de·ter
the *science* of cybersecurity

A Standard Authorization Vocabulary For GENI using ABAC

Ted Faber,

TIED Project

faber@isi.edu

2 Nov 2011

de•ter
the *science* of cybersecurity

Overview

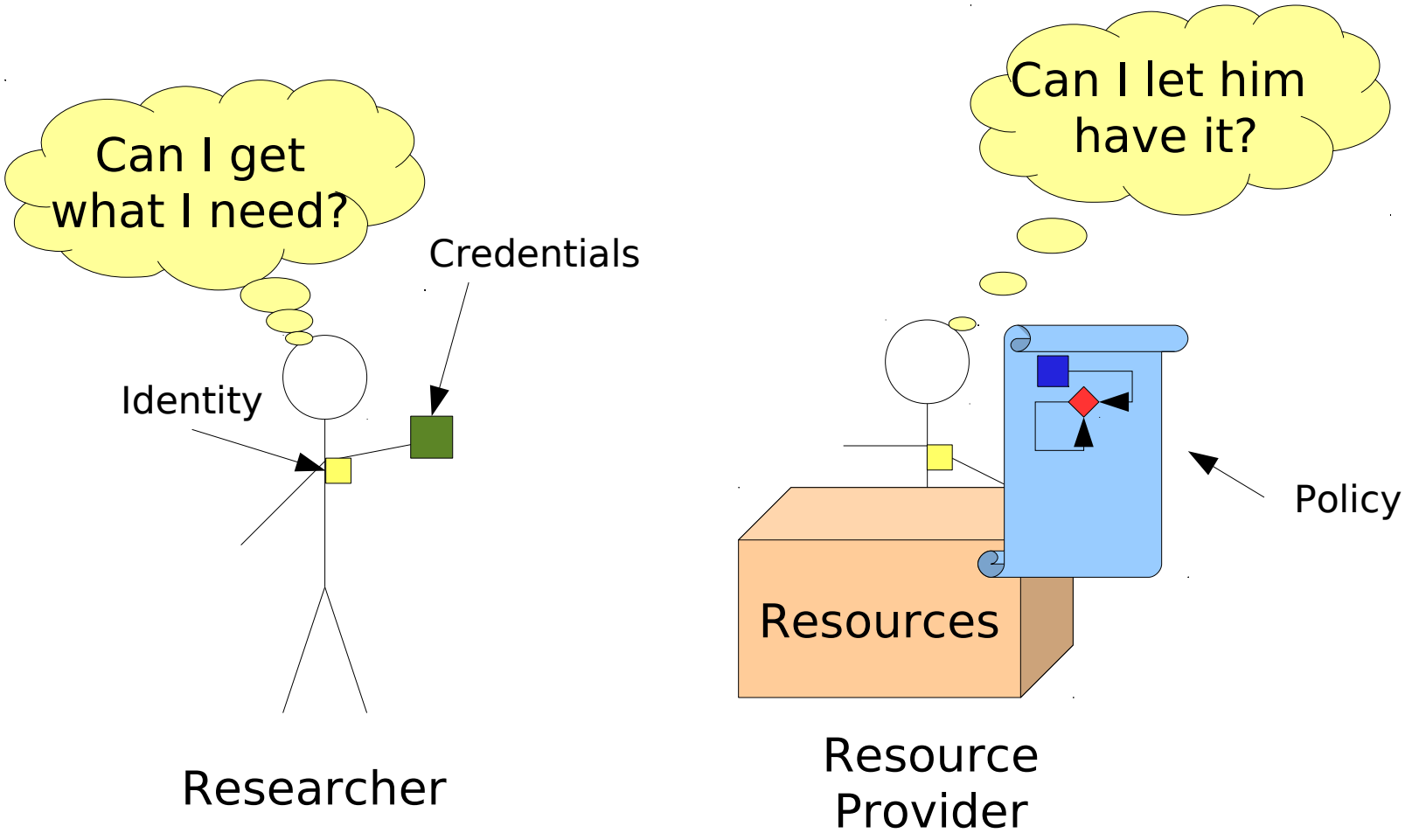
- What's the problem?
  - Why do we need a vocabulary to solve it?
- A proposed vocabulary
  - A little ABAC review for context
- Example solutions
  - Using the vocabulary in policy

