Configuring Apache Web Server for x509 User Authentication

Configuring Apache Web Server for x509 User Authentication

Together Teamlösungen EDV-Dienstleistungen GmbH

Elmargasse 2-4
A-1190
Vienna
Austria
+43 (0) 5 04 04 - 122
+43 (0) 5 04 04 - 11 122
<office@together.at>
http://www.together.at/together/index.html

Table of Contents

Chapter 1. Introduction

This document describes the method of configuring Apache web server for x509 user authentication using MS Active Directory server as a LDAP server for retrieving user information.

The DSO modules mod_authz_ldap and mod_ssl for Apache are used for x509 certificate verification and user mapping. MS Active Directory is used as a LDAP server for retrieving user information (user mapping).

Chapter 2. Scenario

A client wants to access to our web application. He already has his own x509 certificate installed in his browser. Apache web server tries to authenticate the client using mod_ssl and the client's x509 certificate (public key). Apache (mod_ssl) is configured to know where to look for user certificates. The certificates are stored in a directory on the web server.

After successful user authentication Apache has, as the result of authentication, two parameters: issuerDN and subjectDN. Further, the client requests should be forward to the appropriate application server that uses basic authentication system. That means we have to know the client's user name and password. It is necessary to map issuerDN and subjectDN to user name and password. Apache uses mod_authz_ldap DSO to perform such a mapping. Mod_authz_ldap, using issuerDN and subjectDN, retrieves username and password from LDAP server. LDAP server contains the map between issuerDN, subjectDN and username, password pairs. MS Active Directory acts as an LDAPv3 server.

Than mod_authz_ldap overwrites client's HTTP request in a way client could be authenticate by the application server using basic authentication.

Chapter 3. Configuring Active Directory

In order to store the user map in Active Directory (LDAP server) it is needed to add a LDAP schema that represents the map between subjectDN, issuerDN and username, password pairs. It needs to contain the following types:

```
objectClasses: ( 1.3.6.1.4.1.4263.5.3 NAME 'authzLDAPmap' SUP top
STRUCTURAL MUST ( issuerDN $ owner $ subjectDN $ uid ) X-ORIGIN 'user defined' )

attributeTypes: ( 1.3.6.1.4.1.4263.5.1 NAME 'issuerDN' DESC 'The user
friendly version of the distinguished name of the issuer of a
certificate' SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE X-ORIGIN 'user defined' )

attributeTypes: ( 1.3.6.1.4.1.4263.5.2 NAME 'subjectDN' DESC 'The user
friendly version of the distinguished name of the subject of a
certificate' SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE X-ORIGIN 'user defined' )
```

To extend Active Directory schema it could be used MMC (Microsoft management console) schmmgmt. Detail explanation of extending schema could be found here:

ht-
tp://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit
/distsys/part1/dsgch04.asp

After the schema is extended and objectClass authzLDAPmap is added we have to import actual data in to the LDAP server. It is needed to add data entries like the following (in LDIF format):

```
dn: ou=AuthzLDAPCertmap
objectClass: top
objectClass: organizationalUnit
ou=AuthzLDAPCertmap

dn: uid=username,ou=AuthzLDAPCertmap
owner: uid=username,ou=Users
objectClass: top
objectClass: authzLDAPmap
issuerDN: <issuerDN>
subjectDN: <subjectDN>
uid: username

...
```

In this example it is assumed that user entries are located in an organizational unit Users (ou=users).

For adding entries into ActiveDirectory, LDP (ldp.exe, the Microsoft ldap client) could be used. LDP utility is included in Windows Servers Resource Toolkit.

Chapter 4. Configuring Apache

Detail explanation of using mod_authz_module (with examples) could be found here http://opensource.ee.ethz.ch/compet-sites/E/mod_authz_ldap.html

In the first place we have to add these two lines in order to load module mod_authz_ldap:

```
LoadModule authz_ldap_module   libexec/mod_authz_ldap.so
AddModule mod_authz_ldap.c
```

Than we have to add in to the httpd.conf the following section:

```
SSLCertificateFile <path to the crt file>
SSLCertificateKeyFile <path to the key file>
SSLEngine on
<Location /somelocation>
     AuthzLDAPEngine on
     AuthzLDAPServer <active directory server>
     AuthzLDAPUseCertificate on
     AuthzLDAPSetAuthorization off
     AuthzLDAPMapBase ou=AuthzLDAPCertmap
     AuthzLDAPMapScope subtree
     AuthzLDAPUserKey   sAMAccountName
     AuthzLDAPUserBase  ou=Users
     AuthzLDAPUserScope subtree
     AuthzLDAPBindDN  username@domain
     AuthzLDAPBindPassword userpassword

     require valid-user
</Location>
```

Information about generating user certificates and how-to install them could be found here: http://www.giac.org/practical/GSEC/Robert_Colbey_GSEC.pdf.