Emerald Insight

International Journal of Web Information Systems

Controlling privacy disclosure of third party applications in online social networks
Sarath Tomy Eric Pardede

Article information:

To cite this document:
Sarath Tomy Eric Pardede , (2016),"Controlling privacy disclosure of third party applications in online social networks", International Journal of Web Information Systems, Vol. 12 Iss 2 pp. 215 - 241
Permanent link to this document:
http://dx.doi.org/10.1108/IJWIS-12-2015-0045

Downloaded on: 09 November 2016, At: 01:36 (PT)
References: this document contains references to 43 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 173 times since 2016*

Users who downloaded this article also downloaded:

(2016),"Tukuchiy: a dynamic user interface generator to improve usability", International Journal of Web Information Systems, Vol. 12 Iss 2 pp. 150-176 http://dx.doi.org/10.1108/IJWIS-09-2015-0028

(2016),"A QoS-aware approach for runtime discovery, selection and composition of semantic web services", International Journal of Web Information Systems, Vol. 12 Iss 2 pp. 177-200 http://dx.doi.org/10.1108/IJWIS-12-2015-0040

Access to this document was granted through an Emerald subscription provided by emerald-srm:563821 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/1744-0084.htm

Controlling privacy disclosure of third party applications in online social networks

Sarath Tomy and Eric Pardede
Department of Computer Science and Information Technology, La Trobe University, Melbourne, Australia

Received 22 December 2015
Revised 3 January 2016
Accepted 4 January 2016

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Abstract

Purpose – The purpose of this paper is to analyse the problem of privacy disclosure of third party applications in online social networks (OSNs) through Facebook, investigate the limitations in the existing models to protect users privacy and propose a permission-based access control (PBAC) model, which gives users complete control over users' data when accessing third party applications.

Design/methodology/approach – A practical model based on the defined permission policies is proposed to manage users information accessed by third party applications and improve user awareness in sharing sensitive information with them. This model is a combination of interfaces and internal mechanisms which can be adopted by any OSN having similar architecture to Facebook in managing third party applications, without much structural changes. The model implemented in Web interface connects with Facebook application programming interface and evaluates its efficacy using test cases.

Findings – The results show that the PBAC model can facilitate user awareness about privacy risks of data passed on to third party applications and allow users who are more concerned about their privacy from releasing such information to those applications.

Research limitations/implications – The study provides further research in protecting users' privacy in OSNs and thus avoid the risks associated with that, thereby increasing users' trust in using OSNs.

Originality/value – The research has proven to be useful in improving user awareness on the risk associated with sharing private information on OSNs, and the practically implemented PBAC model guarantees full user privacy from unwanted disclosure of personal information to third party applications.

Keywords Facebook privacy, Manage third party Facebook applications, Online social networks, Privacy access control model, Privacy disclosure risks,
Third party applications in online social networks

Paper type Research paper

1. Introduction

Online social networks (OSNs), such as Facebook, Twitter and LinkedIn, have acquired enormous popularity in recent years (Debatin *et al.*, 2009; Luo *et al.*, 2009) as platforms enabling people to consolidate former relationships and establish new friend circles (Xu *et al.*, 2013). OSN user profiles provide rich source of personal information, including people interests, views, likes and other social relations (Clark and Roberts, 2010). Furthermore, many companies use these sites to collect background information on prospective employees and potential target audience for their marketing campaigns (Chaabane *et al.*, 2014). OSN data also have high commercial value to marketing

International Journal of Web Information Systems
Vol. 12 No. 2, 2016
pp. 215-241
© Emerald Group Publishing Limited
1744-0084
DOI 10.1108/IJWIS-12-2015-0045

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

companies, competing networking sites and identity thieves (Hasan, 2013). So while OSNs provide users a platform to develop an online identity and social relationships, there can be some grave privacy concerns about user data.

Privacy disclosure problems can arise on OSNs as the user's identity and data are closely linked and visible to a large audience (Beye *et al.*, 2012). Different definitions of privacy and trust exist in this context to help users determine how others access their personal information. Westin (1967) defines privacy as the claim of individuals, groups or institutions to determine when, how and to what extent, information about them is communicated to others.

Basically, OSN privacy is a person's right to control the usage and distribution of his personal information (Chen *et al.*, 2009). This means keeping one's personal information within its intended scope, and privacy is breached when the information is taken beyond its scope (Beye *et al.*, 2012; Stutzman *et al.*, 2012). As trust is an important element for the success of any website, it is necessary to have highly secure and easily manageable privacy settings in OSNs that can guarantee user privacy.

Facebook is the most widely used OSN in the world with around 1.28 billion monthly active users as of 31 March 2014 (Facebook, 2014a). Facebook contains a good amount of quality information including user's private information relate to one's personal identity (Acquisti *et al.*, 2012). A research conducted by Acquisti and Gross (2006) found that 89 per cent of users on Facebook use their real name and information on Facebook.

Privacy disclosure in Facebook can happen in many ways, such as through tags in photos and posts, sharing content, joining groups, page likes and more. Direct exposures of personal information through such social activities on OSNs have been widely publicized and researched. But it is information leakage from indirect access to users' private data by third party applications that can cause high privacy risk (Cheng *et al.*, 2013).

Third party applications connected to OSNs such as Facebook extract more data from a user than any active user in his network. Users are unaware of who controls these third party applications, have no idea of how and where these data are stored or what purpose they use their information (Tuunainen *et al.*, 2009). Unauthorized access to personal data through third party applications can create further privacy risks, especially if the personal data are processed to reveal other more sensitive information about the users, such as insurance history, medical records, social security data and tax information through various data-matching processes. There are various reports about damaging activities, such as financial fraud, blackmail and terrorism activity, carried out by unauthorized data-matching activities (Aldhafferi *et al.*, 2013).

In this paper, we first review privacy disclosure and control on OSNs and the data access behaviour of third party applications on Facebook. Our goal is to protect users' privacy and prevent privacy disclosure by controlling the access of third party applications to their data in two ways:

(1) make users aware and alert about the privacy risks that can occur from sharing sensitive information with third party applications; and

(2) provide an access control privacy model based on permissions without hindering user freedom to enjoy the benefits provided by third party applications.

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

The rest of the paper is organized as follows. In Section 2, we explain privacy disclosure problems imposed by third party applications on OSNs. Here, we focus on the risk of privacy disclosure on Facebook and examine the drawbacks in the current Facebook architecture through an experimental analysis. In Section 3, we analyse previous studies to identify the main findings on privacy protection on OSNs. In Section 4, we introduce a new model called "Permission-Based Access Control" (PBAC) model that notifies user about the privacy risk of the data being accessed by third party applications and helps them decide about what information is passed on. We also describe the implementation of the model into the Facebook architecture and workflow of our model in detail. In Section 5, we evaluate the implementation of our model through a set of test cases. Finally, we compare our proposed solution with other existing frameworks in terms of protection, awareness and complexity. The conclusion of this paper and future work in this research area are discussed in the last section.

2. Background

While some OSNs allow third party applications to integrate with their platforms via application programming interfaces (APIs) and acquire permission to access user data, other OSNs like Facebook adopts a different approach that allows third party developers to create applications in their own server (Venkatesan *et al.*, 2013). Typically, most users using these applications assume that their privacy preferences are correctly enforced (Singh *et al.*, 2009). However, in reality, these applications hosted on external servers access large amount of profile information, and users have no or minimal control over their data accessed by these applications (Venkatesan *et al.*, 2013).

2.1 Unauthorized use of data by Facebook applications

Facebook provides third party developers access to the users private data, some of which is not even accessible by the user's friends. Unlike regular friend relationships, the users do not have any idea about the developer of the application, and the relationship is not transparent. Moreover, when a user installs an application, third party developers have second degree access to information about his friends and fellow network members. Most Facebook third party applications further interact with "fourth party" entities like advertising networks and data brokers to share user information (Chaabane *et al.*, 2014).

The privacy configuration to control the flow of sensitive information including friends list is quite complex (Felt and Evans, 2008). Facebook's privacy policies as well as its privacy settings in managing applications are changing frequently (Emanuel *et al.*, 2013). So even if third party sites have to follow terms and conditions in accessing and using the user information, Facebook has no control over the data accessed by these applications once it has been released from the database (Cheng *et al.*, 2013).