This is my view of emerging consensus

abac@geni.net

de•ter
the *science* of cybersecurity

Simple Authorization

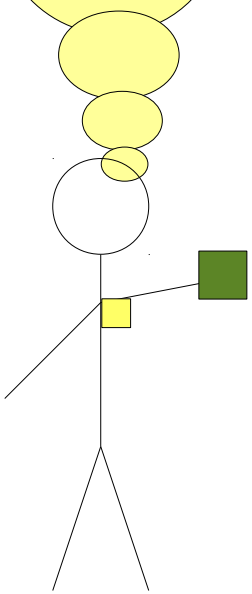


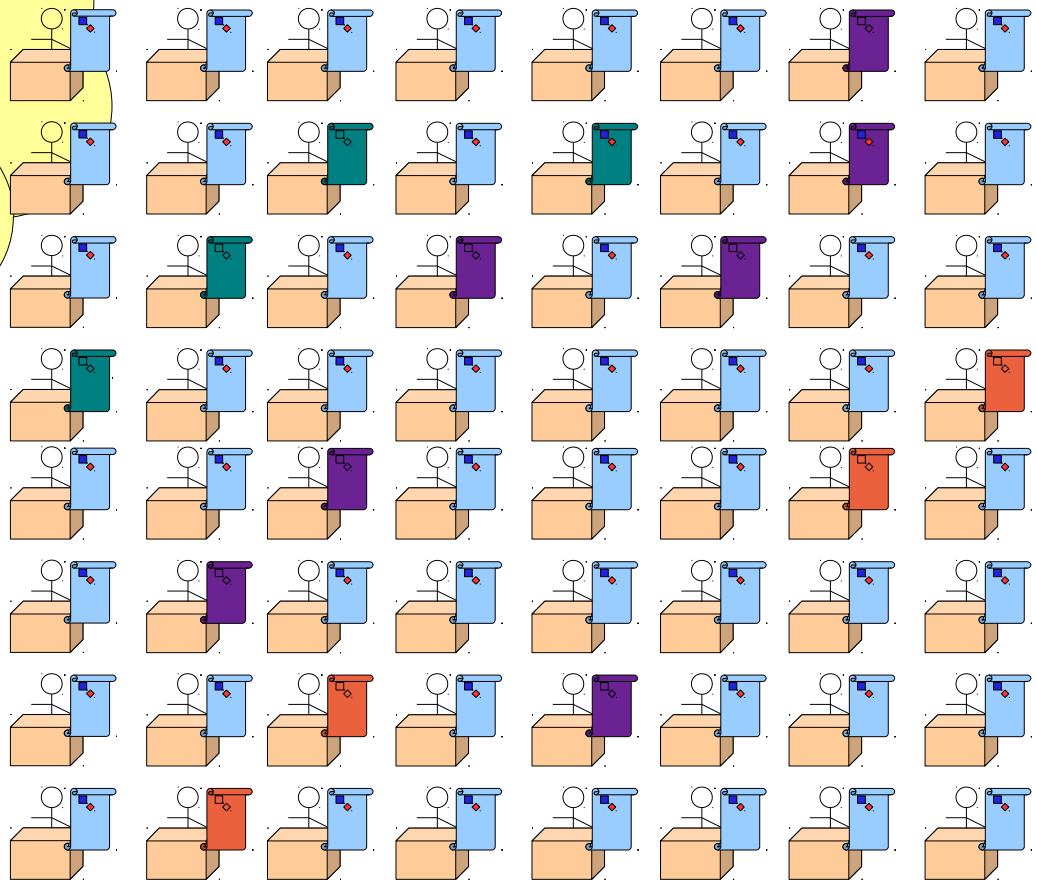
Applying policy answers these questions
This policy can be simple or ad hoc, but...

