Provision of Overcoming the Weakness of OAuth 2.0 Protocol in Online Social Networking

[1] Anu Phogat,[3]A K Sujatha
Faculty of Engineering
Christ University
Bengaluru, India
[1]Anu.phogat@mtech.christuniversity.in
[3]sujatha.ak@christuniversity.in

[2]Il Kon Kim
School of Computer Science and Engineering
Kyungpook National University
Daegu, Republic of Korea
[2]ikkimgg@gmail.com

Abstract**—** The Open Authorization Protocol (OAuth 2.0) was introduced to provide secure and efficient method for providing authorization to the third party applications without sharing user’s credentials. Major social internet players like Facebook, Google and Twitter implement their API’s based on this protocol for enhancing the user experience of social sharing and sign-on. However OAuth doesn’t provides the necessary fine-grained access control or any suggestions. We have proposed an enhancement to the OAuth 2.0 authorization which will provide provision of fine grained authorization suggestions to the users while granting permission to the third party applications in online social networking. Our multi criteria suggestion based model method will utilizes user-based, application based, category-based combination filtering systems. Our category-based combination filtering system is based on decision made by the previous users and the application based permission requests for enhancing the user’s privacy control. We have provided a provision for strengthening the OAuth 2.0 protocol in online social networking websites by proposing OAuth 2.0 extension as a browser based extension which allows various users to compose their privacy settings at the time of installing third party applications.

Keywords- *OAuth 2.0; Social Networking; Permission based model; Privacy.*

*****

I. INTRODUCTION

With the increase of internet user, online platforms has attained rich grounds for the third party applications which utilize the user’s online data for providing various kinds of services. For example, around seven million third party applications on Facebook, its users install application more than 20 million times per day [13].Open standards and development tools of the third party software’s immensely provides internet users to manage their privacy data, identity along with the confidentiality. World Wide Web consortium’s (W3C) defines an open platform for the privacy preferences which lets the websites for conveying their privacy policies in computer readable format. Facebook, Google, Twitter are the major internet players of online social networking providing open application interface giving the access to third party application for accessing the end user resources.

The OAuth 2.0, an open standard protocol for authorization has the ability of providing users a platform where they can easily share their resources and information with the third party applications. For example, its framework might allow sharing of photographs from primary web based photo sharing scheme so that the third party photo printing services can access the permitted photographs easily [3]. In today’s scenario Facebook is one of the most popular online social services which represents the largest OAuth 2.0 implementation providing mechanism for third party web based application to access Facebook user identity, private data and their resources.

OAuth 2.0 has implemented this by using a data structure, called as token, that disjoint the access right from the client login credentials which is well discussed in RFC6749 and RFC6819[1][2]. Moreover, OAuth 2.0 specification defines how to handle delegated authorization in a variety of situations such as client-server web applications, mobile applications and desktop applications defining four client profiles: user agent, web server, native application and the autonomous profiles where the web server profiles is broadly implemented and deployed by various service providers on web like Google, Twitter, Facebook and Yahoo!!The software developers of third party targeted for improvement for users privacy and security while using their own extensible frameworks which are available in chrome, Mozilla Firefox and other web browsers. Mainly browsers extensions are used for protecting users from various unwanted advertisements, malicious software’s installations and hijacking user’s credential. Indeed, Joshi et al [4] provisions a browser plugin which tries to resolve the problems of man in middle attacks prevalent in modern phishing attacks while combining the relationship between the browsers based extensions and standards should be provisioned. We provided our research proposal in providing suggestion based model which enables the users to make their own privacy base decisions at the time of accessing third party application installation. These suggestions or judgements helps users for attaining confidence in acquiring their own decisions for Obtaining especially when many privacy requests are ambiguous or uncertain and doesn’t reflects their proper role of access requests. Our aim is to provide a provision which Helps OAuth 2.0 resource owners to use to use online social networking more securely by using our suggestion based model. It also facilitates the users which can grant or deny the requests according to its priorities or acceptance of sharing resources among others. This will provide more prominent way of using open authorization in a more secure and a user friendly manner which help OAuth providers to gain more capability of usage over Internet.