Felt and Evans (2008) analysed 150 applications in Facebook and found that only 14 applications require the user's private data. But four of these applications clearly violate Facebook's terms of service, as they pull user data into the application profile and make it visible to other application users.

A *Wall Street Journal* investigation found that three of the top ten applications, including Farmville, have been sharing profile information about users and their friends with other advertising and internet tracking companies (Steel and Fowler, 2010).

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Chaabane *et al.* (2014) conducted a study on the interaction of third party applications with external entities by using 997 working applications listed in the Facebook App Center and found that more than 75 per cent of the tested applications exchange traffic with a minimum of six different domains, and the interaction of almost 10 per cent of these applications exceeds 20 unique domains.

Vienna University of Economics created an app with Facebook API to help users understand the data collection behaviour of Facebook third party applications and reveal the depth of information that third parties can collect. The app allows users to compare their data export from Facebook with the Facebook's original tool and their API download tool. The result shows that the data collected through the API download tool disclosed many types of data were not indicated on the Facebook export tool (Europe versus Facebook, 2015).

Third party developers should follow some guidelines when creating new applications which respect user privacy (Delgado *et al.*, 2010). Privacy policy should be enforced by Facebook to protect user privacy instead of relying on these third party applications to follow their terms of agreement (Felt and Evans, 2008). More rigorous implementation of privacy norms will improve user confidence in accessing these applications.

2.2 Privacy risk from Facebook third party applications

Even though third party applications provide added features to serve business and user interests to Facebook (e.g. games), there are huge privacy risks to user's personal information data when they get into the hands of third party developers. Personal data collected through these applications can be used for data matching to reveal sensitive information posing serious financial and personal risks (Aldhafferi *et al.*, 2013). Users accessing these applications may share information with their friends without knowing that these applications can access this sensitive information (Felt and Evans, 2008).

Consumer Report magazine conducted a survey in the USA in May 2012 with 2,002 online users of which 1,340 were active on Facebook that raised some privacy concerns. Twenty-eight per cent of users shared almost all their "wall posts" as public as or with groups wider than their friends, and about 11 per cent revealed that they have problems in using Facebook, ranging from somebody hacking their profile to harassing or threatening them (Ghazinour *et al.*, 2013a). Most users are careless with their private information due to the lack of awareness about the privacy risks which can lead to serious consequences (Debatin *et al.*, 2009).

Unauthorized data collection by third party applications can occur in the form of identity disclosure and attribute disclosure. Identity disclosure happens when adversaries map the user's collected entities to a specific real world entity to reveal the identity of the user. On the other hand, attribute disclosure can happen through these two scenarios. First is the disclosure of the identification of an individual directly from a unique attribute, such as social security number. Second, the use of quasi-identifying attributes or combination of attributes to identify sensitive attributes which users want to keep secret, such as political affiliation or sexual orientation (Zheleva *et al.*, 2012). So even without direct identifiers like name or phone numbers, an adversary can use distinctive attributes, such as date of birth and post code, and link them together to get an electronic image of a person (Sweeney, 2002).

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

About 87 per cent of individuals in the US Census from 1990 can be identified by their gender, date of birth and zip code. A person's sensitive health information can be revealed by matching the health insurance records without any identifying information with the public voter registration records (Sweeney, 2002). So by matching the gender, date of birth and zip code with the two types of records, Sweeney identified the medical record of the Governor of Massachusetts.

An experiment conducted at Heinz College & CyLab at Carnegie Mellon University, using an automatic face recognition system, cross-referenced photos from a famous dating site in the USA with some Facebook profile photos to identify people (Acquisti and Gross, 2006). Most e-commerce websites, including banks, ask for security questions relating to the user's interests, hobbies, phone numbers or birthdates when creating account for secured login. Adversaries can take such personal information given on the OSNs to deconstruct clues for guessing user passwords of bank accounts or answering security questions (Albesher and Alhussain, 2013).

2.3 An experimental analysis

We conducted an experimental analysis in early 2014 to understand how much user data, including private information, can be accessed with a third party application and how the collected data can cause privacy risks. We created an application in Facebook called "Privacy Check". Using the "App ID" and "App Secret", we connect the application to our program which is hosted in a third party external server. Then, we access the "Privacy Check" application using an existing Facebook user account which pops up three authentication dialogue boxes one after the other. The first authentication dialogue box seeks permission to access public profile and other information including sensitive private attributes that the user has not shared with others. Similarly, the second box seeks permission to post on Facebook on behalf of the user, and the third box seeks permission to manage pages, events and notifications. The three authentication dialogue boxes do not provide any information on how this information will be used and whether the operations can create privacy risks.

After being granted access, the collected data are stored in the database by the application. To understand the depth of information accessed by the application, we navigate to the user privacy settings and select the "Privacy Check" app added to the Facebook user profile. There we found that this Facebook application can access private data that can be sensitive, including inbox messages, posts, events, chats, friends and even friend requests. The depth of information access made by the application is quite drastic. A case study on the privacy behaviour of Facebook third party application is shown in Section 5.

To analyse the risk of privacy disclosure, we conducted a data-matching experiment using the profile picture URL extracted from the user using our "Privacy Check" application with Google image search. The result showed quite a startling level of identity disclosure, as we could access all the sites with similar pictures, including Google plus and LinkedIn, with the name and other details. This proves that a user can be easily identified by using a single attribute (profile picture URL) without any other sensitive information.

Many users are fearful of allowing access to Facebook applications because they do not know what information is accessed by the applications and how the applications are

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

going to use this information (Delgado *et al.*, 2010). We conclude this section with these following points about protecting user privacy and increasing user trust in OSN:

- Users need to have full control over how they share their profile information with third party applications and the applications should only be able to access permitted fields.
- Users need to be more aware about the privacy risks before sharing profile information with third party applications.

3. Related works

In this section, we will analyse existing works on protecting user privacy in OSNs. Privacy leakage through third party applications in OSNs cannot be controlled at one point. However, researchers came up with different models to improve the privacy settings and thereby protect the user's sensitive data. We analysed these models and finally a total of 11 research models which are more focussed on securing user information by limiting the application access are selected. As the concept of these models to improve privacy settings is different, we categorize these works into four categories based on the properties of their functionality and performance, namely, backend models, interface models, browser extension models and privacy score and recommendation models.

3.1 Backend models

In this section, we will analyse three different backend models, which involve the application in functional modules with servers and APIs to protect user privacy.

3.1.1 Component-based architectural model. Cheng *et al.* (2013) proposed a framework to protect user privacy where users can leave their private data within the trusted server, while third party external servers can get access to the user's public data with the help of a reference monitor along with a relationship-based policy model for users to control how the application accesses their information. In this model, the functional modules of the application can be divided into internal and external components. Internal components can get essential information only through the OSN API and are restricted from transmitting any private information to the external third party application server, while the external module components are run on the external third party application server. As Facebook continuously adds features and functionalities, it can be difficult to continuously update the model to categorize and split attributes into internal and external components. In addition, there are thousands of applications that are already running on Facebook and accessing user data through API; thus, it is not practical to adopt this model in this situation.

3.1.2 Differential privacy model. Viswanath *et al.* (2012) suggested a Facebook application sandbox model for third party application developers to securely aggregate user information according to differential privacy properties by adopting "XBook" model. This model used two sandboxes – user read-only sandbox, which can only read the information shared from friends, and user read-write sandbox, which can write to the user database and share with friends. The concept of differential privacy used in this model measures the information loss that happens when returning a result of a request over a given data set, and uses the defined privacy budget and injects "noise" in the answer which acts like a control knob. If noise is high, the loss of information is negligible and vice versa. However, the sandboxing structure can be complex and

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

requires extensive changes in the current architecture. In addition, the noise output based on information loss will not always be accurate.

3.1.3 Collaborative privacy management interceptor application programming interface model. Anthonysamy *et al.* (2012) proposed a collaborative privacy management (CPM) interceptor for API model consisting of an interceptor mechanism, which acts as a membrane between the OSN and the third party applications. A user can restrict permissions on certain information requested by the application or return dummy data in case of required fields. A user can also change the privacy configuration and share this new privacy configuration with others in OSN. Alternatively, instead of manually setting privacy, a user can search for pre-defined configurations shared by others and load them when installing an application. Also, it allows users to define the permission settings as to what information can be accessed by a third party application and can share this permission setting with other users in Facebook. This model is more secure in comparison to the previous two models, but the permission checking, transferring and filtering of all data with the access token between two different API's is complicated and can affect the performance of the OSN.

