ISSN: 2320-1363

A Novel method for controlling Access on Users data on OSN using Finite State machine

DUDIKI.SIRISHA*1, K.SRIDHAR*2, R.Pitchaiah*3

1*M.Tech Scholar, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist: Guntur, AP, India,

2*Assistant Professor, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist:Guntur, AP, India,

3*Associate Professor & HOD, Dept of CSE, Universal College of Engineering & Technology, Perecherla, Dist: Guntur, AP, India

Abstract:

Online Social network is one of the tremendous applications which provide a platform to internet users to share their ideas and information like text or image etc. As the Online social networks contain user's personnel data and publically shared information many attackers or malicious users try to hack the information. Online Social network is inefficient to provide the good privacy policies to provide security to the user's data. In this paper, we present an access control framework to manage third party applications. Our framework is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. We model applications as finite state machines, and use the required user profile attributes as conditions governing the application execution. We formulate the minimal attribute generalization problem and we propose a solution that maps the problem to the shortest path problem to find the minimum set of attribute generalization required to access the application services.

Keywords: Access policies, online social networks, Finite state machine, security model.

1. Introduction:

Online Social Networks are becomes a heart to social communication on the internet. The most popular Online Social Networks are Facebook, Twitter, linked in and Google+ etc. The main purpose of these sites is to enable people to share personnel and public information to all the people. We can make social connections with friends, coworkers, colleagues, family, and even with strangers. The main problem with the

ISSN: 2320-1363

Online social Networks is the shared information can shown by many other people those are not related to the actual owner of the information. For example a user shares a photo this can be viewed and by all his friends, friend of friends and their friend of friends. There is no exact controlled access on the shared data. This becomes added advantage to the malicious user to share and get users data.

Even though the OSN provides standard security mechanisms to provide the privacy to the user data but it's not under its control. OSNs cannot control the sharing criteria. These will leads to new access controlled policies and regulations to user's personnel data of the OSNs. The main drawback of the OSNs policies is the decision is binary that means the shared data will delete the data and leave the sharing. That's why many traditional access policies are introduced.

In this paper we address this issue by deploying an access control mechanism for applications in social networks. Our goal is to provide a privacy-enabled solution that is in line with social network ethics of openness, and does not hinder users' opportunities of adding useful and entertaining applications to their profiles. Our access control mechanism is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. Enabling such a mechanism requires applications to be developed to accommodate different user preferences. We model applications as finite state machines, and use the required user profile attributes as conditions governing the application execution. The user is faced with the challenge of specifying the minimum set of attributes and their minimum generalization levels required to acquire specific services provided by the application.

2. Related work

There are many traditional access control mechanisms [2],[3],[4],[5],[6] for handling the OSNs control of the shared data. Trust-based access control is introduced based on the trust and reputation computation in OSNs. S. Kruk, S. Grzonkowski, A. Gzella etc all introduced new system called D-FOAF which is a friend of friend ontology-based distributed identity management system for OSNs, where the relationships are associated with a trust level and that refers the level of friend ship participated in the relationship.

Carminati et al. [2] introduced a conceptually similar but more comprehensive trust-based access control model. This model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. They further presented a semi decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in OSNs [3]. Fong et al. [5] proposed an access control model that formalizes and generalizes the access

ISSN: 2320-1363

control mechanism implemented Face-book, admitting arbitrary policy vocabularies that are based on theoretical graph properties. Gates [6] described relationship-based access control (ReBAC) as one of new security paradigms that addresses unique requirements of Web 2.0. Then, Fong [4] recently formulated this paradigm called a ReBAC model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of these existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs.The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work .Squicciarini et al. [10] provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content. The Clarke-Tax mechanism was adopted to enable the collective enforcement of policies for shared contents. Game theory was applied to evaluate the scheme. However, a general drawback of their solution is the usability issue, as it could be very hard for ordinary OSN users to comprehend the Clarke-Tax mechanism and specify appropriate bid values for auctions. Also, the auction process adopted in their approach indicates that only the winning bids could determine who can access the data, instead of accommodating all stakeholders' privacy preferences. Carminati et al.[10] recently introduced a new class of security policies, called collaborative security policies, that basically enhance topology-based access control with respect to a set of collaborative users. In contrast, our work proposes a formal model to address the MPAC issue in OSNs, along with general policy specification scheme and a simple but flexible conflict resolution mechanism for collaborative management of shared data in OSNs. In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used in OSNs, which has not been addressed by prior work.

3. Access Controlled framework:

We present a mechanism that enables fine grain access control on the profile data. Such a mechanism enables the application developer to select the data items required by the application and at the same time enables the user to opt-in or opt-out or generalize each of the requested data items. The access controlled framework contains three modules called

3.1 Application Registration
3.2 User Application Addition
3.3 User Application Adaption

3.1 Application Registration

The application developers register the application with the social network server. The developers are required to share the application API calls and the application business state diagram describing the application process, as part of the registration process, developers need to tag the application, by labeling each API within the application with the set of user's data items used by the application. The provided application information is used to compile

ISSN: 2320-1363

an application sheet describing the data attributes required by the application.

