ProtoGENI And ABAC

GEC13
March 2012

Nice Properties

- Distribute default policies as ABAC statements
- More complex policies possible
- Proofs useful for proving policy compliance to a third party

Unresolved Concerns

- Tied to public keys, not to user identity
- ~~Encoding URNs, etc. in ABAC statements~~
- Delegation without combinatorial explosion
- Needs high level documentation

Documentation Needed

- For developers
  - Good start in libabac
- For admins
  - Document all assertions in the default set
- For users
  - Particularly, about error messages

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

Jeff Chase
Department of Computer Science
Duke University
{chase}@cs.duke.edu

June 17, 2011

Abstract

This note outlines a GENI authorization architecture based on Attribute-Based Access Control (ABAC). GENI Aggregate Managers and other GENI-related servers may use ABAC to represent authorization policies declaratively at deployment time. We discuss how ABAC can meet key requirements for flexible authorization in GENI, including delegation of ownership rights, endorsement of slices, external identity providers, and proxying of control interfaces.

We also leverage ABAC as a tool to represent candidate GENI trust structures declaratively. We contend that ABAC authorization policies are sufficiently powerful to incorporate key trust structures as optional deployment-time choices for each aggregate, rather than viewing them as fundamental architectural choices in the control framework.

This draft supersedes and extends an earlier version of this document dated 5/2/11.

1 Introduction

This note outlines a design to use an authorization logic to represent trust structure and authorization policy in GENI. We focus specifically on Attribute-Based Access Control (ABAC) as a candidate authorization logic. We outline some structures that can be expressed using the RT0 ABAC implementation in *libabac*.

Implementation

- Prototype from Ted Faber seems reasonable
- We are willing to adopt it and take it over
- ... but we don't have the expertise to update it to RT1 or RT2
- ... and it doesn't support generation of credentials

Summary

- We think ABAC has potential
- We support adding it as an optional credential format in GENI
- ... though it will not go straight to the front of our implementation queue
- Will need help updating to new RT versions