Human Effects of Enhanced Multiparty Secured Access Control for Online Social Networks

Ms.M.Sandhiyah*1,
Research Scholar,
Dept of CS& Applications,
PGP College of Arts & Science,
TamilNadu, India

Mrs.V.Shanmuga priya*2,
Asst. Professor,
Dept of C S& Applications,
PGP College of Arts & Science,
TamilNadu, India

ABSTRACT

Online social networks (OSNs) such as Face book, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs.

A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and WebPages, such as wall in Face book, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education, and work history, and contact information. In addition, users can not only upload a content into their own or others' spaces but also tag other users who appear in the content.

Online social networks (OSNs) have experienced tremendous growth in recent years. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users.

This paper enhances existing and introduces new social network privacy management models and measures their human effects. First, it **introduces a mechanism using proven clustering techniques that assists users in grouping their friends** for traditional group-based policy management approaches. It found

ISSN: 2278 – 1323

measurable agreement between clusters and user-defined relationship groups. Second, it **introduces a new privacy management model** that leverages users' memory and opinion of their friends (called example friends) to set policies for other similar friends.

Finally, **it explores different techniques that aid users in selecting example friends**. It is found that by associating policy temples with example friends (versus group labels), users author policies more efficiently and have improved perceptions over traditional group-based policy management approaches.

In addition, the results show that privacy management models can be further enhanced by utilizing user privacy sentiment for mass customization. By detecting user privacy sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user.

This project also proposes an **approach to enable the protection of shared data associated with multiple users in OSNs**. An access control model is formulated to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, it present a **logical representation of the access control model** that allows us to leverage the features of existing logic solvers to perform various analysis tasks on the model.

The project is designed using Microsoft ASP.Net 2005. The coding language used is C#.Net. The back end used is MS SQL Server 2000.

INTRODUCTION

The Internet and online social networks, in particular, are a part of most people's lives. eMarketer.com reports that in 2011, nearly 150 million US Internet users will interface with at least one social networking site per month. eMarketer.com also reports that in 2011, 90 percent of Internet users ages 18-24 and 82 percent of Internet users ages 25-34 will interact with at least one social networking site per month. This trend is increasing for all age groups. As the young population ages, they will continue to leverage social media in their daily lives.

In addition, new generations will come to adopt the Internet and online social networks. These technologies have become and will continue to be a vital component of our social fabric, which we depend on to communicate, interact, and socialize. Not only are there a tremendous amount of users

ISSN: 2278 – 1323

online, there is also a tremendous amount of user profile data and content online. For example, on Facebook, there are over 30 billion pieces of content shared each month. New content is being added every day; an average Facebook user generates over 90 pieces of content each month. This large amount of content coupled with the significant number of users online makes maintaining appropriate levels of privacy very challenging. There have been numerous studies concerning privacy in the online world [11], [12]. A number of conclusions can be drawn from these studies. First, there are varying levels of privacy controls, depending on the online site.

For example, some sites make available user profile data to the Internet with no ability to restrict access. While other sites limit user profile viewing to just trusted friends. Other studies introduce the notion of the privacy paradox, the relationship between individual privacy intentions to disclose their personal information and their actual behavior [13]. Individuals voice concerns over the lack of adequate controls around their privacy information while freely providing their personal data. Other research concludes that individuals lack appropriate information to make informed privacy decisions. Moreover, when there is adequate information, short-term benefits are often opted over long-term privacy. However, contrary to common belief, people are concerned about privacy [14]. But managing ones privacy can be challenging. This can be attributed to many things, for example, the lack of privacy controls available to the user, the complexity of using the controls [15], and the burden associated with managing these controls for large sets of users.

The paper enhances existing and introduces new privacy management models for online social networks. In addition, it measures the human effects of our improvements. It introduces three new improvements to privacy management models:

1. Assisted Friend Grouping—an incremental improvement to traditional group-based policy management.
2. Same-As Policy Management—a new paradigm improvement over traditional group-based policy management.
3. Example Friend Selection—an incremental improvement to Same-As Policy Management.

