Ingredients of an Early Design for Protecting the GENI Facility

GENI Distributed Services Working Group
Tom Anderson, David Andersen, Mic Bowman, Frans Kaaskhoek, Rick McGeer, Vivek Pai, Mike Reiter, Mothy Roscoe, Ion Stoica, Amin Vahdat

Disclaimer

- This talk summarizes the early design of security mechanisms to protect against abuse of the GENI facility
  - Prior to establishment of BBN as GPO
- I have no knowledge of how this relates to the security facilities envisioned today for GENI
- In particular, I in no way speak for BBN or the current state of GENI on this matter

Some Topics We Considered

- Threat model
- Goals/requirements

- Access control
- Authentication and key management
- Auditing
- Intrusion detection

Threat model

Exploitation of a slice

- Runaway experiments
  - Unwanted Internet traffic
  - Exhausting disk space
- Misuse of experimental service by end users
  - E.g., to traffic in illegal content
- Corruption of a slice
  - Via theft of experimenter's credentials or compromise of slice software

Exploitation of GENI itself

- Compromise of host O/S
- DoS or compromise of GENI management plane

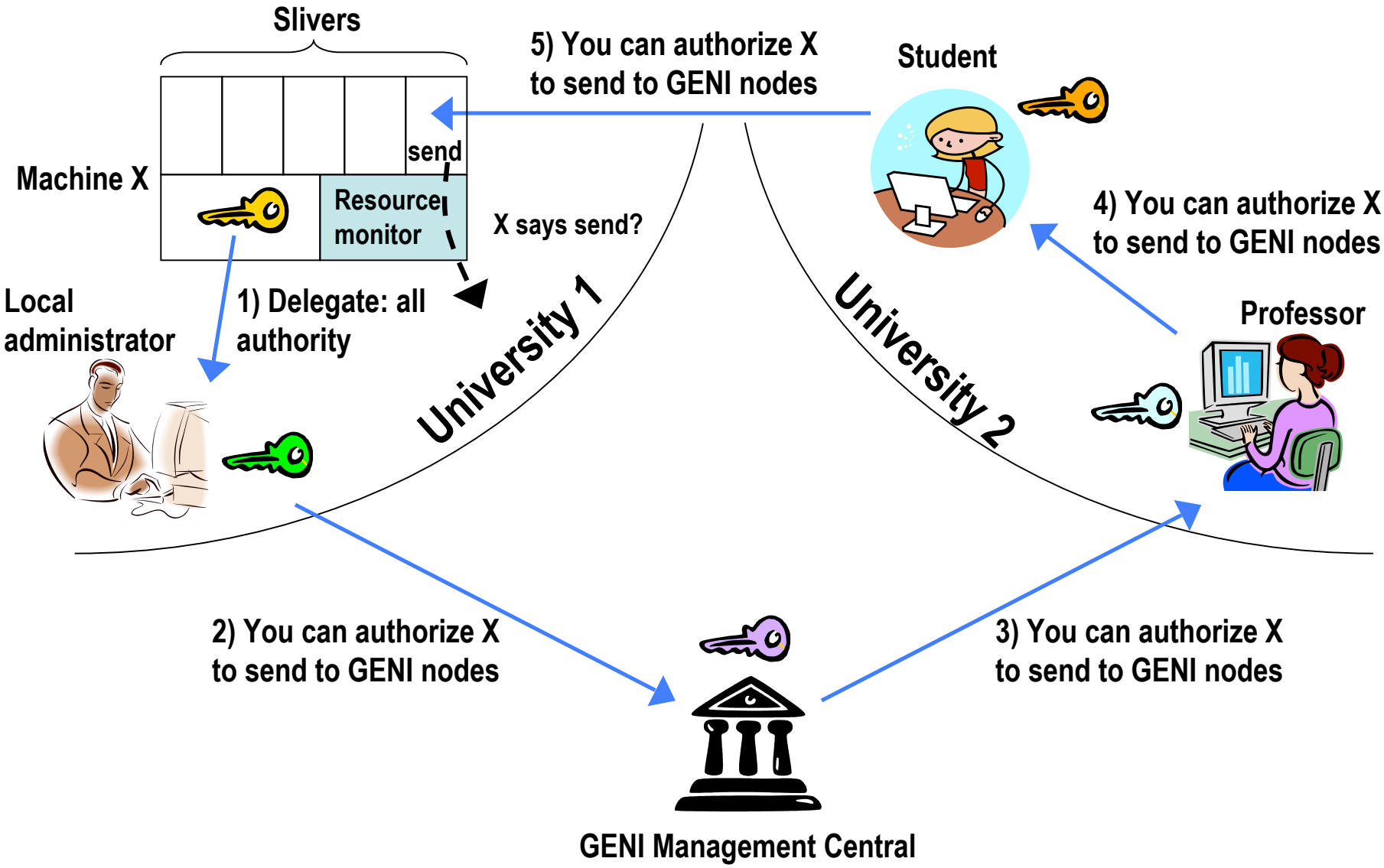
Requirements: Do no harm

- Explicit delegations of authority
  - Node owner → GMC → Researcher → students → …
- Least privilege
  - Goes a long way toward confining rogue activities
- Revocation
  - Keys and systems will be compromised
- Auditability
- Scalability/Performance
- Autonomy/Federation/Policy Neutrality
  - Control ultimately rests with node owners, can delegate selected rights to GMC

