GENI Security Services

Calvin Ko, Alefiya Hussain, Steve Schwab,
Jim Horning and Sandy Murphy

Sparta, Inc.

The Threat Model

- External attacks on the GENI infrastructure, a DoS attack
- Contain and prevent the impact of accidental/malicious misbehaving experiments on the outside world
- Isolation between experiments, so that one experimenter cannot disrupt another

Security Requirements

- **Explicit Trust**: All principal privileges should be managed explicitly
- **Least Privilege**: each principal is given the authority needed to perform a particular task
- **Revocation**: compromised components can be recalled from an experiment
- **Auditability**: compromise incident traceable
- **……Scalability, Usability, Autonomy, Performance**

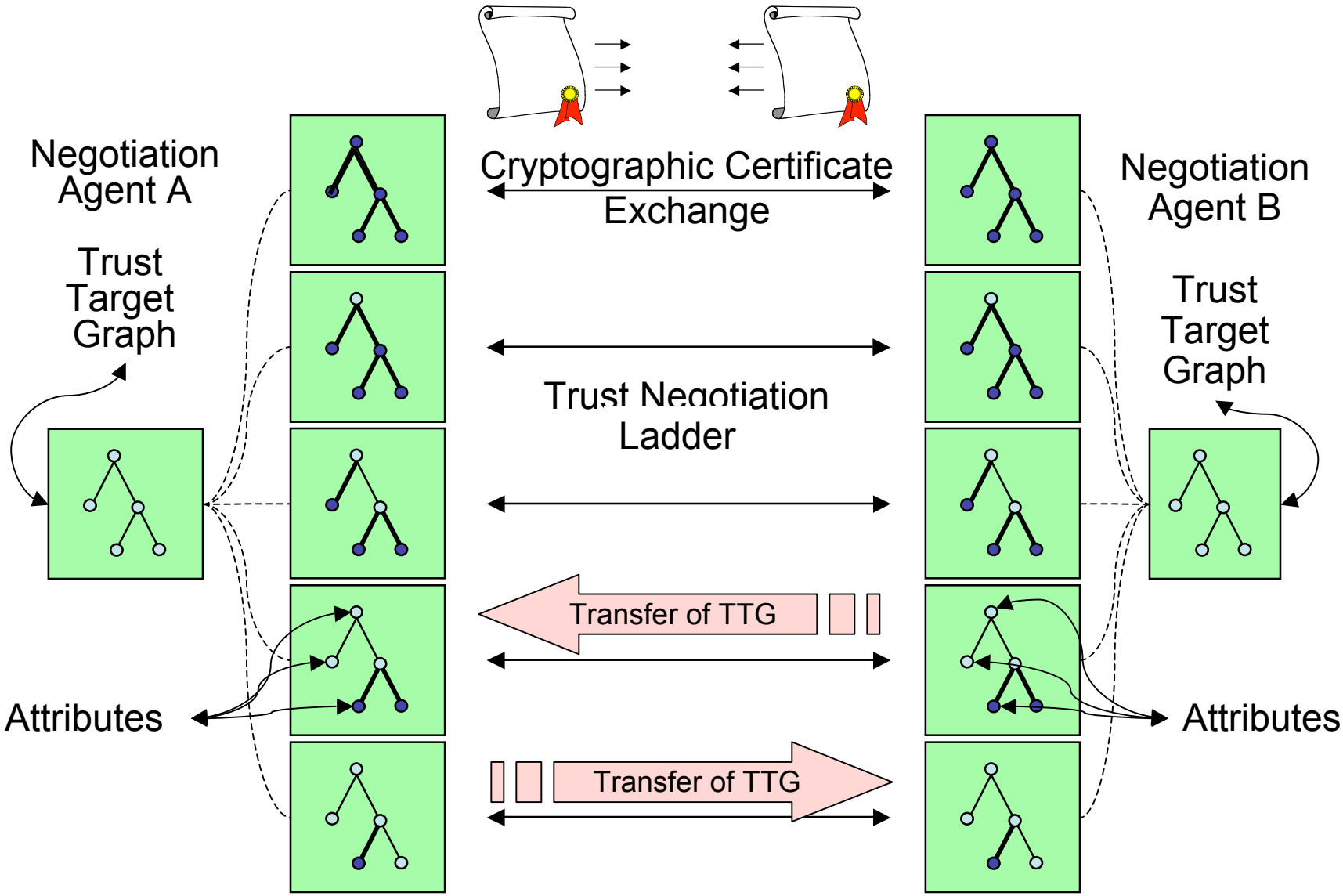
Identities, Authorization, and Accountability Requirements

