A Study of the OAuth 2.0 Protocol Extended Using SMS for Safe User Access

Chae Cheol-Joo
Dept. of R&D Information Convergence
Korea Institute of Science and Technology Information
Daejeon, Korea
cjchae@kisti.re.kr

Kwang-Nam Choi
Dept. of R&D Information Convergence
Korea Institute of Science and Technology Information
Daejeon, Korea
knchoi@kisti.re.kr

***Abstract*—Recently, diverse Web services and applications have been provided to users. Since these services are provided to the authenticated users only, users need to go through the authentication process whenever they use the services. To take care of this kind of inconvenience, the Open Authorization (OAuth) protocol which allows a 3rd party application to have restricted access authority against Web services has emerged. This OAuth protocol provides convenient and flexible services to users, but it has security weaknesses in acquiring authority. Therefore, this study proposes a method to analyze and improve security loopholes, which can occur in the OAuth 2.0 protocol.**

Keywords - OAuth 2.0; User Access; Authentication; Authorization

I. INTRODUCTION

The OAuth is a protocol which authorizes the authority to use the services provided by diverse service providers after going through user authentication just once between the user and 3rd party application. Even though the OAuth provides convenience and scalability, it has several security loopholes in the authentication between the user and 3rd application. Unlike the weakness of the conventional Web application authentication, such problems can cause a serious security problem because once a user successfully passes user authentication once, he/she can get access to multiple services without additional authentication procedures [1][2].

Therefore, this study proposes a 3rd application and user authentication method which can analyze and overcome the security weaknesses of the OAuth protocol. This paper is structured as follows: In Section 2, the OAuth protocol is described. In Section 3, the security weaknesses which can occur in the OAuth protocol are stated. In Section 4, an authentication method which can overcome the security loopholes mentioned in Section 3 is proposed. In Section 5, conclusion is given.

II. USER AUTHENTICATION IN THE OAUTH 2.0

As a general procedure to operate the OAuth 2.0 protocol, the client requests an access token which represents authority to get access to resources to the resource owner. The authorization server issues the authority to get access to the resources after authenticating the client and user information. Then, the client is able to approach user resources. Figure 1 reveals the general operating procedures of the OAuth 2.0 protocol [3][4].

Figure 1. General Operating Procedures of the OAuth 2.0 Protocol.

III. SECURITY VULNERABILITY OF USER AUTHENTICATION IN THE OAUTH 2.0

In the OAuth protocol, if the access token having the authority to get access to resources is stolen, security vulnerability that users are able to approach resources using diverse applications occurs. In terms of a way to steal such access token, there are replay attack, phishing and spoofing which are the common network security problems. In this section the security vulnerability in which authority can be stolen through the said attacks in the OAuth 2.0 protocol [5] is described.

A. Acquisition of authorization code using replay attack

For replay attack, an attacker captures authorization code between the client and resource owner. Then, it can resend a request to the client to login to the resource owner's account associated with authorization code, using the captured authorization code redirection request. Through this kind of replay attack, an attacker is able to acquire the authority to get access to the resource server after getting the information on the resource owner.

B. Acquisition of ID and password using phishing

In order for the client to get the resource owner's information, it should pass the authorization server's authentication. In this process, an attacker is able to steal the resource owner's ID and passwords which are needed for authentication by creating a malicious client. Using the resource owner's ID and password stolen through phishing, an attacker is able to get the authority to login and use the resource server.

 ISBN: 978-1-61208-510-4

C. *Acquisition of authorization code using spoofing*

To attempt spoofing, the attacker first wiretaps and intercepts the authorization code. Then, it actually blocks the authorization code request to maintain the intercepted authorization code. Then, the attacker starts an initial session with the client. Once the session is begun, it can acquire the authority to get access to the resource service, using the intercepted authorization code.

IV. SAFE USER ACCESS AUTHORIZATION IN THE OAUTH 2.0 PROTOCOL USING THE SMS

In this section, a method to issue an access token which is the authority to get access to the resource server safely after authenticating the resource owner, using SMS (Short Message Service) before the issuance as a way to solve the security problems that can occur in the OAuth 2.0 protocol analyzed in Section 3. Figure 2 reveals the OAuth 2.0 protocol extended through SMS authentication to grant safe user authority.