3.2 Interface models

In this section, we will analyse different user interface models for setting access permissions and promoting user awareness of risk in sharing sensitive data with third party applications.

3.2.1 Granular framework. Besmer *et al.* (2009) proposed a new access control model called granular framework to enforce user privacy preferences by introducing a user-to-application policy specifying access restrictions for applications. The policy restricts the application from accessing specific information of the user, and the friendship-based protection restricts the application from accessing his friends on behalf of the user. The user interface specifying the user-application policy will be shown to users whenever they install an application or access the application for the first time. The user's own information that will be shared and random friends information is displayed in the user interface. The interface is easy to modify, but the framework itself is not without flaw. Any user can see his/her friends that are using an application and their pattern of giving permissions.

3.2.2 Authentication dialogue user interface model. Wang *et al.* (2011) proposed a new model that provides better control and notification mechanisms to inform users when third party applications violate the privacy settings. The model has a modifiable authentication dialogue box so that users can have a clear understanding what information they are going to share. The design principles of this model aim to ensure users understanding on what information an application is accessing and whether they have an option to manage the entities. However, users have no control over basic information, including name, profile picture, gender and friend lists. Moreover, the user can be distracted with a number of checkboxes. The users still need to check and give permissions whenever they install an application, even if some applications do not access most information.

3.2.3 Privacy by redesign model. Xu *et al.* (2012) proposed a model called privacy by redesign consisting of two authentication dialogue boxes for users to allow or deny third party application access to their details. This model uses a user-friendly table or grid format separating the reading and writing access control in two columns where users

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

can choose the attributes they are willing to share. Also, the rows are separated with basic information, email, photos, videos, profile and other information that people have shared with the user. Tooltip information is shown on moving the mouse over the "i" mark with blue and red colours depending upon the user's privacy settings. The drawback of this model is that users have to select the fields they want to share even if the application is not requesting these attributes. Furthermore, this model cannot ensure full privacy because users are unable to access the application without providing their basic information.

3.2.4 User notification model. According to Hull *et al.* (2011), information access by third party applications should be made transparent by a system that can notify users with warning alerts. In this model, the user should have an option to allow or deny the access after the notification. The system should also alert the user whenever an application tries to access any information about the user's friends. However, except this notification feature in the user interface, this work does not consider any privacy control mechanism to protect users' private data from third party applications.

3.3 Browser extension models

In this section, we will analyse two browser extension models proposed by researchers to protect user data from third party developers on Facebook.

3.3.1 FBSecure model. Venkatesan *et al.* (2013) proposed a privacy browser extension model called FBSecure adding two more modules to the OAuth 2.0 (Open Authorization Protocol) that helps users to decide whether they should install an application. A recommendation service returns a set of recommendations for the permissions requested by the application and a permission guide helps users to understand the permissions requested. The permission guide extension parses the requested permission by capturing the scope value from the URI requested and allows users to select a subset of permission requested. The recommendation service passes a set of permission to the permission guide and returns a set of permission recommendations requested by the client. However, this model is more of a recommendation service mechanism rather than a privacy protection model. It would be really impractical for all users to install an extension to their browsers just for using Facebook applications.

3.3.2 SudoWeb model. Kontaxis *et al.* (2011) proposed a framework to maintain two Facebook sessions with two Facebook accounts to protect users privacy when accessing third party applications. The model proposed browser extension in Google Chrome called SudoWeb, which maintains two isolated sessions with the two Facebook profiles: a primary profile, which contains all the real information, and a disposable profile for current usage. The identity management function which stands between the loading page and the browser session storage logically detects the need and supplies the appropriate session. However, according to Facebook policy, a person can only maintain one account, and hence this violates Facebook policy. Moreover, most Facebook users usually do not manage two accounts.

3.4 Privacy score and recommender models

The privacy score calculator and recommendation models aim to promote user awareness about privacy risks from sharing sensitive data with third party developers.

3.4.1 Privacy score model. Liu and Terzi (2010) proposed a framework to compute a privacy score by measuring the potential privacy risk of OSN users. The privacy score

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

is calculated as a combination of partial privacy scores of each profile attribute in terms of its sensitivity and visibility.

The model measure privacy score of a user j for a profile item i as $PR(i, j)$:

$$\mathrm{PR}(i,\ j) = \beta i \times V(i,\ j) \tag{1}$$

where βi is the sensitivity of the profile item and $V(i, j)$ is the visibility of profile item i. So the overall privacy score of a user j is:

$$PR(j) = \sum_{i=1}^{n} PR(i,\ j) = \sum_{i=1}^{n} \beta_i \times \mathrm{V}(i,\ j) \tag{2}$$

The system implemented here is called the naïve method, which serves as a baseline methodology in privacy score computing using sensitivity and visibility. Sensitivity of an item i is computed on basis of the proportion of users that are reluctant to disclose that particular information, and the visibility computation requires the computation of probability. While this model is able to quantify the privacy preference of users, it does not provide any functional control over user data to prevent information access by third party applications.

3.4.2 Privacy recommender model. Ghazinour *et al.* (2013b) proposed a privacy monitor and recommendation system tool that checks users‘ current privacy settings, detects the privacy risks and displays that risk in the user interface. The recommender privacy tool shows the important attributes that can cause privacy disclosure and helps the user to set their privacy settings. They reviewed three key elements of purpose, visibility and granularity to predict the level of privacy risk involved in sharing attributes. Purpose defines the intention of the data provider for how their data can be used after collection. Visibility identifies who can view the provided data. Granularity of data refers to the accuracy of the information given by the user. This model is neither specific to application privacy disclosure nor does it provide any functional controls for limiting third party access. It is more of a general recommender model which helps to increase user awareness about the nature of information being passed on.

3.5 Summary

Most of the research models mentioned above are effective in protecting the privacy of user data to some extent. As thousands of third party applications are already running on Facebook, most of the frameworks are quite difficult to implement without affecting the existing functionalities. The user interface approach gives the user a clear understanding of what they are going to share with the third party developer and enables them to control information leakage. However, the users still have no control over applications in accessing their public profile information. On the other hand, browser add-on models can protect user privacy to a high extent, but the practicality of installing add-ons in browsers is highly questionable. The privacy score calculator and recommender model are good in terms of user awareness in general, but the existing models lack functional mechanisms to assure privacy control from third party applications. In general, we can conclude that the models discussed above do not provide comprehensive framework for notifying privacy risks and controlling data access to protecting user data. Some models are not capable of informing the user about

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

the privacy risks, while some others are hard to implement without affecting the existing applications. A comparison of existing research models discussed in this section is shown in Table VI.

4. Proposed model

To protect users' private information, we propose a new model called *PBAC* which protects user privacy based on the defined permission policies. This model can be applied in comformance with the current Facebook privacy policy to control unnecessary access of user data by third party applications. This model is a combination of interfaces and internal mechanisms which can be adopted by any OSN having similar architecture to Facebook in managing third party applications, without much structural changes.

We concentrate on the following methodologies in our solution:

- practical implementation model based on permissions to manage data access by third party applications that can improve user trust of applications on OSNs;
- simple user interface in which users can have full control over their information without affecting the existing settings; and
- improve user awareness on privacy risks by warning mechanisms before sharing data with third party applications, and alert users through notifications whenever a leakage of information occurs.

Access to information is controlled in the PBAC model by the *Access Control Manager* using a set of permission policies. The model has functional modules in *Application Developer Interface*, *Facebook Server* via API call and *Application User Interface*. Using this model, third party applications work according to the defined permission policy. This model guarantees confidentiality and integrity of user data as users should be able to have complete control over their data, and no one should be able to access it unless explicitly authorized by the user. Furthermore, PBAC model provides improved user awareness by visualization enhancements that emphasize the level of privacy risk on the authentication dialogue box. The main components of the model are shown in Figure 1.

