International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Open Authorization with Recommendation Service

Pranita M. Trivedi[1], N. M. Kandoi[2]

[1]Department of Computer Engineering, PG Student, SSGMCE, Shegaon, India
[2]Department of Information Technology, Faculty of Technical education, SSGMCE, Shegaon, India

Abstract: ***OAuth is an open standard for authorization. OAuth provides client applications a secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. The proposed multicriteria recommender model with open authorization system is to have the modules includes End Users, Permission Guide, Recommendation Service, Authorization server. OAuth uses a mechanism where the roles of third-party applications and resource owners are separated. It does not require users to share their private credentials with third-party applications; instead it issues a new set of credentials for each application.***

Keywords: Privacy, OAuth, collaboration, Recommendation social networks

1. Introduction

Usage of third party application is increasing day by day. Online platforms have become rich grounds for third party applications that utilize user online data to provide various services. Third-party applications, especially within social networking platforms have become very popular. It became very essential to Provide user Privacy from third party applications [1]. Before using applications, users are required to authorize them and grant them access to certain permissions they request, e.g., access to a user's e-mail, location, etc. With the pervasiveness of such applications, protecting the user's online private data becomes a necessity [3]. Open standards offers internet users the tools and capabilities to better manage their own identity, privacy, and confidentiality. The OAuth open standard protocol is another example of an available standard created to provide users with the ability to share information and resources with third-party application components.

The Open Authorization Protocol includes browser extensions which protect users, for example, from unwanted advertisements, malicious software installations, and compromise of user credential data. The multicriteria Recommender based model, enables users to make important privacy decisions at the time of third-party application installation. Recommendations give users confidence in making their decisions, especially that many privacy requests do not clearly convey the accesses requested. The decisions that users make are their own of course, but algorithm and model provides a mechanism called recommendation model based on the collaborative decisions (grant/deny)[2].

2. Literature Review

Studies such as the one by Acquisti and Gross indicate user concern over their privacy on social networks while most users did not apply strict privacy settings on their online social profiles. This was mostly due to the lack or poor understanding of what privacy controls are available to them. The focus is on providing a usable tool via a browser extension which allows for users to easily understand and customize their privacy settings at application installation time. Also to increase user awareness by providing them a set of recommendations on the requested privacy attributes.

Using browser-based plug-ins and extensions is another widely used approach in aiding information privacy. Jenkin and Dymond [4]originally identified this approach to address the problem of "an information provider wanting to serve secrets embedded within regular web- pages to authorized users." The authors' original italicized elements hold true for this model, substituting users for information providers, identity attributes for secrets, and authorized third-party applications for authorized users. Today, the "open source" model is routinely used to enable community-contributed plug-ins for web browsers that aid in some aspect of security; as one example, the Mozilla Firefox browser boasts over 500 security and privacy plug- ins available at their add-ons website[3,4].

Felt and Evans [4] detail a novel solution for protecting privacy within social networking platforms through the use of an application programming interface to which independent application owners would agree to adhere to.

The main approach requires no such agreement and, barring a whole- sale adoption of a privacy proxy such as the one which Felt proposes, still enables the user to protect their information attributes [4].

This can be achieving by utilizing the already popular OAuth 2.0 authorization flow and providing a seamless experience to users for customizing and protecting their private information attributes. Recently, Felt et al. reviewed the permissions requested by current applications.While some of their findings apply to the context of Android applications, they confirm our claim that up-front permission requirements for installation may help APIs achieve their full potential in a secure fashion, while still be useful for end-users.

3. OAUTH Flow

The Proposed Technique of Oauth i.e. multicriteria recommender deals with:

A browser-based extension: A browser-based extension that intercepts the default OAuth 2.0 request and, interprets it, and provides the user with an easy and usable interface to

make decisions that provide for the protection of private identity attributes before application installation

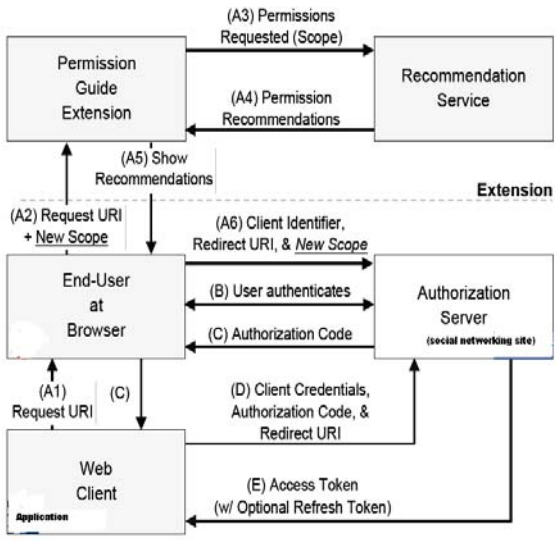
A multi-criteria recommender model approach: that provides users with rating measures on requested privacy attributes based on the collaborative effort of users who have historically made grant/deny decisions for similarly requested privacy attributes[1].