de·ter
the *science* of cybersecurity

More Servers, More Questions

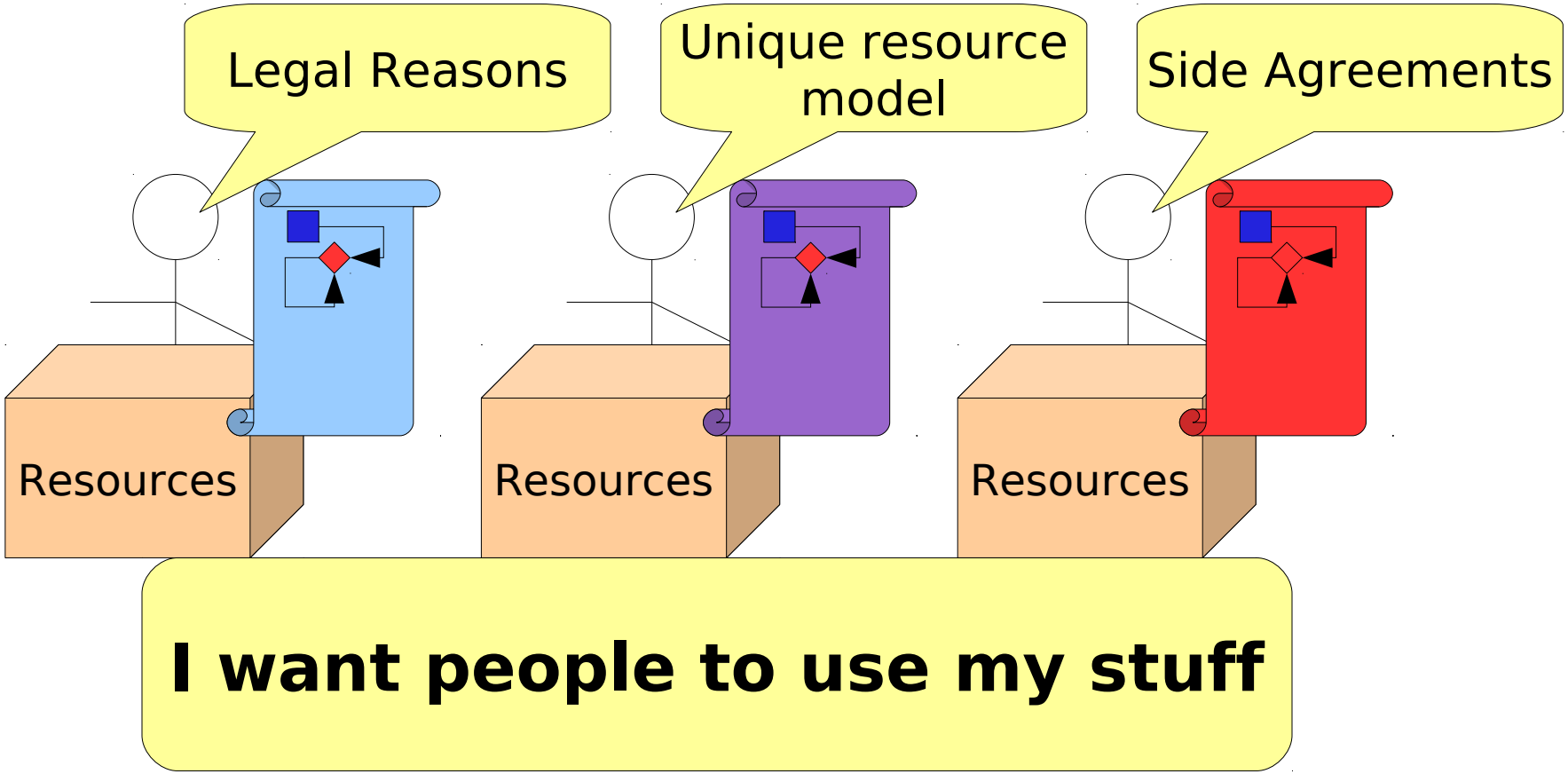
Can I get what I need?
What features do these policies have?
How do I use them?
Are these policies compatible?





de•ter
the *science* of cybersecurity

Why Different Policies?



Need a Basis for Analyzing and Creating Many Policies

Requirements

- Researchers want to
  - Understand and compare policies
  - Discover policy features (delegation)
- Resource Providers want to
  - Provide general policies to attract users
  - Specialize policy for
    - Models
    - Hardware
    - Friends

