and trust level existing between the two users. When a requestor requests some resource, he receives a set of *rules* regulating the release of the requested resource. He then has to acquire the *proof from a central node* showing that he has a relationship with the owner having required depth and trust level.

- Requestor Identity: *(Certificates)* Requestor identity is managed through certificates, which states the relationship type, depth and trust between the two users.
- Mapping Authority: *(Owner)* Owner creates the certificates for identified users stating their relationship.

- Resource Control: *(Full control)* Owner defines the authorized users by means of type, depth and trust level of relationship.
- Relationship Management: *(Social circle)* Owner defines his social circle by creating relationship certificates for other members.
- Credential Distribution: *(Centralized)* A trusted central node is in charge of managing certificates and of computing the trust level of relationships.
- Access Control Decisions: *(Local)* Access control decisions are enforced locally at the client side.
- Delegation: *(System control)* An access right cannot be further delegated. Access rights are only granted to users who have direct relationship with the owner.
- Transparency: *(System oriented)* Resource owner and the requestor don't know the state of system.

B. *Trust based approach*

A multi-level security approach is adopted in [4], where trust is the only parameter used to determine the security level of both users and resources. Each user is assigned a reputation value by other users in the system. Every resource is assigned a confidence level equal to the trust level of the owner, and only users with equal or higher trust level can access it. For each resource, the owner generates a secret key *K*, which can be split into *n* portions and then reconstructed only by using *x* portions of it [11]. The *n* portions of *K* are distributed among trustworthy nodes. When a requestor tries to access some resource, he needs to retrieve the *x* portions of *K* from the set of *n* nodes and then decrypts the challenge for that resource. These portions are only released if the requestor trust level satisfies the resource confidence level.

- Requestor Identity: *(Trust)* Trust is used to determine the security clearance of the requestor, and is assigned by other users in the system.
- Mapping Authority: *(Community)* The requestor needs to acquire the desired trust level in order to reconstruct the key, and the trust is assigned by other community members.
- Resource Control: *(No control)* The trust level on which the access decision is made is not under the control of the owner but of the whole community.
- Relationship Management: *(Shared secret)* The key is distributed among the users, from where it can be collected by any user after fulfilling the requirements.
- Credential Distribution: *(Equal sharing)* The credentials are in the form of a key which is distributed among trusted nodes.
- Access Control Decisions: *(Server based)* The system is in charge of granting access once the key is collected and the requestor provides his proof.
- Delegation: *(System control)* Access rights cannot be further delegated. Any other user accessing the same resource needs to re-collect the encryption key.
- Transparency: *(System oriented)* No one knows exactly which particular user can access the resource.

C. *RBAC in social networks*

In [5], Li et al. extend the RBAC model for social networks. In their proposal, the resource owner defines his own set of roles and access rights over resources related to those roles. When a requestor requests some resource, the owner checks the requestor's role from his role set and grants the access if the requester exist in some role and the role is assigned the access permission of the requested resource. The access control module follows the client and server approach, where server is in charge of role relation management, and client is in charge of resource and permission management.

- Requestor Identity: *(Listing)* Requestors are assigned some role before granting them access overs resources.
- Mapping Authority: *(Owner)* Owner defines his role set and these roles are assigned to requestors.
- Resource Control: *(Full Control)* Owner defines which role can access which type of resources.
- Relationship Management: *(Social circle)* Owner adds other users in his social circle by assigning them roles.
- Credential Distribution: (*Centralized)* The access control policies and credentials are stored on the server.
- Access Control Decisions: *(Server based)* A centralized server is used to take the access control decisions.
- Delegation: *(System control)* Role member cannot further delegate his membership. The resources are accessed on the basis of role assignment.
- Transparency: *(Partial)* Resource owner knows which user can access which object, but requestors don't know any access control state.

D. *Fong-Anwar-Zhao*

An algebraic model of access control is presented in [6], where authorization is based on two factors: communication history - the set of events that happen between each user, and acquaintance topology - the set of relationships between users. Every owner is responsible to manage his privacy policy and whether other users have access to his objects depends on their relationship with him. The communication state between a pair of users is local, but occasionally needs to consume global information.

- Requestor Identity: *(Listing)* Requestors are added in relationship with the owner before access can be granted.
- Mapping Authority: *(Owner)* The relationship with other users is declared and managed by owner.
- Resource Control: *(Full control)* Owner manages his privacy policy and mentions the authorized users to access his resources.
- Relationship Management: *(Social circle)* Every owner defines his relations with other members of the social network.