4.1 Access control manager

Access Control Manager is at the heart of PBAC model. It controls the application permissions as well as the user permissions and manages communication between the

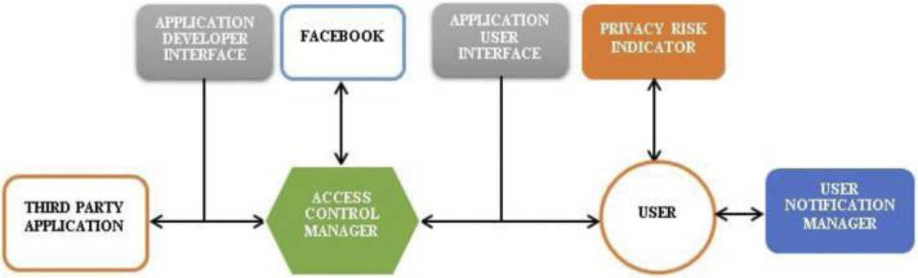

APPLICATION DEVELOPER INTERFACE
FACEBOOK
APPLICATION USER INTERFACE
PRIVACY RISK INDICATOR
THIRD PARTY APPLICATION
ACCESS CONTROL MANAGER
USER
USER NOTIFICATION MANAGER

Figure 1.
PBAC model

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

user and the third party application based on a set of permissions. So basically it stores both user and app permissions and filter the output according to the permission settings.

When a user tries to install an application, the application sends a request to Facebook API to give the user access through the *Access Control Manager* (Figure 2). The *Access Control Manager* checks for the saved attribute permissions associated with that application and shows the attributes with a checkbox requesting the user to allow access in the authentication dialogue box. The user can select attributes to determine the type of information that can be shared with the application, and this selective list is stored as user-permission policy of that individual user for that application.

Once allowed access, the request is handled by the *Access Control Manager,* whenever the application accesses the user‘s profile data. It checks the saved user-permission policy of that user for that application and filters the requested attributes with the permitted attributes and then passes the request to the Facebook API to return the result. The Facebook API only returns the results for the permitted attributes.

Similarly, when an application tries to fetch profile details of a user who is already connected with the application, the request must pass through the *Access Control Manager*. It filters the requested attributes according to the saved user-permission policy, and thus, it prevents unauthorized access and information loss.

4.2 Privacy risk indicator

Privacy Risk Indicator informs users about the risk in sharing sensitive information with the third party applications. We adopt the privacy score measurement developed by Liu and Terzi (2010) and for our privacy risk indicator. Privacy scores are given to each profile attribute in terms of its sensitivity and visibility. It determines privacy risk based on the score and displays it as a coloured bar on top of authentication dialogue box. The higher the sensitivity of information and the wider it spreads, the higher the privacy risk will be.

The privacy settings of user j for profile attribute i is identified as $PR(i,j)$. The privacy risk score is calculated using the naïve method of user perception of the sensitivity and visibility of the attributes which the user is going to reveal. $\mathrm{R}(ij) = 1$ means the user j shared information about the profile attribute i as public, and $\mathrm{R}(ij) = 0$ means that the information about the profile attribute i is made private by the user j.

The overall privacy risk score for user j, $PR(j)$ for all attributes $i_1 \,..\, i_n$, is calculated as:

$$PR(j) = \sum PR(i, j) = \sum \beta_i \times \mathrm{V}(i, j), \tag{3}$$

where β_i is the sensitivity and $\mathrm{V}(i,j)$ is the visibility of attribute i and the range of i varies from $1 \leq \mathrm{i} \leq \mathrm{n}$.

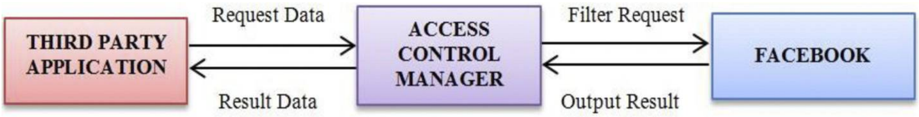


Figure 2.
Access control manager operation

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

The sensitivity β_i is calculated as:

$$\beta_i = \frac{N - |R_i|}{N} \tag{4}$$

where $|R_i| = \mathrm{j}\,\mathrm{R}(ij)$.

The visibility $V(i, j)$ is calculated as:

$$V(i, j) = P_{ij} = Prob\ \{R(i, j) = 1\}. \tag{5}$$

where $Prob\{R(i,j) = 1\}$ is the probability that the value of $R(i,j) = 1$ and $Prob\{R(i,j) = 0\}$ is the probability that the value of $R(i,j) = 0$.

By substituting equation (4) and equation (5) in equation (3), we identify the privacy risk score (Ananthula *et al.*, 2015). As the sensitivity and visibility values must be defined by Facebook on the basis of probability of disclosure, we are assuming these values in our model and convert these values as percentage of disclosure.

In addition to calculating privacy risk score, we added additional risk scores in two exceptional cases which can have serious privacy risks:

(1) when users allow access to their profile information that they have set as private; and

(2) when users share quasi-identifying attributes which can lead to identity disclosure.

If the value of the bar is grey, the information loss is less and thus the privacy risk is average. If the value is high (60 per cent or more), the colour of the privacy risk bar turns to red to indicate that privacy risk in sharing the attributes is high, and warn the user to rethink his access policy.

4.3 Application developer interface

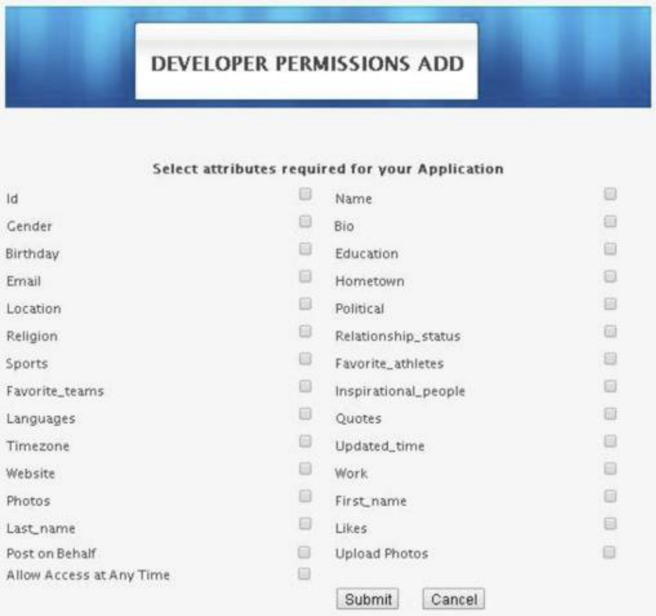
Facebook data usage policy for third party application clearly says "You will only request the data you need to operate your application" (Facebook, 2014b). Therefore, with PBAC model, the developer is provided with a pool of attributes in the *Application Developer Interface* in which he can select the relevant user information and actions, such as post on behalf and upload photos, that are required for the application to run, as shown in Figure 3. The developer then submits the application for approval.

4.4 Application user interface

Our proposed authentication dialogue box design was inspired by the work of Xu *et al.* (2012) in which users have the option to select what information they want to disclose. We focus on authentication dialogue box to give users a clear understanding of what information they are going to share with the third party application. Instead of showing all the attributes, our proposed authentication dialogue box only displays the attributes requested by the application.

According to Beye *et al.* (2012), awareness about privacy can be projected in a more impactful manner by showing users the consequences of their actions. So the privacy risk in sharing sensitive attributes will be shown as an "*i*" mark tooltip, which shows the attribute information on mouse over. The colour scheme of the "*i*" mark projects the user

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)



DEVELOPER PERMISSIONS ADD

Select attributes required for your Application

Id	□	Name	□
Gender	□	Bio	□
Birthday	□	Education	□
Email	□	Hometown	□
Location	□	Political	□
Religion	□	Relationship_status	□
Sports	□	Favorite_athletes	□
Favorite_teams	□	Inspirational_people	□
Languages	□	Quotes	□
Timezone	□	Updated_time	□
Website	□	Work	□
Photos	□	First_name	□
Last_name	□	Likes	□
Post on Behalf	□	Upload Photos	□
Allow Access at Any Time	□		

Figure 3.
Application developer interface

profile privacy setting. Blue "*i*" mark represents the attributes that the user shares with public, orange "*i*" mark represents the attributes shared with friends only, while red "*i*" represents private or sensitive information not shared with others. A screenshot of our authentication dialogue user interface is shown in Figure 4.

The user can set his preferences by selecting the checkboxes of the attributes requested by the application before passing data to the application. The privacy risk calculator, as we mentioned above, calculates the privacy risk percentage, and the output is shown in the privacy risk bar. Another feature in the interface is that of permission reusability giving users the option to save the given permission as his permission policy for future use. A user can have flexibility in managing multiple permission settings with multiple applications. This interface also includes *Allow as Anonymous* button for users to use any third party application without sharing any of profile details.

