eXtreme Scale Identity Management for Scientific Collaborations (XSIM)

Von Welch (PI), Bob Cowles, Craig Jackson

HEPiX 2013 Spring Meeting
April 17th, 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 science collaborations.

ESG/F, NFC, OSG, ATLAS, CMS, TeraGrid, LIGO, GENI, etc.

We now have 15 years of applied research in how the collaboratory should interact with users and resource providers.

Glide-ins, science gateways, community accounts, etc.

Identity Management

From Wikipedia: **Identity management** describes the management of individual identifiers, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.

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.

Trust Relationships

Need a clear definition of trust for XSIM to clarify our thinking.

Large body of research on trust exists, in computer security, CS, and more broadly.

Trust **–**

A disposition willingly **to accept the risk of reliance** on a person, entity, or system to act in ways that benefit, protect, or respect one's interests in a given domain.

Based on Nickel & Vaesen, Sabine Roeser, Rafaela Hillerbrand, Martin Peterson & Per Sandin (eds.), *Handbook of Risk Theory*. Springer (2012)

XSIM Method

Understand the core elements of the trust relationship between scientific collaborations, resource providers and users.

Understand how those trust relationships are (or desirably would be) expressed in IdM systems.

Validate the model and advance the state of practice through software and applied research.

Approach

Analyze implementations – study literature of the different collaboratory IdM approaches and interview members of the community.

Discern the trust model each implementation strived for.

Enumerate the different relationships between collaborations and their resource providers and the evolution of each (lessons learned)

Analyze the trade-offs of the different trust relationships.

Approach

Derive a model for an evolutionary step in IdM that describes trust relationships between collaborations, resource providers and users.

Model must be understandable and useful to non-IdM experts and is accepted by resource providers.

Refine and extend model based on feedback and experience.

Interviews

Key to understanding the “real reasons” behind implementation and lessons learned.

Results will not be disseminated in raw form so people will speak freely.

Scripted, unstructured format.

Interview Goals – understand …

- Who constitutes the VO, what its goals are, and who its stakeholders are.
- Who the RPs are, their relationship to the VO (why are they serving it), and who their stakeholders are.
- The assets and threats that are in play.
- The policy and technical controls in place between the VO and the RPs.
- The policy and technical controls in place between the VO and its users.
- What are the lessons learned (e.g., what would be done differently if done again).

- **Ultimate goal: to understand the trust relationships (accepted risks) between resource providers/VO/users and how those were arrived at.**

Interviewees So Far …

VOs

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

RPs

- Atlas Great Lakes T2
- U. Nebraska (CMS)
- LCLS

Many more planned (with you!)

Please contact me if interested.

Interview Observations so Far

Data volume is driving changes in computing model – greater complexity; inhibiting clean user interface design

- Batch
  - Compute intensive, production -> cloud (e. g. simulation)
  - Production and initial analysis -> grid or supercomputer
  - Specialized analysis -> local clusters
- Web applications -> multi-site, single sign-on
- Interactive – local/remote IdM – little change

Mitigations & benefits so far have offset increased risk

New computing models force explicit trust relationships

XSIM Schedule

Project start: September, 2012

Y1: Publication and presentation of document describing the results of the interviews and the IdM model. (Targeting CHEP and eScience.)

Y2: Develop software implementing the model and revise the model based on feedback and experience from initial field tests

Y3: Further development of the model user trust relationships; documentation and packaging of the software.

Key Project Relationships

OSG Satellite

- http://opensciencegrid.org/
- Share common interests in better understand VOs in order to serve them. Key stakeholder of work.

Center for Trusted Scientific Cyberinfrastructure

- http://trustedci.org/
- NSF-funded project to help science cyberinfrastructure projects with cybersecurity. Will be guided by XSIM's work.

Thank you. Questions?

Bob Cowles (bob.cowles@gmail.com)

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.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the sponsors or any organization.