



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Case Study:
LDAP Authentication and Authorization for Open Source Web Applications

Justin B. Alcorn
9/29/2003

SANS Security Essentials
GSEC Practical Assignment
Version 1.4b – Option 2

© SANS Institute 2003, All rights reserved. Author retains full rights.

Abstract

Many open source web applications use relational databases to hold identifying user information. This model works well for stand-alone Internet applications where the user population is self-chosen and is willing to sign up for and maintain an independent identity for the application. When writing applications for a corporate environment, however, the user population is no longer self-selected. I had some specific challenges that I wanted to solve including an IT Security intranet, tracking of audit issues, and monitoring of corporate email systems where open-source tools could be used to quickly and easily put the information into a HTML format. The information, however, had various levels of classification, and users had to be authenticated and authorized to see the specific applications.

I found a significant number of different examples of using a back-end database to hold the authentication information. However, this simply exacerbated an already existing problem – namely, that corporate environments often have many disparate systems, all with different authentication information. A centralized directory service, such as LDAP, is used by many corporations to unify authentication and authorization and to gain administrative control of provisioning. As part of my job, I am involved in unifying all these different authentication mechanisms and building a central authentication and authorization directory. In this paper, I describe the method I used to solve this problem for the open source PHP applications. I present the actual code and a directory model that can be extended for use as a central corporate directory. I implemented the code on my home intranet as a prototype, and that code is the code presented here.

The Problem - Before

High end Open Source web applications, such as Content Management or Groupware systems, depend upon user authentication to handle security. Most have moved to a session-based model rather than using the web server security available in HTTP Basic and Digest authentication. A form is presented to the user, and the posted information is compared to the user information stored to determine access rights.

Most of these Open Source applications store the user authentication in a relational database, usually because the database is used for other purposes. Each application includes installation of user tables with the attributes needed for that application. Installation of another application will install another set of tables. Users will need to be set up in both applications, and maintained separately. Examples of these applications include geeklog (<http://www.geeklog.net>), PostNuke (<http://www.postnuke.org>), typo3 (<http://typo3.com>) and Mambo Open Source (<http://www.mamboserver.com>). Each of these applications includes administrative tools and unique tables for

maintaining users. Although useful in a isolated context, these tools do not fit in an environment where many different applications are running that need common authentication credentials.

I also built some specific applications for my own use, both on my home network and for my corporate responsibilities. Home applications included photo galleries for organizing pictures of the family, online address books, and journals of my children's activities. For work I built a security issues tracking database, a database for monitoring the logs on our email content filters, web sites that monitored various network devices using tools such as MRTG (<http://www.mrtg.com>) and Nagios (<http://www.nagios.org>). I also had some straight HTML pages that I wanted to have varying levels of classification. Giving people various levels of access to each of these applications meant maintaining user information, and although I wrote many of the applications to take advantage of specific user tables, I still wasn't taking advantage of any central provisioning available in the corporate infrastructure. The default answer was to use Microsoft IIS servers and HTTP authentication to specific directories, allowing the users to use their Windows Network logons to access information. The addition of each Windows Server/SQL Server application increased costs to the enterprise, and the "locking in" of one technology limited our ability to creatively solve problems. I needed to find a way to authenticate users and classify information while still using the open source tools that gave me the flexibility to creatively solve problems.

What I needed was a standards-based way to authenticate users and classify data that would work with any technology.

Putting It Together - During

One of my central responsibilities at my job is to begin to solve this issue of "silos of authentication". Windows networks, email systems, ERP systems, Unix accounts, Web applications, HR systems, and one-off applications are scattered around any enterprise, and provisioning and maintaining these accounts takes a significant amount of effort and resources.

Many of these systems are, to one degree or another, moving to support LDAP authentication mechanisms. A decision had already been made based upon some commitments made and software purchased that a corporate LDAP directory would be used. The specific software used for this directory, however, was in the decision process. I decided to go ahead and prototype the authentication mechanisms I would need using freely-available tools, and make sure that I would be able to use any of the commercial directories as needed when final implementation was done.

Decision - Why Sessions?

Apache, the most popular web server in use today¹, has a module available for LDAP authentication of HTTP connections. This implementation, however, did not meet my needs because I require session based authentication. Some of the reasons for using session based authentication instead of HTTP based authentication include the following:

- ✍ Session Variables – Sessions can store information about the current state of the transactions and retrieve that information between submissions. Session variables allow stateful applications to be built on the stateless HTTP protocol.
- ✍ Session Control – Sessions can be destroyed as well as created, allowing a user to actually log out of an application. HTTP authentication is persistent until the browser is closed. In addition, cookies can be timed out so that idle sessions are automatically logged off.
- ✍ Encryption – Although HTTP authentication has a hashed Digest option available², most HTTP authenticated sites use only basic authentication. Sites mainly choose this limited method for ease of use, but many assume a common misconception that because the password field is obscured, the password must be encrypted in transit. This is incorrect – the password field in Basic authentication is sent in the clear. However, for session based authentication, if the server is SSL encrypted and the form is submitted with a https:// URL, the authentication credentials are also encrypted.