A recommendation to extend the Open Authorization specification: to provide an avenue through which web-browsers (through browser extensions method or otherwise) might assist users in making informed decisions regarding their full privacy attributes before the installation of a third party application.

Steps Involved in OAuth Multicriteria Recommender Model are:

A1. The client redirects the browser to the end-user authorization endpoint by initiating a request URI that includes a scope parameter.
A2. The Permission Guide extension captures the scope value from the request URI and parses the requested permissions. At this step, the extension allows users to choose a subset of the permissions requested.

The following figure shows the open authorization flow. Which has the different modules included,which are End-User,Authorization Server.



A3. The Permission Guide extension requests a set of recommendations on the parsed permissions. This is achieved by passing the set of permissions to Recommendation Service of social networking sites.
A4. The Recommendation Service returns a set of recommendations for the permissions requested by the client.
A5. Using the set of returned recommendations, the extension presents the permissions with their respective recommendations in a user-friendly manner [1, 2].

Module Description:

The system is proposed to have the following modules along with functional requirements.

1. End Users
2. Permission Guide
3. Recommendation Service
4. Authorization server

End Users

End users are the one who initiates the flow by giving their registration details, set permissions etc.

Permission Guide

A Permission Guide that guides users through the requested permissions, and shows them a set of recommendations on each of the requested permissions.It is represented by a browser extension that integrates into the authorization process by capturing the scope parameter value within the request URI generated by a third-party application. Once the scope is captured, the extension parses the requested permissions and presents them in a user-friendly manner.

Recommendation Service

The Recommendation Service returns a set of recommendations for the permissions requested by the client.

Authorization Server

OAuth uses a mechanism where the roles of third-party applications and resource owners are separated. It does not require users to share their private credentials with third-party applications, instead it issues a new set of credentials for each application. These new set of credentials are per application, and reflect a unique set of permissions to a user's online resources. In OAuth, these new credentials are represented via an Access Token. An Access Token is a string which denotes a certain scope of permissions granted to an application, it also denotes other attributes such as the duration the Access Token is considered valid. We are mainly interested in the scope attribute within an Access Token. Access Tokens are issued
by an authorization server after the approval of the resource owner.

4. Conclusion

OAuth, a new protocol for establishing identity management standards across services, provides an alternative to sharing our usernames and passwords, and exposing ourselves to attacks on our online data and identities. The Open Authorization protocol (OAuth) was introduced as a secure and efficient method for authorizing third-party applications without releasing a user's private credentials. One of the main reasons behind OAuth was to increase user privacy by separating the role of users (resource owners) from that of third party applications. OAuth uses the concept of Access Tokens, where a token denotes a set of credentials granted to third party applications by the resource owners. OAuth is an open standard for authorization. OAuth provides client applications a secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. The proposed multicriteria recommender model with open authorization

system is to have the modules includes End Users, Permission Guide, Recommendation Service, Authorization server. OAuth uses a mechanism where the roles of third-party applications and resource owners are separated. It does not require users to share their private credentials with third-party applications, instead it issues a new set of credentials for each application.

The Multicriteria Recommender Model uses the collaborative filtering technique which helps in providing more privacy from third party application. Recommendations give users confidence in making their decisions, especially that many privacy requests do not clearly convey the accesses requested. The decisions that users make are their own of course, but algorithm and model provides a mechanism called recommendation model.

References

[1] G. Adomavicius and Y. Kwon, "Multi-Criteria Recommender Systems," Recommender Systems Handbook: A Complete Guide for Research Scientists and Practitioners, Springer, 2010.
[2] W. Bin, H.H. Yuan, L.X. Xi, and X.J. Min, "Open Identity Management Framework for Saas Ecosystem," Proc. IEEE Int'lConf. E-Business Eng. (ICEBE '09), pp. 512- 517, 2009.
[3] Y. Joshi, D. Das, and S. Saha, "Mitigating Man in the Middle Attack over Secure Sockets Layer," Proc. IEEE Int'l Conf. Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1-5,Dec. 2009
[4] OAuth 2.0. The OAuth 2.0 Protocol, http://tools.ietf.org/html/draft-ietf-oauth-v2-22, 2011K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks.
[5] W. Wang, H. Kargupta, S. Ranka, P. S. Yu, and X. Wu, editors, ICDM, pages 288{297. IEEE Computer Society, 2009
[6] M. R. McLaughlin and J. L. Herlocker. A collaborative _ltering algorithm and evaluation metric that accurately model the user experience. In Proceedings of the 27th annual international ACM SIGIR conference on Research and development in information retrieval, SIGIR '04, pages 329{336, New York, NY, USA, 2004. ACM.
[7] J. Goecks, W. K. Edwards, and E. D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09, pages 5:1{5:12, New York, NY, USA, 2009. ACM.

Author Profiles

Pranita M. Trivedi: PG student at SSGMCE, Shegaon, and her area of interest is Internet Security.

Prof. N. M. Kandoi, Associate Professor at SSGMCE, Shegaon.Chief coordinator Information and Communication Center.Area of interest Web Technologies.