SocBridge: Bridging the gap between Online Social Networks

Research-in-Progress

Raj Kumar Nepali
Dakota State University
rknepali@pluto.dsu.edu

Yong Wang
Dakota State University
yong.wang@dsu.edu

Abstract

Online social networks have become a key component of our digital presence. Users create profiles on these platforms using personal information, which helps others to identify them. Users connect to their friends, make new friends, and interact with each other via chat, like, retweet, comment, sharing files, etc. Most popular online social network platforms these days include Facebook, Twitter, LinkedIn, MySpace, Instagram, etc. All of these services operate separately. Users on one platform cannot connect and communicate with their friends on another platform. This study proposes "SocBridge" a novel way of connecting and communicating between users on different platforms. The framework acts as a proxy between participating service providers and thus protects the identity of communicating users, and preserves the business model of service providers.

Keywords

Online Social Networks, Bridge, Privacy, public-key cryptography

Introduction

When Social Networking services started in the mid-90s, no one knew how far it would go and what it would become. Starting as simple places to interact and share ideas, these services gained popularity rapidly. These services took a variety of ideas and evolved. Early 2000 were the golden years for online social networks when Friendster, MySpace, LinkedIn started and later joined by Facebook. Today these services are worth billions of dollars in market value. Online Social Networks (OSNs) have become ubiquitous services today. OSNs attempt to create and mimic real-life social relationships in digital world. OSNs like Facebook, Twitter, LinkedIn, and MySpace are the main service providers. They have attracted millions of users. According to StatisticBrain, Facebook, the largest Online Social Network, has 1.4 billion users worldwide (StatisticBrain 2014), and the number is expected to grow continuously. Communication is one of the most important factors of human life that sets us apart (Deacon 1997) and it is the reason for the popularity of these websites too. OSNs provide services to allow users post their feelings, pictures, videos, and connect with like-minded people. People with similar interests can form groups and communicate, and share ideas. Friends can like posts, comment on them, and share them. These interactions allow users to connect and communicate with their friends and others through these platforms. This is the new form of communication and socialization in modern world. On average, users spend 15 hours 33 minutes per month using OSNs (StatisticBrain 2014).

OSNs have evolved and are taking many different forms, for example: Facebook is general purpose OSN, LinkedIn is professional OSN, Twitter is for micro-blogging, and Instagram is for sharing pictures. Despite of the different purposes they satisfy, all OSNs share common principles, i.e., connection and communication. However, the problem with existing online social networks is that they operate separately. For example, Facebook users cannot communicate with Twitter users. Current OSN architecture has created a gap for cross platform communication. Because of this, users must create profiles on another platform to connect and communicate with their friends who belong to that platform.

This has raised many issues in OSNs in the digital world. First, it is really hassle to create multiple profiles with many service providers. Second, a user's personal information will be exposed to multiple service providers. Third, because of the lack of a mechanism to let users know what information they share on one platform, there is risk that a user will reveal new information while creating profile on another platform resulting in unwanted personal information disclosure. Attacks are known and can be used to reveal the identity of a user on different platforms (Narayanan et al. 2009; Wondracek et al. 2010). Such attacks can be used to collect personal information of a user, which can be further used for many other malicious activities. Fourth, attackers can create a fake profile of a user on another platform, and connect to his/her friends to collect information about friends or launch social engineering attacks (Bilge et al. 2009).

This study proposes "SocBridge", a novel way of connection and communication among users on different online social network platforms. SocBridge is a bridge that connects social service providers together and helps users to connect with each other across different platforms. The main contributions of the paper include: 1. It provides a vision for future OSNs, and 2. It studies privacy requirements for such framework. The proposed work is conducted in three phases: first, security requirements are examined; second, novel architecture is designed to address the usability as well as privacy requirements; and third, privacy violation possible scenarios from service providers and SocBridge itself is analyzed with respect to privacy requirements mentioned. The rest of the paper is organized as follows: In section 2, we study related works. In section 3, methodology is discussed. Requirements for such a system from stakeholders are discussed in section 4. The architecture of "SocBridge" is described in section 5, followed by analysis in section 6. Section 7 covers evaluation, and section 8 covers implications. Conclusion & future work is presented in section 9.

