IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 4, Ver. II (Jul - Aug 2018), PP 21-24
www.iosrjournals.org

Managing Authorization & Authentication Issues Using Single Sign-On & Server Directory

Rashmi B H
Assistant Professor, Department of Computer Science & Engineering, Global Academy of Technology, INDIA
Corresponding Author: Rashmi B H

Abstract: *Network security deals with basic principles of Authorization and Authentication. Basically, say any organization or in any institution one main principle of maintaining security is to have a well ordering authorization and authentication principles i.e. the process of verification and validation. Authorization is a process of verifying the data, whereas authentication is the process of validating the data. Many issues are involved with the principles of Authentication & Authorization in maintaining security in an organization. There will be problems associated with authentication and access control mechanisms. This paper presents a mechanism called Single sign-on using Kerberos and Directory server using LDAP to employ a solution for managing network security in an organization.*

Keywords: *Security, Authentication, Authorization, Single sign-on, directory Server, Kerberos, LDAP*

Date of Submission: 19-07-2018 Date of acceptance: 02-08-2018

I. Introduction

Managing security is becoming an open challenge in today’s world. Security is one of the core component in any organization or institution. Authorization and authentication are the two important factors concerned with implementing security in an organization. Authorization is a process of verifying the intended data and authentication is the process of validating the correctness of the data [2]. When the word authentication is considered, a common concept called Password comes in to the picture. Password is a unique key used to validate users. Password authentication is one of the common techniques used to verify and validate users present in a corporate network. Implementing password based authentication may vary among individuals [3]. This implementation is based on Point-to-Point protocol. Passwords could be longer or short. Keeping a secured point of view, usually longer passwords are more secure than short passwords and most importantly passwords must be random. If the passwords are long and random, these passwords are treated as good passwords and could impose restrictions on other users i.e. other than the authorized users to remember the passwords. In a large corporate network, there will be lot of issues concerned with password implementation and in turn causes to network security threat by the users who often forget passwords. In a typical corporate organization each and every user has to authenticate them. This process of authentication can be done with the help of Username and password. But the problem arises with the passwords. More good the password is, harder to remember. So in a corporate network, issues related to passwords are increasing. For example many users try to authenticate themselves more than 25 to 30 times per day. One solution to reduce this problem is to Implement Single Sign-on (SSO) in the network [1]. Another problem related to large networks is authorization. All the users present in the organization should not have same access rights. So management of these access controls could be a complex procedure. One solution to this problem is to maintain a centralized sever directory to manage authorization principles. In this paper Single sign on principle and centralized server directory principles are shown.

II. Authentication & Authorization

Authentication: Authentication is the process of verifying one’s identity. Verification can be done in many ways. But these verifications depend on many factors. A factor could be an attribute to rely upon. Below are the outline of different factors.

- What the user knows.
- What the user has.
- What the user is.

The first outline deals with the verification of user information, where only the user is having knowledge of. Each and every user will be provided with username and passwords. So to implement this many password schemes can be used. The Second outline deals with the factors what the user will be having to enter the credentials. It could be some security ID or security token. Using this verification process can be carried out. The outline preferably refers to the context of biometric properties, using which each user's identity can be verified.

Authorization: Authorization is the process of verifying the correctness of the data. Authenticated users can make a request to authorize certain data. This can be implemented using a mechanism called Access Control Lists (ACL) [4].These access control lists consists of security policies and procedures and also specifies the operations to be carried out by each and every individual users. These ACL's perform a combination of users and objects. Each of these combinations will be having a unique operation list. A lookup Table will be maintained so that whenever user tries to perform any operation, he/she should look up the ACL table to see whether that particular operation is allowed to execute or not.

III. Single sign-on

Single sign-on is a new authentication scheme with enables an authorized user to have a single credential which could be authenticated by various or multiple service providers[5].Single sign-on is implemented using Kerberos. Kerberos is computer network authentication mechanism developed to perform authentication using Single sign-on. Kerberos does the process of guarding and managing the network and allows only authenticated users inside the network. So Kerberos can be generally termed as Central authentication Server. Various terms are associated with Kerberos. Some of the Terminologies associated with Kerberos is as shown in the Figure 3.1.

