Authorization in GENI
Engineering Meeting

Leads: Steve Schwab, Ted Faber, Tom Mitchell
March 15, 2011
www.geni.net

Authorization in GENI: Introduction

Tom Mitchell – tmitchel@bbn.com
March 15, 2011
www.geni.net

- Introduction - Tom Mitchell (5 mins)
- Authorization proposal - Steve Schwab/Ted Faber (30 mins)
- Break
- Invited discussion - Jeff Chase (10 mins)
- Invited discussion - Rob Ricci (10 mins)
- Open discussion - All (25 mins)
- Session wrap-up - Tom Mitchell (10 mins)

- GEC 10 format reoriented to focus on three tracks:
  - **software**
  - experimenter
  - operations
- Software track has 4 engineering meetings:
  - identity and attributes;
  - **authorization**;
  - resource specification;
  - stitching

How we got here

- Prior to GEC 10:
  - A few key stakeholders discussed the topic
  - The group generated a consensus proposal
- Today:
  - Steve and Ted will present the proposal
  - Stakeholders will provide various viewpoints
  - Open floor for community discussion
  - Come to agreement on the proposal
  - Decide on next steps

- ## Who collaborated on this work?
  - ### ABAC
    - Steve Schwab – Cobham
    - Ted Faber – ISI
  - ### Control Frameworks
    - Rob Ricci - ProtoGENI
    - Jeff Chase – Orca
  - ### GPO
    - Aaron Helsinger – BBN/GPO
    - Tom Mitchell – BBN/GPO

What is authorization?

- Authorization determines the level of access a particular authenticated user should have
  - Is user X authorized to access resource R?
  - Is user X authorized to perform operation P?
  - Is user X authorized to perform operation P on resource R?

Current Authorization in GENI

- Privileges in GENI AM API are passed as credentials
  - Based on SFA credentials
  - Signed XML documents
  - Encode roles that map to sets of privileges that map to sets of operations
    - Role -> Privileges -> Operations

- In practice, decisions are limited to the slice authority
  - Aggregate managers don't make their own decisions, just act on decisions made by the slice authority

- ABAC should be added to the GENI AM API as a means of authorization
  - Does not replace existing credentials
  - This is an opportunity to gain experience

- Aggregates should accept ABAC-style attribute assertions to enable richer authorization policies than are possible with current GENI credentials
  - Aggregates are not required to add ABAC support
  - This is an opportunity to gain experience

- Agree that GENI should add ABAC authorization to the GENI AM API

- Agree that an existing aggregate should be ABAC-enabled.
  – Experience to be reported at GEC 11
  – Propose next steps for Authorization at GEC 11

- Introduction - Tom Mitchell (5 mins)
- Authorization proposal - Steve Schwab/Ted Faber (30 mins)
- Break
- Invited discussion - Jeff Chase (10 mins)
- Invited discussion - Rob Ricci (10 mins)
- Open discussion - All (25 mins)
- Session wrap-up - Tom Mitchell (10 mins)