Asian Journal of Information Technology 15 (13): 2244-2247, 2016
ISSN: 1682-3915

Analysis of Possibilities for Application of Authentication and Authorization Protocols for Building of Safety Infrastructure for Distributed Information and Computing Environment

[1]Sergej A. Lazarev, [1]Igor S. Konstantinov, [1]Oleg V. Mihalev, [1]Vladimir E. Kiselev and [2]Alexander V. Demidov
[1]Belgorod State University, Pobedy St. 85, 308015 Belgorod, Russia
Orel State University, Komsomolskaya St.95, 302026 Orel, Russia

Abstract: This study provides an analytical overview of the advantages and disadvantages of the protocols that can be used upon building of security infrastructure for distributed information and computing environment. To build such an environment based on a distributed network of portals with a heterogeneous structure, we have considered open protocols applied in implementation of various aspects of secure information exchange.

Keywords: Distributed information and computing resources, virtual secure environment, information access control, protocol analysis, authentication, authorization, information exchange, network of portals

INTRODUCTION

The concept of building of a security infrastructure for a Distributed Information and Computing Environment (DICE) as a network of corporative portals assumes the analysis and development of a complex of solutions on the basis of open protocols that allow for secure authentication and authorization while ensuring the required level of security of information exchange through open channels of the Internet network.

Network of portals as a mechanism having a single entry point and providing a unified access control policy for users and administrators, is described in the work (Lazarev and Demidov, 2010) and represents a set of access control nodes combined into a single network with a portal Network Control Center (NCC). A unified information exchange control policy is implemented within the framework of NCC including the possibility of authorized access to secured information and computing resources throughout the network, a single user session control mechanism to ensure the necessary level of security. For this purpose it is necessary to analyze the authorization and authentication protocols to ensure safe information exchange.

Up till now, multiple protocols have been developed and they are used for authentication and authorization processes, but not all of them are open protocols. The central objective of the article is to analyze the direct authentication and authorization protocols: RADIUS, OpenID, OAuth, SAML (Mishra *et al*., 2003).

MATERIALS AND METHODS

Technique: The main technique applied in the study is a comparative analysis of the open protocols by the most important criteria based on open protocol specifications.

Main part

Radius protocol: RADIUS protocol (Remote Authentication Dial In User Service) is the protocol specified by the Internet Engineering Task Force to access the Internet via Dial-up for a simplified implementation of AAA functions (authentication, authorization and auditing), as well as being published in RFC 2058 and then revised in RFC 2865 and RFC 2866. In addition, the purpose of this protocol at the stage of specification was also the possibility of its use in tariff systems for the resources used by a specific billing user. Currently, this protocol can be used in a wide range of networks and services.

- Let's specify the main advantages of RADIUS protocol
- Openness to incorporate new functionality provided that the equipment would not be replaced or modified
- High response speed when processing user requests due to using of the transport layer protocol UDP
- Algorithm for parallel request processing
- Operation in cluster architectures (OpenVMS) and multiprocessor platforms (DEC alpha, HP integrity) in order to increase productivity and to implement fault tolerance

Corresponding Author: Sergej A. Lazarev, Belgorod State University, Pobedy St. 85, 308015 Belgorod, Russia

RADIUS server function reduced to that a server receives information which is provided by a network user during the authentication process and authorizes the user. This means that the use of the RADIUS server can not make a data transmission process itself more secure in the network, as it can only protect the data transmission process during the authentication. Also, it is worth noting that it should be impossible to make the authorization process without the server being operative.

Open standard of decentralized authentication system openid: OpenID is a concept that allows to use a single account in various web resources which are non-related to each other due to model of account storage on the same server and upon the registration in any web resources it is supposed to use this single account. Being established in 2006, the first specification OpenIDAuthentication 1.1 is updated with a new specification OpenID 2.0 supporting algorithm HMAC-SHA256 (256 bit key length digital signature) that makes authentication of OpenID2.0 message more secure while remaining compatible with OpenID 1.1.