II. RELATED WORK

Establishing tools which provides exquisite control over user private data is a highly emerging problem in online platforms specifically in social networking area like Facebook, twitter, my space, liked in) [5],[6],[7],[8]. Such studies shows that users concern about their privacy on social networks but most users do not follow strict privacy settings on their online social profiles due to poor understanding of what privacy controls are available to them. Our paper focuses on providing a usable tool via browser extension which allows users to understand easily and provides more secure platform to use. We achieve this by utilizing OAuth 2.0 authorization protocol flow and giving a seamless experience to users for protecting their private data available on online social media. Fang and LeFevre's work provides the value for providing highly accurate privacy settings with less user's inputs [9]. Our implemented browser extension is not only based on real user data but also involves user capability of applying their desired privacy decisions to their real online profile. We also note that using a machine learning technique is not optimal in many situations parameters where the instant privacy suggestions are required like in Facebook when users install third party application with in their social networks.

Kelly et al. [11] research notifies exception where the authors demonstrated the advantage of combining collaboration among a user population in the suggestion of an individual user's privacy policies. They also proposed an incremental model for augmenting a user policy over time. We found this approach is not optimal for dealing with the third party applications that once installed, can crop the user's private social network data. Moreover optimal and instant privacy protection model should be given to users at the installation time which we have achieved through our browser extension.

Goecks et al. [12] explores the various measures and effects of community data in the domains of firewall policy configuration and the management of web browser cookies. We found their research indicates user's utilization of community data in making their privacy descisions.they proposed two approaches for reducing the effects and we believe the can complement our work.

Shehab et al [10] proposed an access control framework which allows users to specify their data attributes to share with applications which demands many changes to the existing authorization models and also requires developers to go through a prominent process of deployment model. Our proposed framework consolidate seamlessly into existing authorization model and requires no additional efforts from the developers as well.

III. PROPOSED OAUTH 2.0 FLOW

In this section, we presented a detailed overview of our proposed protocol flow. An extension to OAuth 2.0 authorization code flow is developed by adding two new modules into the authorization flow which are discussed below:

1) Providing a provision to permission guide which helps in guiding the users by permissions which are requested, and shows them a set of suggestions or recommendations whenever requested for permissions, and

2) A suggestion services that retrieves a set of suggestions for requested permission.

Our OAuth 2.0 extension model has focused on step "(A)" of the authorization flow in the OAuth 2.0 protocol. We have amended step "(A)" to make a six stage process showing figure1 and explained the following steps which are as follows:

(A1). Firstly, the client redirects the browser to the user's authorization endpoint by starting a request URI which has the scope parameter.

(A2). The permission Guide extension capture the scope value from request uniform request identifier i.e. URI and determine the requested permissions which grants user to choose a subset of permission requested.

(A3). The permission guide extension requests set of suggestions on the determined permissions. This can be achieved with passing the set of permissions by the user to our suggestion services.

(A4). The suggestion services returns to a set of suggestions for the permissions requested by web clients.

(A5). While using these set of suggestions, the extension provide the permissions with their respective suggestions in a more user friendly way.

(A6). Then our permission guide extension will redirects the end user's browser to the new request URI with the new scope available to the user while giving options which may choose to modify requested permissions as well.

3.1 Permission Guide:

We have provided a browser based extension which integrates into the authorization flow processes of OAuth 2.0 by attaining the scope parameter values within the request URI which is generated by a third party application provider. After capturing the scope, the extension parses the requested permissions and present them. Also extension allows users to select the requested permissions by checking or unchecking the individual permissions where the checked permission resulting to grant permission to the third party application and unchecked introduces to block or deny the access. If the user desires to allow the access to post her wall/access my profile information/send me email/accessing my basic information but denying or restricting permission by users results into blocked from the services as well. We specifies that using a subset of permissions requested can affect the functionality of third

Party application once installed. It also collects the user's decision on the requested permissions which leads to generate the data set of decisions to be used in our suggestion base model. Once the user sets their decisions, they are uploaded to our servers once a user set their desired permissions by clicking button. The data uploaded to our servers includes the app_id, requested _perms, decision,

