ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Survey of Authentication and Authorization based on OAuth

Kuldipsinh Jam[1], Avi Mistry[2], Arpita Shah[3], Amit Ganatra[4]

M.Tech. Student, Department of Computer Engineering, C.S.P.I.T., CHARUSAT, Changa, Gujarat, India [1,2]

Assistant Professor, Department of Computer Engineering, C.S.P.I.T., CHARUSAT, Changa, Gujarat, India [3]

Head, Department of Computer Engineering, C.S.P.I.T., CHARUSAT, Changa, Gujarat, India [4]

ABSTRACT: Authentication and Authorization service is incredibly necessary since it directly impacts to the protection of any Organization or Application. As the authentication and authorization scheme is healthier, it ensures additional security. Nowadays, IoT (Internet of Things) is incredibly rising technology attributable to all the folks moves towards the automation and digitization. There are several application domains within which IoT technology are often accustomed offer terribly helpful services like health care, transportation, infrastructure and residential. The main problem in IoT is security since IoT environment contains constrained devices that are having low power and low memory. This paper presents how Open Authentication protocol OAuth is used in IoT and security analysis of OAuth 2.0.

KEYWORDS: Internet of Things, Open Authentication (OAuth), Authorization, Security.

I. INTRODUCTION

IoT can become dominant day by day as a result of these days, folks don't have time in order that they wish to try and do their daily routine in a very means that there's minimum human interception. As the IoT system deployments increase, it desires higher authentication and authorization schemes to guard non-public data from the unauthorized person or intruder for constrained environment.

The OAuth 2.0 is open standard authorization protocol [5] which permits a third-party application to induce restricted access to associate HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and conjointly the hypertext transfer protocol service, or by permitting the third-party application to induce access on its own behalf. OAuth [6] protocol offers such a method pattern via the employment of access tokens, that square measure requested by consumer, and later on bestowed, to resource servers once rigorous access to preserved resources governed by those resource servers. It explicates four consumer profiles: web Server profile, User-Agent profile, Native Application profile, and Autonomous. The web server profile is wide enforced and established by many major service suppliers like Yahoo, Twitter, Google, and Facebook. OAuth 2.0 defines numerous authorizations flows to deal with the precise want of every of the consumer profiles. They're authorization code flows, implicit grant flows, resource owner password credentials flows and client credentials flow. Generally authorization code grant is used by the server side web applications whereas implicit grant is used by the client-side web applications.

II. LITERATURE SURVEY

In paper [1], Shamini projected one approach which can be used to protect constrained network from unknown users with security manager using OAuth 2.0 framework. In addition to this, it also makes flexible enough the process of managing IoT networks. The authentication service is provided by the protection manager for multiple IoT networks, which might additionally facilitate to cut back the value overhead to maintain secure information in constrained networks. Moreover, they have mentioned the procedure to form and manage the database in security manager so it is advantageous to the user to reduce the burden of registering to multiple networks or applications.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

In paper [2], Swati proposed a sensible fire alarm system which can be used to notify the user regarding the incidence of a fireplace in the house. Whenever there is fire in the house, user is able to get an alert message via twitter and Gmail account at the same time. The system is made by desegregation IoT technology with temperature sensors. Moreover, in order to use Gmail and twitter account, device ought to authenticate on behalf of the user. For this, OAuth protocol is used to obtain delegated access to the social applications like Gmail and twitter. The result discovered that the proposed system has a low latency as compared to the present system. However, the proposed OAuth based system is able to integrate with many cloud service provider, the notifications are often alleviated to multiple channels. Therefore, the proposed system is able to provide better notification with more security into multiple channels without compromising on the latency.

In paper [3], Feng has analysed the OAuth protocol and described a systematic root cause analysis of security threats in numerous phases of the OAuth protocol. The attacker model is used to discover that there are number of common network attacks that would be probably carried out by attackers to imitate the users and use their protected resources, like impersonation attacks, forced-login CSRF attacks, network eavesdropping, and replay attacks. Additionally to the present, he has also examined the root caused of these vulnerabilities. In this paper, he centered on the communication 1. Between the user-agent and the authorization server, and 2. Between the user-agent and the consumer application.