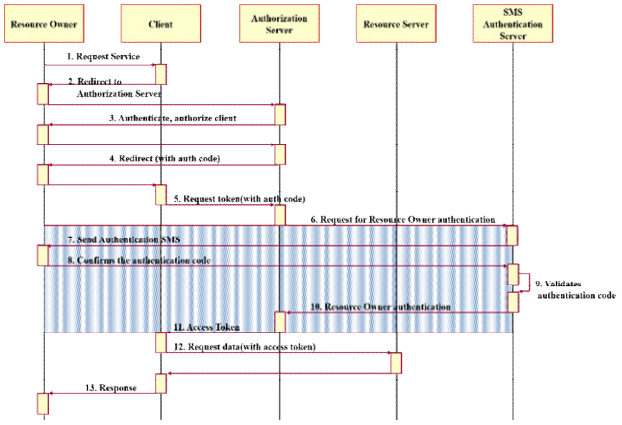

Figure 2. Proposed Method for more Safe User Asscess Grant.

To allow the SMS authentication server to send an email which includes authentication code to the resource owner safely in Step 6, Elgamal algorithm was adopted. The SMS authentication server creates a very large decimal (p) and creates and issues a public key ($y = g^a \ mod \ p$) which can be compared to a private key ($a \in p^*$) needed for the resource owner in the SMS authentication server.

In Step 7, the resource owner decrypts and authenticates {$MAS_{SMS\ addres}$s, $User_{SMS\ address}$, c_1, c_2, MAC_{MAS}, T_{MAS}} received from the SMS authentication server.

Using the proposed method, the user authentication security vulnerability in the OAuth 2.0 analyzed in section 3 can be overcome as follows:

- In the replay attack vulnerability, a malicious attacker can resend a request to the client to login to the resource owner's account associated with authorization code after capturing and using the captured authorization code redirection request between the client and resource owner. Then, the attacker attempts to get the authority to approach the resource server by getting user information. In the proposed method, however, the issuance of an access token to the resource owner is authorized by using the SMS. Therefore, the attacker isn't able to get access to the resource server through the authorization code-based replay attack. In addition, even though the attacker retries replay attack using the SMS during authentication, the validity of TMAS received after going through the verification of $(T_{user} - T_{MAS}) \leq \Delta t$ is verified in the SMS authentication. Therefore, it is able to block replay attack.
- In phishing vulnerability, an attacker can attempt proxy authentication using the values entered by the resource owner after constructing a malicious client. However, the resource owner and SMS authentication server verify the MAC authentication code during the SMS authentication of the proposed method. Therefore, it is able to block the attacker's phishing.
- In spoofing vulnerability, an attacker wiretaps and intercepts authorization code and blocks the user's request. Then, it starts normal protocol, using the intercepted authorization code. In the proposed technique, however, SMS authentication on the user is only performed. Therefore, it is able to avoid spoofing vulnerability.

V. CONCLUSION

The OAuth protocol is developed for the purpose of standardizing different authentication methods. With this, therefore, users are able to use many other applications without going through additional authentication procedures. Even though the OAuth protocol provides convenience and scalability, it has several security loopholes in the authentication between the user and 3rd application. To overcome such security problems which can occur in the OAuth protocol, this study proposed a method which can authenticate user authority safely by verifying the authentication code, using the external authentication server.

The proposed method overcomes the security vulnerability of the OAuth protocol so that it is able to provide active services, compared to the conventional protocol. The proposed method-based OAuth protocol can prevent a security accident. In addition, it could be applied to the emerging OpenID and facilitate the protocol.

REFERENCES

[1] Meng-Yu Wu, Tsern-Huei Lee, "Design and Implementation of Cloud API Access Control Based on OAuth", In Proc. Of TENCON Spring Conference, 2013.

[2] http://en.wikipedia.org/wiki/OAuth

[3] D. Hardt, "The OAuth 2.0 authorization framework," Internet Engineering Task Force(IETF) RFC 6749, 2012.

[4] E. Hammer-Lahav, Ed, "The OAuth 1.0 Protocol", Internet Engineering Task Force(IETF) RFC5849, 2010.

[5] M. Jones and D. Hardt, "OAuth 2.0 Authorization Framework: Bearer token usage", Internet Engineering Task Force (IETF) RFC6750, 2012.

 ISBN: 978-1-61208-510-4