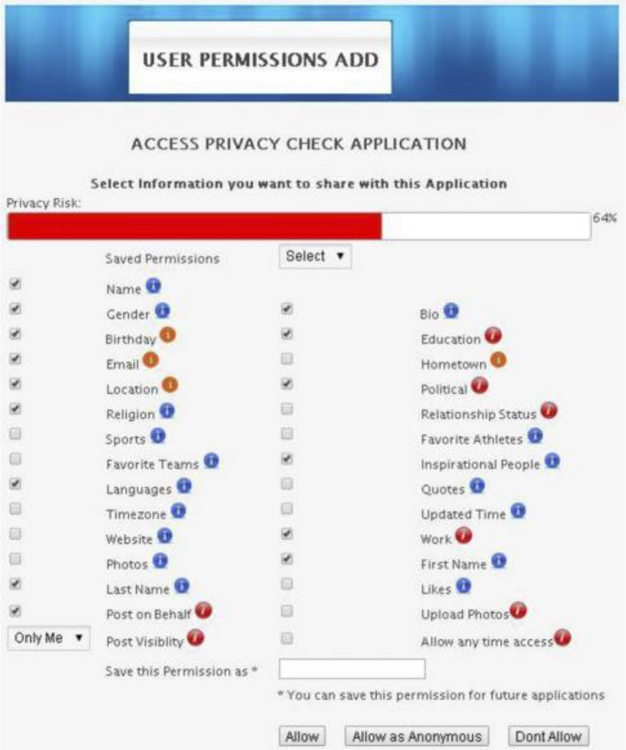
4.5 User notification manager

Hull *et al.* (2011) suggested that information accessed by third party applications should be transparent, and the users should be notified by a warning mechanism. Therefore, in PBAC model, there is a mechanism that notifies a user whenever an application accesses their data. Finally, second degree access by the application is also restricted as the model notifies user's friends about the information accessed by the application, who can then block that application from accessing their data.

4.6 PBAC implementation

To provide complete control and awareness, OSN need to adopt all components of PBAC model to their current architecture. In this section, we describe the implementation of the

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)



USER PERMISSIONS ADD

ACCESS PRIVACY CHECK APPLICATION

Select Information you want to share with this Application

Privacy Risk: 64%

Saved Permissions: Select ▾

☑	Name		
☑	Gender	☑	Bio
☑	Birthday	☑	Education
☑	Email	□	Hometown
☑	Location	☑	Political
☑	Religion	□	Relationship Status
□	Sports	□	Favorite Athletes
□	Favorite Teams	☑	Inspirational People
☑	Languages	□	Quotes
□	Timezone	□	Updated Time
□	Website	☑	Work
□	Photos	☑	First Name
☑	Last Name	□	Likes
☑	Post on Behalf	□	Upload Photos
Only Me ▾	Post Visiblity	□	Allow any time access

Save this Permission as *

* You can save this permission for future applications

Figure 4.
Application user interface

proposed PBAC model components as Web interface with Facebook. Facebook runs a typical LAMP (Linux, Apache, MySQL and PHP) setup. So our proposed model is implemented in HTML Web pages using PHP with a MySQL backend for storing data in a third party server. For validation and privacy risk bar implementation, we used jQuery and Ajax. Along with Facebook SDK library for accessing the Graph API, we used Facebook Query Language which provides SQL-style interface to query user data and retrieve the privacy permission policies.

To implement the developer interface, we used an HTML webpage displaying all the user attributes that third party applications are allowed to access on Facebook. Other than user operational attributes, like post on behalf, upload photos and any time access to user data are also shown in the interface which is optional for the developer. The developer can choose the attributes required by selecting the checkboxes of the corresponding attributes, and the selected attributes along with the application id saved in the database table.

The new authentication dialogue box is designed in a webpage by adapting the current Facebook third party application dialogue page. Basically, all the attributes and operations stored for the application ID are loaded from the database. The *Application User Interface* is displayed to the users, and they need to set a permission policy by selecting the attributes to be shared with that application. The "*i*" mark tooltip and

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

colour scheme is implemented using the jQuery and Ajax for showing the information on mouse over.

The privacy risk progress bar is implemented with the privacy risk algorithm to measure the privacy risk in sharing any sensitive information of the user with the application. As the sensitivity and visibility values cannot be retrieved directly from Facebook, we set the sensitivity and visibility values of the attributes based on various surveys conducted by researches on users privacy disclosure behaviour (Debatin *et al.*, 2009; Delgado *et al.*, 2010; Spiliotopoulos and Oakley, 2013). We stored these values along with each attribute in the database table. When a user selects an attribute, the corresponding values are returned from the database table and the privacy risk score of each attribute is calculated. Then, we calculate the overall privacy score and display it in the privacy risk indication bar.

The user-selected attributes are stored in the database with the application id and the used ID. The same attributes are also saved in the user permission table with the permission policy name along with the user ID if the user provides a valid policy name. The *Allow as Anonymous* button action stores the attribute field as null along with the user ID and application ID. Developer and user permissions are controlled and filtered using the *Access Control Manager* function, which filters the array of attributes requested by the application with the user permitted attributes stored in the database, and returns the allowed attributes that are then passed on to Facebook API to retrieve user details. The result only contains values of the user permitted fields (Figure 5). Furthermore, an alert message in jQuery pop-up box is shown to notify users whenever an application is trying to access their profile information.

PBAC model enforces privacy preferences preset by the user in filtering data. It assists users to understand the privacy risks in sharing sensitive profile information with third parties. We have implemented and thoroughly tested all the functional modules in PBAC model. All the proposed designs interfaces are fully functional. Also, all the functions, queries and other scripts are functioning without any error, and all the modules are working in accordance with the proposed model. To evaluate the efficacy of the PBAC model in avoiding privacy disclosure problem in third party applications, this will be discussed in the next section.

5. Evaluation

In this section, we show that the PBAC model can deliver optimum level of protection of user information on Facebook from third party applications. The evaluation of our

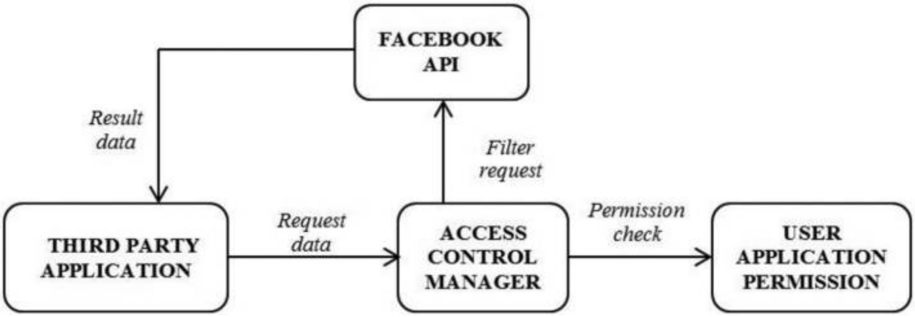


Figure 5. Application user data request operation

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

model is divided into three phases. In Phase 1, we use a case study to describe how third party applications can retrieve user information through Facebook without the user's knowledge or consent. In Phase 2, we evaluate the performance of our proposed model implementation using a set of test cases. In Phase 3, we compare our proposed model with existing frameworks. Our evaluation is based on attribute-based test cases in order to evaluate the unauthorized access to defined attributes with different permissions.

5.1 Case study on Facebook: an analysis

Facebook authentication dialogue box does not reveal the content of the data accessed by the application. In this section, we evaluate the privacy behaviour of the existing functionality using a case study. The objective is to analyse the data collecting behaviour of third party applications and raise user awareness of this behaviour to compare it with our PBAC model later.

Initially, we create an application called *Digital Resume* written in Javascript and PHP. This application can fetch profile information of any user who installs the application. In addition, we also create a Facebook user account with the profile privacy settings as shown in Table I. It shows the information that user Alex is willing to share with everyone along with the information that he wants to keep to himself.

User Alex installs the application through the Facebook app URL. After Alex gives access to the application, it fetches some of his details and makes a resume that contains his information. The requested attributes along with his profile privacy settings and the output result are shown in Table II.

As the table above shows, in the data successfully collected by the application, we can see that the privacy of the user is being violated. Based on the result, we see that the application can get access to user data, including unpublished data, and there is no proper identification before sharing these details with third party applications. Furthermore, the application developer can access Alex's information as well as his friends' information any time once Alex has installed the application. Neither Alex nor his friends are notified by alerts when the application is trying to access their data.