Related Works

Privacy in Online Social Networks is being studied for a long time. OSNs have been studied in the field of computer science, information systems, psychology, and sociology. Most of the studies focus on the privacy of user's personal information or personally identifiable information (PII). The studies cover wide range of topics from information leakage, inference attacks, to relationship identification. Although a few architectures have been developed in the decentralized P2P OSNs (Buchegger et al. 2009; Cutillo et al. 2009; Luo et al. 2009) to protect user privacy, the adoption of these architectures is questionable as per today's situation. People are reluctant to migrate their information from existing providers to a new service provider (Theory of resistance). Some work has been done using cryptography to protect user's information from the prying eyes of the service providers (Anderson et al. 2009; Guha et al. 2008; Lucas et al. 2008; Starin et al. 2009). Other studies propose architecture to protect user information from service providers (Anderson et al. 2009). All of the studies have provided significant contributions to the privacy and security of OSNs. However, none of these works have crossed the boundary of single service provider. Similar idea like the authors' work can be found in chat functions of Skype (go to account settings), which works by linking accounts together. However, this does not support the functionalities the authors propose in the paper (it works for chat only). In addition, the privacy protection is questionable since these services are proprietary. Facebook and Twitter can be connected together to see the posts. However, the functionalities are limited and a user is required to have account on both platforms. To the best of our knowledge, this is the first attempt to resolve the problem using existing architecture of OSNs and propose vision for bridging of OSNs.

The only work which tangentially discusses the similar concept as this paper is presented by Yeung et al (Yeung et al. 2009). However, their work is based on the concept of decentralization and does not consider the difficulty in paradigm shift, for example: usability, functionalities, and specially migration. The authors' work can be implemented using existing architecture and existing service providers.

Methodology

This paper utilizes the Design Science research paradigm and applies the seven guidelines by Hevner et al. (2004), and Simon (1981). An artifact is designed to address a relevant IS problem that makes significant contribution. The research implements 'Build and evaluate' cycle for construction and evaluation of the artifact. The objective of this work is to propose middleware service for all online social networks, and

preserve the business interest of participating service providers, so that users in any platforms can communicate with their friends without boundaries.

Requirements

While designing such a system, user's as well as the service provider's concern should be addressed properly. If user's concerns are not addressed, there will be no one to use the system (perceived usefulness (Davis 1989)). If the provider's concerns are not addressed, such a system will not be put into practice. As expected, there are many requirements that need to be addressed. Here in this section, we will discuss some of those requirements.

First and the most important concern is to protect user privacy. With the amount of personal information available with these services, people are concerned about their privacy. Many flaws have been detected on Facebook's technology over the years, and it has risen bar for privacy in these services. Privacy policy conflicts (Liu et al. 2011), inference (Mislove et al. 2010), PII leakage (Krishnamurthy et al. 2009), and security attacks (Narayanan et al. 2009) are some of the problems. Particularly in our model, privacy concerns should be addressed from traffic analysis (PII leakage) and de-anonymization (Wondracek et al. 2010). Communication requires the identity of the people/system participating. The objective here is to protect personal information of participating users from service providers and also prevent malicious attackers.

Second concern is the functionality of the system. The designed system should bridge all the functionality of the existing OSNs and should not be limited to the function of connections only. Search, friend requests, wall postings, likes, comments, file sharing, and chat, are the examples of some of them. Without maintaining the functionality of the existing service providers, the adoption of the proposed system will be at risk.

Third concern is from the service providers' perspective. Such a system shall ensure that the business model of each participating service providers is not disturbed. The business model of existing service providers depends on their user information. User's information is the commodity for the service providers and is often sold in the aggregated forms to marketing, potential advertisers, and others to generate revenue. It is important to protect the information of a user belonging to one service provider from leaking into the other participating service provider. For example: Facebook should not be allowed to gather user information from users who belong to Twitter, and likewise. This will ensure all participating service provider's concerns (business model) are protected.

For this study, we will address all of the issues discussed above. Finally, the system will be evaluated to meet these objectives.

