COBHAM

March 18, 2010

AVIONICS AND SURVEILLANCE DIVISION

End to end avionics and covert surveillance solutions

DEFENCE SYSTEMS DIVISION

Critical technology for network centric operations

MISSION SYSTEMS DIVISION

Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability

AVIATION SERVICES DIVISION

Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

Attribute-Based Access Control

Stephen Schwab and Jay Jacobs

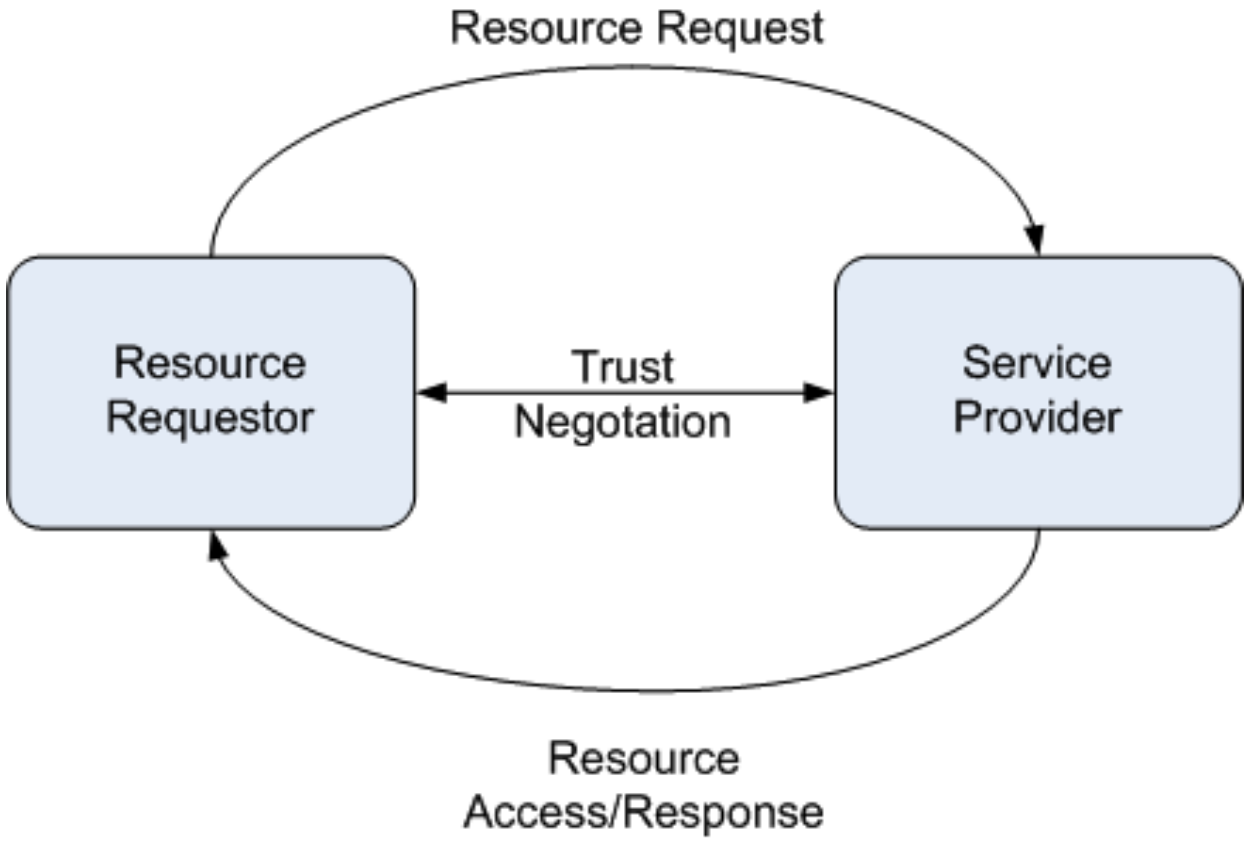
SPARTA ISSO Security Research Division
(d.b.a. Cobham Analytic Solutions)

Topics

COBHAM

- ABAC Usage and Features
- RT_0 Credentials
- Delegation Examples
- ABAC Architecture
- Credential Formats
- Discovery
- Policy
- Integration Summary
- Summary

ABAC Usage


Resource Request
Resource Requestor
Trust Negotation
Service Provider
Resource Access/Response

ABAC Features

Designed specifically for heterogeneous, distributed computing environments, Attribute-Based Access Control (ABAC) extends RBAC with the following features:

1. Decentralized attributes
2. Delegation of attribute authority
3. Inference of attributes
4. Attribute delegation of attribute authority
5. Sensitivity of credentials
6. Trust negotiation provenance

ABAC relies on the RT family of languages described in Ninghui Li, John C. Mitchell, and William H. Winsborough. Design of a role-based trust management framework. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2002.