III. OAUTH BASED AUTHENTICATION MECHANISM

In this approach, they have used the authorization technique OAuth, that is associated authorization protocol for third-party applications. When using standard OAuth in an IoT network, it has a drawback that, all the approved users from the desired service provider are allowed to use the IoT network. The projected approach avoid all users from the service providers to access the IoT network and permit solely the genuine users to access the network. The authentication method will be done by the security manager. Security manager compares the user ID obtained from the service provider using access token with its native information. Only just in case of flourishing authentication it permits the user to access the IoT network. This methodology prevents the unauthenticated users to access the IoT network.

The main aim of this paper is to expeditiously manage the access control of IoT network using the security manager. The planned approach incorporates a two-step method, the authorization, and the authentication processes. The planned approach takes advantage of OAuth protocol for the authorization method. In authorization method, User grants access to security manager through the service provider. For authentication process, it compares the user ID that is obtained by utilizing OAuth protocol with the native information maintained in security manager.

The beginning step of implementation is to create the information in security manager. The information of security manager is made using the access token from the service provider to induce friend list of constrained network manager account. This information maintenance is completed by the security manager. Once a user tries to access IoT network, he or she is going to be redirected to security manager that performs the authentication method.

The database management process in security manager is as follows:

- Database is constructed with the list of user ID obtained from the friend list of IoT network manager.
- Security manager requests for the refresh token before the expiration of access token for future synchronization between friend list and database.
- Database updation are going to be done sporadically using the refresh token obtained by security manager.
- During periodic update, security manager compares the prevailing information with the most recent friend list provided by service provider. information are going to be updated with the users another or deleted from friend list.
- Alternatively IoT network manager has an choice to login to security manager application for instant synchronization between friend list and database.

IV. OAUTH BASED AUTHENTICATION SCHEME FOR FIRE ALARM SYSTEM

The author has projected one unique authentication scheme based on OAuth, by means of that user delegates a constrained application (Device) to obtain the information on behalf of the resource owner. The proposed scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

yields fireplace alarm system (Device) which would possibly wish to send associate alert message. The temperature sensor is connected to the device, so it will enable the buzzer whenever the high temperature is detected by the temperature detector that ought to be satisfied, and finally the notification is going to be sent to the twitter yet as Gmail whenever there's a fireplace incident or emergency.

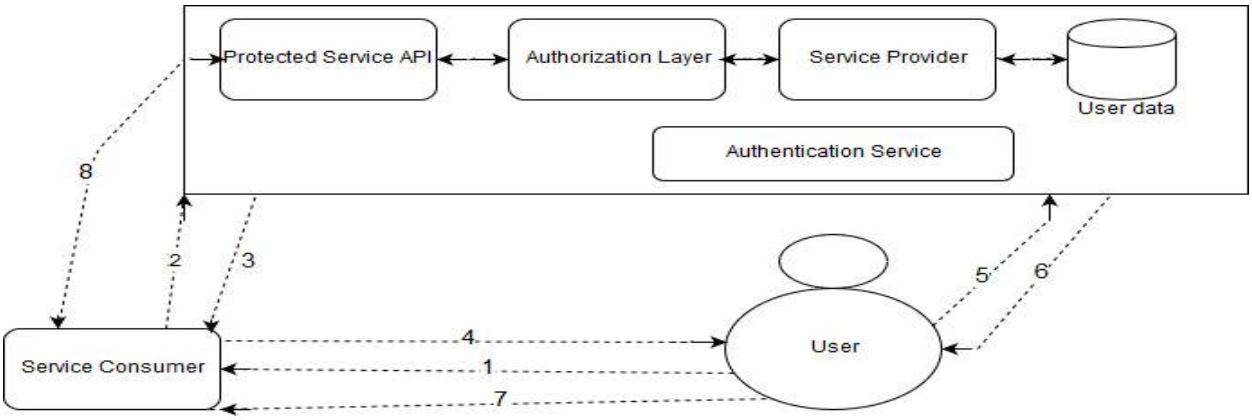

Fig1. Proposed Architecture

The projected work has many modules, which will be consider as follows,

a) Service Consumer: It is act as a 3rd party application. Which has to obtain the information of the user from the service provider on behalf of resource owner. Request token is generated by the user to service consumer (device). Data send over the authentication service first by the service consumer.
b) Authentication Service: Service client ought to exchange information with the service provider and it sends a call for participation to service provider through Authentication service.
c) Protected Services: Once the protected service has the information it will go through the authorization whether the user credentials are available correct or not. If the user credentials are available then protected service sends explicit authentication service that is, it provides the Access Token.
d) Service Provider: When the service provider gets the Access Token, it forwards that Access Token to the consumer, the consumer sends access token to the service consumer; then service consumer is able to communicate directly to the service provider and use the services of the service provider on behalf of resource owner.
e) Dotted Lines: These are nothing but virtual lines which suggests that one is able to use the authentication services from the service provider.