Access Control Requirements

- Arbitrarily flexible
  - Did not want to “hard code” policy into the system
- Dynamically extensible
- Verifiably sound and principled
  - Avoid ad hoc approaches
- Auditable
  - Must be able to determine why an access was granted, and who was responsible

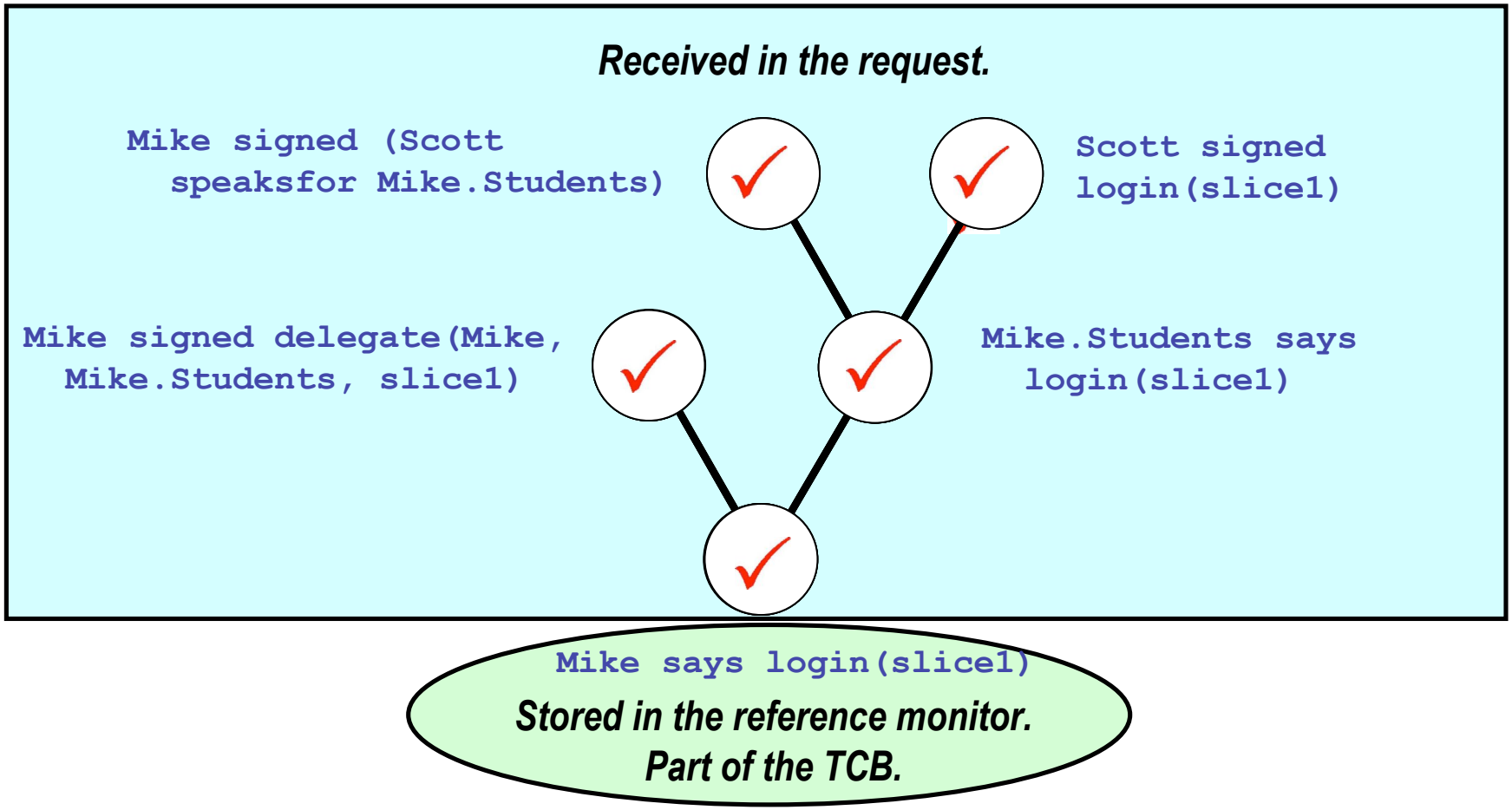
Authorization Example



A Proof-Carrying Approach

- Encode access control decision procedure in a formal logic
  - Can be used to express groups, roles, delegations, and new constructs
  - Can encode other, specific access-control mechanisms
- Digitally signed statements (e.g., certificates) used to instantiate logical statements
- Client submits a proof that its request complies with access-control policy
- Reference monitor checks that the proof is a valid proof of required policy

