A Position Paper: A Usage Control (UCON) Model for Social Networks Privacy

Jaehong Park
Institute for Cyber Security
University of Texas at San Antonio
jae.park@utsa.edu

Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
ravi.sandhu@utsa.edu

I. Usage Control

Since the introduction of multi-user systems in the late 1960s, access control researchers have strived to better understand security and privacy issues and invent better techniques to achieve them in computing systems. Among the noteworthy results during the last 40 years of access control history are mandatory access control, discretionary access control, and role based access control policies and models. These policies and models have been influential for a sustained period of time and continue to be widely practiced. However, the variety and complexity of modern computing environments and applications is beyond the limits of these models.

In late 1990's and early 2000's, digital rights management (DRM) emerged as a hot topic and was predicted to be one of the top ten technologies that would change the future [2]. Although some businesses that are based on DRM technologies have been quite successful, the technology itself has caused tremendous concerns and outcry from the experts and the general public due to its security and privacy issues, showcased by several instances such as SONY's DVD rootkit.

In mid 1990's, the term "use control" emerged in the literature to recognize the earlier DRM technologies. In early 2000's, we coined a notion of Usage Control (UCON) and developed a family of model called the $UCON_{ABC}$ to encompass traditional access control, trust management and digital rights management and to go beyond them in its scope [4], [7], [5]. Usage control and $UCON_{ABC}$ model has been well recognized in access control community due to its several extensions that are not found in traditional access controls [1]. More specifically, as shown in Figure 1, $UCON_{ABC}$ model extended traditional access controls by including three decision factors of *Authorizations*, *oBligations*, and *Conditions*, hence called ABC. In addition it introduced two decision properties of *continuity* and *mutability* as shown in Figure 2. These three decision factors and two decision properties are well recognized and further studied in later literature[3], [6], [8].

Although the Usage Control model was initially inspired by digital rights management, it is a general purpose, policy neutral model that can support various systems of the past and even the future. We think usage control is applicable to today's social network (SN) systems though it needs further discussion and clarification to properly capture several essential and unique characteristics of social networking environments. This position paper attempts to identify some of the necessary extensions of the usage control model to support privacy in social networking systems.

II. Privacy in Social Networks

Supporting user privacy in social networking system needs more than typical access controls which are designed mainly for security purpose. Unlike traditional security systems where a system maintains a policy that applies to all users, to support privacy, a social networking system additionally requires individual policy for each user. While the system-maintained policy is likely to include what users can do

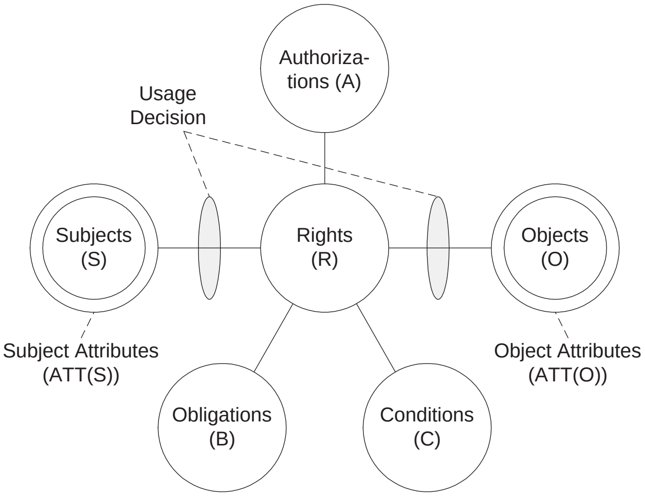

Fig. 1. $UCON_{ABC}$ Model Components

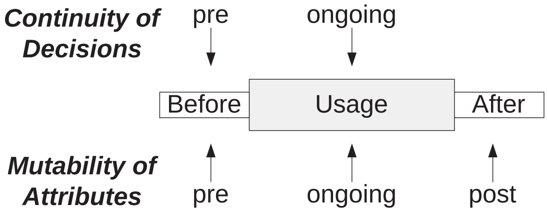

Fig. 2. Continuity and Mutability Properties

with their privacy policies, the individual user privacy policies are likely to include various user configured rules to specify user preferences with respect to their privacy.

More specifically, the following list shows some privacy control examples that SN users may desire to protect user (own or others) privacy[1]. Please note that we do not intend to present a complete list of examples or types that have to considered for privacy in social networks Rather we identify some of the most unique examples that need to be considered to support privacy in social networks.

- A user may want a privacy control so that her or other users' (e.g., her children) private information is accessible only by a certain selected user group(s) such as her direct friends.
- A user may want a privacy control so she or other users don't have to access certain information (such as violent contents) no matter what she or other users ask for.
- A user may want a privacy control so she or other users don't have to receive certain service or information. For example, a user may want to block SN notification of her friends' (or friends of her son's) social activities.
- A user may want a privacy control so SN system does not notify her social activity to her friends. [2]
- A user may want a privacy control so she or other users don't have to or cannot provide certain information to SN or SN users. For example, a user may not want to provide her location information from a mobile device, or a user may configure a privacy policy so her son cannot provide his photos

[1] In addition to the listed examples, a user may also want a control not to perform certain activities in certain circumstance. For example, a user does not want to modify her profile information from a mobile device. We think this is more of a security issue rather than a privacy issue and hence is not included in the list.