5.2 Test cases of PBAC model

We will evaluate our PBAC model implementation by using a set of test cases. As mentioned in the previous analysis, a newly created Facebook application, *Digital Resume*, is used to access the user's profile information to generate information resume. The four main functional components are: *Application Permission*, *User Permission*, *Privacy Risk Bar* and *Access Control Manager*. They are explained in four test cases with a user account named Alex on the newly created application. Finally, we analyse the integrated model using two users with different privacy settings accessing two different applications with different functionalities.

Table I.
Privacy settings of sample Facebook user – Alex

User	Public	Friends or Friends of Friends	Only Me
Alex	Name Gender Religion	Email Birthday Hometown Location	Education Work Relationship status

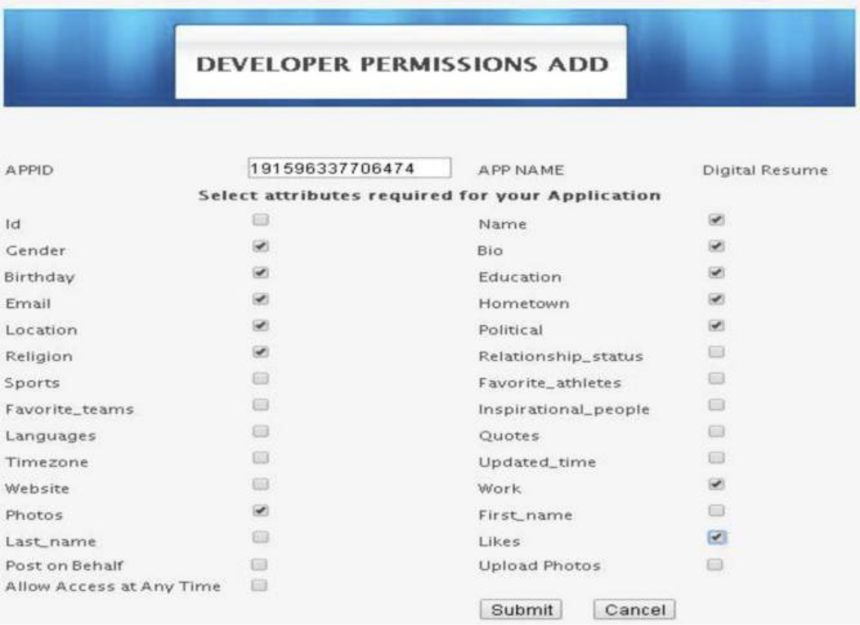
Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Table II. Behaviour of sample Facebook application – digital resume

Application	Requested data	Privacy settings	Output
Digital resume	Name	Public	Name
	Gender	Public	Gender
	Email	Friends	Email
	Birthday	Only Me	Birthday
	Location	Only Me	Location
	Hometown	Friends	Hometown
	Education	Friends	Education
	Work	Friends	Work
	Religion	Only Me	Religion
	Relationship status	Public	Relationship status
	Profile picture	Friends	Profile picture
	Tagged photos	Friends	Tagged photos
	Likes	Public	Likes
	Friends	Friends	Friends

In the PBAC model, the developer needs to select the user attributes stored in Facebook when creating and integrating the application (Figure 6). When the user installs this application, the new authentication dialogue box will request permission to access the attributes for that application as shown in Figure 7. The test cases for *Application Permission* and *User Permission* are shown in Table III.

As mentioned in the previous section, we use *Privacy Risk Indicator* to inform the user about the privacy risk level of the private information that is being revealed to the third



DEVELOPER PERMISSIONS ADD

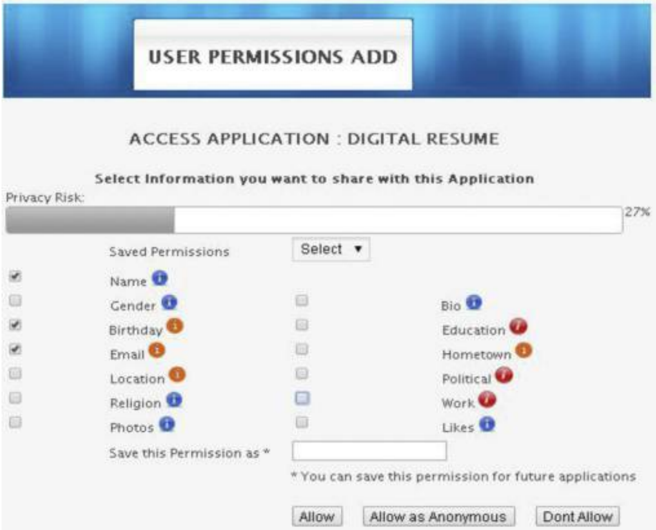
APPID	191596337706474	APP NAME	Digital Resume

Select attributes required for your Application

Id	☐	Name	☑
Gender	☑	Bio	☑
Birthday	☑	Education	☑
Email	☑	Hometown	☑
Location	☑	Political	☑
Religion	☑	Relationship_status	☐
Sports	☐	Favorite_athletes	☐
Favorite_teams	☐	Inspirational_people	☐
Languages	☐	Quotes	☐
Timezone	☐	Updated_time	☐
Website	☐	Work	☑
Photos	☑	First_name	☐
Last_name	☐	Likes	☑
Post on Behalf	☐	Upload Photos	☐
Allow Access at Any Time	☐		

Figure 6. Application developer interface with selected attributes

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)



USER PERMISSIONS ADD

ACCESS APPLICATION : DIGITAL RESUME

Select Information you want to share with this Application

Privacy Risk: 27%

Saved Permissions Select ▾

☑ Name
☐ Gender ☐ Bio
☑ Birthday ☐ Education
☑ Email ☐ Hometown
☐ Location ☐ Political
☐ Religion ☐ Work
☐ Photos ☐ Likes

Save this Permission as *

* You can save this permission for future applications

Figure 7.
Application user interface with allowed attributes

party application. For the implementation, we use the "*i*" mark tooltip. The test case for *Privacy Risk Indicator* is shown in Table III. The core component of the model, *Access Control Manager*, manages the flow of user information from Facebook to the third party application in accordance with the defined permissions. The test case for this component is also shown in Table III.

Finally, we conduct integration testing for our model using two user accounts and two different applications. For this purpose, we create another application called *Birthday Card*. This application requests access to user data and seeks permission to upload photo and post on the user's timeline. A new Facebook user Anna is also created with a different set of privacy settings as shown in Table IV.

The first user, Alex, accessed both applications with different permissions. On the other hand, Anna, who has a different profile privacy setting, installs *Digital Resume* application with a different set of permissions and installs the *Birthday Card* using *Allow as Anonymous* button. The integrated test cases for both users accessing the two applications are shown in Table V.

The result (Table V) demonstrates that by using our privacy indicator, a user can see a potential privacy risk and decide to act as an anonymous user as in Anna's case. The *Access Control Manager* along with user interfaces provides users a full control over their profile information when accessing third party applications in Facebook.

5.3 Comparison with the existing frameworks

As all the existing models that we discussed are not specifically built for protecting user privacy from third party applications, it is difficult to compare them in terms of functional components with our model that focuses on this issue. Therefore, the comparative analysis is conducted on bases of some metrics to measure the model's usefulness rather than their functional components. The main factors in choosing a best model for controlling privacy leakage through Facebook third party applications is high

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Table III. Test case evaluation

Test case	Application permission	User permission	Privacy risk bar	Access control manager
Purpose	Store the attributes required and show only that attributes in user authentication dialogue	Select attributes to allow permissions for the installed application and for future apps	User awareness	Manage the data flow according to the user permission set for the application
Pre-requisites	Store Facebook fields in the database Created an application called digital resume	Install the digital resume application	Select attributes	The application is accessing user details who installed the application
Test data	Name Gender Bio Birthday Education Work Email Hometown Location Political Religion Photos Likes	Name Gender Bio Birthday Education Work Email Hometown Location Political Photos Likes	Name Email Birthday	Name Gender Bio Birthday Education Work Email Hometown Location Political Photos Likes
Steps	Access the application permission UI. Select required attributes	Access authentication dialogue box. Select attributes that need to give permission	Give permission to attributes	Application is accessing the user details

(*continued*)

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Table III.