A Tiny Example



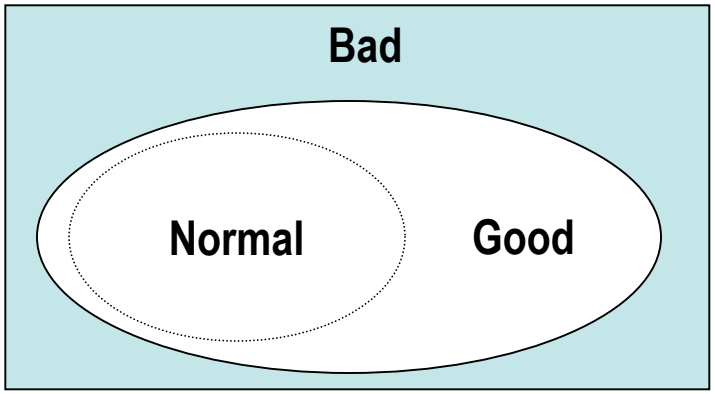
Authentication and Key Management

- GENI would have a PKI (as a corollary of the authorization framework)
  - Every principal would have a public/private key
    - E.g., users, administrators, nodes
  - Certified by local administrator
  - Keys sign certificates to make statements in the authorization logic (identity, groups, authorization, delegation, …)
- Private key compromise an issue
  - Encrypted with user's password? Off-line attacks
  - Smart card/dongle? Most secure, but less usable
  - Capture-resilient protocols: A middle ground
    - An (untrusted) capture-protection server can disable use of a key, e.g., when observing a password-guessing attack

Intrusion Detection

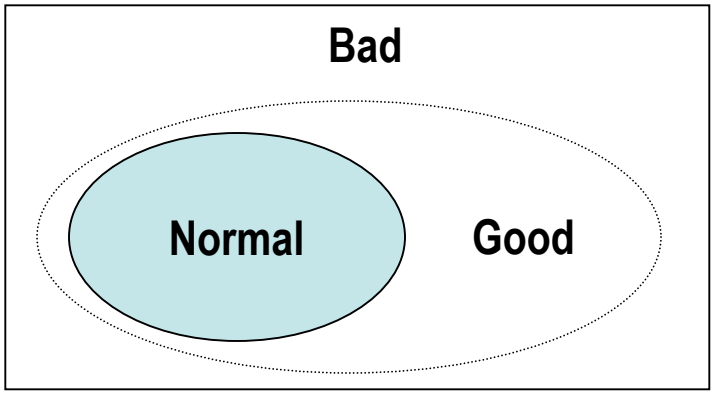
- Traditional intrusion detection methods may not suffice *for monitoring experiments*

Misuse detection
Specify bad behavior and watch for it



Problem: Experiments do lots of things that look "bad"

(Learning-based) Anomaly detection
Learn "normal" behavior and watch for exceptions

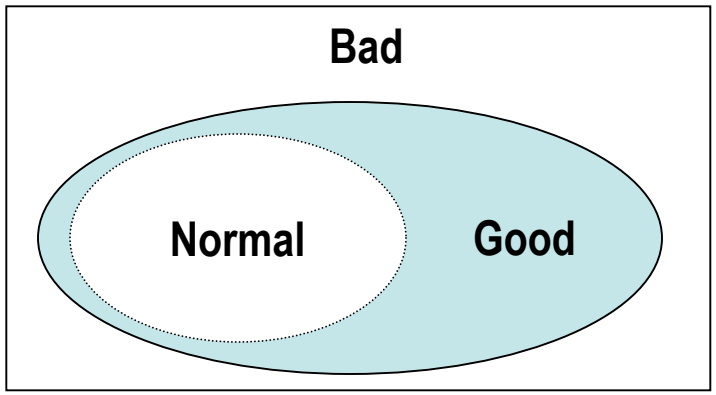


Problem: Experiments may be too short-lived or ill-behaved to establish "normal" baseline

Intrusion Detection

- Specification-based intrusion detection is more appropriate for monitoring experiments
  - Fits in naturally with authorization framework, as well

Specification-based intrusion detection
Specify good behavior and watch for violations



Audit Log Prototype: PlanetFlow

[Huang et al.]

- PlanetFlow: logs packet headers sent and received from each node to Internet
  - Enables operations staff to trace complaints back to originating slice
  - Notify experimenter; in an emergency, suspend slice
- All access control decisions can be logged and analyzed post-hoc
  - To understand why a request was granted (e.g., to give attacker permission to create a sliver)

Issues Left Open

- DoS-resistant GENI control plane
  - Initial control plane would employ IP and inherit the DoS vulnerabilities thereof
  - GENI experimentation may demonstrate a control plane that is more resistant
- Privacy of operational data in GENI
  - Could be a great source of research data
- Operational procedures and practices
  - Central to security of the facility