Authorization in GENI

Steve Schwab, Ted Faber

Jeff Chase

Tom Mitchell

Agenda

- Intro and Recap
- Current Integration Status
- Trust Structures
  - Moving Beyond Subject/Object Credentials
  - ABAC and ORCA
  - Discussion
- Next Steps

Status of ABAC Integration in GENI

Ted Faber,

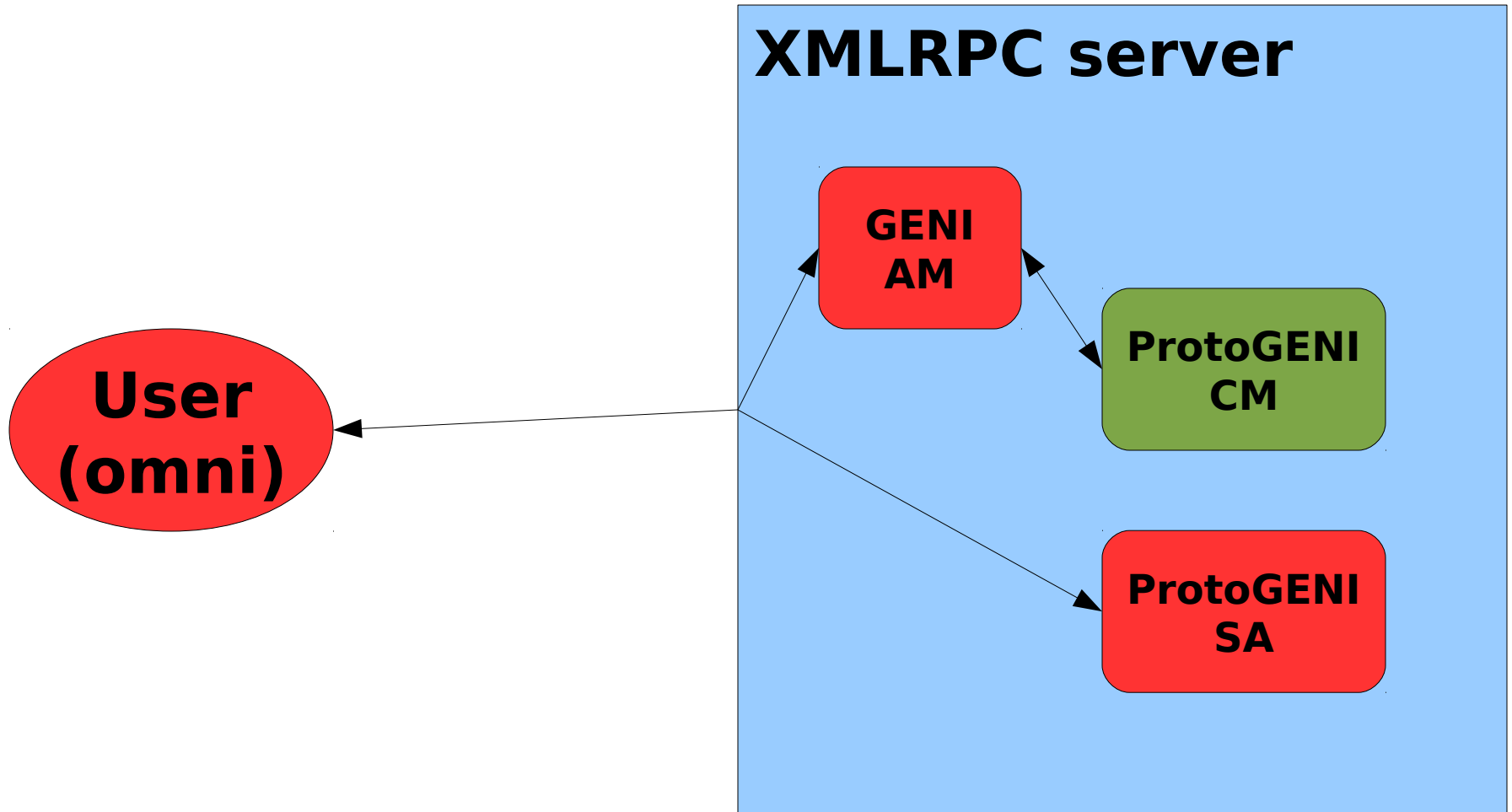`faber@isi.edu`

26 July 2011

GEC 11

Integration Goals and Questions

- Feasibility of ABAC
  - Are implementation libraries robust?
  - Can ABAC integrate with existing frameworks?
- Tool Support
  - Can humans read ABAC proofs and policies?
- ABAC Policies
  - Can ABAC express useful policies?
    - Is RT0 – ABAC's simplest logic – useful?

Current Integration

- Working ProtoGENI/GENI AM system
  - Accepts ABAC credentials for authorization
  - Generates ABAC credentials expressing rights
  - Provides proof logs of transactions
  - Full slice/sliver manipulations via `omni`
    - Systems built on `omni` get it, too (Gush…)
- Visual tools for proof browsing
  - RT0 proofs/policy editor: `crudge`
    - http://abac.deterlab.net/wiki/CrudgeDocs
    - http://abac.deterlab.net/java/crudge.jnlp

Components Modified

Integration Details

- GENI AM API Modifications
  - Add ABAC credentials in GENIAM parameters
    - Credentials are overloaded
    - ProtoGENI cannot handle removing PG credentials yet
  - Return ABAC proofs in GENIAM responses
    - Convert responses to XMLRPC structs
  - Add ABAC proofs to GENIAM error codes
    - Error codes need to be widened, too.
    - GENIAM uses XMLRPC Faults, which are closed form
- ProtoGENI SA API Modifications
  - Add `GetABACCredentials` interface
  - Set ABAC credentials on slice registry

Demo...

Implementation Next Steps

- Buy-in from Framework Developers
  - Experts will be faster and more efficient
  - Internals are complex
    - E.g. ProtoGENI credentials in dataflow
- API defintions
  - The Easy Stuff: Widen AM/CM APIs
  - The Hard Stuff: Standardize other Elements
- But...

Trust Structures and Dataflow...