Analysis of Online Social Networks – Study on Multiparty Access Control Mechanism

N Venkateswara Rao, K. Mehar Prasad, Y Ramesh Kumar

I. INTRODUCTION

Online social networks sites such as Facebook, LinkedIn, Twitter combined to reach over billion users, the popularity of social networks continues to increase sharing information online compound. Users regularly upload personnel business and education details of revealing private details to public, to protect user information security controls have become a central feature of social networking sites but remains to users to adopt these features. Personnel data on social networks has used by employers for job searching they can communicate directly with the concern person but more sophisticated applications of social network data include tracking user behaviour monitoring. Cannot trust users place in social networks exploiting with hackers and attacks, set of threats posed to users has resulted in a number of refinements to privacy controls. However one aspect of security remains largely unresolved friends photos stories and data are shared across the network conflicting privacy requirements between friends can result in information being unintentionally exposed to the public, while social networks allow users to restrict access to their own data currently no mechanism to enforce privacy concerns over data uploaded by other users social network content is made available to search engines and mined for information, personal privacy goes beyond what one user uploads about his/her becomes an issue of every member on the network shares.

In our work controls the shared content can undetermined a user security analyzing the situations in Facebook where asymmetric privacy requirements between two friends weaken one user’s privacy. We develop authorization model to capture the core features of multiparty requirements which have not been accommodated access control systems and models for online social networks and secure networking conflict to explore both the frequency and risk of information leaked by friends whom cannot be prevented with existing privacy controls.

II. RELATED WORK

Multi user access control is introduced for secure network access, existing access control solutions for online social networks trust based access control inspired by the developments of trust and reputation in online social networks. The friend of friend ontology based distributed identity management system for online social network where relationships are associated with a trust level which indicates the level of friendship between the users participating in a given relationship. This model allows the specification access rules for online resource where authorized users are denoted in terms of the relationship type depth and trust level between users in online social networks. Semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in online social network. Fong et al proposed an access control mechanism in Facebook admitting arbitrary policy vocabularies that are based on theoretical graph properties described relationship based access control as one of new security paradigms that addresses unique requirements of Web 2.0 then Fong [7] recently formulated this paradigm called a relationship based access control model that bases authorization decisions on the relationship between the resource owner and the resource access or in an online. The data sharing specially photo sharing in online social network Squicciarini et al provided a solution for collective privacy management in online social networks. Their work considered access control policies of a content that is co-owned by multiple users in online social networks such that each co-owner may separately specify his or her own privacy preference for the shared content. Carminati et al. [9] 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 multiparty access control issue in OSNs, along with a 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

Keywords – Online social networks, Authorization, Multiusers, Sharing.
conduct various analysis tasks on access control mechanisms used

III. SECURITY ISSUES ON SOCIAL NETWORKS

Online social networks like Facebook is rewriting a lot of policies to make easier to understand not act options somebody tagged in a post or photo to untag you and the ability to untag multiple photos at once are helpful. The new Facebook layout presents all of current and past activities on Facebook posts photos comments like and so in a handy timeline format to anyone with access to your profile which may include friend’s colleague’s executives at our professional life. Organizations are finding innovative ways to use these websites their successes have been marred by privacy concerns; in fact popularity of social media continues to grow the focus on privacy protection.

A. Diligent privacy when merging social media websites

Social media websites will merge together so that they are better able to complete with the industry giants. The websites such as Facebook LinkedIn are currently the heavy hitters in the social media world, there are also many smaller websites out there. As social media websites rush to add even more features and functionality to their websites they could potentially overlook key privacy considerations. After all when one company merges with another or when they add new technological features there always seem to be a few growing pains along the way.

B. Single access sign-on can raise red flags for security and privacy

Using single access sign-on technology users can log in once and then use multiple websites without the need to sign in again. Although the convenience of this feature tends to make it popular with users it brings with it a whole other host of security and privacy concerns. As the use of single access sign-on becomes more common it is likely that websites will also start to share information this kind of access will make it easier for a single social media website to show actions and activities on other websites. Social media websites will have to take care to ensure user privacy otherwise this highly convenient feature could become a liability.

C. New website security restrictions and universal legislation

Privacy and security legislation has already started in 2012 and likely to gain even more momentum in 2013. as people increase the amount of information they share on social media websites the need for heightened security and privacy controls also increases. Social media world possess a mind boggling amount of personal information about the people who user their websites. Without good universal guideline on how this information can be gathered and used intentionally or unintentionally, websites have been pretty much on their own to set their privacy policies there is currently a vast amount of variation between websites. Additionally most people do not really understand how to recognize the potential for information misuse, people often share information innocently because they want to use a specific feature or because they wish to qualify for a free product or service.

