

Integrating running apps into federations + JANUS

Terena Eurocamp, 11/2009, Budapest



Ernesto Revilla

erny@yaco.es

Integrating running apps into federations



Background:

- Yaco (30 pers Open Source company)
- Setting up the andalusian (south spanish) federation CONFIA
 - started July 2009, due Jan 2010
 - 10 Public Universities
 - Tasks:
 - Provide common infrastructure (validator, IdP homeless, metadata editor and publishing, CMS,...)
 - Provide LMS SP provisioning connectors (SAML2) for Moodle, ILIAS 4, WebCT.
 - Help to set up IdPs & SPs, etc., Doc (Rules, etc.)

The main problem

- ◆ Create another door to get into the app:
 - ◆ Allow users from outside
 - ◆ SSO
 - ◆ Don't trust apps authn
 - ◆ Reuse authentication infrastructure

Integrating running apps into federations

How

- Put SP (door) before apps
- Great OS Apps (SSP, Shibboleth, OIOSAML, etc.)
- SP != App
 - One SP, several apps
 - One app, several SPs
- MAY live in different nodes
- SHOULD be in same FQDN (use proxy!)
- Adjust SP to apps needs

Integrating running apps into federations

Problems that arise:

- No clean separation between authn/authz
 - Default read permission hold for every authntd user?
- User identifiers
 - Not acceptable? (@, -, _)
 - What happens with existing identifiers?
 - Possible name collisions?
 - Must consider specially local identifiers
- Application logout -> SLO
- SP <-> App coupling

Integrating running apps into federations

Our experienciencies:

- We use SSP
 - Simple to install/config
 - Easy to develop new modules (for SP specific needs!)
 - Good documentation
 - Scalable
 - Open source

Protectings apps: trac

- python-> still no native SAML package (until now, thanx to Roland)
- use authmemcookie
- use memcached (good!) (configure the session store!)
- incorrect default permissions for 'authenticated' -> reconfigure default permissions
- post-logout works! (can modify link text & action)
- explicit provisioning not needed
- not so tightly coupled (good!)

Integrating running apps into federations



Protectings apps: subversion

- Still not done
- Could use svn+ssh://, but infrastructure problem (port 22 reserved)
- Difficult to plugin some oauth style authn
- Google just generates a special password

Integrating running apps into federations



Protectings apps: moodle

- Outdated authn plugin, now updated, part of project in trunk
- Php, integration near to trivial:
 - User provisioning on-the-fly thru API
 - User-course enrollment on-the-fly thru API
- Problems:
 - Need to know all data during login (courses)
 - Still no AttributeQuery (front-channel, back-channel, VO?) (bad)
 - Tightly coupled (bad)

Protectings apps: ILIAS 4

- Outdated shib support in trunk
- Now corrected
- Requested to use this one, so use ship 2.0 SP module
- User provisioning and course enrollment working
- Working on logout

Protectings apps: WebCT

- Uses auto sign-on protocol
- Poor documentation, confusing examples
- Loosely coupled (good!)
- Uses POSTs to 'adapters' to provision users
- Uses MAC (Message Authn Code)
 - Argument ordering/mac important!
- On-the-fly user provisioning already works
- Enrollment still missing (due 30/11)
- Logout?
- Actually it's a module for SSP

Integrating running apps into federations



Protectings apps: When django?

- Very soon!
- Due 12/2009
- Based on Rolands work
- WSGI Middleware

Integrating running apps into federations



Some conclusions:

- On-the-fly provisioning possible
- We like SSP (philosophy, project, people)
- Sending all courses during Authn not very scalable
- Authmemcookie good for apps with basic auth.
- AttributeCollector: get attributes from SIS & other sources (actually RDBMS, should be easy to create LDAP, SOAP/REST, etc.)

Summary

- Federation Metadata editing & publishings
- ARP editing
- Module for SSP
- Open Source (code.google.com/p/janus-ssp)
- Created and sponsored WAYF.DK
- Contributions from YACO

A nearer look:

- stores metadata in SQL
- periodically pulls fresh medatadata from SPs & IdPs (cron)
- checks certificates againts CRLs/OCSP
- sends emails if problems arise
- uses multiauth (saml2, x509)
- REST/Json WS to get IdP & SP state for publishing anywhere
- RESTful API for updating metadata still missing

Integrating running apps into federations + JANUS



Any questions?
Any suggestions?

Thanks for your attention
CU at SSP list &
code.google.com/p/yaco-ssp-modules
erny@yaco.es