Research Journal of Information Technology 5(2): 45-49, 2013
DOI:10.19026/rjit.5.5786
ISSN: 2041-3106; e-ISSN: 2041-3114

Submitted: November 08, 2012 Accepted: January 14, 2013 Published: June 01, 2013

Research Article

Priority User Access for Social Network Security

[1]Suha Hameed, [2]Zahraa Muhsen and [1]Salwa Alsamarai
[1]Departmentof Information Management Systems, Isra University, Amman, Jordan
[2]Iraqi Commission for Computers and Informatics, Baghdad, Iraq

Abstract: Attacking the information of any institute that used social network may affect their business and can cause huge financial losses whose value is immeasurable. Social networking sites are the place where the users not only post their messages but also submit personal details. The weaken security of users' accounts in social networking sites have led to various privacy issues and challenges in security issues. This study highlights types of the most known social network and their security points. In this study we proposed a new idea for social network security, which aim to give each user a full control of his information. It also controlled the types of information the user can access. A delegation rights given to each by proposing a priority to sign for each user according to the relationship intensity between the requester and respondent, also a certificate that consists of all the information needed to verify user authorization which will save from any risk.

Keywords: Access points, social network security, types of social network, user priority

INTRODUCTION

Social Network Sites (SNS) allowed users to share information's which can be personal or global with others. SNS located in the concept of virtual community, where its researches focus on mathematical models of the dynamic networks social structures which made of a set of actors (users) and dyadic ties (links) between these actors. The actors may represent as individuals or organizations and the dyadic ties represent the relation among them. Each actor participates in a number of SNS simultaneously. The SNS is a critical resource for building teams to transmit and maintain the knowledge in an organization (Sharma *et al*., 2012; Hogben, 2012). The most known SNS are shown in Table 1 with description to each site. Figure 1 shows the relation between SNS and users, it also shows the contribution of the user and the community to the social networks. Figure 2 shows the percentage of the number of user in the social network according to ComScore up to end of November 2011 (Wiki, 2012). User in SNS been categorized in three types: members with no activity, inviters to join the social network and fully participated linkers as shown in Sharma *et al.* (2012).

The security and privacy problems have grown with the newer Internet applications which users expect a level of privacy and control over the network. In order to use online services and applications, users typically need to create accounts including usernames and passwords. The username-based identity and the related password problems resulting from users' online behaviors have been a focus of research studies. The hard fact about social networking is that the way private or sensitive information could be gathered and utilized implicitly or explicitly by the adversary is hard to know and control. As the utility and importance of the social networks could not be neglected, there is a need of some amount of privacy preservation in such a way that its utility is still maintained and could be used ethically by analysts. A balance needs to be maintained between privacy and utility (Sharma *et al*., 2012; Jin *et al*., 2011).

Many research focus on the point that there is a need to provide security and access control mechanism for SNS (Alhasib, 2008; Williams *et al*., 2009; McDowell and Morda, 2011; Lawler *et al*., 2011; Ur and McGrath, 2012; Gross and Acquisti, 2005). These works explain the importance of SNS and reviewed the types of threats that may occurs on these sites and try to take people opinions using questioners and interviews about privacy concerns on these sites.

Other researches propose a security model to enforce access control and security on these social sites, as in Beato *et al*. (2012). A system designed and implemented that allows users to define and enforce selective access control policies by using encryption scheme and the implemented the model as Firefox extension and the definition of groups. Another paper by Tootoonchian *et al*. (2008) described the design and implementation of security system in the context of two online systems with very different characteristics a centralized web 2.0 site, flicker and decentralized P2P system. Tootoonchian *et al*. (2009) present an access

Corresponding Author: Zahraa Fadhil Muhsen, Iraqi Commission for Computers and Informatics, Baghdad, Iraq

Table 1: Social network sites

SNS	Description
Facebook	The most widely used, it sport a way for users to connections and share information with others
Twitter	A real-time information share network
LinkedIn	The largest online professional network
Google +	Contacts and integrated the user with other Google products
MySpace	Evolved to focus providing connections related to movies, music games
YouTube	Share and view video content
Flickr	Powerful share management site for digital photographs online
WordPress	Open source blogging tool and a dynamic content management system
Amazon.com	World's largest online retailer

