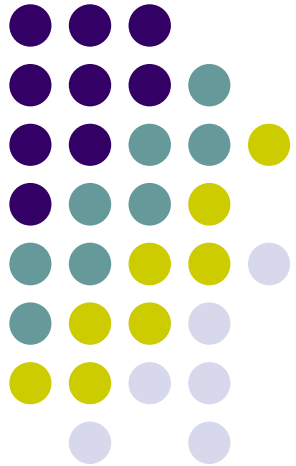
TIED Security

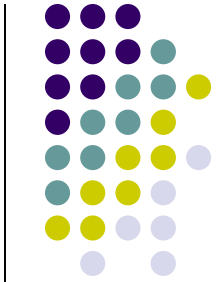
John Wroclawski, *Ted Faber*, Steve Schwab

GEC4

1 Apr 2009



GENI Security



- Traditional Problems, Challenging Environment
- Challenges
  - Large Scale
    - Many resource providers
    - Many experimenters
    - Distributed authorization decisions
    - Partial failures of infrastructure
  - Playground for Disruptive Technologies
    - Wide effects (better or worse)
    - Easy to accidentally constrain
- TIED Directions
  - Disconnect Trust Estab. from Authorization
  - Attribute-based Reasoning

Scale: Resource Providers & Experimenters

- Right Balance of Constraint
  - Too much constraint, too few donations/experiments
- Specific Issues Raised by Many Players
  - Many Trust Models (hierarchy, web-of-trust, reputation)
    - Minimally constrain trust formation
    - Interoperate between trust models
  - Many Different Constraints on Resources
    - Express constraints
    - Enforce constraints
  - Information Flow (who needs to know?)

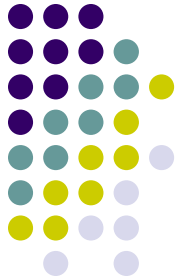
Scale: Large Infrastructure

- Big Enough World: Something Is Down
- Expect Partition/Disconnection
  - Decentralized Authority
  - Fail-Safe Semantics
    - Safe Authorization/Authentication Semantics: ATMs
    - Not Slice Revocation (different problem)
  - Clear, Auditable Semantics and Logs
    - Reconstruct partitioned operations
    - Human audits

Experiment-Driven Semantics

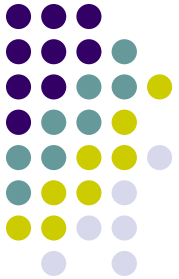
- Authorization to use resource for a reason
  - Experimenters get resources to do unusual things
  - Resource owners care how resources are used
- Security architecture constrains experiments
  - E.g., Anonymous principals?
  - Understand constraints to choose wisely

TIED Directions



- Attribute-Based Reasoning (ABAC)
  - Principals Assert Attributes About Principals
  - Formal Reasoning Derives Authorization Decisions
- Principal Trust Established in Many Ways
- Reasoning Promotes Understanding/Analysis
- Driven by GENI requirements
  - Clear interfaces
  - Usable system

How Does This Help?



- Multiple Trust Establishment Models
  - Can we negotiate?
- Formal Descriptions
  - What can we say?
  - Is authorization in the way of an experiment?
- Clear Decisions
  - What happened? Why?
  - Can we reconcile independent decisions?
- Design Guidance
  - What must be said? When can we disconnect?
  - What have I let you know?