Decision - Why Directories?

A directory server is essentially an information store that is optimized for reads. The Domain Name System (DNS) is a type of directory server that is optimized for both reads and for the type of information it maintains. A generalized directory server, on the other hand, can store information about people, locations, groups, applications, network devices, and anything else for which there is a need for fast retrieval of information that does not change very often. Directory servers should be stable, extensible and distributed, to allow for redundancy and local administration of the information. The DNS system is fast, stable and distributed, but is not very extensible, and so is not a general directory server.

Directory servers are often seen as lightweight databases, and there is some misunderstanding of the use of directory servers. Although a directory server may be implemented with a database on the back-end, a directory server would

¹ Netcraft Survey, July 2003 © Netcraft, Ltd.

http://news.netcraft.com/archives/web_server_survey.html

² HTTP Authentication: Basic and Digest Access Authentication <http://www.ietf.org/rfc/rfc2617.txt>

be a very bad choice for any system that requires any kind of transactional capability. As a matter of fact, directory servers are usually set up to limit updates to a few specific roles, and possibly to allow people to update their own information.

Directory servers allow large organizations to delegate administration of users, networks, names and devices to local administrators, while maintaining a single way of accessing that information from anywhere. Directory servers provide “white pages” functionality, and can bring information in from disparate sources for ease of access, for example updating a person’s name, address, and employee information from an HR system while taking their office assignment from an administrative database and the phone number from the PBX system. A network-focused directory server can provide benefits to an enterprise by:

- Facilitating distributed networking by bringing in information from different network resources into a central location. Directory servers are highly scalable and integrate disparate systems using Internet standards.
- Easing network administration by providing a central store of information for provisioning systems.
- Enhancing network reliability and performance by providing a distributed, redundant core of information.
- Unifying access to those distributed resources, with the ability to use aliases to locate network resources which may move locations of even NOS connections, single network logons across systems, and centralized naming standards.
- Improving security by providing distributed provisioning with central control and providing directory object security through a unified standard.³

Decision - Why LDAP?

LDAPv3, the core of which is defined in RFCs 2251 through 2256, is a “lightweight” implementation of the X.500 Directory Services standard. X.500 is considered “heavyweight” because it requires implementations to be written using the seven layer OSI model. LDAP, on the other hand, is implemented using the TCP/IP stack, which is considerably easier to use. There is nothing “lightweight” about the directories themselves – a LDAP implementation can use the same heavy-duty directory data stores used by X.500 implementations. “Lightweight” refers to the ease of access through the TCP/IP protocols.

LDAP is being adopted as the defacto standard for directory access by many organizations and applications. Microsoft’s Active Directory, Lotus’ Domino Server, Sun/Netscape, Novell, Computer Associates, IBM and many others offer

³ Sheresh and Sheresh, Understanding Directory Services, pp. 8-15

implementations of LDAP that differ widely in administration, implementation and data storage, but all can be accessed via an LDAP client and all implement the concept of a directory schema.

Classification Of Data

An important decision in the implementation of any data security scheme is the classification of the data – how will the authorization work? We are moving to a Role-Based Security model, and the design of the LDAP authentication supports that model. In a Role-based model, data is classified according to the roles of the users who will have access to the data. Roles are implemented by including users in groups set up to define each role. So, for example, we have a ‘anonymous’ group that defines the role of someone whose identity is currently unknown to the application, and an ‘allusers’ role which is composed of anyone who has a valid logon and is currently logged on. Note that these are both different from the ‘all’ role, which is everyone, whether logged on or not.

Other roles/groups can be defined by who you are – a ‘family’ role on a home intranet, a ‘it security’ group – or a function of your job, for example a ‘mail admins’ role. Again, your role is defined by including you in the appropriate groups. Data is then classified and secured by making it an ‘app’ in the LDAP directory. As an example, this paper is classified for authenticated users by including the following entry in the directory:

```
# gsecpaper, app, jalcorn.net
dn: cn=gsecpaper,ou=app,o=jalcorn.net
cn: gsecpaper
member: cn=allusers,ou=group,o=jalcorn.net
labeledURI: http://jalcorn.net/gsecpaper/index.php
~gsecpaper/index.php~~GSEC
  Paper Online~
objectClass: groupofnames
objectClass: labeleduriobject
objectClass: top
```

(Note that there is some extra code in the labeledURI attribute used to modify how the menu is displayed). The ‘gsecpaper’ application will now be available to any authenticated user of the website, but an authenticated user will be denied access. The data is then secured by changing the HTML file to a PHP file and including the following code at the beginning:

```
1. <?php
2. $appname='gsecpaper';
3. $needauth=1;
4. require_once "secure.php";
5. ?>
```

Implementation

I used an implementation example of Session-based authentication as a starting point found at <http://martin.f2o.org/php/login>. This implementation focused on securing sessions and used the PHP PEAR Database libraries available at <http://pear.php.net>. Although the PEAR Database module contains a LDAP implementation, I found that the code was poorly documented and difficult to use, so I used the direct LDAP PHP calls documented at <http://php.net>.

