the globus alliance
www.globus.org

GridShib
Grid-Shibboleth Integration

Von Welch, NCSA
Tom Barton, U. Chicago
Kate Keahey, U. Chicago/ANL
Frank Siebenlist, ANL

GlobusWORLD 2005

Some Background: Shibboleth

- http://shibboleth.internet2.edu/
- Internet2 project
- Allows for controlled inter-institutional sharing of web resources
  - Federation of identities and attributes
  - Uses attribute-based authorization
  - Standards-based (SAML)
- Being extended to non-web applications
- Part of NMI/EDIT distribution

Some Background: Globus Toolkit

- http://www.globus.org
- Collaborative work from the Globus Alliance
- Toolkit for Grid computing
  - Job submission, data movement, data management, resource management
- Security based on X.509 identity- and proxy-certificates
- Mix of Web Services and pre-WS (e.g. GridFTP) protocols

What is GridShib?

- NSF Middleware Initiative (NMI) Grant: Policy Controlled Attribute Framework
- We call it “GridShib”
- In a nutshell:
  - Allow the use of Shibboleth-issued attributes for authorization in NMI Grids built on the Globus Toolkit
- 2 year project which kicked off December 1, 2004

Why?

- Attribute-based authorization has shown itself to be useful in large grid, far-flung participants with several types of roles among them
  - NEESgrid, Earth System Grid, TeraGrid, Grid3 (GriPhyN, iVDGL, and PPDG), SCEC
  - Identity-based approach not scaling
- Shibboleth is well supported and deployed by Internet2 project
- SAML is used by larger identity federation world, e.g. Liberty Alliance - integrating SAML support into Grids opens the door to leveraging this large technology space

Leveraging Internet2 Work

- Shibboleth & SAML have shown how to
  - Authorize the anonymous user
  - Extend integration of common infrastructure across administrative and operational domains
- Others are now trying non-browser-based "shibbolization" approaches roughly analogous to what we envision
  - E.g. LionShare
- Plug: all code elements above are NMI components. We're building on 3 years' work of many people.

GridShib Integration Principles

- No modification to typical grid client applications
- Leverage shibboleth's attribute administration and end-user maintenance of attribute release policies
- Leverage high-quality Campus Identity Provider operations
- Leverage high-quality Shib and Grid software
- Try to keep modifications to Grid Services and security clients (e.g. grid-proxy-init)

GridShib Challenges

- Integration of SAML and X.509 identity certificates
  - Use of X.509 certificate identifier as a subject handle for use by the Shib Attribute Authority (SAA)
  - Shibboleth v1.3 should help with this
- Integration of SAML and X.509 attribute certificates
  - E.g. Enable the use of both Shibbolath and VOMS for authorization decisions in the same runtime
  - Derive common attribute expression to allow for use of both/either of this in Globus runtime

GridShib Challenges (cont)

- Distributed Attribute Administration
  - What happens when the folks running the attribute authority are not the ones authoritative for the attributes?
  - Many projects don't have resources to run a 7x24 security service, but are the only ones who know the attribute space.
  - Explore Signet, Grouper (from Internet2)

GridShib Challenges (cont)

- Attribute Authority identification
  - “Where are you from” problem
  - Grids often have different identity providers and attribute authorities
- Plumbing interconnect
  - Getting attributes from Shib into Grid
  - GT4 Web Services base helps with this

Project objectives

- Priority 1: Pull mode operation
  - Globus services contact Shibboleth to obtain attributes about identified user
  - Service has a list of trusted Shib AAs that it can ask about a user
  - User can also present pointer to service
  - Support both GT4.x Web Services and pre-WS code
  - No client side modifications needed

Objectives (cont)

- Priority 2: Push mode operation
  - User obtains Shib attributes and push to service
  - Allows role selection
  - Similar to VOMS and CAS

Timeline

- December 1, 2004: formal start
- February, 2005: Developers on board and coding
- Summer 2005: First release
  - Basic integration: code supporting pull model with user identified
  - Selection and simple implementation of policy description language
  - Targeting GT 4.2
  - Shibboleth 1.3

Acknowledgements

- Working in collaboration with Steven Carmody and the Internet2 Shibboleth Design team
  - Providers of much valuable advice.
- Funded under NSF NMI award SCI-0438424

Questions?

- Project website:
  - http://grid.ncsa.uiuc.edu/GridShib/
- Or contact:
  - vwelch@ncsa.uiuc.edu