The thesis leverages traditional group-based policy management as our baseline and progressively improves upon this privacy management model. With each new enhancement, we measure their human effects including cluster/userdefined

ISSN: 2278 – 1323

relationship group alignment, user privacy sentiment, efficiencies and user perceptions.

The thesis introduces a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches. Assisted Friend Grouping leverages proven clustering techniques to aid users in grouping their friends more effectively and efficiently.

It introduces a new privacy management model that is an improvement over traditional group-based policy management approaches. The new paradigm leverages a user's memory and opinion of their friends to set policies for other similar friends, which we refer to as Same-As Policy Management. Users associate the policy with an example friend and in doing so have this friend in the forefront of their mind. This allows users to be more selective and careful in assigning permissions. Users are thinking of people, not groups. Using a visual policy editor that takes advantage of friend recognition and minimal task interruptions, Same-As Policy Management demonstrated improved performance and user perceptions over traditional group-based policy management approaches.

It further enhances Same-As Policy Management by introducing Example Friend Selection—two techniques for aiding users in selecting their example friends that are used in developing policy templates. Both techniques reduced policy authoring times and were positively perceived by users. In addition, the thesis proposes an approach to enable the protection of shared data associated with multiple users in OSNs.

REVIEW OF LITERATURE

BARBARA CARMINATI et al [1] stated that the existence of online social networks that include person specific information creates interesting opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address some of the current limitations, they have created an experimental social network using synthetic data which they then used to test the efficacy of the semantic reasoning based approaches they have previously suggested.

However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible

ISSN: 2278 – 1323

by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

YUAN CHENG et al [2] stated that users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure, and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be allowed to specify which access can be granted in terms of existing relationships.

They proposed a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. They developed a path checking algorithm to determine whether the required relationship path between users for a given access request exists, and provide proofs of correctness and complexity analysis for this algorithm.

PAUL DUNPHY et al [3] stated that Graphical password systems based on the recognition of photographs are candidates to alleviate current over-reliance on alphanumeric passwords and PINs. However, despite being based on a simple concept – and user evaluations consistently reporting impressive memory retention – only one commercial example exists and overall take-up is low. Barriers to uptake include a perceived vulnerability to observation attacks; issues regarding deploy ability; and the impact of innocuous design decisions on security not being formalized.

Their contribution is to dissect each of these issues in the context of mobile devices – a particularly suitable application domain due to their increasing significance, and high potential to attract unauthorized access.

This produces:

1) A novel yet simple solution to the intersection attack that permits greater variability in login challenges;

2) Detailed analysis of the shoulder surfing threat that considers both simulated and human testing;

3) A first look at image processing techniques to contribute towards automated photograph filtering.

CATHERINE DWYER et al [4] stated that it is not well understood how privacy concern and trust influence social interactions within social networking sites. An online survey of two popular social networking sites, Facebook and MySpace, compared perceptions of trust and privacy concern, along with willingness to share information and develop new relationships.

ISSN: 2278 – 1323

Members of both sites reported similar levels of privacy concern.

Facebook members expressed significantly greater trust in both Facebook and its members, and were more willing to share identifying information. Even so, MySpace members reported significantly more experience using the site to meet new people. These results suggest that in online interaction, trust is not as necessary in the building of new relationships as it is in face to face encounters.

LUJUN FANG et al [5] stated that Privacy is an enormous problem in online social networking sites. While sites such as Facebook allow users fine-grained control over who can see their profiles, it is difficult for average users to specify this kind of detailed policy.

In this paper, they proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically.

PROBLEM DEFINITION

EXISTING SYSTEM

The existing system introduces three new improvements to privacy management models:

1. Assisted Friend Grouping—an incremental improvement to traditional group-based policy management.
2. Same-As Policy Management—a new paradigm improvement over traditional group-based policy management.
3. Example Friend Selection—an incremental improvement to Same-As Policy Management.

