introduction to PEAR::LiveUser

Lukas Smith
BackendMedia

smith@backendmedia.com
overview

• introduction
• architecture
• authentication
• permission
  – simple container
  – medium container
  – complex container
• future
• resources
what LiveUser can do for you

• multiple authentication sources
• permissions: rights, groups etc.
• API scales with your needs!
• flexible architecture
• admin API with SQL generator
• supports multiple backends
• integrates with PEAR::Auth
some additional metadata

- PEAR Package (since mid 2002)
- Install via:
  - $> pear install LiveUser-beta
  - $> pear install LiveUser_Admin-beta
- already being used in production
- more than half a dozen active contributors
- over 22,000 total downloads (20 releases)
overview

- separation of authentication and permission storage and handling
- “client“ API: LiveUser.php
- “admin“ API: LiveUser/Admin.php
  - separated from client API
  - follows the structure of the client API
- add own containers / extend existing
- add custom code via observers
- RDBMS independent xml based schema
LiveUser API

// create object
$LU = LiveUser::factory(...);

// user logged in?
$LU->isLoggedIn();

// what happened?
$LU->getStatus();

// check a right
$LU->checkRight($right);

// check a right based on ownership
$LU->checkRightLevel($right, $user, $group);
LiveUser Admin API

// create object
$LUA = LiveUser_Admin::factory(..);
// add a user
$LUA->addUser();
// get all users in perm with auth data
$LUA->getUser('perm', $filter);
// add a right
$LUA->perm->addRight($data);
// get all rights
$LUA->perm->getRights();
LiveUser Admin API

```php
$LUA->per->getGroups(array(
    'fields' => 'group_id',
    'filters' => array('right_id' => array(1, 5)),
    'select' => 'col',
    'orders' => array('perm_user_id' => 'DESC'),
));
/* generates sql and gets the first column
SELECT lu_groups.group_id AS group_id
FROM lu_groups, lu_groupusers, lu_grouprights
WHERE lu_grouprights.right_id IN (1, 5)
AND lu_groups.group_id = lu_grouprights.group_id
ORDER BY lu_groupusers.perm_user_id DESC */
```
overview

- authentication containers
- available containers:
  - database, XML and PEAR::Auth
- PEAR::Auth provides:
  - plaintext, LDAP, POP3, IMAP, vpopmail, RADIUS, Samba, SOAP
- configurable table name
- user definable columns
- extend to fit your needs
overview

• permission container: 
  *simple, medium, complex*

• supported backends: 
  *XML and database*

• client containers are stackable

• switch between complexity levels

• entire storage structure configurable

• extend to fit your needs
simple container

• perm_users
  map auth users to a unique id; user types
• rights
  all rights
• userrights
  assign rights to a user
simple container

- areas
  rights are organized into areas
- applications
  areas are organized into applications
- translations
  metadata for applications, areas, groups and rights
medium container

- groups
  *all groups (user groups and roles)*
- grouprights
  *assigns rights to groups*
- groupusers
  *assigns users to groups*
- area_admin_areas
  *assigns users to area (area admins)*
complex container

- subgroups
- (user|group)rights (revisited)

assign levels

- rights (revisited)
  right implies other right(s)
- right_implied
  right implies other right(s)
same concepts - different names

• RBAC
  – users
  – roles (groups with rights assigned)
  – permissions (assigned rights)
  – objects (areas)
  – operations (rights)
what we are planning on adding

• before stable
  – improve right caching
  – move auth admin API over to SQL generator
  – documentation/unit tests

• future
  – remove dependency on session
  – new authentication methods: NTLM, Kerberos..
  – weak/strong authentication
  – single sign on
  – “on the fly” group membership
where to get more information

• wiki: http://pear.limbourg.com
• website: http://pear.php.net/LiveUser
• mailinglist: liveuser@lists.21st-hq.de
• liveuser article: http://phpmag.net/itr/online_artikel/pseco
• database schema: http://www.backendmedia.com/LiveUser/liveuser
questions? comments? discussions?

smith@backendmedia.com