3.2 User Application Addition

Once the application is registered with the social network server, it becomes available for social network users to add to their profiles. Upon selecting the application, the application sheet is presented to the user, who is prompted with the following options for each data item required by the API: choose to opt-in, opt-out, or generalize. Intuitively, the user opts-in for the data items he is willing to disclose to the application. If the user opts-out for some data the application needs to adapt in order to be properly executed without such input. In case the generalize option is chosen for a certain data item, then the user only accepts the application to employ generalized data attribute The user selections are input in the user sheet, which indicates the user access preference for the added application.

3.3 User Application Adaption

At this stage the user sheet is used to generate a version of the application executable using the input obtained by the profile data items. This phase requires the application to differentiate provisioning according to the permissible data items and their respective generalization levels. We discuss in the next section how this not trivial task is achieved.

4. Customized application provisioning

The user sheet provides a mechanism for users to specify generalization preferences on the profile attributes to restrict the data accessible to the application. On the other hand, by enabling attribute generalizations the application is faced with the problem of missing data, and might not ensure the provisioning of the request service based on the provided data generalizations. To address this issue we propose that during the application registration phase the application developer is required to provide the process execution description of the application. The process execution description describes the interactions between the composed APIs. To address the access policies we define an application transition system.

The application transition system can be defined as tuple $TS = \{S, \delta, \sum\}$ where

- S is a finite set of states. The set of states includes a single initial state s0 and a finite set of final states F⊆S.
- $\sum$ is the alphabet of operations offered by the service and the data required by this service.
- $\delta: S \mathrm{X} \sum \rightarrow S$ is the transition function that maps states and alphabets to another state. The transition $\delta(S_i, \alpha) = S_j$ represents that transition from state S_i to state S_j subject to services and data in a.
- The set of final states represents the different service levels provided by the application.

We model the application transition system TS as a directed graph G=(V,E), where the vertices V represent the states, and the edges E represent the state transitions. The edges E are labeled with the minimum attribute generalization levels required to enable the state transition. For an edge e¸E the edge label e.h represents the generalization level

ISSN: 2320-1363

required for the state transition. For example, in Fig. 1(a) the edge (S0, S1) is labeled with h12 indicating that the generalization level 2 is required for attribute x1 to enable transition from state S0 to state S1. A user preference is said to satisfy a transition if the specified user attribute generalization level is greater than or equal to the edge generalization level. The reduced application transition system is computed by generating a graph GR =(VR, ER), where VR = V and ER⊆E includes only the transitions E that satisfy the user preferences. Fig. 1(b), shows an example reduced application transition graph for the user preference vector$up = \{h_1^1, h_1^2, h_2^1, h_1^4\}$and the original application state diagram in Fig. 1(a).

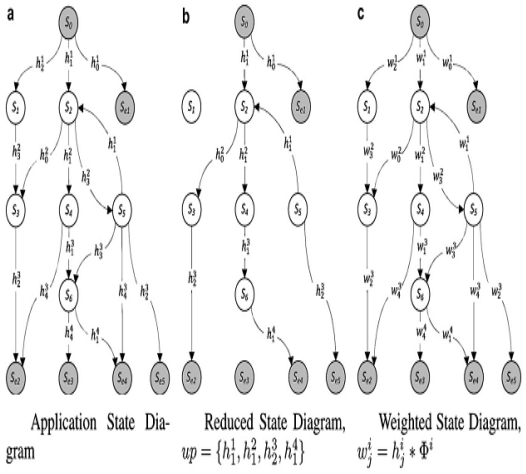

Fig: Application state diagram and user preferences

Conclusion:

In this paper we have presented an access control framework for social networks a developer application that enables users to specify profile attribute preferences and requires applications to be designed so to be customized based on users' profile preferences. Our framework provided a privacy enabled solution that is in line with social network ethics of openness, and does not hinder users' opportunities of adding useful and entertaining applications to their profiles. We modeled the applications as finite state machine with transition labeling indicating the generalization level required to enable application state transitions.

References:

[1] Hongxin Hu, Gail-Joon Ahn, Jan Jorgensen " Multiparty Access Control for Online Social Networks: Model and Mechanisms" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013

[2] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

[3] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[4] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[5] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-

ISSN: 2320-1363

Style Social Network Systems," Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 2009.
[6] E. Carrie, "Access Control Requirements for Web 2.0 Security and Privacy," Proc. Workshop Web 2.0 Security & Privacy (W2SP), 2007.
[7] H. Hu and G. Ahn, "Multiparty Authorization Framework for Data Sharing in Online Social Networks," Proc. 25th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy, pp. 29-43, 2011.
[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks," Proc. 27th Ann. Computer Security Applications Conf,pp. 103-112, 2011.
[9] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi,"D-FOAF: Distributed Identity Management with Access Rights Delegation," Proc. Asian Semantic Web Conf. (ASWC), pp. 140-154,2006.
[10] A. Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social networks," Proc. 18th Int'l Conf. World Wide Web, pp. 521-530, 2009.
[11] Mohamed Shehab , Anna Squicciarini, Gail-Joon Ahn , Irini Kokkinou "Access control for online social networks third party applications" computers & s e c u rity 3 1 (2 0 1 2) 8 9 7 e9 1 1