[2] This example is similar to the first example on the list, though this example controls a SN service (SN resource) that includes a user's private information rather than controlling a user information (user resource).

or other private information to social networks.

These controls need a user's capability to control users' activities, SN's activities and 3rd party application provider's activities. In social networks, this capability is provided by a SN system. In other words, to provide this capability to users, a SN system need to configure a policy that controls users' policy management. Therefore, a user's control capability is bounded by this policy. In case of P2P based social networks where there is no central authority to define this policy, what a user can do to protect their privacy is likely to be bounded by the capability provided by the distributed system protocol. Also to support privacy controls listed above, a SN system needs to provide a control capability not just for usage on resource but also for user activity. With a policy that controls resource, a user can configure rules that applies to a specific resource while with a policy that controls activity, a user can control own or other users activities. Specifically, controlling a user activity can be either incoming filtering or outgoing filtering. In the above list, the second and third items are incoming filtering while the fifth item is outgoing filtering. The first and fourth items are viewed as a controlling usage on user or SN resources rather than controlling user activity. We think these policy related issues are some of essential features that should be captured in usage control model to support privacy in the model.

III. UCON Model Extensions

In our UCON model, we assumed that policy was given to system. In a typical traditional system, an authority such as security officer or administrator provides a policy that is applied to all users in the system. However todays' SN systems require a policy for each individual user and resource together with SN provided policy. In SN systems, it is the individual users who define policies for certain users, user resources and even some SN resources while a SN system provides a policy to define what kind of policy management can be done by the users.[3] At the same time, unlike traditional computing system, individual users are likely to hold a policy set that is tailored and applicable to only a specific user. This is largely because of the fact that privacy and access control in social networks are personal matters rather than system wide matters. However, it is different from user preference since it can be influenced by other users such as a parent or guardian. Therefore, usage control is in need to be expended to include the individual policy related aspects in the model especially to support user privacy in SN. In fact, individual policies for each user's activity (activity policy) and for the use of each resource (resource policy) are similar to subject and object attributes in the current UCON model in a sense that they are dedicated to a specific user or resource.

In usage control, attributes are either immutable or mutable. Immutable attribute can be modified only by administrative actions (by security officer or users) while mutable attributes are modified as a side effect of user activity. As discussed, to expand the UCON model for social networking systems, we should include individual policy as part of the model. Similar to mutability of subject and object attribute, policy can be also immutable or mutable. Individual policies in SN are mostly immutable since they are created and modified through administrative actions by users. It can be mutable if the policy is generated through a learning process of user's preference. For example, a SN system can learn a user's privacy preference by asking and monitoring what kind of private information the user want to allow to others or what kind of information or service the user want to get. This mutability of policy needs to be further explored for better understanding of user privacy in social networks.

In addition to mutability, UCON also recognized continuity of decision. This means usage decision can be enforced throughout the period of a usage and the usage can be terminated in case the usage is no longer valid. This continuity of decision is likely to be applied to and equally effective for privacy protection in SN. At the same time, in UCON, usage decision is made through authorization (by utilizing

[3] Note that administering what a user can configure in these individual policies is likely to be done by SN through configuring a SN policy and can be viewed as a administrative model issue which is typically discussed in a separate model hence not considered here.

subject and object attributes and requested rights), obligation (by checking whether a user performed certain requested activities) and condition (by checking system or environmental status). We think all three decision factors can be utilized in social networking system for privacy protection without much extension though it may need further discussion to show how these decision factors can be applied in social networking system environments. In this position paper, we briefly discussed what are the unique aspects of user privacy in social networks from the access control point of view and how usage control models can be extended to incorporate these aspects. We believe further studies toward this direction will benefit the security and privacy research community for better understanding on user privacy issues in social networks.

References

[1] Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori., Usage control in computer security: A survey, Computer Science Review Volume 4, Issue 2, May 2010, Pages 81-99

[2] Ten emerging technologies that will change the world., MIT Technology Review., (Jan/Feb). 2001

[3] Alexander Pretschner , Manuel Hilty , David Basin, Distributed usage control, Communications of the ACM, v.49 n.9, September 2006

[4] Jaehong Park and Ravi Sandhu., Towards usage control models: beyond traditional access control. In Proceedings of the seventh ACM symposium on Access control models and technologies, pages 5764. ACM Press. 2002

[5] Jaehong Park and Ravi Sandhu., The $UCON_{ABC}$ usage control model. ACM Transactions on Information and Systems Security, 7(1):128174. 2004

[6] Jaehong Park , Xinwen Zhang , and Ravi Sandhu., Attribute Mutability in Usage Control, In Proceedings of the Proceedings of 18th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2004

[7] Ravi Sandhu and Jaehong Park. Usage control: A vision for next generation access control. In Proceedings of The 2nd International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, pages 1731. 2003

[8] Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu, and Jaehong Park, Formal Model and Policy Specification of Usage Control, ACM Transactions on Information and System Security (TISSEC), 8(4): 351-387, 2005