System Software

For the example implementation, I have used the following software:

- OpenLDAP v 2.1.22
- BerkeleyDB v 4.1.25 (Required for OpenLDAP)
- Apache v 1.3.27
- PHP v 4.3.2 (compiled `-with-ldap`)
- RedHat Linux 8

All software (except the operating system) was compiled from source from the latest releases. Examples are written in PHP, but could also have been written in other languages such as C/C++ or Perl.

LDAP configuration

One of the security concerns with using a relational database to authenticate users is that the application must store and pass its credentials for accessing the database. LDAP on the other hand allows anonymous binding for accessing the directory, allowing us to implement the authentication routines without the need for any password storing. However, the access controls must be set correctly to allow searching the directory data. The access controls set for this example are:

```
access to dn.base="cn=Subschema" by * read
access to attrs=userPassword
    by self write
    by * auth
access to attrs=uid,entry
    by * read
access to dn.children="ou=app,o=jalcorn.net" by * read
access to dn.children="ou=group,o=jalcorn.net" by * read
access to *
    by self write
    by users read
    by anonymous auth
```


This access list allows authentication to the LDAP server with an anonymous bind, and allows the anonymous user to search the 'app' and 'group' organizational units, plus search the person ou and see the uids. Complete LDAP configuration information is beyond the scope of this paper but can be found at the OpenLDAP page (<http://www.openldap.com>) and more LDAP information can be found at the LDAP Zone (<http://www.ldapzone.com>) .

Directory Design

To accomplish our goals of authentication and authorization using LDAP directory services, we are going to store three kinds of information in the directory. First, user information including a unique ID and password, along with name and other information. Authorized users will be stored in the organizational unit ou=person and will use the inetOrgPerson object class defined in RFC 2798⁴. The DN for users will be constructed from the uid, rather than the common name (cn), to ensure uniqueness and make logons easier.

Application information will be stored in ou=app. Application objects will be constructed of objectClass groupOfNames (RFC 2256)⁵ and labeledURIObject (RFC 2079)⁶. The groupOfNames gives us a 'member' attribute which is a DN of another object (in this case, groups) while the labeledURI attribute will contain a URL and some text describing the application.

Group information will be used to tie the applications and users together, and will be stored in ou=group. Groups are built from the objectClass groupOfNames and the 'member' attributes are the DNs of users or of other groups.

⁴ Definition of the inetOrgPerson LDAP Object Class <http://www.ietf.org/rfc/rfc2798.txt>

⁵ A Summary of the X.500(96) User Schema for use with LDAPv3
<http://www.ietf.org/rfc/rfc2256.txt>

⁶ Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs) <http://www.ietf.org/rfc/rfc2079.txt>