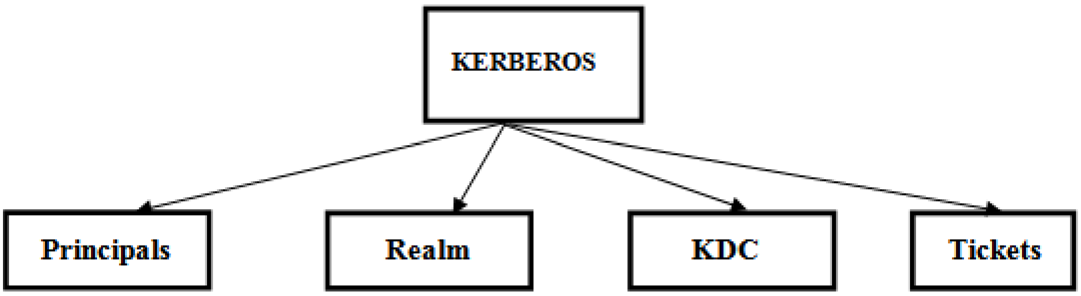

Figure 3.1: Terminologies of Kerberos

Principals: The term principal in Kerberos describes the user or a service, which is usually termed as describing an entity. Each and every user who is authenticated will be associated with principals. These principals are authenticated using a long term password.

Realm: Kerberos realm consists of certain Kerberos principals maintained and administered by Kerberos server. Certain conventions used to denote should be denoted using Upper case.

Tickets: Kerberos use tickets to identify or validate the user's identity. There are two types of tickets namely Ticket Granting Tickets (TGT) and Service Tickets. Ticket granting tickets are used to ask for a service ticket. Usually Ticket granting tickets are generally termed as Master Tickets. Service Tickets are used to provide appropriate services in the network.

Knowledge Distribution Center: KDC consists of 3 parts namely

- Principal Database.
- Authentication Server.
- Ticket Granting Server.

A principal who needs to access the databases ask for an authentication server to provide a Ticket granting ticket. This ticket in turn asks for a service ticker, wherein this ticket provides the services appropriately. The Kerberos authentication scheme to enable Single sign-on is as shown in the following Figure 3.2.

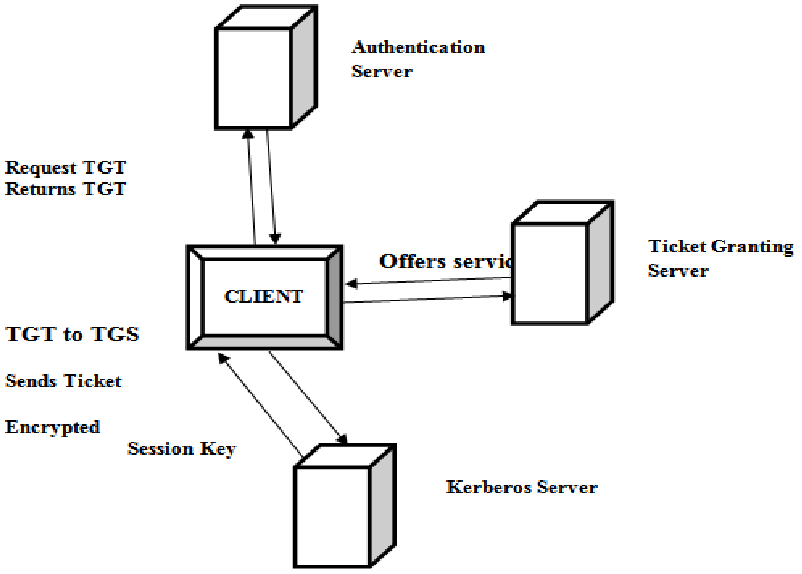

Figure 3.2: Single sign-on Using Kerberos Authentication

The steps followed to enable single sign-on using Kerberos server is as follows:

Step 1: The client starts the Authentication Process by requesting a Ticket Granting Ticket from the authentication server.

Step 2: In the next step, the authentication server returns the ticket back to the client. As the ticket is encrypted with authentication credentials i.e. Password, it can’t be used by any other users.

Step 3: After the ticket is returned from the authentication server, the client sends a Ticket Granting ticket to Ticket Granting server to request for a specific service ticket to provide appropriate service.

Step 4: Here the Ticket granting server receives the ticket and verifies the Ticket and sends the appropriate service to the client.