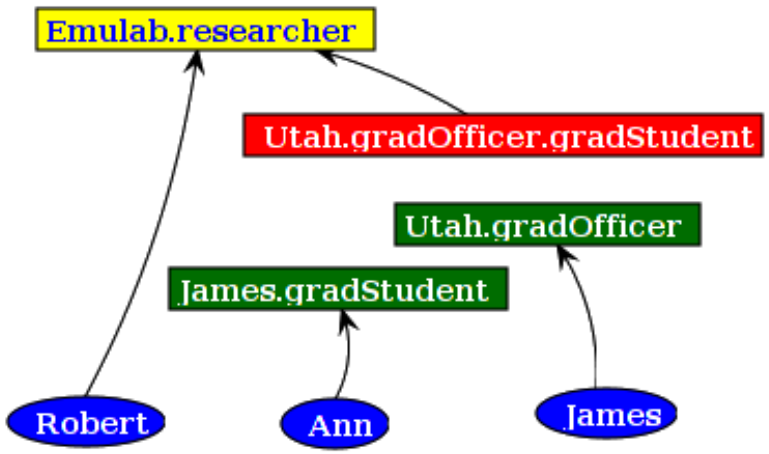
RT_0 Credentials

RT credentials have two parts: The left hand side contains the required attributed role and the right hand side contains the subject, which can be an entity or an attributed role.

Type 1: $A.r_1 \leftarrow S$	(simple member)
Type 2: $A.r_1 \leftarrow B.r_2$	(simple inclusion)
Type 3: $A.r_1 \leftarrow B.r_2.r_3$	(linking inclusion)
Type 4: $A.r_1 \leftarrow B.r_2 \wedge C.r_3$	(intersection inclusion)

RT credentials support union with multiple credentials as shown with the credential examples above.

Delegation Examples



Emulab.researcher ← Robert (1)

Emulab.researcher ← Utah.gradOfficer.gradStudent (2)

Utah.gradOfficer ← James (3)

James.gradStudent ← Ann (4)

ABAC High-level View

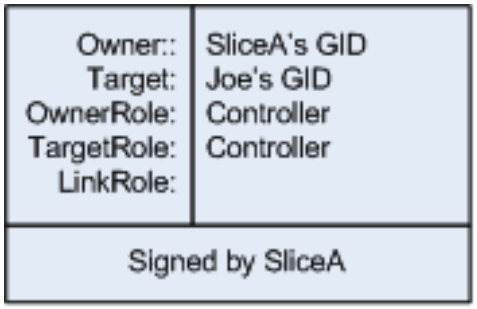
Policy Initialization:

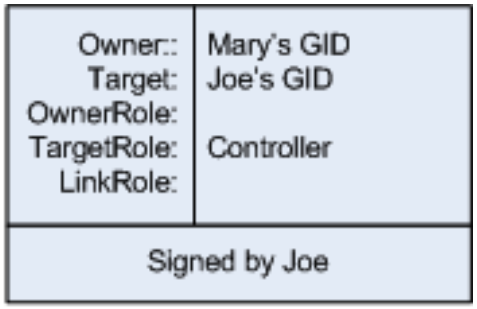
1. Create the identity certificates and private keys needed for an ABAC policy.
2. Generate ABAC credentials using the private key(s) of the issuer(s).
3. Add the identity certificates needed for a negotiation.
4. Add the issuer based credentials to the service-side negotiator (or discovery service)
5. Add the subject credentials to the requestor-side negotiator.