SocBridge

Being aware of the importance of such bridging architecture for the future of OSN, we propose "SocBridge", a framework connecting OSNs together. The framework currently meets three goals:

- Connecting users across multiple platforms
- Protecting privacy interests of users and business interests of service providers
- Search and add, comment, like, retweet, and chat functionalities

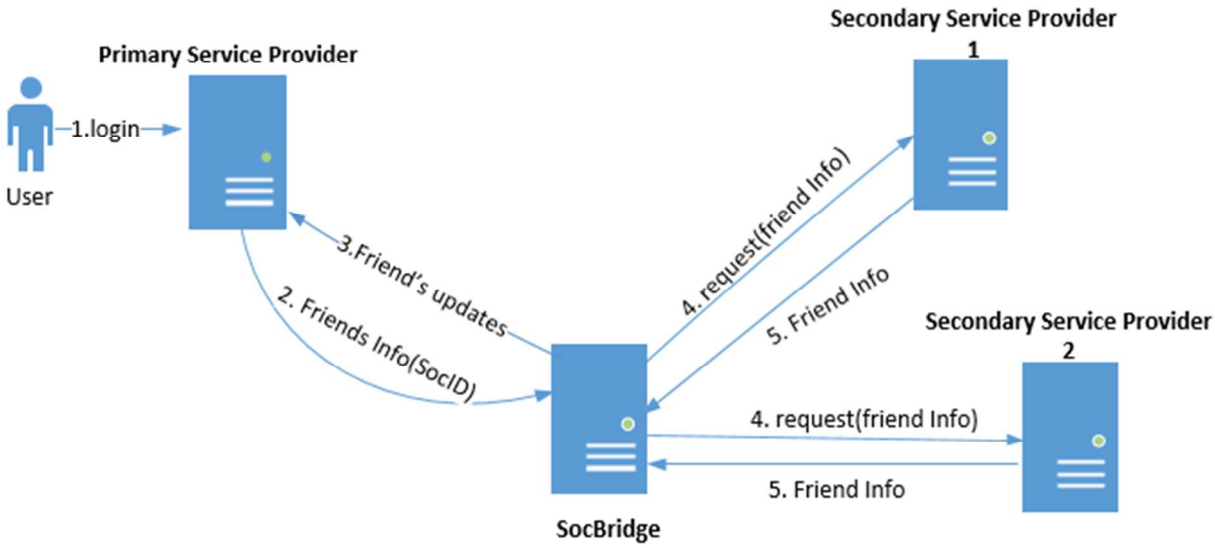

Figure 1: SocBridge in action

Before diving into the details, some of the terms are defined for ease of understanding. Primary service provider is the one where the (requesting) user has an account. Secondary service provider/s are the ones where user's friends belong. For example: If Alice uses Facebook and wants to see what her friends on Twitter are doing then, Facebook is her primary service provider and Twitter is secondary service provider. There can be many secondary service providers for a user where her friends belong. Primary service provider and secondary service provider both maintain the SocID information of their registered users (when they register to use SocBridge) and the SocID of their friends (when a friend request is accepted) who use SocBridge.

Register

Users register with their names, email addresses, and service provider names (Facebook, Twitter, etc.) to the SocBridge. SocBridge will then generate a unique SocID upon successful registration and sends it to the user. Primary service providers will be notified that users are now also associated to SocBridge and their SocIDs will be sent as well. Primary service provider will store that user's SocID for later use. At the client-side, private key and public key are generated. Public key is then sent to the SocBridge for future encryption processes. The user will then login to the primary service provider.

Search and Add

The basic assumption here is that a user knows the email address of his/her friends and their service providers. The user starts search with email address or SocID of a friend (which can also be shared out of band), SocBridge will check to see if the user is already registered. If the user is already registered, it will create FOAF file encrypting primary user's information except SocID with public key of the searched user and send it to secondary service provider. Secondary service provider will forward request to the searched user as notification. If the user accepts the friend request, SocBridge will keep the friend relationship in its database and informs both primary and secondary service provider about the friend relationship between the users with their SocID. Service providers store the friendship information for future communication. If the user is not already registered to SocBridge, email request will be sent.

Information Retrieval

When a user logs into primary service provider, a request will be sent to SocBridge for any update on the user's friend from secondary service provider/s. The request contains requesting user's SocID and friend's

SocID with secondary service provider's name. SocBridge will create FOAF request file requesting updates on a user, then forwards it to secondary service provider along with requesting user's public key. Secondary service provider will check the SocID for the relationship with the targeted user and upon verification, encrypts its user data with requestor's public key. This way only the requesting user can get information about his/her friend on secondary domain and even SocBridge will have no idea about the content of communication. Figure 1 shows the communication process.