de•ter
the *science* of cybersecurity

Have a Logic
Need a Vocabulary

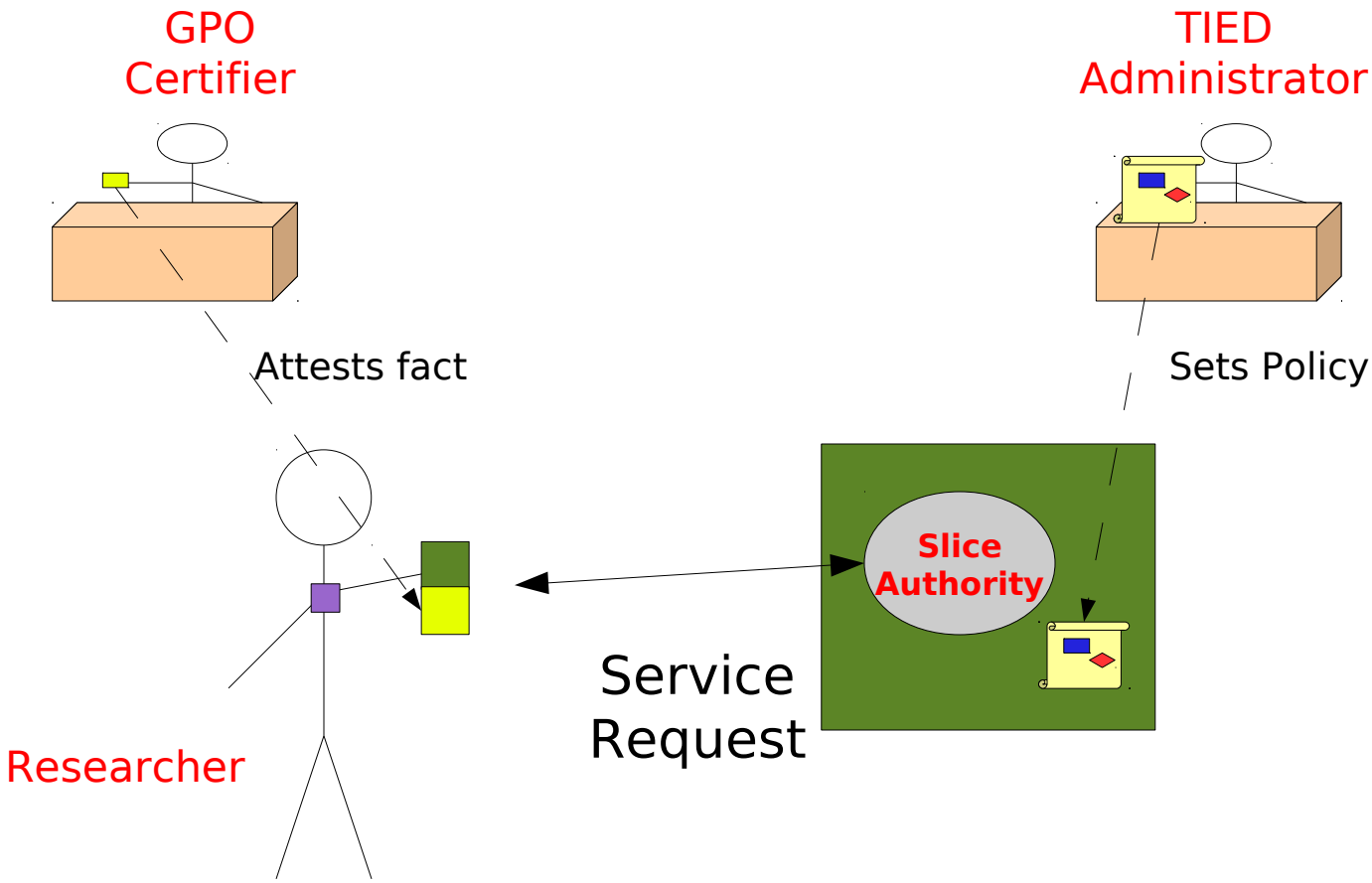
- Logic: grammar of discourse
  - ABAC is simple, formal, expressive
  - Admits specialization
  - libabac implementation
- Vocabulary: universe of discourse
  - Broad enough to be widely useful
  - Narrow enough to be meaningful
  - Embrace specialization

First an ABAC refresher

What is ABAC?