OpenID is an open decentralized system which allows the user to use a single account for authentication in the multiple portals which are not connected to each other. If a portal involves usage of user authentication or authorization, the possible embodiments of this action are presented below:

- Use a standard signing up by entering e-mail and filling the necessary data
- Use authentication by specifying the personal identifier of OpenID-provider
- Use authorization through the open protocol OAuth

The main purpose of using OpenID is to simplify the user logging achieved in a decentralized single sign-on system. This allows a single login and password to use in many web portals, as well as to support the necessary level of protection against unauthorized access.

The main advantages of authentication using OpenID Users do not have to sign up each time in various network resources and to remember the sign-in data for each portal Simplifying the authentication process in network resources that support OpenID Due to the fact that OpenID is a decentralized technology, the software can be used as an OpenID login tool in any web-portal Upon authorization using OpenID, user's personal data can be transferred at once to the visited resources: e -mail, name, gender, date of birth. This saves user from having to input this information: it is enough to do this once at the site of the OpenID provider.

OpenID is an authentication tool: with this system, it is possible to make sure that the user is that who he/she claims to be. What actions a user authenticated by the OpenID can make is determined by the party carrying out authentication.

Specification for OpenID technology (currently OpenIDAuthentication 2.0) does not describe how the authorization security should be provided upon using OpenID. In connection with this, long discussions are conducted on the methods of retrieval by malefactors of users' confidential data (such as a password to their OpenID account).

With all specified advantages of the OpenID protocol the work (Sun *et al*., 2012) shows with use of a formal methodology "Model checking" that the protocol may be vulnerable to a number of attacks, as well as provides recommendations on how these attacks can be avoided.

RESULTS AND DISCUSSION

Outdoor authorization protocol oauth: Outdoor authorization protocol OAuth allows a third party to provide limited access to user's protected resources without the need to transfer username and password to it (the third party). There is a misconception that OAuth is an extension of the OpenID protocol but even though there is a large number of similarities between OpenID and OAuth, the latter is a separate protocol not related to OpenID. The specification of the authorization protocol OAuth 2.0 was published in RFC 6749. Additional RFC documents are still being developed.

Oauth 2.0 is an authorization protocol that allows giving out to a service (application) the right to access to user's resources in another service that provides the work in a heterogeneous environment of Web services (Torroglosa-Garcia *et al*., 2013). The protocol eliminates the need to commit login and password to an application and also allows a limited set of rights to give, rather than all at once. For example, upon authorization through OpenID on a specific web portal via OAuth provider the latter can provide continuous access to some user information.

The principle of work of the protocol OAuth 2.0 is the following: even if there is a user (resource owner) who is going to carry out some actions with his/her resources uploaded to a third party web portal (server) using a specific web service (client).

The sequence of interactions between OAuth protocol entities A client sends using the HTTPS protocol the request to the server which contains the client's ID, a timestamp, a callback address according to which it is necessary to return the token and used type of digital signature and the signature itself. The server

Table 1: Comparison of authentication and authorization protocols

Characteristics	RADIUS	OpenID	Oauth	SAML
Current version	-	OpenID 2.0	OAuth 2.0	SAML 2.0
Main purpose	AAA-server	Single Sign-On for clients	API authentication between services	Single Sign-On for corporate users
Protocols used	UDP	XRDS, HTTP	JSON, HTTP	SAM, XML, HTTP, SOAP

acknowledges the request and responds to the client with the Request Token and a part of the shared secret.

The client sends the token to the owner of network resources (user) and forwards it to the server to pass authentication. Having gained the token from the user, the server requests its login and password from it and in the case of successful authentication the server prompts the user to confirm the user's access to resources (authorization) and then the user should be redirected by the server to the client. The client sends the token (Request Token) to the server via TLS protocol and requests access to resources. The server acknowledges the request and responds to the client a new Access Token. The client accesses the resources of the server using the new token. The server acknowledges the request and provides resources.

Disadvantages of the authorization protocol OAUTH 2.0: OAuth 2.0 is a developing standard that says about its unsettled specification. On the other hand, it gives the opportunity to be a participant in the process of writing the standard. Secure of OAuth 2.0 is largely based on SSL / TLS. This approach greatly simplifies the development of web portals and software, but requires additional computing resources and administration. This can be a significant issue in the highly loaded projects. It is worth mentioning that OAuth can be used in Enterprise-level cloud services; the example of such an implementation is given in (Noureddine and Bashroush, 2013; Zhao and Yue, 2014).