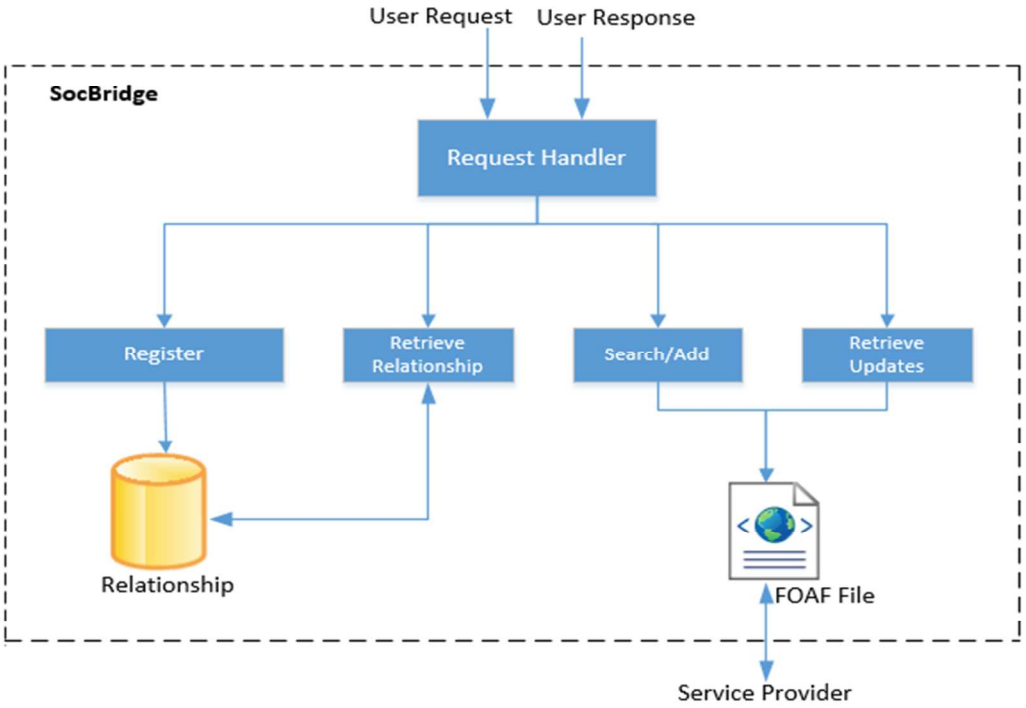

Figure 2: Internal Architecture of SocBridge

Chat and other functions work similarly like information retrieval. The only difference is that a user has to initiate the communication unlike information retrieval where the updates are retrieved automatically. Public key are used to encrypt the content of communication.

The FOAF file is looks like (more info at: (Dodds ; Project)):

```
<foaf:Person rdf:"me">
        <foaf:SocID>12345</foaf:SocID>
                <foaf:Like>
                        <foaf:Content>
                                <foaf:friendSocID>98765</foaf:friendSocID>
                                <foaf:ContentID>1234abcdef</foaf:ContentID>
                                <foaf:Destination>www.twitter.com</foaf:Destination>
                        </foaf:Content>
                </foaf:Like>
</foaf:Person>
```

Figure 3: FOAF file generated for Like

Analysis

This section analyzes the requirements with theoretical, internal (service providers and SocBridge) attack scenarios. The objective here is to test how much information service providers and SocBridge can learn about users and if they can collect extra information on users.

Service Providers

Service providers cannot be trusted not to sneak and try to collect information about the users from other platforms. In order to protect the identity and PII of the users communicating cross platforms, SocID and public key encryption is used. Encrypting personal information, comments, and messages with public keys protects the confidentiality of the communication and hence only the destined users can read it. Beside that, the request does not include details about the primary service provider where the user belongs. The only information that is available to the secondary service providers is SocID and requesting user's public key, which does not tell much about a user and hence ensures identity protection.

SocBridge

It is possible that SocBridge administrators try to glean information about the users. The information that SocBridge stores during registration includes name, email, service provider, SocID, and public key of users. During the communication process, since the message is encrypted with destined user's public key, SocBridge administrator cannot know the content of the message. However, the administrators can see where the request is generated and where it is forwarded with no knowledge about the content of the communication.

Evaluation

The evaluation can be performed with SocBridge implemented as cloud service. HTML5 and PHP can be used for interface development, and Javascript can be used for AES encryption. 256 bit keys will be used for private keys and public keys.