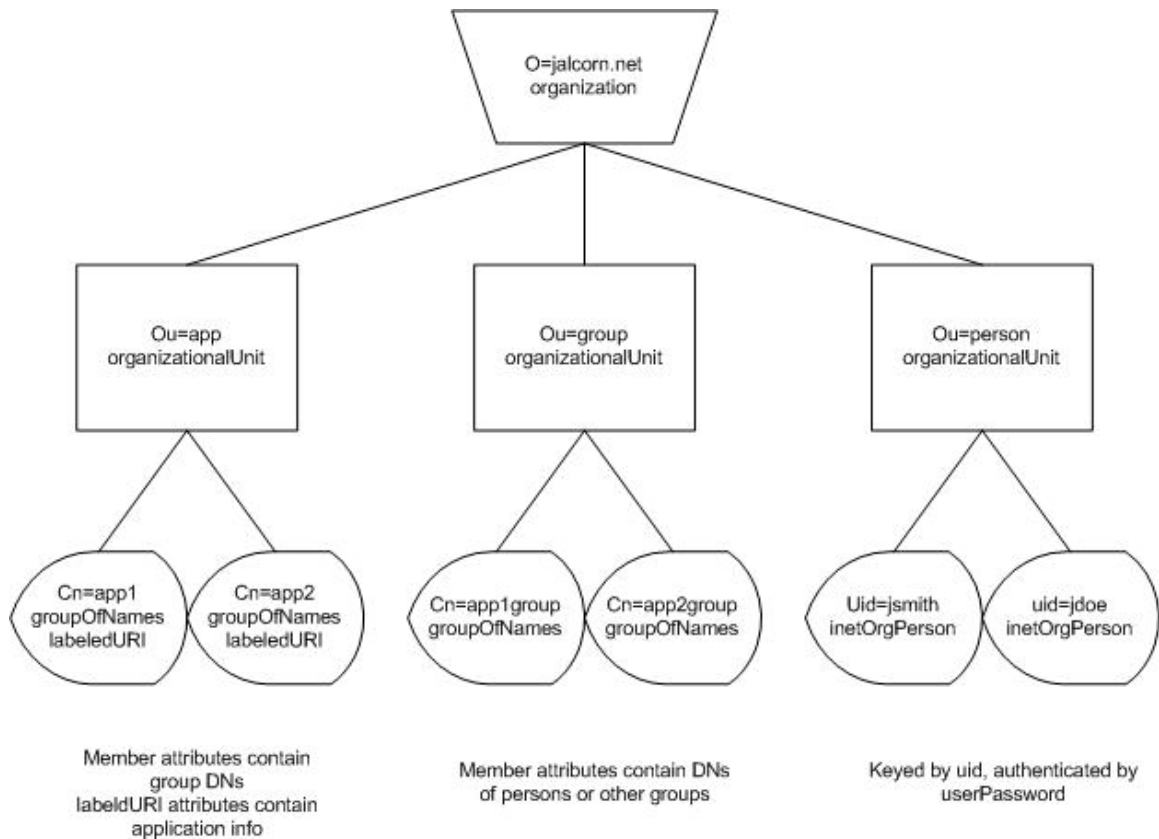


Figure 1 - LDAP Organization

Object Code

The code to implement LDAP integration is contained in 2 PHP classes. The `ldapDB` is a class representing a LDAP directory connection. The class file `ldapDB.php` is stored on the web server in a directory specified in the PHP search path.⁷

```

6. <?php
7. class ldapDB {
8. //
9. // ldapUser.php (c) 2003 Justin B. Alcorn
10. /*
11. * This script is free software;
12. * you can redistribute it and/or modify
13. * it under the terms of the GNU General
14. * Public License as published by
15. * the Free Software Foundation;
16. * either version 2 of the License, or
17. * (at your option) any later version.
18. *
19. * The GNU General Public License can be found at
20. * http://www.gnu.org/copyleft/gpl.html.

```

⁷ For information on configuring PHP, see <http://www.php.net>

```

21.  *
22.  * This script is distributed in the hope
23.  * that it will be useful,
24.  * but WITHOUT ANY WARRANTY; without even
25.  * the implied warranty of
26.  * MERCHANTABILITY or FITNESS FOR A PARTICULAR
27.  * PURPOSE. See the
28.  * GNU General Public License for more details.
29.  */
30.  //
31.  // Based on an idea from http://martin.f2o.org/php/login
32.  //
33.  var $conn = null; // LDAP Connection Object
34.  var $bound = 0;
35.  var $anon = 0; // Anonymous Connection
36.  var $binddn = null; //
37.  // basedn for all searches
38.  var $base = null;
39.  var $host = null;
40.
41.  function ldapDB($host,$base,$uid="", $pwd="") {
42.      $this->host = $host;
43.      $this->base = $base;
44.      $this->conn = ldap_connect($host) or die("Cannot connect
to LDAP $host\n");
45.      // We always start with an anonymous bind
46.      ldap_bind($this->conn) or die("Anonymous bind
failed\n");
47.      $this->bound = 1;
48.      $this->anon = 1;
49.      $this->binddn = null;
50.      if ($uid) {
51.          // Make sure that attempts with NULL passwords do not
succeed
52.          if (! $pwd) {
53.              $pwd = crypt(microtime());
54.          }
55.          $filter = "(cn=$uid*|uid=$uid*)";
56.          $res = ldap_search($this->conn,$this->base,$filter);
57.          $cnt = ldap_count_entries($this->conn,$res);
58.          if ($cnt == 1) {
59.              $entry = ldap_first_entry($this->conn,$res);
60.              if ($entry) {
61.                  $bdn = ldap_get_dn($this->conn,$entry);
62.                  if ($bdn) {
63.                      if (@ldap_bind($this->conn, $bdn, $pwd)) {
64.                          $this->anon = 0;
65.                          $this->binddn = $bdn;
66.                      }
67.                  }
68.              }
69.          } else {
70.              if ($cnt == 0) {
71.              } else if ($cnt > 1) {
72.              } else {
73.              }
74.          }