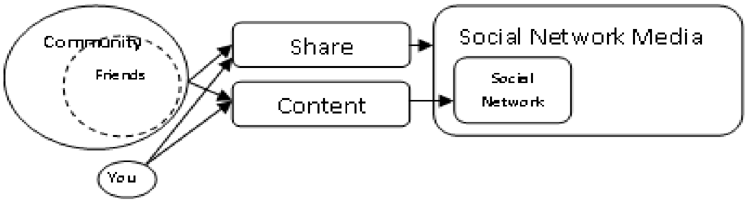

Fig. 1: The relations between social network and user

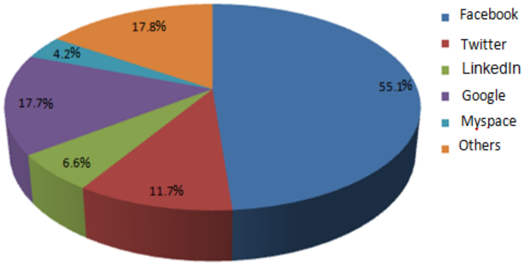

Fig. 2: Percentages of social network users

control scheme based on social relationships, which based on social Access Control List (ACL) and social attestation to gain access to other people data. Yamada *et al.* (2012) examines real OSN services in terms of their policy combining and resolution process and they propose three attacking scenario and a recovery algorithm from it. All these works focus on controlling user's access to data on SNS whether using encryption, ACL or recovery algorithms.

While in this work we have built a system based on the relationships degree among users as a measure of the powers. First the proposed method create a priority number to each person according to its access, second an essential certificate point is giving for each person determining the user name and priority allocated to him. So the main objective of this study is to give the user a dominance of his information plus the freedom to partition his friends according to their friendship and decide if anyone who has the right to access user's data can delegate this right to other users.

SOCIAL NETWORK SECURITY SYSTEMS

Social network maintains the accessing privacy and confidentiality of personal data stores, they provide the personal information with a portable data rules. Allowing the users to control their social features at their social network but it is still not enough to protect the personal data (they need more security options). The fine-grained authorization schemes which can delegate access are very important in such open architectures (Prakash and Avadhani, 2012).

The social networks provide services for user to create and share the information across the network. This situation creates an increasing on personal privacy in the networks sites to protect the user information. Social networks provide management security in variety ways for the different data usage policies and privacy protection conditions as follow:

Identity management: Is the management of data defining a user’s identity. This is an adequate requirement for the profiles maintained in social networks. Also manage it allowing query, transfer and display of the data in the system. This is one of the main functions of Social Networks. Additionally, user location can be used as an extra authentication factor when considering user security technologies based on the SIM card (Prakash and Avadhani, 2012; Monjas and Suárez, 2009).

Management personal data: Provide user which allow them to define in considerable detail how their personal profiles are displayed, both in terms of visual layout and the data fields which are displayed. They also provide sophisticated tools for searching and mining profile data (Prakash and Avadhani, 2012; Monjas and Suárez, 2009). The user set the sharing and privacy conditions of his data, generated content and applications, networks of friends and professional contacts and even delete them. As such, the user should be given tools to effectively control his “identity map” regardless of the place where any piece of it is actually stored. Such requirements may only be met if the user is been given sort of virtual single access point(s) to his/her identity map, not only in social network sites but also in network providers (operators), ISPs, payment

Table 2: Social networks types according to our serve

Social networks types	Description
Social networking	Services that combine and building relationships among people of similar interests and background. The most popular are Facebook, LinkedIn and MySpace
Blogging	The most popular free blogging platforms are WordPress.com, TypePad and Blogger. We include the following in this category:
	Micro-blogging: Information is delivered in short bursts such as Twitter
	Blog networks: A large collection of blogs. Many blog networks provide exclusive content and require approval for bloggers to join, which gives those who are accepted a certain level of prestige such as Gawker, b5Media, 9Rules
	Blogging communities: Encourage bloggers to share and interact among people and create regular blog posts such as BlogHer, LiveJournal
Multimedia sharing	We include video sharing, photo sharing, online video, media releases, messages/bull boards, comment communities, and regional social media in this category. It is a service that allows you to upload and share various media. The most popular are YouTube and Flickr
	News: Users submit and vote on news stories such as Digg, PopURLs and Reddit
Product	Buying and selling products online such as Ebay and Amazon.com.Wikis (content-driven communities): popping up everywhere such as Wikipedia. Search: such as Google, Yahoo!
Email	Such as Gmail

providers, GAMEYs and any other site where a digital fingerprint of the user is present. The user should be as well able to trace the use of its identity information, both in terms of knowing “who” uses them and “how” it is being used (Monjas and Suárez, 2009).