For example, there is one home in which the fire alarm system is placed. So whenever there is a fire in the home that is detected by the temperature sensor and now we want to post these data about the fire in the home. To do this the data should be posted to the service provider site in order to do that application gets an OAuthentication through the service provider. When the authentication data is received by the service provider (SP) it will send the access token in response and now application can retrieve or send data from or to the service provider (SP). As soon as the fire is detected it can send data to the service provider, that data will be sent on behalf of the resource owner. Here the user is able to put the authorization service without any implementation or hard coding the authorization service by using Google, Twitter, Facebook.

V. SECURITY ANALYSIS OF OAUTH 2.0

Here author implements the attacker model which is able to evaluate the security of the OAuth 2.0. The model is able to imitate common network attacks on the OAuth 2.0 protocol automatically. In addition to this, the attacker model includes intercepting modules as well. A single attack is represented by each module. Author has implemented four attack modules during this work. Moreover, author examined attack module, phishing attack module, replay attack

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

module, and impersonation attack module. Only for analysis purpose author monitoring the attack module and it simply detects the HTTP traffic.

The attacker model is made on the following attack assumptions:

- The first assumption is that the assailant has complete access to the network which has three parties: the client application, the resource owner's user-agent and the authorization server. Three message exchange channels (between the client application and resource owner's user-agent, between the authorization server and the resource owner's user-agent and the authorization server and the client application) are eavesdropped by the attacker model.
- The second assumption is that the attacker model has unlimited resources to attack.

a) *Replay Attack Module:* In the OAuth 2.0, the authorization code flow contains an authorization code which act as the resource owner's access grant to the client. Once the authorization code is consumed by the client application, it has to be void. Any authorization code has to be used only once. If this is not the case the replay attack can possible. In this scenario, an unknown attacker is able to catch the authorization code redirection request during the transmission between the client application and the resource owner's user-agent. Afterward the assailant will resend the old request to the client application in order to gain access to the accounts linked with the authorization code.

