Identity Management for Virtual Organizations

Von Welch (PI), Bob Cowles, Craig Jackson

2014 DOE NGNS PI Meeting

September 16, 2014

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

Our Context, Mission, Approach...

The virtual organization (VO) has emerged as key enabler of science. VOs have been incorporated into traditional user-to-resource provider identity management (IdM) in numerous ways (Atlas, CMS, KBase, NFC, ESGF, etc.)

Our mission is to develop a VO-IdM model that (a) expresses and explains observed variations in collaboratory identity architectures and (b) can be leveraged into guidance for selection.

Approach: Semi-structured interviews with 20+ VO-RP relationships, analysis, publication, feedback...

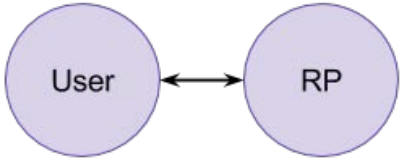
Some core findings….

1. The VO nearly always alters the traditional direct trust relationship between users and resource providers (RPs).
2. That alteration manifests itself as the RP-to-VO *delegation* of IdM tasks based on trust.
3. There are a number of factors motivating and demotivating that delegation.
4. Trend is toward *transitive trust*, utilizing the VO's capacity to represent its members.

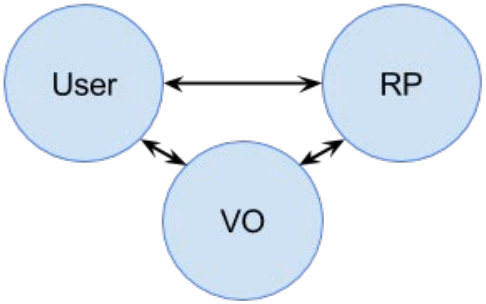
VO IdM Trust Models

... via 800-39

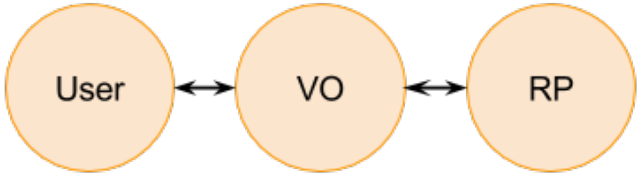
Classically RPs produced and consumed all IdM data.



Brokered trust relationships entail VOs & TTPs generating user data, to be consumed by RPs.



Transitive trust relationships forego all user data consumption by RP.



Types of Factors Affecting IdM Delegation

- Motivators
  - These factors drive the delegation of IdM functions due to the perceived benefits.
- Enablers
  - These factors provide a receptive environment making the delegation of IdM functions easier.
- Barriers
  - These factors prevent or at least inhibit delegation of IdM functions.

Motivators for Delegation

- Scaling and Dynamicity of VO
  - RP incurs significant costs to supply IdM for large VOs or VOs with high turnover rates.
  - Number of institutions involved is secondary factor -- influences use of 3rd party identity provider.
- Complex VO roles and policies
  - RP must track and implement access controls.
  - Can require greater communication between VO and RP.
- VO-run collaboration services
  - Wikis or forums isolated to the VO.
  - VO-supplied IdM rather than depending on RP.
- VO using multiple RPs