Test case	Application permission	User permission	Privacy risk bar	Access control manager
Expected output	Name Gender Bio Birthday Education Work Email Hometown Location Political Religion Photos Likes	Name Email Birthday	27%	Name Email Birthday
Actual output	Name Gender Bio Birthday Education Work Email Hometown Location Political Religion Photos Likes	Name Email Birthday	27%	Name Email Birthday

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

protection, high awareness support facility and low complexity (Besmer *et al.*, 2009; Xu *et al.*, 2012).

Third party applications hosted in the external servers are not always trustworthy. Malhotra *et al.* (2004) identified sensitive data collection, lack of user control over their data and lack of awareness as the main privacy concerns. Cheng *et al.* (2013) suggested that most OSNs adopt a simple all-or-nothing strategy in managing privacy. So *Protection* in this context means that users should be able to connect with third party applications to enjoy the services while maintaining a complete control on their data (Shehab *et al.*, 2012). The model should prevent information leakage from the user's profile accessed by third party applications, and thus ensure protection from identity disclosure and attribute disclosure (Albesher and Alhussain, 2013). Additionally, the users should be able to prevent the application from posting on their timeline or upload photos on their behalf.

Privacy infringements on Facebook usually happen due to lack of understanding among users about the risks of information leakage (Chen *et al.*, 2009). By *Awareness*, we mean that the model has to enhance users‘ awareness on what information the application is requesting and the implications of these requested attributes in terms of privacy. A warning mechanism is needed to alert users when the application requests access to sensitive private information and inform them about the privacy risk involved in sharing sensitive data (Mohtasebi and Borazjani, 2010; Wang *et al.*, 2011; Xu *et al.*, 2012). Additionally, the users should be alerted by notifications each time an application is accessing their data (Hull *et al.*, 2011).

Complexity is the measure of difficulty in implementing the model in its current form. Wang *et al.* (2011) suggested that privacy protection model should be simple and easy to manage and implement. The model should be self-contained and must provide all possible functionalities to protect user privacy with an easy to adopt architecture, which can cope with the current OSN architecture (Besmer *et al.*, 2009). The authentication dialogue interface should be easy for users to understand regardless of their technical skills, and have a simple mechanism for users to manage their privacy preferences (Good *et al.*, 2007; Luo *et al.*, 2009; Wang *et al.*, 2011).

Finally, to indicate the degree of satisfaction with their performance, we rank all the models that we discussed in the Section 4 as *High*, *Average* or *Low* in terms of *Protection*, *Awareness* and *Complexity*. We use judgemental approach to rank these models and present a comparison chart based on these three main factors below in Table VI.

Some of the models, especially the component-based model and the CPM interceptor API model, can ensure high protection, but there is high level of complexity in adopting this model, as it affects the existing application operations, and the feature of user awareness is also not fully supported. The three UI models of four provide high user awareness support on information disclosure. However, the protection is average and

User	Public	Friends/Friends of Friends	Only Me
Anna	Name Gender Education Work	Email Relationship status	Hometown Religion Birthday Location

Table IV.
Privacy settings of sample Facebook user – Anna

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Table V.
Integrated model test case

App	Requested data	Allowed	Anna Output	Risk (%)	Allowed	Anna Output	Risk (%)
Digital resume	Name Gender, Bio, Birthday, Education, Work, Email, Hometown, Political, Interest, Religion, Photos, Likes,	Name, Email, Birthday	Name, Email, Birthday	27	Name, Hometown, Friend list	Name, Hometown, Friend list	37
Birthday card	Name, Gender, Birthday, Photo-upload, Post on timeline	Name, Photo upload, Post on timeline	Name, Photo upload, Post on timeline	22	Anonymous	Anonymous	0

Model	Protection	Awareness	Complexity
Component-based model	High	Average	High
Differential privacy model	Average	Average	High
CPM interceptor API model	High	Average	High
Granular framework	Low	Average	Average
Authentication dialogue UI model	Average	High	Average
Privacy by redesign UI model	Average	High	Average
User notification model	Average	High	Low
FBSecure – model	Average	Average	Average
Sudo Web – model	Average	Low	Average
Privacy score computing model	Low	High	Average
Privacy recommender model	Low	High	Average
Permission-based access control (PBAC) model	High	High	Low

Table VI. Comparison of existing research models

some of them are not user-friendly. Most of them are accompanied with practical difficulties in implementation. Of these, the user notification model is a model of less complexity with a functionality of high awareness but provides average protection. The browser extension models are less practical in ensuring full user information privacy, and these models do not provide high user awareness support. Finally, the privacy score and recommender models support a high level of user awareness about information sharing, but there is no operational method to control access from third party applications into user data.

In comparison with other models, our PBAC model ensures a high level of protection and creates awareness among users about privacy risks before they share information with a third party application. The *Access Control Manager* controls the flow of information from Facebook to third party applications by filtering the requested attributes according to the permission setting defined by the user. The "*i*" mark tooltip and privacy risk bar alert the users about the privacy risks before sharing the details with third party applications. The proposed model fully uses Facebook base architecture and interfaces without affecting the performance, which makes the complexity of adopting this model reasonably low. Once Facebook adopts this model, app developers can only create apps within the limits of the proposed structure and only access information of users who are willing to disclose. There are benefits for both users as well as the OSN because it not only protects user's privacy but also helps in building user trust in the OSN.

5.4 Limitations

Currently, we have implemented our proposed PBAC model on Facebook, which is the largest social networking site and most active platform for third party applications (Luo *et al.*, 2009). However, we do not foresee any technical difficulties in implementing this model in other social networking sites, which have a similar architecture and functionality as Facbook for managing the third party applications. We leave such implementations and evaluations to future work. Another limitation is that Facebook already has thousands of applications and millions of users connected to it. As the user preferences of our model are not set for applications that are already active on Facebook, the permission-based data filtering is not applicable for those applications. Although by

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

adopting the authentication dialogue user interface, the user data protection can be ensured for users accessing those existing applications in future.

6. Conclusion and future work

Preserving privacy in OSNs is always a challenge especially when numerous features and applications are continually added. In this paper, we reviewed different types of privacy disclosures that might happen on OSNs through third party applications, and the consequences involved in sharing sensitive personal information. Even if Facebook provides some guidelines on information usage, we have found that once third party applications acquire access the user profile, the application developers can retrieve and collect users' private information at any time without the user's knowledge. Currently, Facebook has no holistic mechanism to control how the developers of third party application use this sensitive information.

Even though their limitations were not discussed in detail, the analysis of existing frameworks discussed in the Section 4 shows that there is lack of a simple and widely acceptable protection scheme for privacy disclosure by third party applications in OSN. Building on the existing models, we have devised our solution with a new framework, PBAC model, to give users complete control over their data. They can decide which information they want to safeguard and which information they wish to share with third party applications in OSNs. Furthermore, it provides the users a clear understanding of the privacy risk involved in sharing sensitive data.

To demonstrate the functionalities of our model, we implemented a proof-of-concept prototype using Web interfaces connected with Facebook API. We conducted user studies on the existing functionalities to identify privacy challenges and evaluated the efficacy of our proposed model using test cases. Finally, we compared our model with existing models in terms of protection, user-awareness support and complexity. Based on our assessment, we concluded that the proposed model ensures high protection, high user awareness and low complexity. Overall, we can confidently conclude that this model is more efficient than existing ones and can be used to safeguard user privacy on third party applications, and thus benefit both the OSN as well as its users.

This paper leads us to consider areas in which we can extend the ideas of this research and integrate our PBAC model to existing applications in OSNs. In this paper, we evaluated our application using test cases. In a future work, we would like to do a usability testing and a user experience survey to give a more robust indication of the utility of the PBAC model. To further extend this research, we hope to examine how OSNs can control external applications, even already installed ones, from accessing user information by implementing our model. Furthermore, we need to examine how this model can help users in protecting their privacy from disclosing their information not only to third party applications but also from direct exposures of personal information. We hope that the analysis accomplished in this paper and also the limitations identified here give a clear picture of how our proposed model can offer an alternative solution for privacy disclosure problem from third party applications on OSNs.

References

Acquisti, A. and Gross, R. (2006), "Imagined communities: awareness, information sharing, and privacy on the Facebook", *Proceedings of the 6th International Workshop on Privacy Enhancing Technologies*, *Cambridge*, *28-30 June*, pp. 36-58.

