UNDERSTANDING THE WORKING OF OAUTH PROTOCOL

MRITUNJAY OJHA[1], SAYALI GOREGAONKAR[2] & POOJA DURGE[3]

[1]Assistant Professor, Department of Computer Science, Fr. C. R. I. T, Vashi, Navi Mumbai, Maharashtra, India

[2,3]Student, Department of Computer Science, Fr. C. R. I. T, Vashi, Navi Mumbai, Maharashtra, India

ABSTRACT

O Auth stands for Open Authorization. It's a free and open protocol, built on IETF standards and licenses from the Open Web Foundation, and is the right solution for securing open platforms. OAuth 2.0 framework was published in October of 2012, is an open standard used for providing authorization to third-party applications. The OAuth is implemented with help of authorization token with limited rights, which the user can revoke at any time should they become suspicious or dissatisfied with the app they're using to access your application. This method allows an application provider to gain access to selective APIs without the need for entire user-data. OAuth 2.0 was succeeded by its 1.0 standard which soon got replaced because OAuth 2.0 provided better non-browser based application support, less complicated signatures (no special parsing, sorting or encoding) i.e. SSL is required for all communication, only one security token on every API call and more security features. OAuth 1.a overcame with all the problems associated with 1.0 and is more secure than 2.0. OAuth is a widely used standard by several Resource Providers and social networking sites. This paper deals with the working of OAuth Protocol.

KEYWORDS: Authorization Server, Access Token, Consumer (Client), Request Token, Resource Owner (User), Refresh Token, Resource Server (Service Provider)