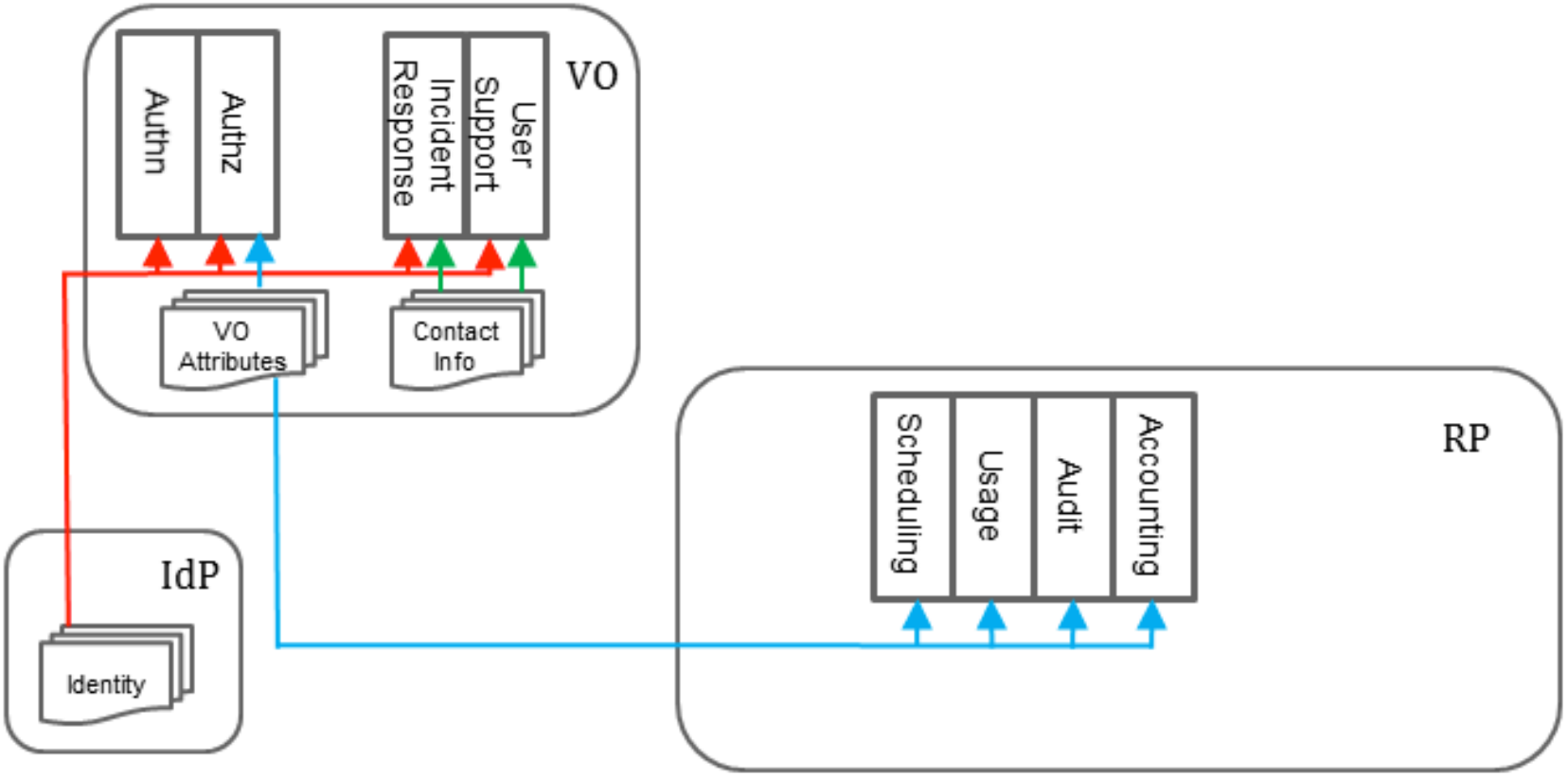
Enablers of Delegation

- Available VO IT/IdM effort and expertise
  - IT knowledgable staff to install/maintain servers.
  - IdM knowledgeable staff for secure configuration.
- Established trust relationships
  - VO has close association with RP or good reputation.
  - VO has history or prior collaboration with RP.
- Available tracing mechanisms
  - Facilitate user support and incident response.
  - Helps mitigate perceived risks from delegation.
- Alignment with RP's mission

Barriers to Delegation

- Low risk tolerance and historical inertia
  - or "We've always done it this way"
  - Changes risk profile
- Compliance and assurance requirements
  - Government regulations or
  - Other oversight or stakeholder requirements
- Technology limitations
  - e. g. Software requires userid/password