Step 5: The client after obtaining the service sends a ticket to Kerberos Server to initiate a Session.

Step 6: The Kerberos service verifies the ticket and sends back a message encrypted with the session key. As the ticket is encrypted with the session key, the client can verify the identity of the service.

IV. Centralization

Each and every user has to go through the process of authentication, when he/she wants to access any service. In certain scenarios the user needs to authenticate twice to access any service, which proves to be cumbersome in an organization or in a large corporate network. The procedure still becomes complicated when the user wants to remember many usernames and passwords for various systems. One more problem arouse is the managements of user accounts, as each user needs one separate account. To overcome these problems, there should be a concept called Centralization. Centralization means, the process of authentication and authorization will be done at the central location. The main advantage of having a centralization concept is that all the user accounts will be stored at one place called Central location. Many authentication and authorization protocols could be implemented using Centralization concept. Most commonly Single sign-on can be implemented using Kerberos authentication process, wherein the users who have entered the credentials once need not have to enter many times. The disadvantage with respect to centralization is that by chance if any server doing authentication and authorization process fails, then that particular server causes inaccessibility to all services .In other words, centralization causes single point of failure.

V. Directory Server

Lightweight Directory Access Protocol(LDAP)is a software protocol for enabling administrator to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. Hence LDAP acts as a Central Directory. LDAP uses a X.500 Directory structure to tore all the files and information related to user accounts. LDAP allows the users to locate the information regarding an individual without knowing the Location. The LDAP Directory Tree is as shown in the Figure 5.1.

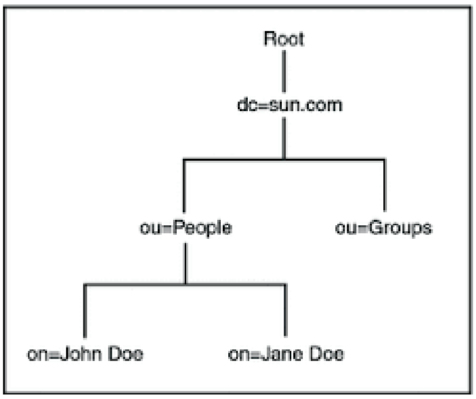

Figure 5.1: Simple LDAP Directory Tree

The LDAP Directory Tree consists of Following Levels.

- The root directory (the starting place or the source of the tree)
- Countries
- Organizations
- Organizational units (divisions, departments, and so forth)
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a Duplicated version of the total directory. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user. So using these Directory sever there will be a centralized authorization process inside the network.

VI. Conclusion

Managing security in any organization or in a large corporate network involves the principles of Authentication and Authorization. This paper solved issues related to Authentication and Authorization by enabling a new authentication mechanism called Single sign-on authentication using Kerberos and authorization issues were managed by the concepts of Centralization and using a server directory called Lightweight directory Access Protocol(LDAP). So using these techniques corporate networks or any organization do not come up with issues related to authentication and authorization.

References

[1]. Guilin Wang, Jiangshan Yu, and Qi Xie," Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE Transactions On Industrial Informatics, Vol. 9, No. 1, February 2013.

[2]. Manvi Mishra,Shivangi Tyagi,Nikitha Jaiswal, Shivangi bJohri," Authentication and Authorization issues for Multi-hop Networks, IJICT,ISSN 0974-2239,volume 3,number 10(2013).

[3]. S.schwoon,S.Jha,T.Reps,S.Stubblebine," On Generalized Authentication Problems".

[4]. Rashmi B H, Usha C.R, Jayanth.P.Raj, "Firewall: A Perimeter Security solution", International Journal of Scientific & Engineering Research, Volume 8, Issue 1,Jan-2017

[5]. Fabian Alenius," Authentication and Authorization", Examensarbete 15 hp August 2010.

[6]. Bo Li, Sheng Ge, Tian-yu Wo, and Dian-fu Ma," Research and Implementation of Single Sign-On Mechanism" pp. 161–166, 2004. © Springer-Verlag Berlin Heidelberg 2004.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Rashmi B H "Managing Authorization & Authentication Issues Using Single Sign-On & Server Directory." IOSR Journal of Computer Engineering (IOSR-JCE) 20.4 (2018): 21-24.