DRAWBACKS OF EXISTING SYSTEM

- If one person (A) specifies a policy to hide her friend list from the public and (B) one of the friends in that list specifies a weaker policy that permits his friend list visible to anyone, then relationship between A and B could be learnt
- Automatic configuration of privacy preferences is not included.
- Conflict resolution between privileges is not effective.

ISSN: 2278 – 1323

For example, A uploads one photo which can be shared between friends list (F) and not visible to friends of friends, then B (one of the friends in F) can share it to friends list in F but not to all others.

PROPOSED SYSTEM

In addition to the existing system approaches, the proposed system takes care of conflict resolution in privilege settings. Moreover, weaker policy settings of a person will not violate the policy settings of his/her friends. Privacy settings adjustments are shown such that violaters if included in the friends list, they are shown and suggested that they cannot allow to disseminate the photo contents to others. Privacy settings like Owner overrides are implemented.

ADVANTAGES OF THE PROPOSED SYSTEM

- Weaker policy on one of the friends will not violate his/her friends' policy.
- Automatic configuration of privacy preferences is included.
- Conflict resolution between privileges is effective.
- Uploading duplicate content is description is avoided.
- More number of privacy settings is suggested.

CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

The proposed system is used to filter message from OSN walls. The system is classifier to customizable content dependent for FR and flexibility of the system in term of filtering option through the management of BLs. In this proposed system is an early encouraging results user obtained on the classification procedure prompt and to improve the quality of classification. In particular, future plans contemplate a deeper investigation on two interdependent tasks. The first concerns the extraction and/ or selection of contextual features that have been shown to have a high discriminative power. The second task involves the learning phase. Since the underlying domain is dynamically changing, the collection of pre-classified data may not be representative in the longer term. The present batch learning strategy, based on the preliminary collection of the entire set of labeled data from experts, allowed an accurate experimental evaluation but needs to be

ISSN: 2278 – 1323

evolved to include new operational requirements.

The dissertation has been successfully completed within the time span allotted. Every effort has been made to present the system in more user-friendly manner. And the GUI provided here make the user feel friendly. All the disadvantages of the existing system have been overcome by using the present system**.** A trial run of the system has been made and is giving good results. The system has been developed an attractive dialogs fashion and the entire user interface is attractive and user friendly and suites all the necessities lay down by the users initially. So user with minimum knowledge about the computers and the system can easily work with the system.

SCOPE FOR FUTURE ENHANCEMENT

In future work, user plan to address this problem by investigating the use of online learning paradigms able to include label feedbacks from users. Additionally, it is planned to enhance the system with a more sophisticated approach to decide when a user should be inserted into a BL. The development of a GUI and a set of related tools to make easier BL and FR specification is also a direction user plan to investigate, since usability is a key requirement for such kind of applications. In particular, it aims at investigating a tool able to automatically recommend trust values for those contacts user does not personally known. Users do believe that such a tool should suggest trust value based on users actions, behaviors, and reputation in OSN, which might imply to enhance OSN with audit mechanisms.

Several areas to be developed in future, so the application must be upgraded for the new ones required and it is possible to modifications according to new requirements and specifications. The thesis work adds the facilities like fast data backup and restoration in case of data loss situations and planned to share the multi media content data. The policy creation process is improving security in advances automatic configuration for social relationship between users. The experimental result is designed such that the required enhancements can be integrated with each policy management easily with less integration work without modifying the present system.

ISSN: 2278 – 1323

C. JOURNAL REFERENCE

[1] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari, "Content-Based Filtering in On-Line Social Networks," Proc. ECML/PKDD Workshop Privacy and Security Issues in Data Mining and Machine Learning (PSDML '10), 2010.

