gPLAZMA: grid-aware Pluggable AuthoriZation Management
(Introducing Role-based Access Control in dCache)

The XVth International Conference on Computing in High Energy and Nuclear Physics (CHEP’06)
February 15, 2006
TIFR, Mumbai
Authors

RANA, Abhishek Singh (University of California, San Diego, CA, USA)
WÜRTHWEIN, Frank (University of California, San Diego, CA, USA)
PERELMUTOV, Timur (Fermi National Accelerator Laboratory, Batavia, IL, USA)
KENNEDY, Robert (Fermi National Accelerator Laboratory, Batavia, IL, USA)
BAKKEN, Jon (Fermi National Accelerator Laboratory, Batavia, IL, USA)
SKOW, Dane (Fermi National Accelerator Laboratory, Batavia, IL, USA)
FISK, Ian (Fermi National Accelerator Laboratory, Batavia, IL, USA)
FUHRMANN, Patrick (DESY, Hamburg, Germany)
ERNST, Michael (DESY, Hamburg, Germany)
Outline

• OSG AuthZ approach
• gPlazma architecture
• gPlazma implementation
• Example of end-to-end AuthZ for CEs and SEs
• Status
• Future Work
OSG AuthZ Approach

• VO-Global specification of privilege attributes per Role.
• Site central mapping of Role to site’s implementation of privilege attributes.
• Local enforcement of privilege attributes.

• Use of VOMS extended X.509 Attribute Certificate specification for defining extra attributes (FQANs or Fully Qualified Attribute Names).
• Based on RFC-3281. FQANs contain Role and VO membership information for a User.
OSG AuthZ Approach

• VO defines Roles and associated privileges by specifying expected functionality.
  – E.g. *cmssoft* may install software in area that is read-only by all *cmsuser* jobs running on site/campus.
  – E.g. *cmsphedex* may have special access to SRM/dCache system.

• Site maps VO scope identities to local scope identities.
  – Site wide management of mapping.
  – Service level granularity of mapping.

• Site enforces VO privilege policies within local scope identities.

• Authorization = (VO-allowed) && !(Site-vetoed)
The diagram illustrates the architectural components and interactions within the Open Science Grid (OSG) framework. It shows how different services interact, including VO (Virtual Organization) Attribute Repository, Site-wide Mapping Service, and Site-wide Authorization Service.

- **Local or Remote Client**: This represents the client's proxy, which can be local or remote and is equipped with VO Membership and Role Attributes.
- **Site-wide Mapping Service**: This service maps requests to the appropriate Site-wide Authorization Service.
- **Site-wide Authorization Service**: This service authorizes requests for specific services X, Y, Z.
- **Auxiliary Mapping Service**: Additional mapping service for Service Z.
- **Auxiliary Authorization Service**: This service authorizes requests for Service Z.
- **Veto**: Service X, Y, and Z have veto mechanisms in place.
- **Site-wide Assertion Service**: This service asserts service requests.
- **Policy Enforcement Points (PEP)**: These are located at Host 1 and Host 2.
- **Policy Decision Points (PDP)**: These points make decisions on policy enforcement.

The diagram highlights the flow of information and decision-making processes within the OSG framework, emphasizing the roles of PEPs and PDPs in the authorization and enforcement of policies.
gPLAZMA Architecture

- SRM Door
- GridFTP Door
- GridFTP Callout
- SRM Callout

Priorities Switches

Plugins
- Storage Provider's Policies
- Storage Metadata AuthZ
- Legacy Grid AuthN (gridmapfile)
- Legacy Storage AuthZ (dcache.kpwd)
- GUMS-based VO Role Mapping AuthZ
- VO Role Mapping AuthZ (gPLAZMA native)
- Storage Metadata AuthZ

Authorization Services
- https/SOA
- SAML

Bias: ACCESS
Priority: 2
Apply: Authorization
Response: AuthZ Record

Bias: DENIAL
Priority: 1
Apply: Assertion
Response: Allow OR Deny
gPLAZMA Implementation

voms-proxy-init
Proxy with VO
Membership | Role attributes

SRM-dCache

SRM Server
GridFTP Server

DATA

srmcp

SRM Callout

gPLAZMA

PRIMA
SAML Client

GUMS
Identity Mapping Service

gPLAZMALite
Lite Authorization Service
gPLAZMALite grid-mapfile
dcache.kpwd

Storage Authorization Service

Storage metadata

User Authorization Record

Get storage authz for this username

If authorized, get username

https/SOA

SAML response
SAML query

Abhishek Singh Rana, UCSD
gPLAZMA Implementation

voms-proxy-init
Proxy with VO
Membership | Role attributes

srmcp

SRM Server

GridFTP Server

GridFTP Callout

SRM Callout

SRM-dCache

1

2

3

4

4a

4b

4c

4d

5

6

7

8

9

10

11

12

13

gPLAZM

PRIMA Client

GUMS Identity Mapping Service

Storage Authorization Service

User Authorization Record

Get storage authz for this username

https/SoA

SAML response

If authorized, get username

Get storage metadata

GUMS

Identity Mapping Service

dcache.kpw

gPLAZM Lite Authorisation Service

gPLAZM Lite grid-mapfile

get authorization

If authorized, get username
Example of end-to-end AuthZ for CEs and SEs
SE: SRM-dCache

• Different *doors* for different authz methods.
• Same underlying local authz mechanism.
• Can be mapped to site’s UID/GID domain.
• Or be restricted to SRM-dCache only.
• Examples:
  – USCMS-VO at FNAL: Site UID domain.
  – CDF-VO at FNAL: Site Kerberos domain.
SE: SRM-dCache

• gPLAZMA extends SRM-dCache separation of SE authz and CE authz to OSG approach.