Thus, we can conclude that OAuth is a simple authentication standard grounded on the basic principles of the Internet that makes it possible to use authorization on almost any platform. The standard has the support of the largest web portals and it is clear that its popularity will only grow.

Security assertion markup language SAML: SAML (Security Assertion Markup Language) uses the XML language concept that has been developed by a consortium OASIS Security Services Technical Committee. An open protocol based on the SAML was developed for data exchange on authentication and authorization between the secure domains, in particular, between the Identity Provider (IdP) and the Service Provider (SP), thus solving the problem of providing a pass-through authentication at work via a Web-browser (Mishra *et al*., 2003) .

SAML specification is defined by three roles: a user (primary role), an Identity Provider (IdP) and a Service Provider (SP). In the case of authentication through the use of SAML, the service provider requests verification service from the Identity provider. Based on a statement received from the Identity provider, the Service provider can make a decision on servicing the connected user.

The standards on which the open protocol SAML are based are the following: Extensible Markup Language (XML); XML Schema (XSD); XML Signature; XML Encryption; Hypertext Transfer Protocol (HTTP); SOAP.

SAML protocol is mainly used for the organization of Single Sign-On (SSO) concept. The user requests a web resource protected for providers of SAML services. The Service Provider which wants to know the identity of the requesting user creates an authentication request to the Identity Provider via the user. Open protocol SAML uses such mechanisms as TLS 1.0 or higher to ensure security in the transport layer and XML signatures and XML Encryption to ensure security at the message level.

Resume: The main results of the study are recommendations for the use of open protocols to ensure security and reliability of DICE operation. Table 1 shows the results of the analysis of the direct authentication and authorization protocols: RADIUS, OpenID, OAuth, SAML.

During the analysis, we have identified the main protocols for secure interacttion in the conditions of DICE application, specified the main advantages and disadvantages of the protocols. In the future, development of DICE building technology in a global network space in the form of a secure portal network will be based on the described protocols.

CONCLUSION

It should be noted that in the process of analysis we have identified the advantages and disadvantages of open protocols suitable for building of authentication and authorization services within DICE. Based on the analysis results, we have formed a most preferred subset of protocols for implementing DICE that are

suitable for use and testing in the process of creation of an experimental software package sample (Lazarev *et al*., 2015a, b).

REFERENCES

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev and V.E. Kiselev, 2015a. Implementation of unified session access model in a closed virtual environment of distributed information and computing resource system as a secured portal network. Res. J. Applied Sci., 10: 629-632.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev, A.V. Demidov and R.V. Shateev, 2015b. The development of infrastructure security for distributed information computer environment based on secured portal network. Int. J. Applied Eng. Res., 10: 38116-38120.

Lazarev, SA. and A.V. Demidov, 2010. The concept of construction of a control system of an information exchange in the network of corporate portals. Inform. Syst. Technol., 4: 123-129.

Mishra, P., D. Chopra, J. Moreh and R. Philpott, 2003. Differences between OASIS Security Assertion Markup Lang uage (SAML) V1.1 and V1.0. May 21, 2003. https://www.oasis-open.org/committees/download.php/3412/sstc-saml-diff-1.1-draft-01.pdf.

Noureddine, M. and R. Bashroush, 2013. An authentication model towards cloud federation in the enterprise. J. Syst. Software, 86: 2269-2275.

Sun, S.T., K. Hawkey and K. Beznosov, 2012. Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation and practical countermeasures. Comput. Security, 31: 465-483.

Torroglosa-Garcia, E., A.D. Perez-Morales, P. Martinez-Julia and D.R. Lopez, 2013. Integration of the oauth and web service family security standards. Comput. Networks, 57: 2233-2249.

Zhao, R. and C. Yue, 2014. Toward a secure and usable cloud-based password manager for web browsers. Comput. Secur., 46: 32-47.