- Identities and Identity records
  - Every principal will have an identify for accountability
  - Principal may have multiple identities
  - GENI identity will map to a real world identity
- Authorization
  - Before any GENI resource is accessed, but should also allow for support of anonymous use
- Accountablity
  - Activity should be traceable to a principal, mainly to identify sources of bad traffic

Attribute Based Access Control

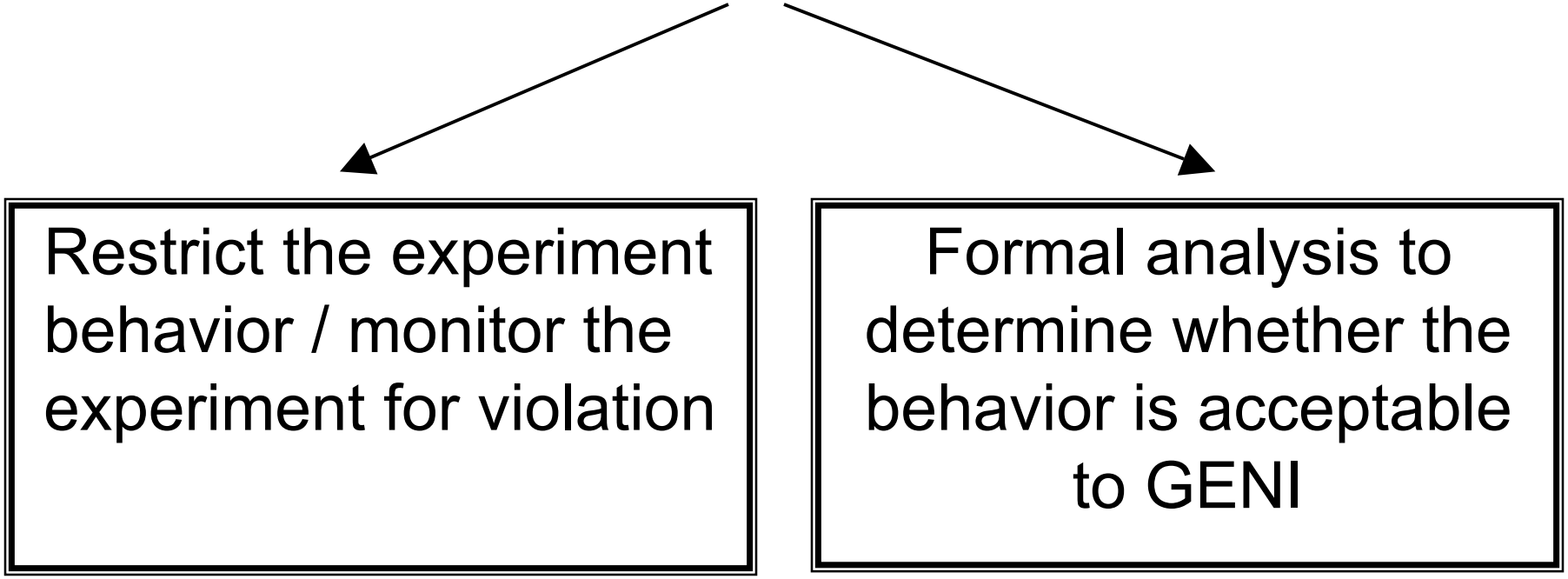
- Authorization decision is based on attributes of the principal
  - Credentials carry cryptographically signed claims about an principal's attributes
  - Requestor and provider may be strangers
  - Automated **Trust Negotiation** protects sensitive attributes while enabling unanticipated users to gain access in accordance with policy, and principal's authorization attributes

ABAC Trust Negotiation



Experiment Monitoring

- Specification-based detection
  - Specify valid experiment behavior of a slice
    - interaction with the outside



GENI Security Services for Experimental Slices

- Provide security services in the form of a security library and/or toolkit interface
- Reusable security components
- Allow researchers to plug in GENI facility security mechanisms without having to re-invent the wheel.

Issues and Questions

- Should each slice have a standard way of accessing security services exported from the GENI substrate
- What services are relevant?
- How should access be provided?
- Should a GENI slice be able to access services in another GENI slice?