Identity Flow for Transitive Trust

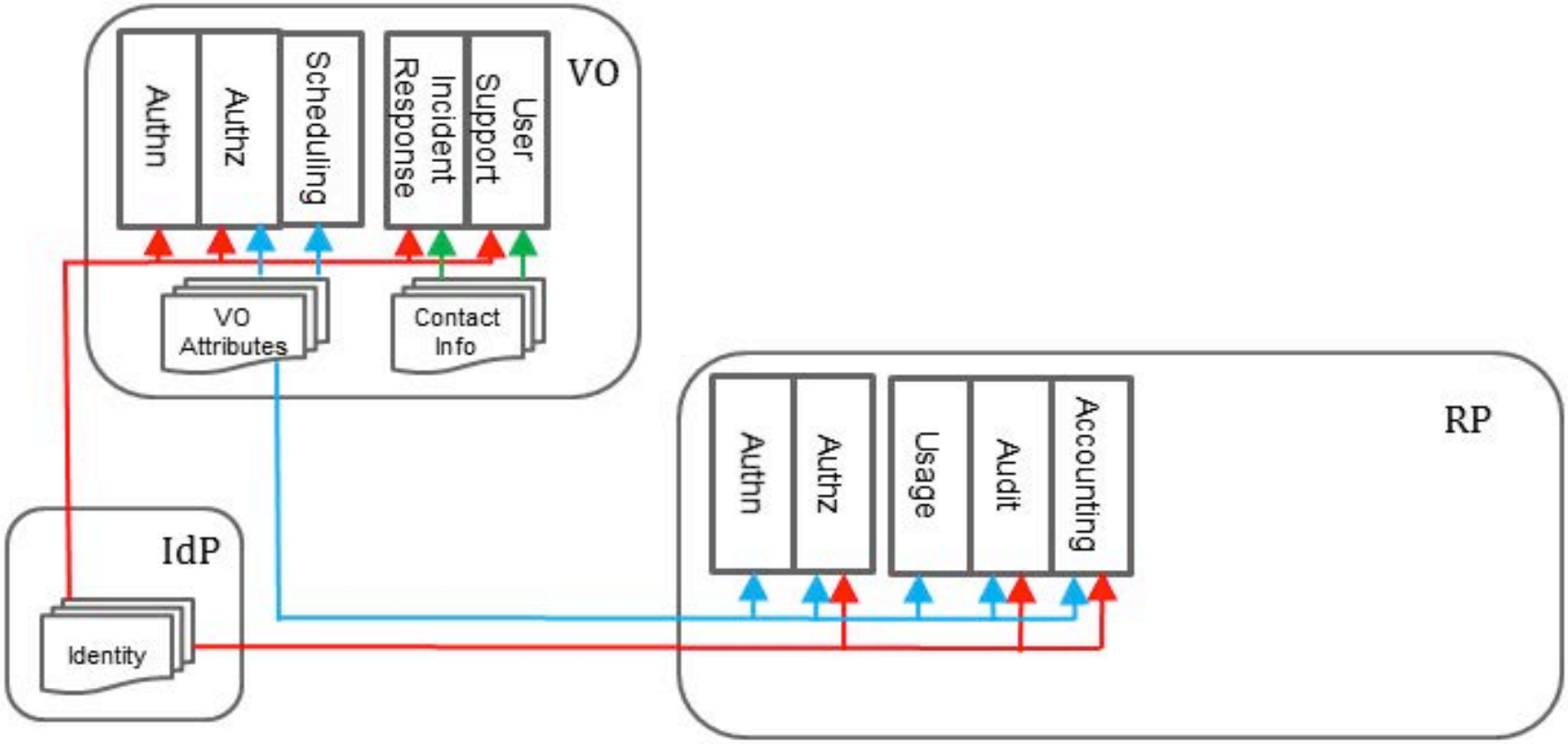


Issues for Transitive Trust

- Lack of persistent personal storage at RP
  - RP is not aware of user identity
  - Data must be staged in/out as part of batch job
- Shared collaborative services
  - Wikis or forums isolated to the VO
  - VO-supplied IdM
- User Support and Incident Response
  - RP has no ability to contact user
  - RP must trust VO to resolve issues

- Roadmap
  - Start with a transitive trust approach (simple) and adjust, as needed, to address particular risks or requirements

Identity Flow--Modified Transitive Trust



Related Work

- Work by I2, Klingenstein, et al.
- NSTIC IDESG Functional Model Group.
- NIST 800-39 (Trust Models).
- Lin, Vullings, and Dalziel. "Trust-based Access Control Model for Virtual Organizations."
- Efforts funded in the EU such as FIM4R and SCI
  - Federated Identity Management for Research https://indico.cern.ch/event/301888/
  - Security for Collaborating Infrastructures https://www.eugridpma.org/sci/

FY2014 XSIM Papers and Documents

Robert Cowles, Craig Jackson and Von Welch. *Identity Management for Virtual Organizations: A Survey of Implementations and Model.* 9th IEEE International Conference on eScience, 2013.
http://www.vonwelch.com/pubs/VOIdM13

Robert Cowles, Craig Jackson and Von Welch. *Identity management factors for HEP virtual organizations*. 20th International Conference on Computing in High Energy and Nuclear Physics (CHEP2013), 2013. http://www.vonwelch.com/pubs/CHEP2013

Robert Cowles, Craig Jackson, Von Welch and Shreyas Cholia. *A Model for Identity Management in Future Scientific Collaboratories*. (DRAFT) International Symposium on Grids and Clouds (ISGC) 2014, 2014.
http://www.vonwelch.com/pubs/XSIMISGC2014

Von Welch, Robert Cowles, and Craig Jackson. *Identity Management Guidance to OSG Virtual Organizations and Resource Providers*. 2014. OSG Documentation Database.
http://osg-docdb.opensciencegrid.org/cgi-bin/RetrieveFile?docid=1199;filename=XSIM%20OSG%20IdM%20Guidance%20-%20June%202014%20-%20v1.pdf;version=1

Bob Cowles, Craig Jackson, and Von Welch (PI). *DESC Identity Management: Analysis and Recommendations* (DRAFT) for review by DESC. August, 2014.

(Pending) Article in monthly OSG Newsletter.

What questions does your research motivate you to now ask?

- What are the failure modes (and possible mitigations) for different IdM delegations?
- Can a risk-based approach allow us to more quickly converge on consensus for such situations (despite social factors)?
- How will “big data” impact the RP-VO relationship?

Thank you

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.

Extra Slides

"Essentially, all models are wrong, but some are useful."

--George E. P. Box