Shibbolizing Podcast

Overview

This document explains how to Shibbolize Podcast@UCSF. It might be missing some details...

Required Shibboleth Attributes

Podcast@UCSF requires the following attributes from GALEN LDAP, and, therefore, requires them from Shibboleth:

- UID (GALEN ID) which will be mapped to EPPN
- givenName
- sn
- eduPersonPrimaryAffiliation

Components

Podcast@UCSF controls authentication with the following items:

- login.php
- sessionManagement.php
- fileHelper.php
- logout.php
- database

PHP Code Changes

The following are changes that need to be done to the PHP code.

login.php

- Change the login form to be a button that points to MyAccess shibboleth, with text that reads, "Log in via MyAccess". The form would be something like this:

```
<form method="get" action="/podcast/shibboleth.php">
<intput type="hidden" name="target" value="/podcast/index.php" />
<input type="submit" value="Log in via MyAccess" />
</form>
```

The login code at the top of the page should be moved into a new page, called `shibboleth.php`, as that page will be the page which is protected by the `shibd` daemon running on the Podcast server.

In `shibboleth.php`, the auth code should look like:

```
   if (isLoggedIn()) {
      header("Location: $target" );
      exit;
   } else {
      if ($_SERVER['REMOTE_USER']) {
         shibLogin();
         header( "Location: $target" );
         exit;
      } else
         header("Location: login.php");
      }
   }
```

sessionManagement.php

Add a new method to `sessionManagement.php` that works as follows:

```
function shibLogin() {
    $_SESSION['uid']       = $_SERVER['REMOTE_USER'];
    $_SESSION['givenName'] = $_SERVER['givenName'];
    $_SESSION['sn']        = $_SERVER['sn'];
    $_SESSION['eduPersonPrimaryAffiliation'] = $_SERVER['eduPersonPrimaryAffiliation'];
}
```

Modify `userLogout()` to actually end the `shibd` session, as well:

```
function userLogout() {
    $_SESSION = array();
    if ( isset( $_COOKIE[ session_name() ])) {
        setcookie( session_name(), '', time()-42000, '/');
    }
    session_destroy();
    header("Location: /Shibboleth.sso/Logout");
}
```

fileHelper.php

The in the function `setAccessFile(...)`, in the file `fileHelper.php`, writes out a `.htaccess` file to protect a podcast directory. The output needs to be changed from this:

```
  AuthType Basic
  AuthName "Galen Login Authentication"
  AuthLDAPURL "ldaps://ldap.ckm.ucsf.edu/ou=people,dc=library,dc=ucsf,dc=edu?uid"
  AuthLDAPAuthoritative on
  require valid-user
```

to this:

```
  AuthType shibboleth
  ShibRequireSession On
  ShibUseHeaders On
  require valid-user
```

logout.php

The file `logout.php` also handles logout, so the code in this file needs to be changed from:

```
header( "Location: index.php" );
```

to:

```
header("Location: /Shibboleth.sso/Logout");
```

Database Changes

Podcast@UCSF uses the database for admins and owners, and for each, the GALEN ID is used in the record. The following needs to be change in the database:

1. The values of the column `uid` of the `administrators` table needs to be changed to the user's EPPN
2. The values of the column `galenid` of the `owner` table needs to be changed to the user's EPPN

.htaccess File Changes

The podcast files themselves are in directories which are protected by .htaccess files. These files all have GALEN LDAP login AuthN information in them, so they need to be replaced with files that have the Shibboleth AuthN information. This can be done by finding all the podcast-related .htaccess files, and then write a script that will replace each one with an updated .htaccess file.