- Credential Distribution: *(Equal Sharing)* Most of the access control information resides at the user side but some information is maintained globally as well.
- Access Control Decisions: *(Local)* The access control decision is made locally most of the times.
- Delegation: *(System control)* The relationship is managed by the owner and cannot be delegated by users.
- Transparency: *(Partial)* Only resource owner knows which user has access to his resources.

E. Distributed Access Control

A distributed access control model for social networks is presented in [7]. The model divides the object space into sub-domains termed as namespaces and users requesting access are considered as virtual users. The system uses distributed certificates to differentiate among friends, family and colleagues. Objects are also categorized in privacy classes and a security clearance is associated with every object class. Virtual users cannot assess objects directly but an abstraction of local roles and object classes is provided.

- Requestor Identity: *(Certificates)* Distributed certificates are used to differentiate virtual users and their mapping in namespace.
- Mapping Authority: *(Owner)* Owner manages the mapping between domain based local role and the virtual user within his namespace.
- Resource Control: *(Full control)* Owner manages the certificates used for object clearance as well as local role membership. The certificate mapping decides which local role has access to which object class.
- Relationship Management: *(Fine grained)* A fine grained relationship model is used to differentiate friends, family and colleague.
- Credential Distribution: *(Decentralized)* The complete state required for any access control decision is stored at the owner side.
- Access Control Decisions: *(Local)* The access control decisions are taken and enforced locally at the client side.
- Delegation: *(System control)* Certificates are not given to the virtual users but stored at the owner side, so it cannot be delegated. Access rights are only granted to virtual users who has direct mapping to local roles.
- Transparency: *(Partial)* Only the resource owner knows what domain based role has access to which object class.

F. Tie-RBAC

Based on RBAC advantages, Tie-RBAC [8] was proposed to support users in online communities. It allows actors in the social network to define their own relations and provides a powerful method for actors to concede access rights to their contacts at the same time as they establish relationships. A centralized server stores access control policies and is responsible for enforcing them.

- Requestor Identity: *(Listing)* A relationship is established between the actor and his contacts in order to grant access.
- Mapping Authority: *(Owner)* Actor has the ability to define his own relations and decides in advance which requestor has access to his resources.
- Resource Control: *(Full control)* Owner concedes the access rights to their contacts on adding them.
- Relationship Management: *(Social circle)* Actor defines his social circle by adding contacts.
- Credential Distribution: *(Centralized)* The server stores all the access control policies of all the users.
- Access Control Decisions: *(Centralized)* The server is responsible for enforcing access control decision.
- Delegation: *(System control)* A contact cannot delegate his relationship with the resource owner.
- Transparency: *(Partial)* The resource owner knows which contact has access to which object.

V. EVALUATION

The taxonomy provides interesting patterns relating access control in social networks. It highlights some problems with the current access control models and provides various new directions for future access controls. It also stresses the fact that access control in social networks still lacks social requirements of online communities. Following are the most noticeable elements:

- Not many access control models incorporate the social requirements of communities. Rights delegation can be seen as a major example of it, which is the core in any rights managements system but hardly any model provides it. Also, transparency is one of the features that is mostly required by the community to flourish but currently completely or partially ignored by all models. Other social requirements of social networks like rights transfer and sharing is hardly done by any access control model.
- Likewise, scalability is one of the major concerns in social networks. It is interesting to note that currently some access control models claim that centralized approach for credentials distribution is best while others argues for distributed. A comparison of these implementations with respect to scalability and efficiency can be a valuable contribution.
- The taxonomy exhibits the similarities and differences among the design of various access control models, and gives a formal mean to compare different implementations. The standing of explored models over various axes of the current lattice is given in Fig. 2, where B is the most community-oriented access control model for social networks whereas E is the most owner-oriented. C, D and F are similar over owner control axes but different in access control decisions and social needs. The lattice can be used for the comparison of other current and future access control models as well.