Access control management: Any identity management system must give its users control over who accesses which parts of their personal data. Usually this is based on knowing whether the person accessing the data fulfils certain criteria. Social Networks are increasingly offering this functionality. In social networks, the main boundary protecting a user’s data is whether a person attempting to access it has been defined as a friend or is a member of a shared group. Recently, however, Social Networks have added features which allow users to restrict access down to the level of individual friends (or business associates) for each field of their personal profile. In other words, they are now offering very granular access control (Prakash and Avadhani, 2012; Monjas and Suárez, 2009).

Accessing data: Most identity management systems provide data tracking tools so users can see who has accessed personal data. This functionality is often not fully implemented in Social Networks because users browsing other people’s profiles generally prefer to remain anonymous. It is possible to install profile trackers on some Social Networks however and many Social Networks provide quite detailed anonymous statistics on accesses to user profiles. It leads to unquestionable benefits to the user (not only as a means to help the user to choice among the increasing offer of services and contents, but also as automated personalization, security or usability recommendations). That inferred user knowledge can be automatically created and updated by using machine learning techniques. Ericsson wishes to promote the standardization of the exchange format for social network information, beyond current de facto standards, thus covering that kind of inferred information (Monjas and Suárez, 2009).

TYPES OF SOCIAL NETWORKS

The social networks consist of many categories according to different classification. White (2006) shows seven major categories, another perspective was shown by Austin (2012), which has classified it in five categories, Herman (2012) declares in 2012 shows the most commonly used types into eleven types, Grahl (2012) shows six types. Social network classified into two types in (HudsonhorizonsSite, 2012). Fulkerson (2010) classified it by twenty three types; Bard (2010) classified it into fifteen, (Kim, 2009) into nineteen and (Oshima, 2009) into seven. Dyer (2012) shows a different classification according to the customer engagement at the social network. According to our observation we classify the social network into eight categories as shown in Table 2.

Proposed methods: In this section, we present a proposed method for ensuring information security in OSN, by using the data types in the most popular social network sites and at the same time this method can be fitted to other SNS, the need only to change the data types according to each site.

Data types in OSN: Here we present the data types in most popular OSN and we give a code to each of them to be used in the next sections:

Data type	Code
Profile information	I1
Friend list	I2
Comment	I3
Group information	I4
Like	I5
Photo-tag	I6
Video-tag	I7

The suggested solution: In the suggested solution two major issues are presented the first one is assigning a priority to each user and the second is using certificates for access authorization. For the first issue, anyone can conduct that according to the human nature the strength