```

```

75.         }
76.     } // function ldapDB
77.
78.     function isConn() {
79.         if ($this->conn) {
80.             return TRUE;
81.         }
82.         return FALSE;
83.     }
84.
85.     function isBound() {
86.         if ($this->bound) {
87.             return TRUE;
88.         }
89.         return FALSE;
90.     }
91.
92.     function isAuthUser() {
93.         if ($this->binddn) {
94.             return TRUE;
95.         }
96.         return FALSE;
97.     }
98.
99.     function isAnon() {
100.        if ($this->anon) {
101.            return TRUE;
102.        }
103.        return FALSE;
104.    }
105. } // class ldapDB

```

The class' constructor takes the hostname and a basedn as required arguments. It first attempts an anonymous bind to the server, and searches for the user's UID. This allows the directory to be set up hierarchically - the user doesn't need to authenticate with their complete Distinguished Name (i.e. uid=jalcorn,ou=itsecurity,ou=person,o=jalcorn.net) but only needs to use their Unique ID (jalcorn).⁸ Note that we allow the uid to be a 'cn' also, this is to allow the rootdn to also authenticate, as the rootdn is usually implemented as a organizationalRole, which has no uid attribute. Once the anonymous bind is successful, the user's dn is found, and a bind is attempted with the supplied password. If the bind is successful, the user has successfully authenticated.

Methods in this class simply allow for human-readable implementations of information needed from the class, for example 'is this user authenticated?'

The class that implements the methods needed for session authentication and

⁸ Note that the code could allow uids to clash, but this code is not implemented in this example. The code would loop through all found dn's until it found one that was able to bind with the supplied password. A glitch in the design would create an issue if two people had the same uid and same password – an argument for making uid unique throughout the directory.

authorization is the ldapUser class, implemented in the file ldapUser.php.

```
106. <?php
107. class ldapUser {
108. //
109. // Copyright © 2003 Justin B. Alcorn
110. // All Rights Reserved
111. /*
112. * This script is free software;
113. * you can redistribute it and/or modify
114. * it under the terms of the GNU General
115. * Public License as published by
116. * the Free Software Foundation;
117. * either version 2 of the License, or
118. * (at your option) any later version.
119. *
120. * The GNU General Public License can be found at
121. * http://www.gnu.org/copyleft/gpl.html.
122. *
123. * This script is distributed in the hope
124. * that it will be useful,
125. * but WITHOUT ANY WARRANTY; without even
126. * the implied warranty of
127. * MERCHANTABILITY or FITNESS FOR A PARTICULAR
128. * PURPOSE. See the
129. * GNU General Public License for more details.
130. */
131. //
132. // Based on an idea from http://martin.f2o.org/php/login
133. //
134.     var $ldadb = null; // ldapDB pointer
135.     var $failed = false; // failed login attempt
136.     var $date; // current date GMT
137.     var $dn = null;
138.     var $logged = 0;
139.     var $attrs = array();
140.
141.     function ldapUser(&$ldapdb) {
142.         $this->ldapdb = $ldapdb;
143.         $this->date = $GLOBALS['date'];
144.         // Does the user have an existing session?
145.         if ($_SESSION['logged'] & $_COOKIE['ldapUserTimeout']) {
146.             $this->_checkSession();
147.         }
148.         return $this;
149.     }
150.
151.     // checkLogin
152.     //     authenticates the user against the LDAP server
153.     //
154.     function checkLogin($username, $password) {
155.         $newdb = new ldapDB($this->ldapdb->host,
156.                             $this->ldapdb->base,
157.                             $username, $password);
158.         if ( $newdb->isAuthUser() ) {
159.             error_log("We have a good logon",0);
```

```

160.     $this->ldapdb = $newdb;
161.     $this->dn = $newdb->binddn;
162.     $this->logged = 1;
163.     if ($res = ldap_search($newdb->conn,
164.                           $newdb->base,
165.                           "(uid=".$username.*)",
166.                           array("uid","cn","sn","givenName","title")))
    {
167.         if ($entry = ldap_first_entry($newdb->conn,$res)) {
168.             $this->attrs =
169.                 ldap_get_attributes($newdb->conn,$entry);
170.         } else {
171.             $this->attrs = array();
172.         }
173.         $saveattrs = serialize($this->attrs);
174.         $_SESSION['attrs'] = $saveattrs;
175.         $_SESSION['dn'] = $this->dn;
176.         $_SESSION['logged'] = true;
177.
178.         $this->_updateCookie();
179.         return true;
180.     } else {
181.         error_log("LDAP err".ldap_error($this->ldapdb-
182. >conn),0);
183.     }
184.     } else {
185.         error_log("Failed LDAP Bind for $username $password",0);
186.         $this->failed = true;
187.         $this->logout();
188.         return false;
189.     } // checkLogin
190.
191. //
192. // inGroup - return true if $this->dn is a member of $group,
193. // or a member of any group within $group.
194. //     Function is recursive.
195. //
196. function inGroup($group) {
197.     $dnparts = ldap_explode_dn($group,0);
198.     // all is a pseudo-group. All, including anonymous,
199.     // are in this group.
200.     //     Make sure cn=all,ou=group,o=<org> is in the dir.
201.     if ($dnparts[0] == "cn=all") {
202.         return true;
203.     }
204.     //allusers is a pseudo-group that includes anyone logged in.
205.     //     make sure cn=allusers,ou=group,o=<org> is in the dir
206.     if ($this->logged && $dnparts[0] == "cn=allusers") {
207.         return true;
208.     }
209.     // users who are not logged in.
210.     //     again, create the pseudo-group
211.     if ($dnparts[0] == "cn=anonymous") {
212.         if ($this->logged) {
213.             return false;
214.         } else {