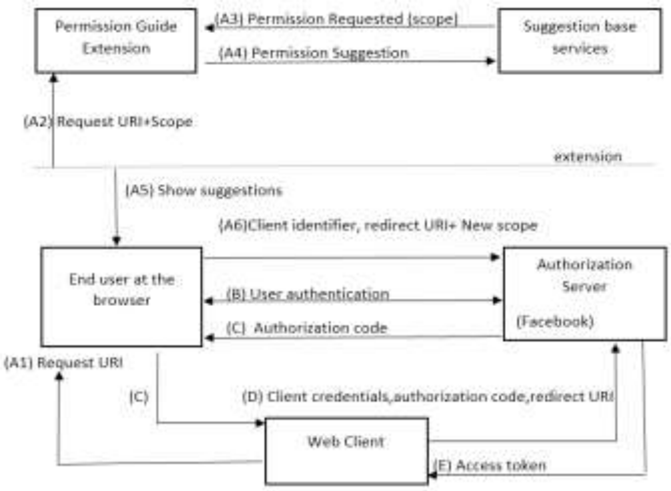


Fig.1 Proposed method of OAuth 2.0 flow

Recommendation or the suggestions. App_id is assigned by the service provider, requested _perms is the scope of permissions requested by third party application, but the decision are individual users decisions which can be granted or denied on each requested permissions. Our mission is to provide a simple user interface for interaction and permitting requests involving users to make their own decisions and providing guidance for awareness towards their privacy control mechanism.

3.2 Suggestion Based Model:

We propose a suggestion base service component which extends upon our permission guide extension. Also, a user can makes a decision on a permission for an application. An application which will be requesting permissions is mapped to a set of all decisions made by the user.

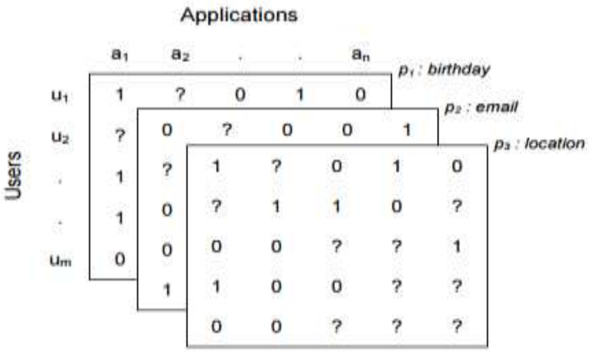


Fig.2. A three permissions model, based on the decisions made by user on application per requests

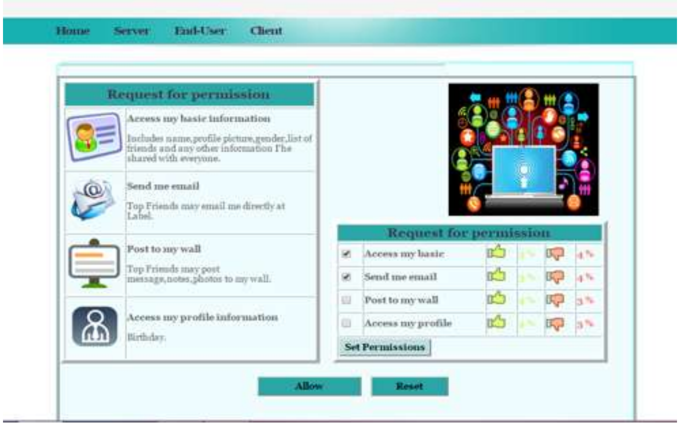
C. Combination Filtration:

Our model represents the multiple criteria suggestions base model where the user's recommendations are calculated accordingly to criterion. Our model provisions set of permissions as a set of criterion like permissions represents an individual criteria inside the model. Providing multiple criteria's approach called as multicriteria is accepted to our model and decision are made per permissions instead of taking by application. User's makes decisions on an application based on individual permission. Our model provides suggestion or recommendations to users which helps them for making decisions in future.

