GENI Authorization
GEC 13

Tom Mitchell
March 13, 2012
www.geni.net

Sponsored by the National Science Foundation

Open Issues

- Vocabulary and Policy
- Revocation or expiration
- Attribute distribution
- Policy distribution
- Tools and infrastructure
- Aggregate integration
- Implementation schedule

GENI ABAC Vocabulary

vocabulary *n*. the body of words used in a particular language.

The GENI ABAC vocabulary is the set of attribute roles that have a common semantic meaning.

Example: *How does a slice authority (SA) assert that an experimenter (E) can allocate resources to a slice (S)?*

? SA.can_allocate(S) ← E

SA.write(S) ← E ?

SA.CreateSlivers(S) ← E ?

SA.bind(S) ← E

? SA.author(S) ← E ?

Vocabulary and Policy

GENI needs a single vocabulary and policies based on that vocabulary.

There are three documents that enumerate, at least in part, possible vocabulary and policy.

How do we choose between them or merge them into a satisfactory whole?

Who can create and publish an initial GENI authorization policy?


Authorization and Trust Structure in GENI:
A Perspective on the Role of ABAC

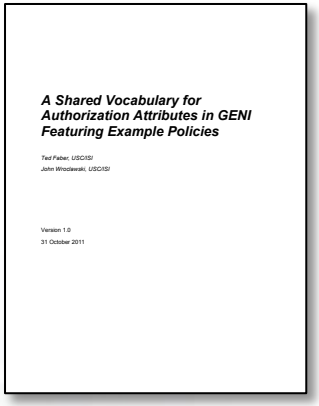
Jeff Chase
Department of Computer Science
Duke University

June 17, 2011

Abstract

1 Introduction

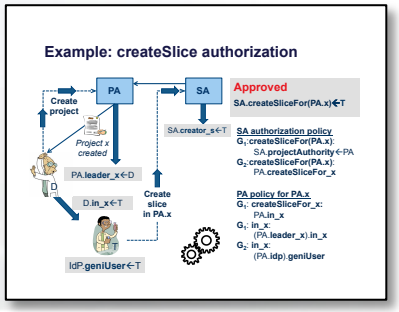
Chase
June, 2011


A Shared Vocabulary for Authorization Attributes in GENI Featuring Example Policies

Ted Faber, USC/ISI
John Wroclawski, USC/ISI

Version 1.0
31 October 2011

Faber, Wroclawski
October, 2011



Chase
December, 2011

Policy Implementation

Templates & RT1-Lite
vs.
RT1 & RT2

- During the past year we have discussed using “RT1-lite” and policy templates as workarounds for the lack of an RT1 implementation in libabac.

- libabac now supports RT1 *and* RT2 as alpha test features.

Should GENI policies use RT1 and RT2?

Revocation or Expiration

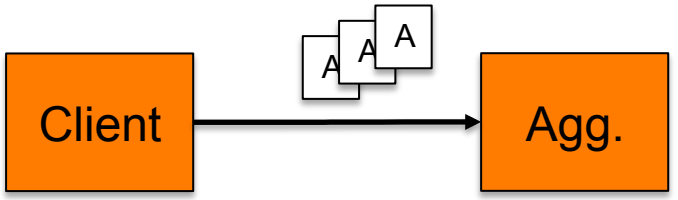
- Revocation of assertions adds too much complexity to the system and the actors

- Recommendation: use short expiration times
  - How short? 24 hours? 1 million seconds (~12 days)?
  - Should expiration vary?
    - Short-lived & long-lived assertions?
  - How do actors retrieve renewed assertions?

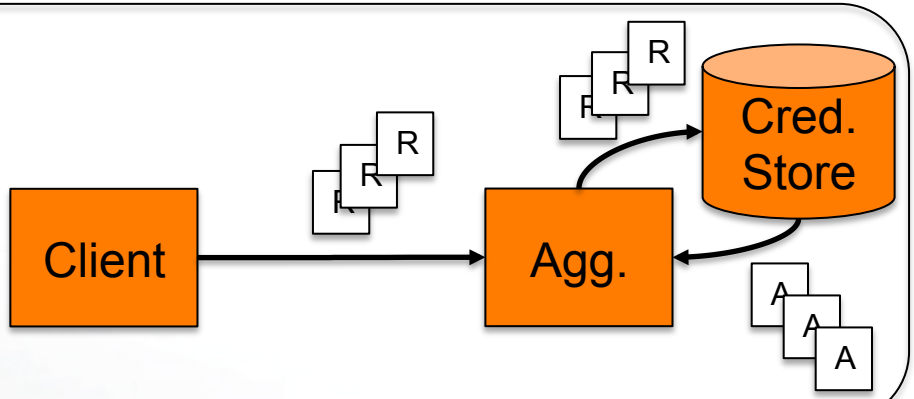
Who can create and circulate a concrete proposal?