```

```

215.         return true;
216.     }
217. }
218. if ($this->dn) {
219.     $srch = "objectclass=*";
220.     if ($res = @ldap_read($this->ldapdb->conn,$group,$srch))
221.     {
222.         if ($e = @ldap_get_entries($this->ldapdb->conn,$res))
223.         {
224.             $entry = $e[0];
225.             if (in_array('groupofnames',
226.                 $entry['objectclass'])) {
227.                 $i = 0;
228.                 while ($i < $entry['member']['count'] ) {
229.                     if ($this->dn == $entry['member'][$i]) {
230.                         return true;
231.                     } else {
232.                         if ($this->inGroup($entry['member'][$i]))
233.                         {
234.                             return true;
235.                         }
236.                         $i++;
237.                     }
238.                 }
239.             }
240.         }
241.         if (ldap_errno($this->ldapdb->conn)) {
242.             error_log("inGroup:". $group. ":" . ldap_error($this->
243.                 >ldapdb->conn), 0);
244.         }
245.         return false;
246.     } // inGroup
247.
248. //
249. // appPerm - return true if $this->dn a part of any
250. // group listed in the members of the $app object
251. //
252. function appPerm($app) {
253.     if (!$app) {
254.         return false;
255.     }
256.     $srch = "objectclass=*";
257.     $sbase = "cn=".$app.",ou=Apps,".$this->ldapdb->base;
258.     if ($res = @ldap_read($this->ldapdb->conn,$sbase,$srch)) {
259.         if ($e = @ldap_first_entry($this->ldapdb->conn,$res)) {
260.             $entry = @ldap_get_attributes(
261.                 $this->ldapdb->conn,$e);
262.             $j = 0;
263.             while ($j < $entry['member']['count'] ) {
264.                 if ($this->inGroup($entry['member'][$j])) {
265.                     return $entry['labeledURI'][0];
266.                 }
267.                 $j++;
268.             }

```

```

269.     }
270.     if (ldap_errno($this->ldapdb->conn)) {
271.         error_log("appPerm:". $app. ":". ldap_error($this->ldapdb-
>conn), 0);
272.     }
273.     return false;
274. } // appPerm
275.
276. //
277. // listApps - return a list of apps that the user is
278. // allowed to access. Useful for building a dynamic
279. // menu
280. //
281. function listApps() {
282.     $srch = "(objectClass=labeledURIObject)";
283.     $sbase = "ou=Apps,". $this->ldapdb->base;
284.     if ($res = @ldap_search($this->ldapdb->conn, $sbase, $srch,
array("cn", "labeledURI"))) {
285.         if ($entries = @ldap_get_entries(
$this->ldapdb->conn, $res)) {
286.             $i = 0;
287.             while ($i < $entries['count']) {
288.                 if ($this->appPerm($entries[$i]['cn'][0])) {
289.                     $apps[] = $entries[$i]['labeleduri'][0];
290.                 }
291.                 $i++;
292.             }
293.         }
294.     }
295.     if (ldap_errno($this->ldapdb->conn)) {
296.         error_log("listApps:". ldap_error($this->ldapdb-
>conn), 0);
297.     }
298.     return $apps;
299. } // listApps
300.
301. //
302. // logout - destroy the session, set all variables to defaults
303. //
304. function logout() {
305.     $_SESSION['logged'] = false;
306.     $_SESSION['dn'] = null;
307.     $this->logged = 0;
308.     setcookie('ldapUserTimeout', 0, time()-86400);
309. } // logout
310.
311. //
312. // _updateCookie - utility that sets the timeout cookie
313. //
314. function _updateCookie() {
315.     setcookie('ldapUserTimeout', 1, time()+(60*30), '/');
316. } // _updateCookie
317.
318. //
319. // _checkSession - make sure the session has not been hijacked
320. function _checkSession() {