D. Fine Line between effective marketing and privacy intrusion

Companies focused on advertising dollars on traditional media or on websites. However in recent years more companies have been dabbling with the advertising and marketing aspects of social media. Websites like Facebook Twitter LinkedIn as well as the companies who use them for marketing will have to be careful to walk a fine line between effective marketing and privacy intrusion. As more people become aware of privacy intrusion issues they will also likely become more leery and distrustful. Companies that wish to be successful with these kinds of marketing and advertising efforts will have to pay close attention to the privacy needs of their users.

E. Social media websites using location based services need to avoid privacy

Today’s social media websites are not even limited to traditional online use as social media continues to take advantage of mobile devices and location based services users will be exposed to even more privacy concerns. Social media websites utilize location based services will have focus on user privacy and security concerns if they expect people to put their trust in them. If used properly these services could open up a whole new world of social media interactivity.

IV. PROBLEM DEFINITION

An online social network provides the conversation on different activities such as business education entertainment advertisement etc. attractive means of digital social interactions raise the number of security concerns associated with multiple online users. The access control captures a multiuser authorization requirement which provides the privacy issue. For example frequently used social network Facebook user only accepts his/ her friends but all are in different domains, to share information on same domain need to accept the profiles of unauthorized users trigger security and privacy issue our system provides multi access control to share relation, profile & information.

Profile sharing feature is to support social applications written by external party developers to build functionalities of user profiles. Relationship sharing is that users can share their relationship with other members inherently bidirectional and carry potential sensitive information that associated users may not need to disclose. Content sharing provide built in mechanisms enabling users to communicate and share contents with other members.
V. IMPLEMENTATION DETAILS OF MULTIPARTY USER CONTROL: MULTIPARTY

A policy evaluation mechanism for the specification and enforcement of MPAC policies in online social networks

A. Owner: In Owner module let \( d \) be a data item in the space \( m \) of a user \( u \) in the social network. The user \( u \) is called the owner of \( d \). The user \( u \) is called the contributor of \( d \). We specifically analyze three scenarios profile sharing, relationship sharing and content sharing to understand the risks posted by the lack of collaborative control in online social networks. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

B. Contributor: In Contributor module let \( d \) be a data item published by a user \( u \) in someone else’s space in the social network. The contributor publishes content to other’s space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor.

C. Stakeholder: In Stakeholder module let \( d \) be a data item in the space of a user in the social network. Let \( T \) be the set of tagged users associated with \( d \). A user \( u \) is called a stakeholder of \( d \), if \( u \notin T \) who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder’s privacy concern may be violated. A shared content has multiple stakeholders.

D. Disseminator: In Disseminator module let \( d \) be a data item shared by a user \( u \) from someone else’s space to his/her space in the social network. The user \( u \) is called a disseminator of \( d \). A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content), and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator’s space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator’s friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been redisseminated, the original access control policies should be always enforced to protect further dissemination of the content.

E. MPAC: MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. Accessor Specification: Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

VI. COMPARATIVE STUDY

Before this system, the 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 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. Compare to previous work our new system implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs. Ovursively, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the
stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision.

VII. CONCLUSION

In this paper, presents sharing to access multiple users in secure manner, A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. A proof-of-concept implementation of our solution called Multiuser Control has been discussed as well, followed by the comparative study and system evaluation of our method. Future work extends to investigate more analysis services for collaborative management of shared data in online social networks.

REFERENCES


AUTHOR BIOGRAPHY

N Venkateswara Rao B.Sc from Andhra University M.Sc from Andhra University M.Tech computer science engineering from Avanthi College of Engineering currently he working as Asst Prof at Avanthi College of Engineering Hyderabad. His research areas include Network Security, Information Retrieval System, Data mining & warehousing.

K. Mehar Prasad B.Sc from Andhra University M.Sc from Andhra University M.Tech computer science engineering from JNTU Kakinada, currently he working as Asst Prof at Avanthi Engineering College and has guided many UG & PG students. His research areas include Information Retrieval System, Data mining and Databases.

Y Ramesh Kumar M.Tech from Andhra University currently he is working in Avanthi College of Engineering has guided many UG & PG students. His research areas include Information Retrieval System, Data mining & warehousing.