Attribute-based Authorization for Science Gateways Using GridShib

Tom Scavo
trscavo@ncsa.uiuc.edu
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
May 14, 2008
Overview

- GridShib Project Update
  - GridShib SAML Tools
  - GridShib for Globus Toolkit
- The TeraGrid Science Gateway Use Case
  - Community Account Model
  - Grid Authorization Model for Science Gateways
  - TeraGrid Deployment Strategy
  - Federated Identity Model for Science Gateways
Acknowledgments

- **Original Project PIs**
  - Von Welch, Tom Barton, Kate Keahey, Frank Siebenlist

- **Developers**
  - Rachana Ananthakrishnan, Jim Basney, Tim Freeman, Raj Kettimuthu, Terry Fleury, Tom Scavo

- The GridShib work was funded by the NSF National Middleware Initiative (NMI awards 0438424 and 0438385). Opinions and recommendations in this paper are those of the authors and do not necessarily reflect the views of NSF.

- The Science Gateway integration work is funded by the NSF TeraGrid Grid Integration Group through a sub-award to NCSA.
GridShib Project Update
History of GridShib

Nonbrowser user; Attribute pull

Browser user; Attribute push

Classic GridShib

TeraGrid Science Gateway Use Case

Dec 2004

Aug 2006

Apr 2008

TeraGrid Authentication, Authorization and Account Management Workshop (ANL)
GridShib Software

- **GridShib for GT**
  - Consumes X.509-bound SAML assertions issued by the GridShib CA or the GridShib SAML Tools. Issues SAML attribute queries to a Shibboleth IdP with GridShib for Shibboleth installed.

- **GridShib for Shibboleth**
  - Responds to attribute queries from GridShib for GT.

- **GridShib CA**
  - Issues short-lived X.509 credentials to browser users.

- **GridShib SAML Tools**
  - Issue or requests SAML assertions and optionally binds these assertions to X.509 proxy certificates.
Deployment Scenarios

http://gridshib.globus.org/docs/gridshib/deploy-scenarios.html
Recent Releases

- GridShib for Globus Toolkit v0.6.0
  - Released April 30, 2008
- GridShib SAML Tools v0.3.2
  - Released March 20, 2008
- http://gridshib.globus.org/download.html
The GridShib SAML Tools (GS-ST) are a standalone suite of Java-based client tools:

- Binds a SAML assertion to an X.509 proxy certificate
- The same X.509-bound SAML token can be transmitted at the transport level or the message level (using WS-Security X.509 Token Profile)

Includes the GridShib Security Framework, an API for producing and consuming X.509-bound SAML tokens.

GS-ST is a SAML producer
GS-ST Features

- Easily installed and configured
- Binds arbitrary content (e.g., SAML) to a non-critical certificate extension
- Multiple output options (SAML, X.509 proxy credential, DER-encoded ASN.1)
- CLI with shell scripts (UNIX and Windows)
- Includes a Java API for portal developers
- Leverages the Globus SAML Library, an enhanced version of OpenSAML 1.1
X.509-bound SAML Token

- GridShib SAML Tools produces *X.509-bound SAML tokens*, a new type of security token that enables attributed-based authorization in X.509-based Grids
- The SAML token is bound to a noncritical X.509v3 certificate extension
Security Tokens

- **X.509 Token**
  - SOAP Envelope
  - SOAP Header
  - X.509 certificate
  - SOAP Body

- **SAML Token**
  - SOAP Envelope
  - SOAP Header
  - SAML assertion
  - SOAP Body

- **X.509-bound SAML Token**
  - SOAP Envelope
  - SOAP Header
  - X.509 certificate
  - SAML assertion
  - SOAP Body
GridShib for GT

- GridShib for GT (GS4GT) is a plug-in for GT 4.x
  - GS4GT is compatible with both GT 4.0 and 4.2
- GS4GT is an implementation of a *Grid Service Provider* (analogous to a Shibboleth Service Provider)
- GS4GT is a **SAML consumer**
GS4GT Features

- Introduces *attribute-based authorization* into GT
- Exposes a single comprehensive *policy decision point* called the *GridShibPDP*
- Implements an *attribute push* model
- Restricts access based on *blacklists* of IP addresses and/or name identifiers
- Provides *attribute-based account mapping*
- Supports optional *gridmap short-circuiting*
- Defines an *attribute-based authorization policy language* (in XML)
GS4GT adds a layer of abstraction that permits both GT4.0 and GT4.2 to be supported simultaneously.
In GT4.0 (deny-overrides), this works because the PDP is at the end of the chain

In GT4.2 (permit-overrides), this authz chain does not honor SAMLBlacklistPDP
GridShibPDP

Permit

Indeterminate

Deny
Complex Authz Policy

- PushPIP → AAIP → BlacklistPDP → MapPIP → MapPIP
- PermitPDP → SAMLDPD → SAMLDPD → SAMLDPD
- Permit → Deny → Deny → Deny
Gridmap File

➢ Flat file format:
  DN → [user_0, user_1, …, user_{n-1}]

➢ Dual function identity-based gridmap file:
  1. Authorization Policy
  2. Username Mapping Policy

➢ A single gridmap file serves both functions
DN₁ username₁
DN₂ username₂
...

