Identity Management for the LIGO Project: Growing Pains

Scott Koranda for LIGO

LIGO and University of Wisconsin-Milwaukee

November 4, 2010
LIGO-G1001038-v2
LIGO Science Mission

LIGO, the Laser Interferometer Gravitational-wave Observatory, seeks to detect gravitational waves – ripples in the fabric of spacetime. First predicted by Einstein in his theory of general relativity, gravitational waves are produced by exotic events involving black holes, neutron stars and objects perhaps not yet discovered.
LIGO Laboratory =
LIGO Caltech + LIGO MIT +
LIGO Hanford Observatory +
LIGO Livingston Observatory
The LIGO Scientific Collaboration (LSC) is a self-governing collaboration seeking to detect gravitational waves, use them to explore the fundamental physics of gravity, and develop gravitational wave observations as a tool of astronomical discovery. The LIGO Scientific Collaboration was founded in 1997 and currently has more than 800 members from 70 institutions worldwide.
LIGO Scientific Collaboration

[Logos of various universities and research institutions]
LIGO Identity Management: We Had a Mess

LIGO scientists struggled in early 2007:

- **web** Many servers, wikis, log books—multiple identities
- **grid** Request, renew, manage own X.509 certificates
- **shell** Multiple identities each with distinct credential
- **email** Each list managed separately
LIGO Identity Management: We Had a Mess

No single event precipitated new approach

It really came down to two things:

1. Sustained whining from frustrated users
2. Chatting with Ken Klingenstein over drinks
LIGO Identity Management Project

Started in Summer 2007

Knit together existing technologies and tools

Goals:

▶ Single identity for each LIGO person
▶ Single source of membership info
▶ Single credential for each LIGO person
▶ SSO across web, grid, command-line
LIGO Identity Management Project

Found we had two building blocks:

1. The nascent “LIGO Roster” project
   - PHP + Apache + MySQL

2. Kerberos principal for each LIGO member
   - unused at the time
   - scott.koranda@LIGO.ORG
   - users call it their “at LIGO.ORG login”
   - also known as their “albert.einstein” login
LIGO Identity Management Project

Selecting solid tools was the easy part...

- **Kerberos** single identity and credential
- **Grouper** single source of membership info
- **OpenLDAP** solid distributed replication
- **Shibboleth** web SSO with eye towards federation
- **Sympa** sophisticated email list management
- **MyProxy** flexible and easy X.509 from Kerberos
- **CoManage** coming soon!
LIGO Identity Management Project: Pain Points

...hard part is in the details for our VO

- building the UIs for basic identity management
- policy debate blackholes
- rediscovering lessons learned by others
- domestication ain’t done ’till it’s done
- no corner case shall go unexplored
- provisioning and de-provisioning
- highly distributed community
- federating with smaller VOs
Pain Point: Building VO-Specific UIs

Focus on 3 UIs initially

1. MyLIGO for basic identity management
2. per-group membership management
3. per-group email list management
Update My Business Contact Information

Please Select an Affiliation: LSC - UW Milwaukee

LSC - University of Wisconsin - Milwaukee

Office Address 1: UWM Physics Department
Office Address 2: P.O. Box 413
Office Address 3:
City: Milwaukee State: WI
Postal Code: 53201
Country: (Please begin by selecting one of the following Continents)

- North America  ○ Europe  ○ Asia  ○ South America
- Africa  ○ Oceania  ○ Antarctica

UNITED STATES

Office Number:
- Country Code: +1
- City Code: 414
- Local Number: 229 5056

Fax Number:
- Country Code: +1
- City Code: 414
- Local Number: 229 5689

Change Contact Info

Please do not submit any kind of personal contact information.
### Manage LSC Members

No changes are made to the my Ligo database until you click "Commit All Changes" when you are finished.