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Acquisti, A., Gross, R. and Stutzman, F. (2012), "Faces of Facebook: privacy in the age of augmented reality", paper presented at BlackHat USA, available at: www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf (accessed 27 May 2014).

Albesher, A. and Alhussain, T. (2013), "Privacy and security issues in social networks: an evaluation of Facebook", *Proceedings of the International Conference on Information Systems and Design of Communication, ACM, New York, NY*, pp. 7-10.

Aldhafferi, N., Watson, C. and Sajeev, A.S.M. (2013), "Personal information privacy settings of online social networks and their suitability for mobile internet devices", *International Journal of Security, Privacy and Trust Management*, Vol. 2 No. 2, pp. 1-17.

Ananthula, S., Abuzaghleh, O., Alla, N.B., Chaganti, S.B., Kaja, P.C. and Mogilineedi, D. (2015), "Measuring privacy in online social networks", *International Journal of Security, Privacy and Trust Management*, Vol. 4 No. 2, pp. 1-9.

Anthonysamy, P., Rashid, A., Walkerdine, J., Greenwood, P. and Larkou, G. (2012), "Collaborative privacy management for third-party applications in online social networks", *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media, Lyon*.

Besmer, A., Lipford, H.R., Shehab, M. and Cheek, G. (2009), "Social applications: exploring a more secure framework", *Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA*.

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. and Tang, Q. (2012), "Privacy in online social networks", in Abraham, A. (Ed.), *Computational Social Networks: Security and Privacy*, Springer, Heidelberg, pp. 87-114.

Chaabane, A., Ding, Y., Dey, R., Kaafar, M.A. and Ross, K.W. (2014), March), "A closer look at third-party OSN applications: are they leaking your personal information?", *Proceedings of the 15th International Conference on Passive and Active Measurement, Los Angeles, CA*, pp. 235-246.

Chen, S. and Williams, M.A. (2009), "Privacy in social networks: a comparative study", *Proceedings of the Pacific Asia Conference on Information Systems, Hyderabad*.

Cheng, Y., Park, J. and Sandhu, R. (2013), "Preserving user privacy from third-party applications in online social networks", *Proceedings of the 22nd International Conference on World Wide Web Companion, Rio de Janeiro*, pp. 723-728.

Clark, L.A. and Roberts, S.J. (2010), "Employer's use of social networking sites: a socially irresponsible practice", *Journal of Business Ethics*, Vol. 95 No. 4, pp. 507-525.

Debatin, B., Lovejoy, J.P., Horn, A.M.A. and Hughes, B.N. (2009), "Facebook and online privacy: attitudes, behaviors, and unintended consequences", *Journal of Computer-Mediated Communication*, Vol. 15 No. 1, pp. 83-108.

Delgado, J., Rodriguez, E. and Llorente, S. (2010), "User's privacy in applications provided through social networks", *Proceedings of the 2nd ACM SIGMM Workshop on Social Media*, Firenze, Italy, pp. 39-44.

Emanuel, L., Bevan, C. and Hodges, D. (2013), "What does your profile really say about you?: Privacy warning systems and self-disclosure in online social network spaces", *Proceedings of the Extended Abstract 13th International Conference on Human Factors in Computing Systems, Paris*, pp. 799-804.

Europe versus Facebook (2015), "Facebook application, Vienna University of Economics", available at: http://app.europe-v-facebook.org/ (accessed 10 September 2015).

Facebook (2014a), "Key facts", available at: https://newsroom.fb.com/key-facts/ (accessed 20 March 2014).

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)

Facebook (2014b), "Platform policy", available at: https://developers.facebook.com/policy/ (accessed 20 March 2014).

Felt, A. and Evans, D. (2008), "Privacy protection for social networking platforms", *Proceedings of the Workshop on Web 2.0 Security and Privacy*, *Oakland, CA*, pp. 1-8.

Ghazinour, K., Matwin, S. and Sokolova, M. (2013a), "Monitoring and recommending privacy settings in social networks", *Proceedings of the Joint EDBT/ICDT Workshops*, *Genoa*, pp. 164-168.

Ghazinour, K., Matwin, S. and Sokolova, M. (2013b), "YourPrivacyProtector: a recommender system for privacy settings in social networks", *International Journal of Security, Privacy and Trust Management*, Vol. 2 No. 4, pp. 11-25.

Good, N.S., Grossklags, J., Mulligan, D.K. and Konstan, J.A. (2007), "Noticing notice: a large-scale experiment on the timing of software license agreements", *ACM Conference on Human Factors in Computing Systems*, pp. 607-616.

Hasan, M.R. (2013), "Emergence of privacy conventions in online social networks", *Proceedings of the International Conference on Autonomous Agents and Multi-Agent Systems*, *Saint Paul, MN*, pp. 1433-1434.

Hull, G., Lipford, H.R. and Latulipe, C. (2011), "Contextual gaps: privacy issues on Facebook", *Ethics and Information Technology Journal*, Vol. 13 No. 4, pp. 289-302.

Kontaxis, G., Polychronakis, M. and Markatos, E.P. (2011), "SudoWeb: minimizing information disclosure to third parties in single sign-on platforms", *Proceedings of the 14th International Conference on Information Security*, *Xi'an*, pp. 197-212.

Liu, K. and Terzi, E. (2010), "A framework for computing the privacy scores of users in online social networks", *Journal of ACM Transactions on Knowledge Discovery from Data*, Vol. 5 No. 1.

Luo, W., Xie, Q. and Hengartner, U. (2009), "FaceCloak: an architecture for user privacy on social networking sites", *Proceedings of the International Conference on Computational Science and Engineering*, *Vancover, BC*, Vol. 3, pp. 26-33.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Journal of Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Mohtasebi, A. and Borazjani, P.N. (2010), "Privacy concerns in social networks and online communities", paper presented at the VALA2010 Conference, available at: www.vala.org.au/vala2010/papers2010/VALA2010_62_Mohtasebi_Final.pdf (accessed 25 May 2014).

Shehab, M., Squicciarini, A., Ahn, G.J. and Kokkinou, I. (2012), "Access control for online social networks third party applications", *Journal of Computers & Security*, Vol. 31 No. 8, pp. 897-911.

Singh, K., Bhola, S. and Lee, W. (2009), "xBook: redesigning privacy control in social networking platforms", *Proceedings of the 18th Conference on USENIX Security Symposium*, *Montreal*, pp. 249-266.

Spiliotopoulos, T. and Oakley, I. (2013), "Understanding motivations for Facebook use: usage metrics, network structure, and privacy", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3287-3296.

Steel, E. and Fowler, G.A. (2010), "Facebook in privacy breach", *The Wall Street Journal*, 18 October, p. 1.

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R., Lampe, C. and Heinz, H. (2012), "Privacy in interaction: exploring disclosure and social capital in Facebook", *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media*, pp. 330-337.

Sweeney, L. (2002), "Achieving k-anonymity privacy protection using generalization and suppression", *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10 No. 5, pp. 571-578.

Tuunainen, V.K., Pitkanen, O. and Hovi, M. (2009), "Users' awareness of privacy on online social networking sites – case Facebook", *Proceedings of the Bled Conference*, Bled.

Venkatesan, K.G.S., Mondal, K. and Kumar, A. (2013), "Enhancement of social network security by third party application", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3 No. 3, pp. 230-237.

Viswanath, B., Kıcıman, E. and Saroiu, S. (2012), "Keeping information safe from social networking apps", *Proceedings of the ACM Workshop on Online Social Networks*, Helsinki, pp. 49-54.

Wang, N., Xu, H. and Grossklags, J. (2011), "Third-party apps on Facebook: privacy and the illusion of control", *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, *Cambridge, MA*.

Westin, A.F. (1967), *Privacy and Freedom*, Atheneum, New York, NY.

Xu, F., Michael, K. and Chen, X. (2013), "Factors affecting privacy disclosure on social network sites: an integrated model", *Electronic Commerce Research Journal*, Vol. 13 No. 2, pp. 151-168.

Xu, H., Wang, N. and Grossklags, J. (2012), "Privacy by redesign: alleviating privacy concerns for third-party applications", *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL.

Zheleva, E., Terzi, E. and Getoor, L. (2012), *Privacy in Social Networks*, Morgan Claypool, Lexington.

Corresponding author
Sarath Tomy can be contacted at: ssarathtomy@students.latrobe.edu.au

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:36 09 November 2016 (PT)