```



```

321.     // This is where a session can be 2xchecked.
322.     // For these purposes, if the session exists, we're logged
    in
323.     if (TRUE) {
324.         $this->dn = $_SESSION['dn'];
325.         $this->logged = 1;
326.         $this->attrs = unserialize($_SESSION['attrs']);
327.         $this->_updateCookie();
328.     } else {
329.         $this->logout();
330.     }
331. } // _checkSession
332. }
333.
334. ?>

```

The constructor for `LdapUser` takes as a parameter an existing `LdapDB` object, and checks to see if the user has an existing session. If there is no session, the object is created and returned. Otherwise, the session is checked. In this example implementation, we assume that if the session exists it is valid. Note, however, that PHP session hijacking is a known possibility, and any production implementation should have code in the `_checkSession` utility function that would double check the validity of the existing session. The cookie used is a idle timeout, and is updated with each call to the object. Absolute timeouts can also be implemented by setting a time-limited cookie at login and checking for it's existence.

New logins are handled by the `checkLogin` method. We create a new `LdapDB` object using the authentication parameters. If the `LdapDB` object returns as a authenticated user, the user is now logged on and we store the relevant information about the user in the `LdapUser` object. We also save certain attributes useful to applications in the PHP session variables. If the website wants to use a 'remember me' option for logins, a third parameter should be implemented here and some information should be saved in a persistent store, allowing a permanent cookie to authenticate a user. The constructor method can then check for this cookie. This should not be implemented for any site where the authentication and authorization is used for sensitive information.

The other methods implemented in `LdapUser` are used for the authorization function of the class. The `inGroup()` method is used to determine if the current user is a member of the named LDAP group. The function is recursive, so if the user is a member of any subgroups, the method will return true. Method `appPerm()` is used to determine if the current user has authorization to use the named application, as listed in the `ou=app` LDAP subtree. The app's 'member' attribute contains the distinguished names of each group that has authorization to use that application. `appPerm()` uses the `inGroup()` method to determine if the user should be allowed to use the application.

The method `listApps()` uses `appPerm()` to check each listed application and

return a list of applications that the current user is authorized to use. This method is useful to build a dynamic menu of usable applications.

Using the class objects

To simplify securing any PHP applications on a web server, a PHP include file can be used. As an example, the following file, 'secure.php', can be placed in the PHP include path:

```
1. <?php
2. //
3. // based on an idea from http://martin.f2o.org/php/login
4. //
5. require_once "ldapDB.php";
6. require_once "ldapUser.php";
7.
8. $LOGIN_PAGE = "/index.php";
9.
10. // Start the session
11. session_start();
12. session_register();
13.
14. $date = gmdate("'Y-m-d'");
15. $ldapdb = new ldapDB("localhost", "o=jalcorn.net");
16. $user = new ldapUser($ldapdb);
17.
18. if (! $user->logged ) {
19.     session_defaults();
20.     if (! $noredirect == 1) {
21.         header ("Location: ".$LOGIN_PAGE);
22.         exit;
23.     }
24. }
25. if ($needauth && (! $appname || ! $user->appPerm($appname))) {
26.     header("Location: ".$LOGIN_PAGE);
27.     exit;
28. }
29.
30. function session_defaults() {
31.     $_SESSION['logged'] = false;
32.     $_SESSION['dn'] = '';
33.     $_SESSION['cookie'] = 0;
34. }
35.
36. ?>
```

The code here starts the PHP session, creates the anonymous bind to the ldap server, and instantiates the ldapUser object. If the user has an authenticated PHP session, the ldapUser object will have the user's information, with an anonymous bind to the LDAP server.

If the user is not logged on, any session parameters related to the authentication are set to the defaults, and the user is redirected to the page to login, unless an

\$noredirect parameter is set. If the user is required to be authorized to use the application, as signaled by the \$needauth variable, and is not authorized, the user is redirected again. The login page need not be secured, but it can be with the following code snippet:

```
1. <?php
2. $noredirect = 1;
3. $appname = "loginform";
4. require_once "secure.php";
5.
6. if (! $user->logged ) {
7.     // display login form for non-authenticated users
8.     exit;
9. }
10. if (! $user->appPerm($appname)) {
11.     //code For authenticated, but not authorized users
12. } else {
13.     // Code for authorized users
14. }
15. ... remainder of code, for all authenticated users
```

Line 2 tells the application not to redirect if the user is not logged on. The secure.php then sets up the user information, but does not redirect when the user is not logged on. Then the application checks to see if the user is a logged on user, and if not displays the correct form and exits. Line 10 then checks to see if the current user is authorized. If not, some code is executed that could display an error message, redirect the user, reset the session, or provide some other information.