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>FTE %</th>
<th>Research %</th>
<th>LSC %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Bruce Allen</td>
<td>Faculty, Sr. Sci/Eng</td>
<td>20%</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>2. Eduardo Xavier Amador Caron</td>
<td>Scientist / Engineer</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>3. Warren Anderson</td>
<td>Faculty, Sr. Sci/Eng</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>4. Patrick Brady</td>
<td>Faculty, Sr. Sci/Eng</td>
<td>100%</td>
<td>55%</td>
<td>90%</td>
</tr>
<tr>
<td>5. Jordi Burguet-Castell</td>
<td>Postdoctoral Scholar</td>
<td>100%</td>
<td>100%</td>
<td>80%</td>
</tr>
<tr>
<td>6. Sydney JoAnne Chamberlin</td>
<td>Graduate Student</td>
<td>100%</td>
<td>100%</td>
<td>10%</td>
</tr>
<tr>
<td>7. Jessica Clayton</td>
<td>Postdoctoral Scholar</td>
<td>100%</td>
<td>100%</td>
<td>80%</td>
</tr>
<tr>
<td>8. Jolien Creighton</td>
<td>Faculty, Sr. Sci/Eng</td>
<td>100%</td>
<td>50%</td>
<td>60%</td>
</tr>
</tbody>
</table>
my Ligo

Your subscription status to DASWG

Hello scott.koranda@LIGO.ORG.

You currently **are not a member** of the DASWG group.

Click to join the DASWG group:

Join

---

LIGO Directory Services and Authentication & Authorization Services Infrastructure are supported by the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
Per-group Email List Management

No progress yet...

Need SOAP expertise to leverage Sympa API
VO-Specific UIs: Pain Points

- No dedicated FTE for UI design and implementation
- Small pool of talent and resources to draw on
  (NSF does not fund us to develop identity management UIs)
- Ever evolving requirements and use cases and corner cases
- High user expectations (if Google can...)
Pain Point: Policy Debate Blackholes

- Does FERPA apply to LIGO? If so, how?
- What is required for managing demographics?
- ADA, DDA in the UK, German privacy laws?
- Opt-in, opt-out, information backup & archiving, logging,...

We’re just trying to detect gravitational waves!

LIGO doesn’t have expertise or experience to easily address these types of issues when they come up.
Pain Point: Rediscovering Lessons Learned By Others

- People get married and change name
- People change gender and change name
- People leave and come back
- People leave and come back with different name
- People leave and join a federating VO
Pain Point: Domestication Ain’t Done ’till It’s Done

LIGO cannot take a greenfield approach

We domesticate the tools already being used:

▶ TWiki/Foswiki: must hack the Perl code
▶ MoinMoin: must hack the Python code
▶ Dokuwiki: must hack the PHP code
▶ eLOG: must hack the PHP code

Where is the roadmap for domesticating “simple” tools like wikis?

So busy domesticating legacy apps no time to explore Foodle, Google, other solutions
Pain Point: No corner case goes unexplored

Requirements for the MoinMoin wiki at UWM:

*Most pages should require authentication to view, and LIGO users should use @LIGO.ORG credentials to authenticate, but UWM users should use their ePantherID, and still others should be able to use once-off passwords we give them. Some pages should be viewable by the public, and fine-grained ACLs should work for everything.*

Doable, but don’t underestimate the FTE cost!
Pain Point: Provisioning and De-provisioning

Primary concern is LIGO Data Grid computing cluster accounts

10 different sites, each managed independently
▶ Is an automated approach even technically possible?
  ▶ uid/gid mapping via NIS+, LDAP, plain text files
  ▶ different storage models at each site
  ▶ different file systems at different sites
▶ Would local admins allow automated account creation?
▶ How should a 10 TB home directory be de-provisioned?
▶ When should de-provisioning happen?
  ▶ When Important Person signs off?
  ▶ At a specific date and time?
  ▶ Just how many corner cases can we discover?
▶ How can we be sure it happens at the appointed time?
Pain Point: Highly Distributed Community

- PIs only way identities and membership vetted
  (some PIs can’t be bothered to keep roster current)
- services distributed and ephemeral—coordination difficult
- some providers lack expertise, have no campus IT backstop
- still identifying our sticks and carrots...
- LIGO/Virgo collaboration dysfunction spills over into IdM
Pain Point: Federating With Smaller VOs

Real (and in some cases urgent) science drivers

Need collaboration spaces with
  ▶ astronomers
  ▶ astrophysicists
  ▶ numerical relativists

Requirement to leverage existing @LIGO.ORG identities

Smaller VOs have no (managed) identities to offer!

Until everyone federated try to offer @LIGOGUEST.ORG identities

Plumbing isn’t the problem...it’s all the UI and process work