Attribute Distribution

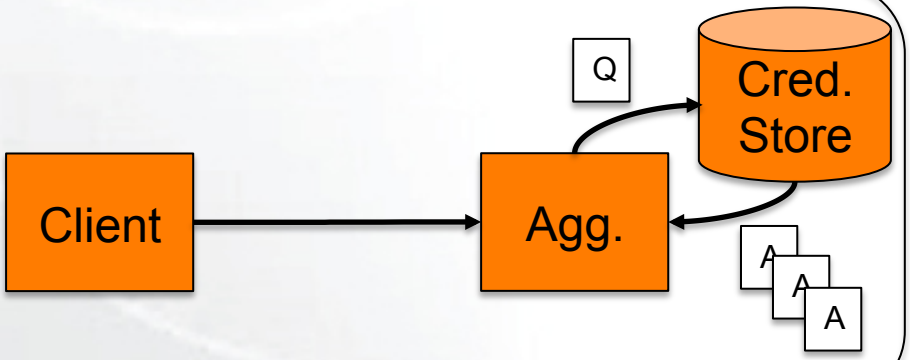
- Pass attributes by value in API calls



- Pass attributes by reference in API calls
  - Authorizers resolve references in a credential store

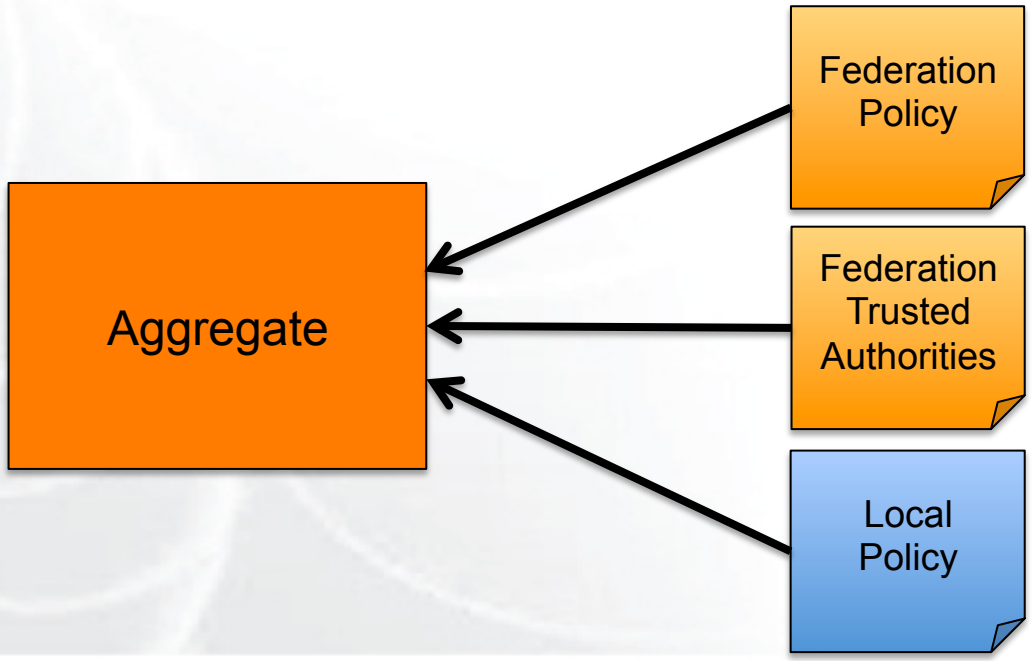


- Pass no attributes
  - Authorizers query a credential store



Policy Distribution

- Securely distributing policy updates
- Adding or removing trusted authorities
- Adding local policies to federation policies
- Are policies one size fits all?

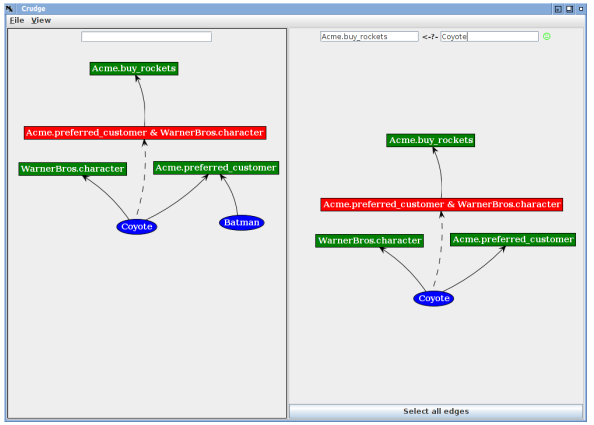


Tools and Infrastructure: libabac

- Stability
- Performance
- Command line tools
  - Creddy
  - Prover
- Language bindings
  - C/C++, Python, Perl, Java
- RT1 / RT2 readiness
  - Currently alpha

Tools and Infrastructure: Policy

- Policy tools
  - Create, view, debug, and edit policies
- Crudge
  - Visual editor for ABAC policies and proofs
  - Requires ABAC expertise



- Sufficient in the near term, but could use improvement in the longer term

Tools and Infrastructure: Attributes

- These are primarily programmer tools
  - Language bindings for working with libabac
  - Command line tools
  - *Not for experimenter or operator use!*
- Current tools seem sufficient:
  - Creddy for command line
  - Support for a variety of programming languages
- Are other attribute tools required?