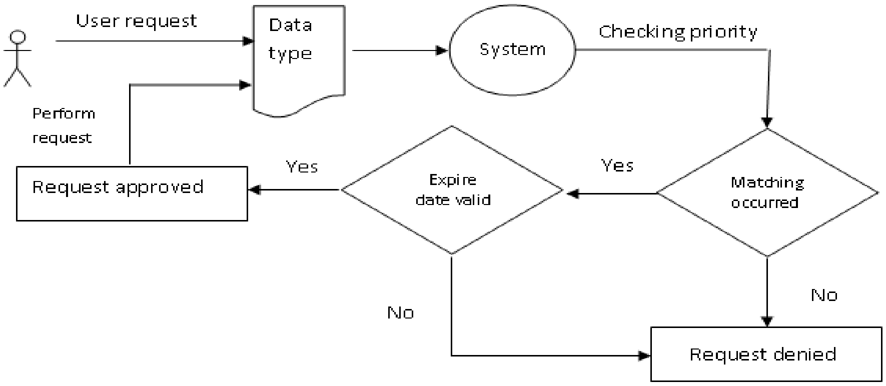

Fig. 3: Diagram for the priority user access methods

of relationships and friendships are different between people so there must be an indication that differentiate one from the other, in the proposed solution apriority is used to achieve this. The priority idea in computer system is usually attached to scheduling algorithms in operating systems and other fields, where in operating system a priority is associated with each process and the CPU is allocated to the process with the highest priority. Priorities are generally indicated by some fixed range of numbers, such as 0 to 7 or 0 to 4.095. However, there is no general agreement on whether 0 is the highest or lowest priority. Some systems use low numbers to represent low priority; others use low numbers for high priority [Operating system concepts book]. In this solution we use low numbers for high priority. The word priority in this solution means the level of permissions and powers given to each user in OSN, such that when the user has priority 0 means that he has all the permissions needed to access the information in 7 types of data plus all the rights to give these permissions to other user on the same page, while Priority 1 means that the user has all the permissions needed to access the information in 6 types of data plus the rights to give these permissions to other user on the same page and in this way when the priority number increase 2, 3, 4, 5, 6 the number of data types that the user given permissions to decrease 5, 4, 3, 2, 1, respectively. When the user gets priority 7 this means that he has all the permissions needed to access the information in 7 types of data, but he can't give these permissions to any other user, priority 8 means that he has all the permissions needed to access the information in 6 types of data, but he can't give these permissions to any other user and on the same way priority numbers 9, 10, 11, 12, 13 means the ability to access 5, 4, 3, 2, 1 data types respectively but without any rights to give these permissions to other users. It’s the responsibility of the page owner to assign priority to the requester, when the requester submit a friend request and the owner confirm it, also the owner has the possibility of upgrade or downgrade the priority for any of its friends. The second issue in the proposed solution is giving certificate to each user filled by the owner and takes the following form:

User: user 1		
Owner name	Priority	Expire date

The expire date is used to determine the period on which the certificate is valid.

Example: Suppose that user1 is the owner of a face book page, while user 2 knows user 1 and wants to be one of his friends, according to the friendship degree user1 decides to let user 2 able to see only his profile information, can't delegate this to other people and the expire date is un determined, then user 2 certificate will look like the following:

User: user 2		
Owner name	Priority	Expire date
User 1	13I1	Un determined

When a user requests access to any of the data types belongs to a specified owner, the proposed system first check the list of all certificates given to the requester searching for the owner name, when owner found the request is compared with the priority type determined in the certificate if matching occurred and the expire date is valid then request approved as shown in Fig. 3.

CONCLUSION

Online social networks offer exciting new opportunities for interaction and communication, but also raise new privacy concerns. In this study we have built a system based on the adoption of the degree of personal relationships between users as a measure of the powers given to the user, this done by first, giving priority number for each person determines what he can do, the second essential point is giving certificate for each person determines the user name and priority given to him.

When there is any request to the system all that is required is to examine the user certificate to make sure the request can be confirmed or not, by this way the amount of research required can be reduced compared to the amount needed in case of the use of social ACL which needs significant amount of search each time there is a request perform an operation to an object since it needs to check the whole list of the object verify the possibility of the execution of the request or not and this search increases whenever the list become bigger and bigger.

REFERENCES

Alhasib, A., 2008. Threats of Online Social Networks. Retrieved from: http://www.cse.hut.fi/ en/publications/B/1/papers/Hasib_final.pdf.

Austin, B., 2012. Different Types of Social Networks. Retrieved from: http://www.seo-positive.co.uk/ blog/different-types-of-social-networks/.

Bard, M., 2010. 15 Categories of Social Media. Retrieved from: http://www.mirnabard.com/ 2010/ 02/15-categories-of-social-media/.

Beato, F., M. Kohlweiss and K. Wouters, 2012. Enforcing Access Control in Social Network Sites. Retrieved from: http:// www.cosic.esat. kuleuven.be/publications/article-1240.pdf.

Dyer, P., 2012. The 6 Types of Social Media Users', Social Media Today. Retrieved from: http://socialmediatoday.com/pamdyer/564409/6-types-social-media-users.