Globus Gridmap file

GridShib Mapping Policy

<XML>

<XML>

GridShib Authz Policy
GridShib Policy Files

- Two separate attribute-based policy files:
  1. Authorization Policy
     \[ [A_0, A_1, \ldots, A_{m-1}] \]
  2. Username Mapping Policy
     \[ [A_0, A_1, \ldots, A_{m_1-1}] \rightarrow [\text{user}_0, \text{user}_1, \ldots, \text{user}_{n_1-1}] \]
     \[ [A_0, A_1, \ldots, A_{m_2-1}] \rightarrow [\text{user}_0, \text{user}_1, \ldots, \text{user}_{n_2-1}] \ldots \]
- A single XML-based policy file may encapsulate both types of policies
The TeraGrid Science Gateway
Use Case
Science Gateway

Web Browser

Web Interface

Webapp

WS GRAM Client

Java WS Container

WS GRAM Service

proxy certificate

community account

Science Gateway

Resource Provider

community credential

proxy credential

Key
Community Account Model

- A *community credential* is issued to each gateway.
- The gateway issues proxy certificates (on-the-fly) and makes grid requests on behalf of the user.
- This *community account model* is easy to implement but has some significant drawbacks.
- All requests look exactly the same to the resource provider.
The proposed model incorporates GridShib SAML Tools at the gateway and GridShib for GT at the resource provider.

Using GridShib SAML Tools, the gateway:
1. issues a SAML assertion containing the user's authentication context and attributes
2. binds the SAML assertion to a proxy certificate signed by the community credential
3. authenticates to the resource by presenting the SAML-laden proxy certificate

http://gridfarm007.ucs.indiana.edu/gce07/images/e/e4/Scavo.pdf
GridShib-enabled Gateway

[Diagram showing the flow of information and components involved in a GridShib-enabled Gateway, including Web Interface, Web Browser, Webapp, GridShib SAML Tools, WS GRAM Client, GridShib SAML PIP, WS GRAM Service, Java WS Container (with GridShib for GT), Logs, Policy, Security Context, and attributes, username, community credential, proxy certificate, SAML, Key, and Web Authn.]
User Attributes

- **Gateway entityID:**
  - [https://gridshib.gisolve.org/idp](https://gridshib.gisolve.org/idp)

- **Subject name identifier:**
  - trscavo@gisolve.org

- **Authentication statement**
  - authentication method: urn:oasis:names:tc:SAML:1.0:am:password
  - authentication instant: 2007-08-02T12:10:34-0400
  - IP address: 10.81.193.244

- **Attribute statement**
  - isMemberOf attribute: group://gisolve.org/gisolve
  - mail attribute: trscavo@gmail.com
Current Work

Resource Provider

Java WS Container
(with GridShib for GT)

GridShib
SAML PIP

WS GRAM
Service

Security Context

Logs
Policy

Security table
GRAM audit table

TGCDB
TeraGrid Deployment Strategy

1. GridShib SAML Tools at the Gateway
   • http://www.teragridforum.org/mediawiki/index.php?title=Science_Gateway_Credential_with_Attributes

2. GridShib for GT at the RP
   • Integrate GS4GT into CTSS4

3. Evaluate Shibboleth as a browser-facing federated identity solution
   • Planned Shib work at the TG user portal
   • For the most part, Shibboleth has not yet entered the TeraGrid consciousness
Federated Identity Model

TeraGrid Science Gateway

Shib-enabled Grid Portal → SAML Assertion → response → GridShib-enabled Grid Client → SAML Request → X.509 proxy certificate

Shib-enabled Grid SP

Shibboleth Identity Provider

Browser

Shibboleth SSO Service

GridShib-enabled Attribute Service

X.509 end entity credential

SAML Request

SAML Assertion

X.509 proxy certificate

SAML Request

SAML Assertion

SAML Request

SAML Assertion
Thank you!

Tom Scavo
trscavo@ncsa.uiuc.edu

GridShib
http://gridshib.globus.org/