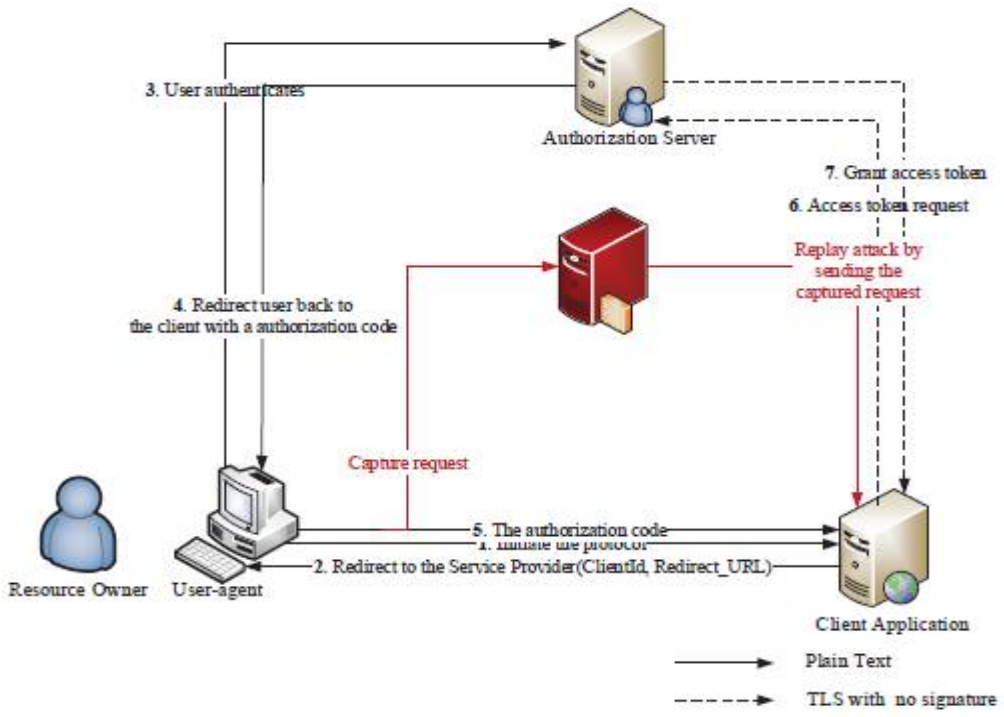

Fig2. Replay Attack Model

In figure2 first of all, user agent will start the process by accessing the client application in response client application will send the clientId and the redirection URL so the user-agent will be redirected to the authorization server. After that user-agent will be authenticated by the authorization server and it will redirect the user back to the client with a authorization code. Then, user-agent will forward the authorization code to the client application which is going to be used by client application to get the access token from the authorization server. Here the problem can arise and that is if intruder will capture the authorization code then he can be used it later to get the access token.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

b) *Phishing Attack Module:* Phishing may be a common method during which the attacker masquerades as a trustworthy entity like a web site to achieve counsel like usernames, passwords, access code, and alternative security info. As we know, it's very straightforward to get a client id from a service provider. for instance, as long as you have got an account with Google, you'll register a client application to consume Google internet services in any time. thus this suggests not all the client applications allowed to use internet services from a well known service supplier respect user privacy. a number of them could masquerade as a legitimate web site so as to achieve authorization codes. in order to launch a phishing attack, the attack will poison DNS cache records on the user's machine. As a result, whenever the victim tries to go to some legitimate sites, he or she is redirected to a malicious client website that he or she isn't meant to visit. during this attack module, the resource owner is redirected to a malicious consumer application instead of the legitimate clientsite he or she supposed to. once the victim initiates the flow, he's directed to the authorization server with the request containing the malicious consumer's client id and redirect URI. Once the malicious application receives the authorization code, it constructs a call for participation with the authorization code and sends it to the request terminus of the legitimate consumer.

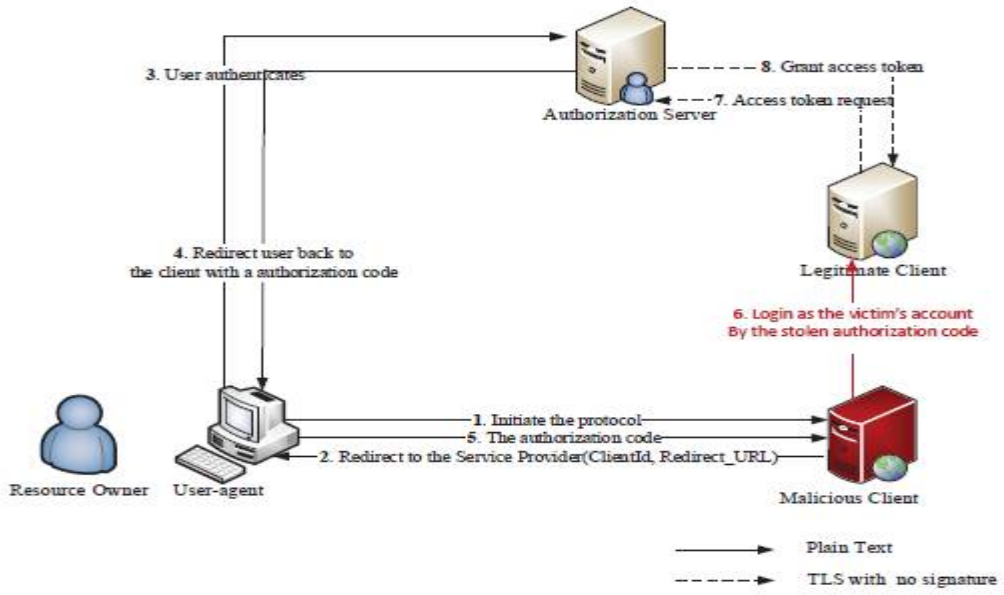

Fig3. Phishing Attack Model

In figure3, how phishing attack can be possible by the intruder is shown step by step. Here, first four steps are same as explain in figure2. But when user-agent send the authorization code to the legitimate client at that time intruder will act as a legitimate client and get the authorization code from the user-agent and afterward use it to get the access token from the authorization code and then by using access token he will be able to access the protected resources from the resource server.

c) *Impersonation Attack Module:* The impersonation attack module grabs advantage of the protection penetrability that the recall termination of a consumer application isn't needed to utilize transport layer security (TLS) mechanism to safeguard the communication. First, the attacker has eavesdropped the authorization code. Secondly, the assailant block the native request to keep the purloined authorization code in an exceedingly contemporary state since the authorization code is only used once. At last, the assailant will begin the session with the consumer application by starting the authorization flow and send the fake request with the purloined authorization code.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Fig4 is showing that it is easily able to get the authorization code from the user-agent by misguide him and once that is done, intruder will initiate the protocol and after that he will request with the victim's authorization code to the client application in order to get the access to the protected resources.