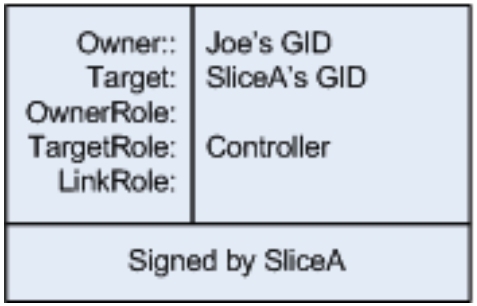
Policy Enforcement:

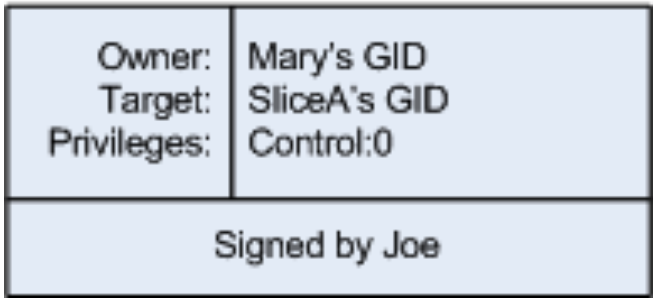
1. Decision control points issue an access request based on local policy.
2. Peer negotiators exchange messages until a decision is reached.
3. The decision is returned to the access mediator

Credential Examples









Discovery

*How does an ABAC negotiator get the correct set of credentials from the subject and issuer to make a **decision**?*

What is the simple way to begin with a centralized solution where everything is stored at the Utah clearinghouse?

What is the scalable implementation that we want to consider for the future?

- Credential discovery appears straight forward and is needed for credential integrity if not distributed a priori. ABAC currently uses standard X.509 identity certificates.
- For ABAC credential discovery, indexing of credentials must be available for forward searching and backward searching.
- Service providers use the backward search, while subjects need to forward search.
- Index by issuer is useful for revocation and auditing but not strictly needed for discovery.
- Discovery will be needed for scalability of non-sensitive credentials.

Policy

COBHAM

What is ABAC policy?

- Policy in ABAC is the set of credentials used by two negotiators to complete a negotiation. It may also include acknowledgement (ack) policy, which defines sensitive credentials and the roles required for their release during a negotiation.
- We need to define *policy* for GENI and each aggregate or component manager joining the ProtoGENI cluster.
- Ack policy is not immediately necessary, but as more users and applications projects are added to the GENI environment, some sensitive credentials should be anticipated.
- Is it initially necessary to refine roles beyond users and administrator? We are currently looking for application layer examples!

Integration Summary

COBHAM

What does ABAC need added to ProtoGENI for reference implementation use?

ProtoGENI Features

- *Current*
  - Uses X.509 identity certificates
  - Supports simple member credentials
  - Signs XML credentials
- *Needed*
  - Supports simple inclusion credentials
  - Supports linking inclusion credentials
  - *Credential searching for discovery service*

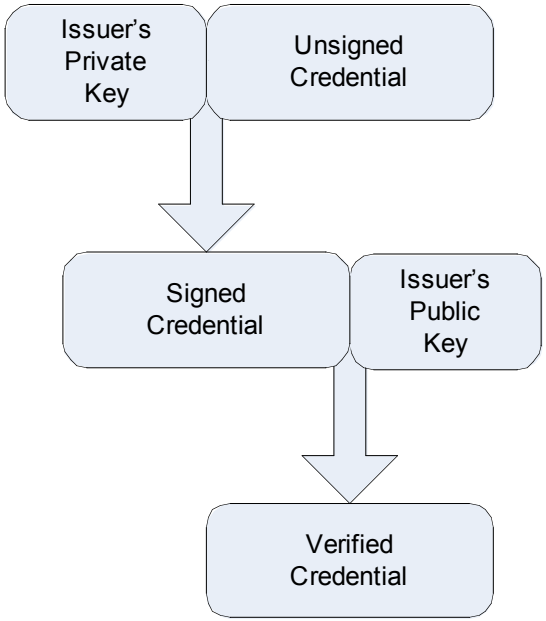
ABAC Features

- *Current*
  - Uses X.509 identity certificates
  - Has extendable credential format
  - X.509v2 attribute certificates
- *Needed*
  - Use-case policy examples
  - Discovery client for clearinghouse
    - Identity certificates
    - *Signed Credentials (non-sensitive)*

