Managing (Dis)Honorable Guests --
A Role for Grid Security

Dane Skow
University of Chicago and Argonne National Laboratory
Glossary

u **Identity**
   v A unique identifier for a grid actor.
   v Most commonly the DN (but implies agreements among CAs)

u **Authentication (AuthN)**
   v Proof that the requestor is legitimately associated with the identify.
   v Most commonly possession of the private key

u **Authorization (AuthZ)**
   v Permission to have the request granted
Glossary (cont)

u Audit (Troubleshooting)
  v Associating an action with the requests that caused it to happen
  v May have to survive in the face of attempts to thwart this association

u Groups
  v Collections of identities all of whom have similar characteristics

u Roles
  v A collection of privileges which one wishes to assert
  v Always within the context of a particular group
Grid Interoperation Now (GIN)

- Begun its work in GGF17 in Athens in February
- Approved as GGF Community Group in March

**Already Contributing Effort:**
- C. Catlett – TeraGrid
- S. Matsuoka - NAREGI
- E. Laure – EGEE
- M. Green - OSG
- V. Alessandrini - DEISA
- P. Arzberger – PRAGMA
- N. Geddes- UK NGS
- O. Sminova - NorduGrid

**Pledged to Contribute Effort:**
- H. Jin - China Grid
- M. Mazzucato - Italian Grid
- A. Wu - Taiwan National Grid
- W. Gentzsch - D-Grid
- R. Davies - APAC
- R. Lee - Korean National Grid

**Intending to Collaborate**
(testing, use cases, evaluation)

- S. Moralis - GridCC
- P. Kunszt - Swiss Grid
- B. Ugolotti - NEES
- T. Sasaki - Japanese HEP Grid
- D. Kelsey - GridPP
GIN agreements in Security

- IGTF Identity space for interoperation
- X509 authentication (RFC 3820, 3280)
- VOMS proxy transport of group/role authorization
Defining Roles by Privileges

- Roles useful for implementing principle of least privilege
- Privilege often expressed as “credit limit”
- Hard for RP to implement
  - Generically privileges have to be individually assigned
  - Scales as the number of objects (files/directories, jobs)
- General grammar difficult
  - Need a common ontology
  - Enumeration of the privileges tedious
Reversing the Problem

u What sets of privileges do we implement for a resource?
  v Scales as # groups ( * # resources)

u User
  v Common privileges to use a resource (within the permission of the group)

u Delegated User (user privileges but restricted to a single context/resource)
  v Would this be useful?
  v Can it be defined with current technology? (e.g. no ability to delegate?)

May 4, 2006 Dane Skow (skow@mcs.anl.gov)
Resource Admin Roles

u Group Resource Administrator
  v Privilege to reassign resource within the group

u Resource Administrator
  v Full privileges to administer the resource
  v (should we have this? Equiv. “root”)

May 4, 2006 Dane Skow (skow@mcs.anl.gov)
Authorization

- Use Lease concept
  - privilege management outsourced to the lessee.
  - “night desk” just checks the guest list
- Resource provider must retain ability to “change the locks” if lease is breached.
In Teragrid:

u Project PIs
  v have ability to add/remove users to their project (VO)
  v Ability to request additional resources

u Project members
  v Ability to make requests against the project quotas
  v May request information about remaining quota

u Grid Developers
  v Act either as Project PIs or members

May 4, 2006    Dane Skow (skow@mcs.anl.gov)
Teragrid Roles (cont’d)

- Resource administrators
  - Typically don’t use grid interfaces other than to test

- Grid administrators
  - Ability to monitor resource usage

- User Support
  - Ability to reproduce reported errors

May 4, 2006
Dane Skow (skow@mcs.anl.gov)
Compute

u User
  v Submit jobs drawing on group resources
  v Protection of local execution environment from other user jobs
  v Ability to act upon ones own job (stop, kill, reorder, restart, ..)

u Group Code Admin
  v Ability to configure the Group software base (service instances)

u Group Resource Admin
  v User +
  v Ability to act upon any jobs authorized by the group
  v Configure the group execution environment

u Resource Administrator
  v Is this needed ? Local methods only ?

May 4, 2006 Dane Skow (skow@mcs.anl.gov)
Data

- Take parallel from Unix filesystem permissions
- Owner, Group, World
- Base permission set
  - Read
  - Write
  - Change permissions
  - Delete (a subset of write ?)
  - List
  - Execute

May 4, 2006

Dane Skow (skow@mcs.anl.gov)
Data Roles

u User
  v Read from group spaces
  v Full control of user’s own files
u Group Data Admin
  v Full control of all group spaces
u Resource Admin

May 4, 2006 Dane Skow (skow@mcs.anl.gov)
Hierarchy of Scope

- Subgroups within groups. Grids containing groups
- Roles throughout VO, grid, resource
Dishonorable Guests

Who Does the enforcement?

- RP
  - Have to distribute ACL admin
- VO
  - Have to identify authority decisions
Open items

- How are VOMS registered/namespace?
- What protection needed for execution environment?
  - May jobs be multiplexed onto single UID (exposure of credentials, etc.)?
- How should we express/implement priority?
VOMS expression

- Formal definition of the protocol now a GGF draft.
- Is there a need for roles restricted to a single resource?
- Are roles merely another form of subgroup? Do we need them?