Aggregate integration

- Aggregates will need to:
  - Install and update Policies and Trusted Authorities
  - Integrate libabac at policy decision point(s)
  - Log proofs on success and failure
  - Optionally create local policy if desired
  - Maybe acquire credentials (see attribute distribution)
  - Maybe instantiate policy templates (see policy implementation)
- Integration has been prototyped at most aggregates

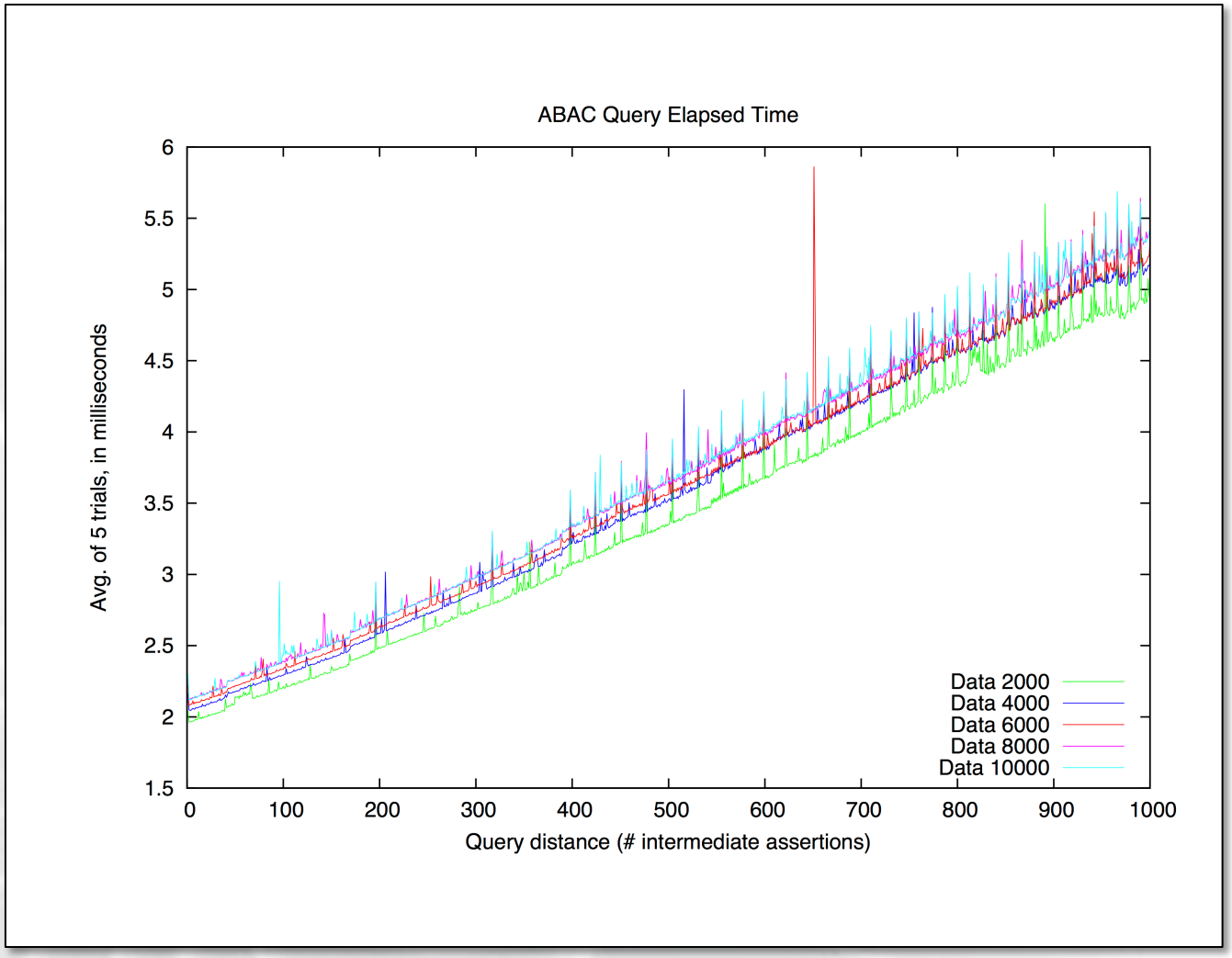
(Rough) Implementation Schedule

- Notional Schedule
  - Ramp-up Phase
    - Aggregates prepare to receive assertions
    - Authorities prepare to send assertions
    - Initial policies available
  - Overlap Phase
    - Mixed credentials flow
    - ABAC trial period
  - Ramp-down Phase
    - Cease using old credentials
- How soon can aggregates be ready?
- How soon can the Clearinghouse be ready?

No Flag Day

The End.

ABAC Prover Performance



Ted's list

- Credential and policy flow issues
  - base policy
  - who issues credentials
  - logic of policy (RT0 vs RT1 vs RT2)
  - where do credentials reside and how do actors to get them

- Uptake and deployment issues
  - library stability and logic support (extensions of logics?)
  - Aggregate uptake
  - GENIRacks - a special case of uptake
  - Integration with Clearinghouse/federation