For example Fig.2 shows taking p1=birthday, p2= email, p3=located area which represents a single criteria inside three criteria model. Here u1, u2, u3…. $u_{n\text{ are}}$ the users where u1 is Alice who installed application a1 among a1, a2, a3…a_n which requests access to the permissions like birthday, emails, location, post where d_1=grant and d_3=deny. A symbol "?" represents Alice yet have not decided its decision that has to be made by him.

IV. EXPERIMENTAL ANALYSIS

We have evaluated our proposed OAuth 2.0 extension using the Facebook as a targeted platform, keeping in mind that our method is also applicable to other OAuth 2.0 platforms. Facebook is an optimal target since its abundant popularity in usage by users involving around 500 million active users, and its extensive directory for third party application [13]. For evaluating our proposed method we have implemented two components introducing permission guide and a suggestion base services.



Request for permission

Access my basic information

Includes name,profile picture,gender,list of friends and any other information I'he shared with everyone.

Send me email

Top Friends may email me directly at Label.

Post to my wall

Top Friends may post message,notes,photos to my wall.

Access my profile information

Birthday.

Request for permission

☑	Access my basic	👍	[illegible]	👎	4 %
☑	Send me email	👍	[illegible]	👎	4 %
☐	Post to my wall	👍	[illegible]	👎	3 %
☐	Access my profile	👍	[illegible]	👎	3 %

Fig.3. Showing permission guide user interface (UI)

1. Permission guide.

We have proposed a permission guide which was implemented as a browser extension for Chrome, Firefox browsers by using combination of XML user interface language, API's and JavaScript for the Chrome browser. The extension we have tested on latest Firefox and chrome browsers on windows 7 machines. After installation the extension resides with the user's browser and start checking, waits for the Facebook application to start. While Facebook application installations process is detected extension will activate and present the user. A permission request for Facebook applications can be easily identified by substring as permissions.request or by facebook.com/dialog/permissions.request. When request is detected, the extension will find for the type of request issued.

2. Suggestion base guide:

It involves the solution running on apache server with MySQL for the database storage. We are running the service on desktop machine running windows 7, with 4GB RAM and a 2.0 GHz

Intel Xeon CPU. Our suggestion service applies the suggestion based schema with the help of two API methods which is used in our extension. The first API method is GetSuggestions methods which will accepts app_id and the set of requested permission altogether. After that it will returns a set of suggestions in JSON format which helps the suggestion value to each of the permission. And the second method is called as API method which takes app_id as a set of requested permissions where a set of user's decisions on these permissions, and the set of suggestion values also will be displayed at the decision making.

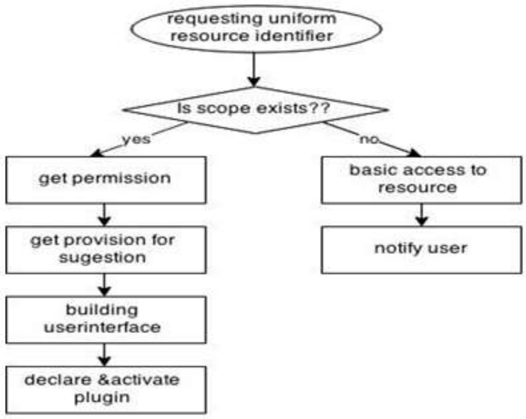


Fig. 4. Handling the permission requests.

Our focus is on extended permission requests for evaluation purpose because those are permissions which are easily customizable by the various users on the platforms like Facebook which we have considered here. Following are the steps which are performed for application in the case of extended permission requests:

1. Extracting the extended permissions requested by parsing the scope values in the request URI.

2. Retrieving the suggestions for the set of requested permissions by invoking our getSuggestion API. Once the suggestions are retrieved should be taken properly.