Fulkerson, L., 2010. 23 Types of Social Media Sites.Retrieved from: http://onbloggingwell.com /23-types-of-social-media-sites/.

Grahl, T., 2012. The 6 Types of Social Media.Retrieved from: http://outthinkgroup.com/tips/the-6-types-of-social-media.

Gross, R. and A. Acquisti, 2005. Information Revelation and Privacy in Online Social Networks (The Face Book Case). Retrieved from: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

Herman, J., 2012. Types of Social Media.Retrieved from: http://www.howto.gov/social-media/social-media-types/.

Hogben, G., 2012. Security Issues in the Future of Social Networking. W3C Workshop on the Future of Social Networking. Retrieved from: http://www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf.

HudsonhorizonsSite, 2012. Types of Social Networking Websites. Weab Solutions, Retrieved from: http://www.hudsonhorizons.com/Custom-Website-Solutions/ Social-Networking/ Types-of-Social-Networks.htm.

Jin, L., H. Takabi and J.B.D. Joshi, 2011. Analyzing security and privacy issues of using e-mail address as identity. Int. J. Inform. Privacy Secur. Integr., 1(1): 34-58.

Kim, P., 2009. Types of Social Media Distribution. Retrieved from: http://www.zazoo.com.au/ 2009/ 03/31/types-of-social-media-distribution/.

Lawler, J.P., J.C. Molluzzo and V. Doshi, 2011. An expanded study of net generation perceptions on privacy and security on Social Net-working Sites (SNS).Proceeding of the Information Systems Educators Conference.Wilmington North Carolina, USA, 28(1634).

McDowell, M. and D. Morda, 2011. Socializing Securely: Using Social Networking Services. Retrieved from: http://www.us-cert.gov/reading_room/safe_social_networking.pdf.

Monjas, M.A. and D. Suárez, 2009. Identity Management in Social Networks. W3C Workshop on the Future of Social Networking. Position Papers, 15-16 January, Barcelona.

Oshima, L., 2009. Social Media Experiencing 3rd Year of Consecutive Growth in Inc. 500. Retrieved from: http://socializemobilize.com/2009/ 11/18/ social-media- experiencing-3rd-year-of- consecutive-growth-in-inc500/.

Prakash, T.M.G.S. and P.S. Avadhani, 2012. Security and sociability issues in online social networks.Int. J. Knowl. Eng. Technol., 1(2): 1-7.

Sharma, S., P. Gupta and V. Bhatnagar, 2012. Anonymisation in social network: A literature survey and classification. Int. J. Soc. Netw. Min., 1(1): 51-66.

Tootoonchian A., K.K. Gollu, S. Saroiu, Y. Ganjali and A. Wolman, 2008. Lockr: Social Access Control for Web 2.0. Retrieved from: http://research.Microsoft.com/en-us/um/people/alecw/wosn-2008.pdf.

Tootoonchian, A., S. Stefan, G. Yashar and W. Alec, 2009. Lockr: Better Privacy for Social Networks. Retrieved from: http://research.microsoft.com/en-us/um/people/ ssaroiu/publications/conext/2009/ lockr.

Ur B. and R. McGrath, 2012. Grouping Friends for Access Control in Online Social Networks. Retrieved from: http://www.eecs.harvard.edu/cs199r/fp/BlaseRob.pdf.

White, M., 2006. What Types of Social Networks Exist? Retrieved from: http:// socialnetworking. lovetoknow.com/What_Types_of_Social_Networks_Exist.

Wiki,2012.SocialNetworkingService.Retrieved from: http://en.wikipedia.org/wiki/Social_net working_ service.

Williams, K., A. Boyd, S. Densten, R. Chin, D. Diamond and C. Morgenthaler, 2009.Social Networking Privacy Behaviors and Risks.Retrieved from:http://csis.pace.edu/~ctappert/srd2009/a2.pdf.

Yamada, A., T.H.J. Kim and A. Perrig, 2012. Exploiting Privacy Policy Conflicts in Online Social Networks. CMU-CyLab-12-005, Carnegie Mellon University, Pittsburgh, PA 15213.Retrieved from: http://www.cylab.cmu.edu/ files/pdfs/ tech_reports/ CMUCyLab12005.pdf.