  • gPLAZMA authenticates.
  • gPLAZMA uses PRIMA Java SAML libraries to form a SAML query and contacts Storage Authz Service.
  • Storage Authz Service contacts GUMS and Storage Metadata Service.
  • GUMS translates {DN, Membership, Role} to Username.
  • Storage Metadata Service translates Username to Storage-privilege Set.
  • Storage-privilege Set is {UID, GID, permitted storage area, R/W permissions}.
  • Storage-privilege Set is User-level ACL governed by {DN, Membership, Role}.
  • Storage Authz Service forms a User Authorization Record into a SAML response and sends it back to gPLAZMA at SE.
Local or Remote Client
Proxy with VO Membership | Role Attributes

Site

CE

SE

VOMS

Site-wide Mapping Service

Storage Authorization Service

gPLAZMA
Storage metadata

GUMS

Auxiliary Mapping Service

Site-wide Assertion Service

SAZ
Local or Remote Client

Proxy with VO Membership | Role Attributes

Site

CE

SE

VOMS

GUMS

Storage Authorization Service

Site-wide Mapping Service

gPLAZMA

Storage metadata

Auxiliary Mapping Service

SAZ

Site-wide Assertion Service
Local or Remote Client

Proxy with VO Membership | Role Attributes

Site

CE

PRIMA
C SAML libraries

Site-wide Mapping Service

GUMS

Storage Authorization Service

gPLAZMA
Storage metadata

SE

SAZ

VOMS

Site-wide Mapping Service

Globus Gatekeeper PRIMA callout

C SAML libraries
Local or Remote Client
Proxy with VO Membership | Role Attributes

Site

Globus Gatekeeper PRIMA callout

PRIMA
C SAML libraries

Site-wide Mapping Service

Site-wide Mapping Service

Storage Authorization Service

Auxiliary Mapping Service

Storage metadata

Site-wide Assertion Service

CE
PEP

SE

GUMS

VOMS

Abhishek Singh Rana and Frank Wuerthwein UC San Diego
www.opensciencegrid.org

CHEP 2006 Mumbai INDIA February 15 2005
Local or Remote Client

Proxy with VO Membership | Role Attributes

Site-wide Assertion Service

Globus Gatekeeper PRIMA callout

Site-wide Mapping Service

CE

PRIMA C SAML libraries

GUMS

Storage Authorization Service

gPLAZMA Storage metadata

Site-wide Assertion Service

SAZ

VOMS

Abhishek Singh Rana and Frank Wuerthwein UC San Diego

www.opensciencegrid.org
Local or Remote Client
Proxy with VO Membership | Role Attributes

Site

Globus Gatekeeper PRIMA callout

Site-wide Mapping Service

PRIMA C SAML libraries

Storage Authorization Service

Site-wide Mapping Service

SAZ

Auxiliary Mapping Service

VOMS

GUMS

Site-wide Mapping Service

Storage metadata

gPLAZMA

Site-wide Assertion Service

PRIMA Java SAML

gPLAZMA

gPLAZMA Lite

Authorization Services suite

SRM-GridFTP gPLAZMA callout

CE

SE
Local or Remote Client

Proxy with VO Membership | Role Attributes

Site

CE

PRIMA C SAML libraries

OGSA AuthZ interface

Site-wide Mapping Service

VOMS

SE

gPLAZMA

gPLAZMA Java SAML

PRIMA Authorization Services suite

gPLAZMALite

Storage Authorization Service

gPLAZMA Storage metadata

GUMS

Site-wide Mapping Service

AUXIAL Mapping Service

SAZ

Globus Gatekeeper PRIMA callout

SRM-GridFTP gPLAZMA callout

Abhishek Singh Rana and Frank Wuerthwein UC San Diego

www.opensciencegrid.org

The Open Science Grid Consortium

CHEP 2006 Mumbai INDIA February 15 2005

21
Local or Remote Client
Proxy with VO Membership | Role Attributes

Site

VOMS
Virtual Organization Membership Service

GUMS
Grid User Management System

GUMS
Site-wide Mapping Service

VOMS
Virtual Organization Membership Service

PRIMA
A System for Privilege Management and Authorization in Grids

PRIMA
Grid User Management System

Storage
Authorization Service

gPLAZMA
grid-aware Pluggable Authorization Management System

gPLAZMA
Java SAML

gPLAZMA
Storage Authorization Service

gPLAZMALite
Authorization Services suite

SAZ
Site Authorization Service

SAZ
Site-wide Authorization Service

Site-wide Mapping Service

Globus Gatekeeper PRIMA callout

Auxiliary Mapping Service

PRIMA
C SAML libraries

PRIMA
Callout

SE

gPLAZMA

CE

Abhishek Singh Rana and Frank Wuerthwein UC San Diego

www.opensciencegrid.org

CHEP 2006 Mumbai INDIA February 15 2005
Status

• gPLAZMA native role-based authz mode deployed at USCMS tier-2 production site at UCSD. Work in progress for deployment at tier-1 at FNAL.

• GUMS role-based authz mode in final stages of development/packaging.

• Deployment and usage of all modes on USCMS production dCache sites expected before Service Challenge 4.
Known Limitations

- Not (yet) implemented for dcap.
- Scalability of site central call-out not yet understood. (gPLAZMA native a viable fallback)
- vi/emacs is only administrative interface.
- Options for communicating desired policies from VO to site are less than satisfactory. (general problem of role based authz!)
Future Work

• Add MySQL based backend to replace storage authz records configuration file.
• Complete gPLAZMA for dcap.
• Understand scalability of site-wide call-out.
• Add XACML based authorization engine to dynamically assign storage authz mappings at Site.
• Explore XACML/SAML rule-based policy declaration (VO-level) and policy computation (Site-level).
Thank You.