3. After this user interface will be shown to the user based on the requested permissions and their permission values respectively. Fig 3 shows the example of interface for

Scope = postmy_wall, access_profile, emails, access_basic

4. Providing fascination to the users by providing option like customizing plugins status for the users updating.

Moreover Fig.4 shows how we are handling the overall process and detecting application permission request. Once the user has made the decision on permissions, it should grant or deny the permission by clicking tab. After that two action will be performed. 1) Invoking our postDecisions API method which is passed along the user decisions. 2) Generating a new scope value while using the permissions granted by the users. While using this new scope, the user will be redirected to the requested URI. At this stage user has to defend itself against the unnecessary applications' access

V. CONCLUSION & FUTRE WORK

In today's scenario usable privacy configuration tools plays an essential role in providing user privacy and protecting data from the third party applications in online social networks. We have proposed an extension to the web server authorization flow of OAuth 2.0 protocol in order to provide security and privacy which gives users the ability for configuring their privacy settings for third party applications at the installation time. We developed a multiple criteria based suggestion model which helps the users to take decision while using application which are new to it by considering the decision made by previous individual users. Moreover among the popular requested permission, individual users when given choices are more likely to deny the requested permission. We also have demonstrated the significance of the suggestion through a casual group of users who have not given any suggestions or recommendations and found that they were more willing to grant the permissions to the third party application providers than those who has given recommendations.

In future work we have planned to provide more précised options to the user while taking decision over application installation in order to achieve more secure privacy settings. We will be planning to provide the better prediction method in the case of user decision data. Also our future work includes the extending the model to model the OAuth 2.0 at much more layer of the granularity for making it more secure protocol by rectifying some of its attacks issues on users data.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MSIP/KEIT [10047273, Development of EHR Platform and Application Systems based on International Standards for Multi-Countries Hospital Information Systems] and the IT R&D program of MSIP/KEIT [10041145, Self-Organized Software platform (SOS) for Welfare Devices]

REFERENCES

[1] D. Hardt, "The OAuth 2.0 authorization framework," *The Internet Eng. Task Force RFC 6749*, October 2012

[2] E. Hammer-Lahav, "The OAuth 1.0 protocol," *The Internet Eng. Task* Force *RFC 5849*, April 2010

[3] W. Bin, H. H. Yuan, L. X. Xi, and X. J. Min. Open identity management framework for SaaS ecosystem. In e-Business Engineering, 2009.

[4] Y. Joshi, D. Das, and S. Saha. Mitigating man in the middle attack over secure sockets layer. In 2009 *IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, pages 1–5. IEEE, December 2009

[5] A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," Proc. Int'l Workshop Privacy Enhancing Technologies, pp. 36-58, 2006.

[6] K. K. Gollu, S. Saroiu, and A. Wolman. A social networking-based access control scheme for personal content. Proc. 21st ACM Symposium on Operating Systems Principles (SOSP '07). Work in progress.

[7] D. Carrie and E. Gates. Access control requirements for web 2.0 security and privacy. In Proc. of Workshop on Web 2.0 Security & Privacy (W2SP 2007), 2007.

[8] M. Hart, R. Johnson, and A. Stent. More content - less control: Access control in the Web 2.0. Web 2.0 Security & Privacy, 2003

[9] L. Fang and K. LeFevre, "Privacy Wizards for Social Networking Sites," Proc. Int'l Conf. World Wide Web (WWW), M. Rappa, P. Jones, J. Freire, and S. Chakraborty, ed., pp. 351-360, 2010.

[10] M. Shehab, A.C. Squicciarini, and G.-J. Ahn, "Beyond User-to User Access Control for Online Social Networks," Proc. 10th Int'l Conf. Information and Comm. Security (ICICS '08), pp. 174-189, 2008.

[11] P.G. Kelley, P. Hankes Drielsma, N. Sadeh, and L.F. Cranor, "UserControllable Learning of Security and Privacy Policies," AISec '08: Proc. First ACM Workshop AISec, pp. 11-18, 2008

[12] J. Goecks, W.K. Edwards, and E.D. Mynatt, "Challenges in Supporting End-User Privacy and Security Management with Social Navigation," Proc. Fifth Symp. Usable Privacy and Security (SOUPS '09), pp. 5:1-5:12, 2009

[13] Facebook, Facebook Press Room, http://www.facebook.com/ press /info.php? Statistics, 2011