- Attribute-Based Access Control
  - Li, Winsborough et al. from Stanford/TIS
- Formal Expressive Attribute Logic
  - Expresses authorization policy
  - Used to make authorization decisions
  - Records reasoning of decisions
    - Success: tells why
    - Fail: tells why not, suggests path to success
- System code that implements this
  - Come see a demo...
- Policy tools under development

ABAC Principals



de•ter
the *science* of cybersecurity

Attested Attributes

Attribute name: Principal.Role

- Principals attest attributes about principals
  - Principal has *attribute* ↔ Principal in *set*
  - ABAC syntax: Q.admin ← P
- Each Principal Defines An Attribute Space
  - P.admin differs from Q.admin
  - Each Principal Controls Its Attribute Space
- Attributes can have parameters
  - Q.owner(chevy)

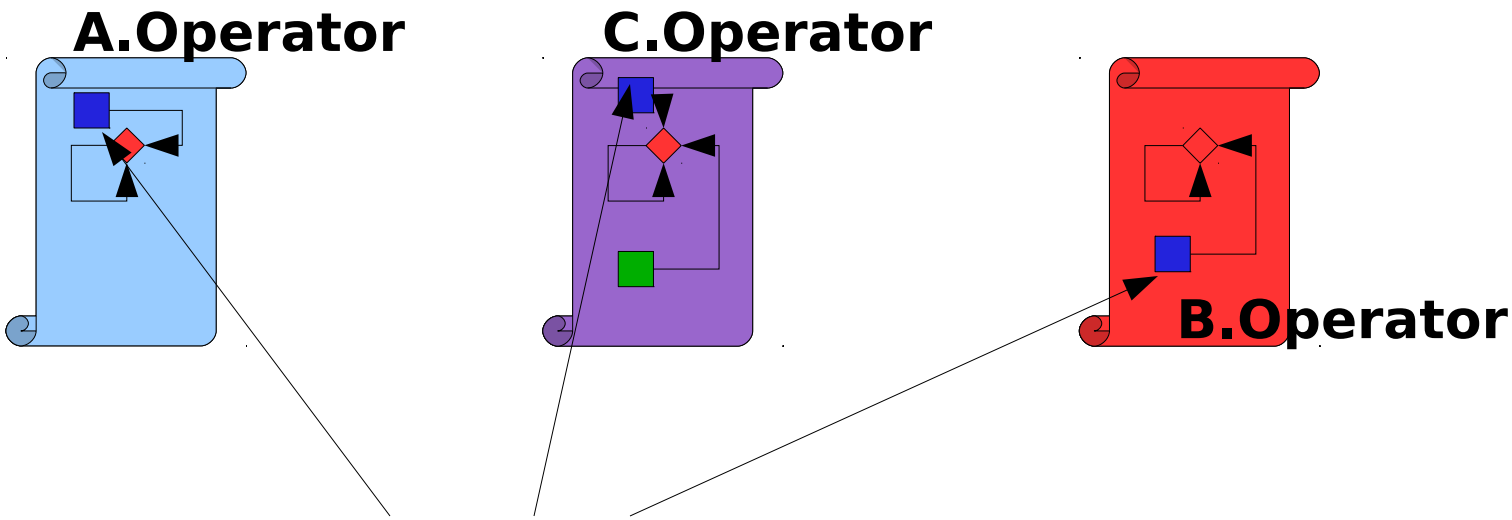
Rules to Derive Attributes

- Direct connection
  - Q says "P assigns Q.friend by assigning P.friend"
    - "P's friends are Q's friends"
    - Controlling Principal (Q) Delegates to a Principal
  - ABAC syntax: Q.friend ← P.friend
- Indirect connection
  - Q says "anyone with P.friend can assign Q.friend by assigning friend in their namespace"
    - "Friends of P's friends are Q's friends"
    - Controlling Principal (Q) Delegates to a set of principals
  - ABAC syntax: Q.friend ← (P.friend).friend

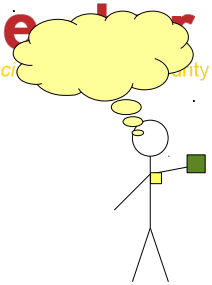
Powerful system: Worth the cost at scale

