eXtreme Scale Identity Management (XSIM) in Scientific Collaborations

Bob Cowles, Craig Jackson, Von Welch (PI)

OSG Council - Satellite Update
3 October 2013

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

Background

The collaboratory (VO) has proven itself as the key way of allowing large-scale, multi-organization science collaborations. We now have 15 years of applied research in how the collaboratory should interact with users and resource providers in terms of trust and identity management (IdM).

- Prior OSG talk: http://www.vonwelch.com/pubs/XSIM-OSG-Mar13

XSIM Goal

Enable the next generation of trustworthy extreme-scale scientific collaborations by understanding and formalizing a model of identity management (IdM) that includes the collaboratory.

XSIM Approach

Research and develop a VO-IdM model to express the trust relationships between resource providers (RPs) and VOs.

We are here → Validate the model and determine the motivations that lead to different choices.

Develop guidance to VOs and resource providers in architecting their IdM and trust choices.

Interviewees So Far

RPs

- Atlas Great Lakes T2
- FermiGrid
- GRIF
- U. Nebraska (CMS)
- LCLS
- LLNL
- NERSC
- Blue Waters

VOs

- Atlas
- BaBar
- Belle-II
- CMS
- Darkside
- Engage
- Earth System Grid
- Fermi Space Telescope
- LIGO
- LSST/DESC

eScience Paper

Robert Cowles, Craig Jackson and Von Welch. Identity Management for Virtual Organizations: A Survey of Implementations and Model. eScience 2013 (to appear).

– http://cacr.iu.edu/collab-idm

In a nutshell…

- Primary faction is: when does user-specific information flow from VO to RP?
- When is expressed in VO lifecycle
  - Enrollment, provisioning, request, usage, user support/incident response, (de-provisioning,) never.
- Secondary factors at each stage.
  - Details…

What does model mean?

- Early identification of user by VO to RP -> less delegation and trust by RP.
  - At extreme, VO is just an interface to RP.
- Later/no identification of user by VO to RP -> either…
  - More trust of VO by RP.
  - Desire of RP to have less effort.

Factors Affecting IdM Design

- User-user Isolation
- Persistence of user data or state
- Complexity of VO roles
- Scaling in terms of VO users
- Incentive balance between VO and RP
- Inertia – early relations were more conservative
- Technology limitations

OSG VOs and RPs

- We have modeled a number of OSG VOs
  - ATLAS -> incident response, CMS -> request, Engage -> request, etc.
- And RPs
  - Fermilab -> provisioning, Nebraska -> never.

OSG – specific Future Work

- Documentation of current VOs and RPs in terms of model.
  - From current work, plus more interviews.
  - To help guide future IdM and technology efforts.

- Guide for new VOs and Sites
  - Subset of VO IdM options that are most popular.
  - Guidance based on criteria which is appropraite.

XSIM Future Work

Inclusion of Exascale, Clouds, Portals, Federated IdM.

Understand relationship between model and ramifications of trust violation.

Following our vision, addition of guidance in addition to description by working with VOs.

Guidance and suggestions welcome.

Thank you. Questions?

Von Welch (vwelch@iu.edu)

Our full eScience paper is at:

http://cacr.iu.edu/collab-idm

We thank the Department of Energy Next-Generation Networks for Science (NGNS) program (Grant No. DE-FG02-12ER26111) for funding this effort.