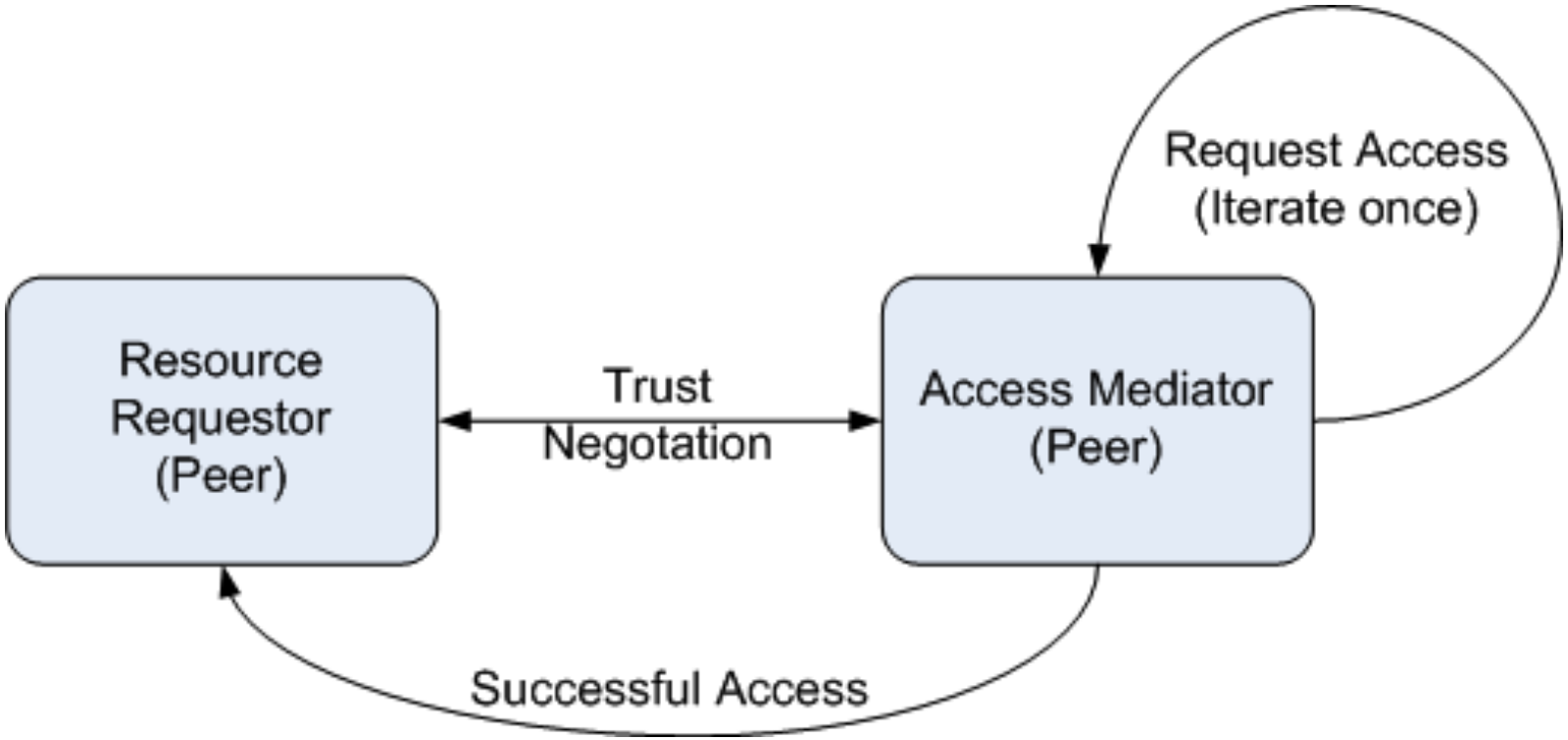
Extra Slides

Credential Integrity

- To ensure integrity all entities (issuers and subjects) require a key pair for:
  - digital signatures
  - secure communications
- Issuers use their private keys to sign credentials.
- Credential creation requires an RT credential and the issuer's private key.
- Credential verification occurs during an ABAC negotiation.
- The signed RT credential is provided through the negotiation dynamically or at initialization.
- The issuer's public key can be distributed manually a priori or dynamically at run-time.
- Signed credentials can be given to the subject (the current ProtoGENI model) or discovered dynamically by the resource provider.



Peer Communications



Draft Policy Workflow

COBHAM

Comments

- Slice authorities generate/remove slice credentials when slices are created/destroyed.
- Designated authorities can be delegated on a per slice or global basis.
- Designated authorities also include ProtoGENI agreements (i.e. sliver locales, groups, etc.)

Questions

- Can the clearinghouse restrict credentials? (Not needed for discovery)
- What flexibility does the slice authority need?
- What is the current mechanism for transferring credentials in ProtoGENI between the owner and signatory?
- Where does the Emulab certificate generator fit into this?