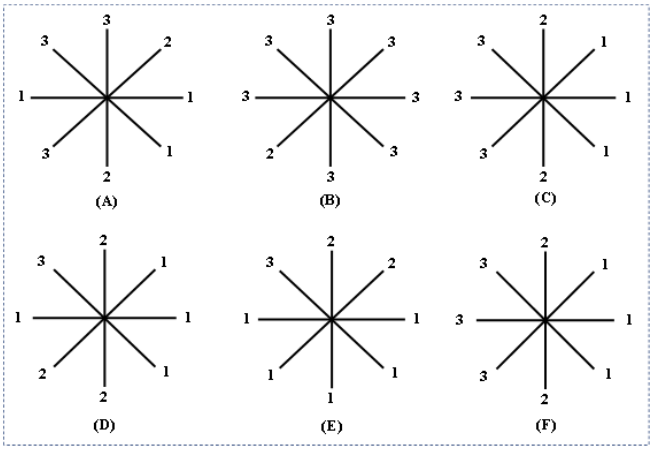

Figure 2. Lattice standing for various models

- We have not seen many implementations taking the advantage of distributed nature of social networks for access decisions. Lattice reveals that only one model supports pure user side access decisions and storage which can be used against denial of service attacks.
- It is common to expect that access control in social networks can only be owner-oriented as resources are mostly contributed by users. However, the taxonomy shows that there are other possibilities as well and these controls can reside with system or community.
- The gaps on the taxonomy provide the possible future research directions as currently all models lie between owner-oriented and community-oriented space, with no model completely on one side. Models with all community or owner oriented features can be of great interest and answer various current questions.

VI. CONCLUSION AND FUTURE WORK

This paper has presented a lattice classification of access control models for social networks depending on various properties. It is observed that these models are not completely confronted to the social requirements of online communities. This study then becomes a basis towards the identification of a perfect access control model for social networks, based on the social requirements of online communities.

The presented lattice may incorporate additional axes on further exploration of properties or other points on every axis. However, the current taxonomy gives sufficient insight about the behavior of current access control models for social networks, presents a test bed to check their similarity and differences, raises critical questions and provides some future directions where one can see the vacant spaces on the lattice.

Future work would be the modeling of a pure owner-oriented access control model for social networks including delegation framework and public transparency, and its integration in a NSF granted open knowledge exchange system project [16].

ACKNOWLEDGEMENT

This work has been sponsored by National Science Foundation (NSF), USA, under award number 0968445. “OKES: An open knowledge exchange system to promote meta-disciplinary collaboration based on socio-technical principles”.

REFERENCES

[1] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. M. Thuraisingham, “A semantic web based framework for social network access control,” pp. 177-186 SACMAT 2009.

[2] Kane, K., and Browne, J. C., “On classifying access control implementations for distributed systems”, SACMAT'2006.

[3] Carminati, B., Ferrari, E., and Perego, A. ,”Rule-based access control for social networks”. In On the Move to Meaningful Internet Systems 2006: OTM Workshops 2006.

[4] Ali, B., Villegas, W., and Maheswaran, M. ,”A trust based approach for protecting user data in social networks”. In 2007 Conference of the Center for Advanced Studies on Collaborative research (CASCON’07), pages 288–293, 2007.

[5] Li, J., Tang, Y., Mao, C., Lai, H and Zhu, J., "Role Based Access Control for social network sites", In Joint Conferences on Pervasive Computing (JCPC), 2009.

[6] Fong, P. W. L., Anwar, M., and Zhao, Z., "A Privacy Preservation Model for Facebook-Style Social Network Systems". In Proceedings of the 14th European Symposium on Research In Computer Security (ESORICS'09), volume 5789 of Lecture Notes in Computer Science, pages 303-320, Saint Malo, France, September 21-23, 2009.

[7] Ahmad, A. and Whitworth, B., "Distributed access control for social newtorks", submitted in 7th international conference on information assurance and security, Malaysia, 2011.

[8] Tapiador, A., Carrera, D. and Salvachúa, J., "Tie-RBAC: an application of RBAC to Social Networks". Web 2.0 Security and Privacy , Oakland, California, 2011.

[9] Tripunitara, M. V. and Li, N., “Comparing the expressive power of access control models”. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Oct 2004.

[10] Bertino, E., Catania, B., Ferrari, E. and Perlasca, P., "A logical framework for reasoning about access control models". ACM Transactions on Information and System Security, 6(1):71–127, Feb 2003.

[11] Shamir, A. “How to share a secret”. Commun. ACM 22, 11 Nov. 1979.

[12] Ben-Ghorbel, M., Cuppens, F., Cuppens-Boulahia, N., Bouhoula, A., “Managing Delegation in Access Control Models”. In 15th International Conference on Advanced Computing and Communications 2007.

[13] Mabuchi, M., Shinjo, Y., Sato, A. and Kato, K., “An Access Control Model for webservices that supports delegation and creation of Authority”, 7th International Conference on Networking, IEEE CS, 2008.

[14] Oliver, R., “What is transparency?”, New York: Mc-Graw Hill, 2004.

[15] Johnson, V., “Living within glass houses: Coping with organizational transparency”. In Social, ethical, and political implications of information technology 2004.

[16] National Science Foundation (NSF), award number 0968445. “OKES: An open knowledge exchange system to promote meta-disciplinary collaboration based on socio-technical principles”, 2010-2011.