“Taking the LiveUser Tour”
php|works 2005

Lukas Smith
smith@pooteeeweat.org
Agenda:

- Introduction
- Architecture
- Authentication
- Permission
  - Simple Container
  - Medium Container
  - Complex Container
- Advanced Usage
- Future
Introduction: 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 back ends
- Integrates with PEAR::Auth
Introduction: Some Additional Meta Data

- 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 contributors
- Over 30,000 total downloads
- Last release got 500 downloads within 2 weeks
**Architecture: 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
  - Currently only supports database backend
- Add own containers / extend existing
- Add custom code via observers
- RDBMS independent xml based schema
Architecture: LiveUser Client 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);
// create object
$LUA = LiveUser_Admin::factory(..);
// add a user
$LUA->addUser();
// get perm users with auth data
$LUA->getUser('perm', $filter);
// add a right
$LUA->perm->addRight($data);
// get all rights
$LUA->perm->getRights();
$LUA->perm->getGroups(
    array(
        'fields' => 'group_id',
        'filters' => array('right_id' => array(1, 5)),
        'select' => 'col',
        'orders' => array('perm_user_id' => 'DESC'),
    )
);
Authentication: Overview

- Authentication containers
- Available containers: database, XML and PEAR::Auth
- PEAR::Auth provides: plaintext, LDAP, POP3, IMAP, vpopmail, RADIUS, Samba, SOAP
- Entire storage structure configurable
- Extend to fit your needs
Permission: Overview

- Permission container: simple, medium, complex
- Supported back ends: XML and database
- Client containers are stackable
- Switch between complexity levels
- Entire storage structure configurable
- Extend to fit your needs
Permission: Simple Container

- perm_users
  map auth users to a unique id and permission user types
- rights
  all rights
- userrights
  assign rights to a user
Permission: Simple Container

- areas
  rights are organized into areas
- applications
  areas are organized into applications
- translations
  meta data for applications, areas, groups and rights
Permission: Medium Container

- groups
  all groups (user groups and roles)
- grouprights
  assigns rights to groups
- groupusers
  assigns users to groups
- area_admin_areas
  assign users to area (area admins)
Permission: Complex Container

- subgroups
- (user|group)rights (revisited)
  assign levels
- rights (revisited)
  right implies other right(s)
- right_implied
  right implies other right(s)
Advanced Usage:  
Same Concepts - Different Names

- RBAC
  - Users
  - Roles (groups with rights assigned)
  - Permissions (assigned rights)
  - Objects (areas)
  - Operations (rights)
Advanced Usage: Avoiding the LiveUser Client API

- Embed rights checks in queries
- Embed ownership checks in queries

```php
$level = $LU->checkRight($right_id);
$user_id = $LU->getProperty('perm_user_id');
.group_ids = $LU->getProperty('group_ids');
if ($level < LIVEUSER_MAX_LEVEL) {
    unset $chk[] = 'owner_user_id = '.$user_id
    if ($level == 2) {
        unset $chk[] = 'owner_group_id IN
            ('.implode(',', $group_ids).')';
    }
    unset $query.= ' AND ('.implode(' OR ', $chk).')';
}
Future: Planned Additions

• Before stable
  - Improve right caching
  - Documentation
  - Unit tests

• Future
  - Remove dependency on session
  - New authentication container
  - Weak/strong authentication
  - Single sign on
  - Dynamic group membership
References:

- These slides:

- Websites:
  - http://pear.php.net/LiveUser
  - http://pear.limbourg.com

- Mailing list:
  - liveuser@lists.21st-hq.de

- LiveUser article:
  - http://phpmag.net/itr/online_artikel/psecom,id,595,nodeid,114.html
Thank you for listening .. Comments? Questions?

smith@pooteeweet.org