de•ter
the *science* of cybersecurity

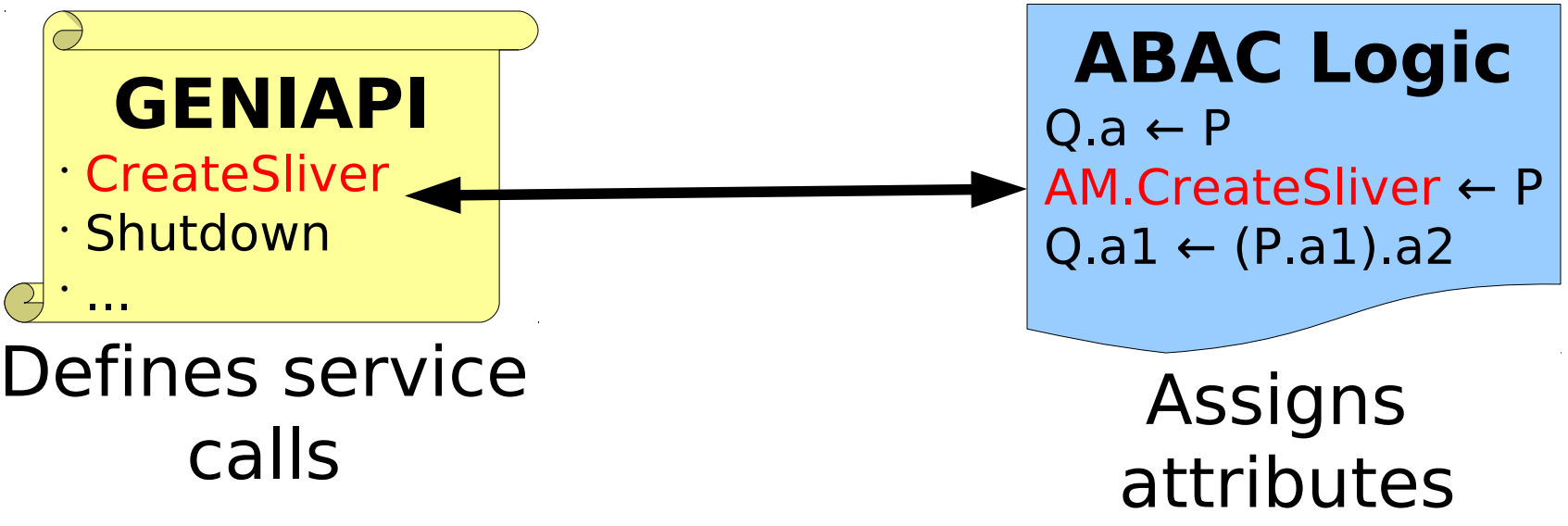
Vocabulary: Specifying Common ABAC Attributes



Common attributes with consensus meaning



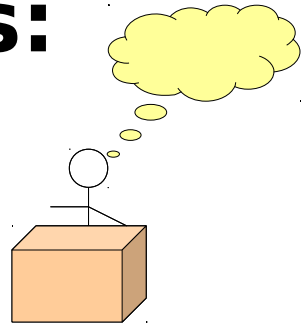
Operational Attributes: What can a researcher do?



- Vocabulary connects them
  - One attribute for each GENIAPI call
  - Can I call CreateSliver at AM? becomes do I have AM.CreateSliver?
  - Global attribute ↔ basic access

de•ter
the *science* of cybersecurity

Researcher Attributes: Who's asking?



- GENI project attributes
  - GPO.ProjectLeader(project) attribute
    - The GPO holds me responsible for a project
  - GPO.ProjectMember(project) attribute
    - The GPO holds someone responsible for me
- Hierarchy attributes
  - USC.Supervises(P)
    - USC says I supervise principal P
- Other Attributes
  - USC.Student, TIED.Operator

de•ter
the *science* of cybersecurity

Service and Endorsement Attributes

- Services
  - ProtoGENI.SliceAuthority
    - ProtoGENI attests I am a Slice Authority
  - ProtoGENI.AggregateManager
    - ProtoGENI attests I am an Aggregate Manager
  - SA.Creator(*slice*)
    - SA says I created *slice*
- Endorsement
  - General 3rd party approval
    - GPO.Endorses → I have signed GPO agreements
  - Indicating Specialization
    - CoolKids.Endorses → I speak the CoolKids attribute vocabulary

Policy Examples

- Any GPO project leader can register a slice at SA:
  - SA.RegisterSlice ← GPO.ProjectLeader
- Anyone who created a slice at a GENI slice authority can create a sliver at AM
  - AM.GPOSliceAuthority ← (GPO.Endorses).SliceAuthority
  - AM.CreateSliver(slice) ← (AM.GPOSliceAuthority).Creator(slice)

Conclusions

- Explained the need for a vocabulary
- Walked through draft vocab
- Sketched policy bits
- Details are in the document & mailing list
  - abac@geni.net
  - http://groups.geni.net/geni/attachment/wiki/TIED/ABAC_Vocabulary_1.0.pdf
  - That's a document on the TIED wiki