Security measures such, as user's personal information privacy will be tested with the help of traffic analysis and cryptanalysis. Inference as well as direct revelation of any user information is critical. Performance of the system will be tested for efficiency of encryption/decryption.

Implications

The implications of this work are manifold. First, it will become much easier for a user to create only one profile and use that to connect and communicate to his/her friends, despite which service providers they belong to. Second, user's personal information will reside with only one service provider thereby minimizing the exposure of PII. Third, since each user has only one profile to manage, users have better knowledge about what information they are sharing, and control what information they want to share.

Conclusion & Future Work

SocBridge is presented as a middleware to bridge existing OSN service providers. This work is the very first step towards designing architecture for the future OSNs where the users can connect and communicate with each other despite where their profile is located. The privacy requirements of the participating users as well as business model of participating service providers are protected using public-key cryptography. The functionalities like search/add, comment, like, retweet, chat, and so on, are preserved. Although evaluation is theoretical, it is believed that such architecture is the future of OSNs and this work will play vital role in initiating the discussion. Future work will address the implementation of SocBridge, key management (distribution, revocation), access control, security challenges, and the performance of the system.

REFERENCES

Anderson, J., Diaz, C., Stajano, F., Leuven, K. U., and Bonneau, J. 2009. "Privacy-Enabling Social Networking over untrusted networks," in *WONS*: Barcelons, Spain, pp. 2-7.

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., and Antipolis, S. 2009. "All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks," in *WWW 2009*, pp. 551-560.

Buchegger, S., and Schi, D. 2009. "PeerSoN: P2P Social Networking — Early Experiences and Insights," in *SNS'09*, ACM: Nuremberg, Germany.

Cutillo, L. A., Strufe, T., and Antipolis, S. 2009. "Privacy Preserving Social Networking Through Decentralization," in *WONS*.

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* (13), pp 319-340.

Deacon, T. W. 1997. *The symbolic species: The co-evolution of language and the brain*, (WW Norton & Company.

Dodds, L. "FOAF-a-Matic," http://www.ldodds.com).

Guha, S., Tang, K., and Francis, P. 2008. "NOYB: Privacy in Online Social Networks," in *Proceedings of the first workshop on online social networks*, pp. 49-54.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *MIS Quarterly* (28), pp 75-105.

Krishnamurthy, B., and Wills, C. E. 2009. "On the Leakage of Personally Identifiable Information Via online social networks," in *WOSN'09*: Barcelona, Spain, pp. 7-12.

Liu, Y., Gummadi, K. P., and Mislove, A. 2011. "Analyzing Facebook Privacy Settings : User Expectations vs . Reality," in *IMC' 11*: Berlin, Germany.

Lucas, M. M., and Borisov, N. 2008. "flyByNight: Mitigating the Privacy Risks of Social Networking," in *WPES'08*, ACM: Alexandria, Virginia, US, pp. 1-8.

Luo, W., Xie, Q., and Hengartner, U. 2009. "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in *2009 International Conference on Computational Science and Engineering*, Ieee, pp. 26-33.

Mislove, A., Viswanath, B., Gummadi, K. P., and Druschel, P. 2010. "You Are Who You Know : Inferring User Profiles in Online Social Networks,").

Narayanan, A., and Shmatikov, V. 2009. "De-anonymizing Social Networks," in *2009 30th IEEE Symposium on Security and Privacy*, Ieee, pp. 173-187.

Project, F. "FoaF project," http://www.foaf-project.org).

Simon, H. A. 1981. "The Sciences of Artificial (2nd ed.)," *MIT Press, Cambridge, MA*).

Starin, D., Baden, R., Bender, A., Spring, N., and Bhattacharjee, B. 2009. "Persona : An Online Social Network with User-Defined Privacy Categories and Subject Descriptors," in *SIGCOMM'09*: Barcelona, Spain, pp. 135-146.

StatisticBrain 2014. "Social Networking Statistics," in http://www.statisticbrain.com.

Wondracek, G., Holz, T., Kirda, E., and Kruegel, C. 2010. "A Practical Attack to De-anonymize Social Network Users," *2010 IEEE Symposium on Security and Privacy*), pp 223-238.

Yeung, C. A., Liccardi, I., Lu, K., Seneviratne, O., and Berners-Lee, T. 2009. "Decentralization: The future of Online Social Networking," *W3C workshop on Future of Social Networking Position*).