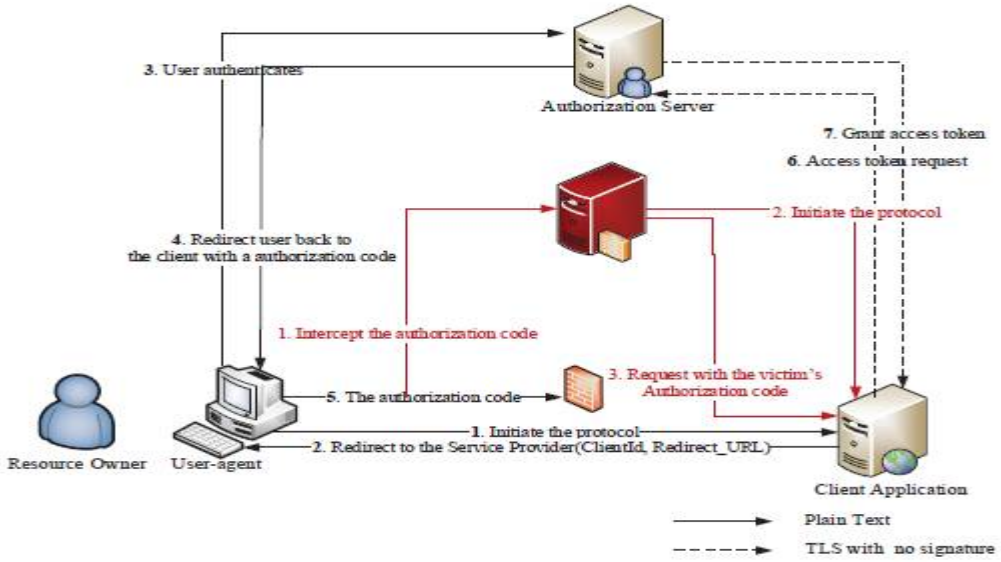

Fig4. Impersonation Attack Model

VI. CONCLUSION

Nowadays, IoT is spreading with the lightning speed since people want simpler and automate life. As the use of IoT technology increase, more and more devices will be connected to the internet and so the data will also be increased in size and variety. To provide privacy to one's data authentication and authorization is needed and currently for authorization most of the users used OAuth 2.0 mechanism but OAuth 2.0 doesn not contain TLS so it doesn't provide much security but it is very easy and flexible enough to provide authorization so most of the company like Google, Yahoo etc. uses it for their webapplications. This paper explain basic way to implement authentication and authorization server based on OAuth and it also explains some attacks which can occur in OAuth 2.0.

REFERENCES

1. S. Emerson, Y. K. Choi, D. Y. Hwang, K. S. Kim and K. H. Kim, "An OAuth based authentication mechanism for IoT networks", 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1072-1074.
2. S. Kinikar and S. Terdal, "Implementation of open authentication protocol for IoT based application", 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-4.
3. F. Yang and S. Manoharan, "A security analysis of the OAuth protocol", 2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, 2013, pp. 271-276.
4. D. Hardt, "The OAuth 2.0 authorization framework,"The Internet Eng.Task Force RFC 6749, October 2012.M.
5. E. Hammer-Lahav, "The OAuth 1.0 protocol,"The Internet Eng. TaskForce RFC 5849, April 2010.
6. J. Richer, W. Mills, and H. Tschofenig, "OAuth 2.0 message authentication code (MAC) tokens," November 2012. [Online]. Available: http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-00
7. OpenID.net, "OpenID authentication 2.0," OpenID Foundation, December 2007.
8. Ed.L.Seitz,SICS Swedish ICT,"Authentication and Authorization in Constrained Environments'', Internet Engineering Task Force(IETF) S.Gerdes,Universitaet Bremen,ISSN:2070-1721 Philips Research January 2016.
9. T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol, RFC 5246", Network Working Group, Aug. 2008.