For regular, secured applications, the \$noredirect parameter is not set. Users who attempt to execute the application without authenticating will be redirected to the login form by the 'secure.php' include file. For example:

```
1. <?php
2. $appname = "myapp";
3. $needauth = 1;
4. require_once "secure.php";
5.
6. ... application code
```

Note that the application need not do anything about authentication or authorization. It is all handled by the 'secure.php' include file and the objects.

The Results - After

This code has been implemented as a prototype and example at <http://jalcom.net>. Authentication and authorization is used to provide access to Family photos, personal blogs, calendars, a contacts directory, and

administrative tools. Upon accessing the webpage as an unauthenticated user, a login screen is presented:



This paper was made available to authenticated users by saving it as html, renaming it 'index.php', and adding the following code to the top:

```
1. <?php
2. $appname='gsecpaper';
3. $needauth=1;
4. require_once "secure.php";
5. ?>
```

The app 'gsecpaper' has been included in the directory with authorization allowed for 'allusers'. A user has been set up with username 'example' password 'example'. (Note that the Change Your Password application has a some hardcoded code that disables it's functionality for the example user). Note that the menu of applications, built with the listApp() method, changes on login.



ToDoS

The classes presented here are usable in their present form, but should have more checks to counteract the possibility of session hijacking and other application attacks. Absolute timeouts, 'remember me' functionality, and IP address checking are all ideas that can be incorporated into these classes. Some of these changes have been made in the live code running on the prototype systems.

Impact

After prototyping the code, it was implemented on development systems in a corporate environment with the same tools. The applications that were written for the MySQL database were changed to implement the LDAUser class. Static webpages were secured by changing them to PHP code, as the GSEC paper was, and other applications were rewritten or front-ended with PHP code. All of

these ad-hoc applications, which had previously been running on various machines scattered around the department, were now brought together, along with public security weblogs and virus warning applications, into a IT Security intranet. Communications with the end user population has significantly improved with this tool, and other IT personnel, including the Help Desk, can use some of the applications to find information and build new resources.

During the process of testing different commercial LDAP servers, we imported the authentication information and pointed our IT Security intranet's authentication information to the test servers. In most cases, The LDAP authentication worked with the commercial products as easily as with the OpenLDAP implementation. When we ran into problems with the implementation, it pointed out some places where the directory's implementation of the LDAP protocol may have been somewhat non-standard, and this information was documented and used as part of the decision-making process.

The use of open source tools has allowed us to solve problems in creative ways, and it's adherence to what will soon be corporate standards allows us to expand our possible toolset to solve any future problems to include open source tools. Management, which had originally never considered open source tools for applications building, is now willing to look at open source alternatives when making buying decisions. This project, originally undertaken as a quick proof of concept, has opened the doors to new ways of solving problems.

Conclusion

Using an LDAP server and these objects provides a way for PHP application developers to write secured applications that can use centralized, LDAP provisioned usernames and passwords. In this way, corporations can begin to leverage the flexibility and availability of PHP source code without losing centralized provisioning and strength of a corporate directory server. These PHP examples can easily be extended to Perl, Java, C++ and other languages, and corporations can then build applications in the languages best suited to the task.

References

Sheresh, Beth and Sheresh, Doug. Understanding Directory Services 2000 New Riders Publishing

Wilcox, Mark Implementing LDAP 1999 Wrox Press

Carter, Gerald LDAP System Administration 2003 O'Reilly & Associates

JasonSmith, Michael P. "LDAP Authentication and Session HOWTO"
<http://ldots.org/ldap/>

M. Smith “Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)” <http://www.ietf.org/rfc/rfc2079.txt>

M. Wahl, T. Howes, and Kille, S. “Lightweight Directory Access Protocol (v3)” <http://www.ietf.org/rfc/rfc2251.txt>

M. Wahl “A Summary of the X.500(96) User Schema for use with LDAPv3” <http://www.ietf.org/rfc/rfc2256.txt>

J. Franks, P. Hallam-Baker, et. al. “HTTP Authentication: Basic and Digest Access Authentication” <http://www.ietf.org/rfc/rfc2617.txt>

Martin Tsachev “Creating a Secure PHP Login Script “ <http://martin.f2o.org/php/login>

John Coggeshall “Session Authentication” <http://www.zend.com/zend/spotlight/sessionauth7may.php>

Mark Burnett “Auditing Web Site Authentication, Part Two” <http://www.securityfocus.com/infocus/1691>

O’Reilly & Associates “Web Database Applications with PHP & MySQL” <http://www.wdvl.com/Authoring/Languages/PHP/WebDBApps/>

Netcraft, Ltd, “Netcraft” <http://news.netcraft.com>

© SANS Institute 2003. Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event