[2] V. Bobicev andM. Sokolova, "An Effective and RobustMethod for Short Text Classification," Proc. 23rd Nat'l Conf. Artificial Intelligence (AAAI), D. Fox and C.P. Gomes, eds., pp. 1444-1445, 2008.

[3] B. Sriram, D. Fuhry, E. Demir, H. Ferhatosmanoglu, and M. Demirbas, "Short Text Classification in Twitter to Improve Information Filtering," Proc. 33rd Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR '10), pp. 841-842, 2010.

[4] J. Golbeck, "Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering," Proc. Int'l Conf. Provenance and Annotation of Data, L. Moreau and I. Foster, eds., pp. 101-108, 2006.

[5] D.D. Lewis, Y. Yang, T.G. Rose, and F. Li, "Rcv1: A New Benchmark Collection for Text Categorization Research," J. Machine Learning Research, vol. 5, pp. 361-397, 2004.

[6] M. Carullo, E. Binaghi, I. Gallo, and N. Lamberti, "Clustering of Short Commercial Documents for the Web," Proc. 19th Int'l Conf. Pattern Recognition (ICPR '08), 2008.

[7] U. Hanani, B. Shapira, and P. Shoval, "Information Filtering: Overview of Issues, Research and Systems," User Modeling and User-Adapted Interaction, vol. 11, pp. 203-259, 2001.

[8] K. Strater and H. Richter, "Examining Privacy and Disclosure in a Social Networking Community," Proc. Third Symp. Usable Privacy and Security (SOUPS '07), pp. 157-158, 2007. Rackspace Mosso. http://www.mosso.com/

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53(4):50–58, 2010.

[10] R. Meushaw and D. Simard. A network on a desktop. NSA Tech Trend Notes, 9(4), 2000. http://www.vmware.com/pdf/TechTrendNotes.pdf.

ISSN: 2278 – 1323

[11] P. England and J. Manferdelli. Virtual machines for enterprise desktop security. Information Security Technical Report, 11(4):193 – 202, 2006.

[12] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: a virtual machine-based platform for trusted computing. In ACM Symposium on Operating Systems Principles, pages 193–206. ACM, 2003.

[13] Fang, L., LeFevre, K.: Privacy wizards for social networking sites. In: WWW '10: Proceedings of the 19th international conference onWorld wide web. pp. 351–360. ACM, New York, NY, USA (2010)

[14] Banerjee, S., Ramanthan, K., and Gupta, A. Clustering short text using Wikipedia. In Proc. SIGIR (Amsterdam, The Netherlands, July 2007), 787-788.

[15] Phan, X.-H., Nguyen, L.-M., and Horiguchi, S. Learning to classify short and sparse text & web with hidden topics from large-scale data collections. In Proc. WWW (Beijing, China, Apr. 2008), 91-100.

[16] Java, A., Song, X., Finin, T., and Tseng, B. 2007. Why we twitter: understanding microblogging usage and communities. In Procs WebKDD/SNA-KDD '07 (San Jose, California, August, 2007), 56-65.

[17] Bratko, A.; Cormack, G. V.; Filipič, B.; Lynam, T. R.; and Zupan, B. 2006. Spam-filtering using statistical data compression models. Journal of Machine Learning Research 7:2673–2698.

[18] D. D. Lewis, R. E. Schapire, J. P. Callan, and R. Papka. Training algorithms for linear text classifiers. In Proceedings of the 19th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 96), pages 298–306, 1996.

[19] D. Koller and M. Sahami. Hierarchically classifying documents using very few words. In International Conference on Machine Learning (ICML'97), pages 170–178, Nashville, 1997.

[20] T. Rose, M. Stevenson, and M.Whitehead. The Reuters Corpus Volume 1 – from Yesterday's News to Tomorrow's Language Resources. In Proceedings of the Third International Conference on Language Resources and Evaluation, 2002. http://about.reuters.com/researchandstandards/corpus/LREC camera ready.pdf

ISSN: 2278 – 1323