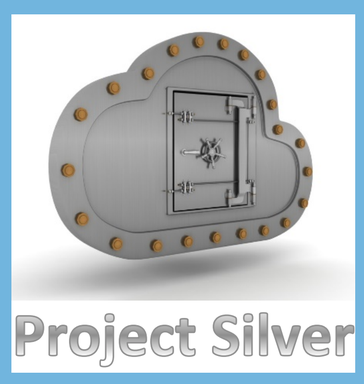


Logical Trust: SAFE and STRONG

Qiang Cao, Jeff Chase, Vamsi Thummala
{qiangcao, chase, vamsi}@cs.duke.edu

Motivation

Silver clouds need a variety of trust and authorization models, and declarative policy languages for attested evaluation.

- Rich access control with groups, roles, delegations (e.g., AWS IAM)
- Secure hierarchical name spaces (e.g., IAM, DNSSEC, GENI)
- Cross-tenant metadata assertions by trusted cloud provider
- Software identity and attestation
- Virtual network control and secure interconnection
- Trust agility: flexible trust anchors in a federated cloud systems

Logical trust is a powerful foundational tool to meet these needs, and it extends naturally to federated environments.

Design

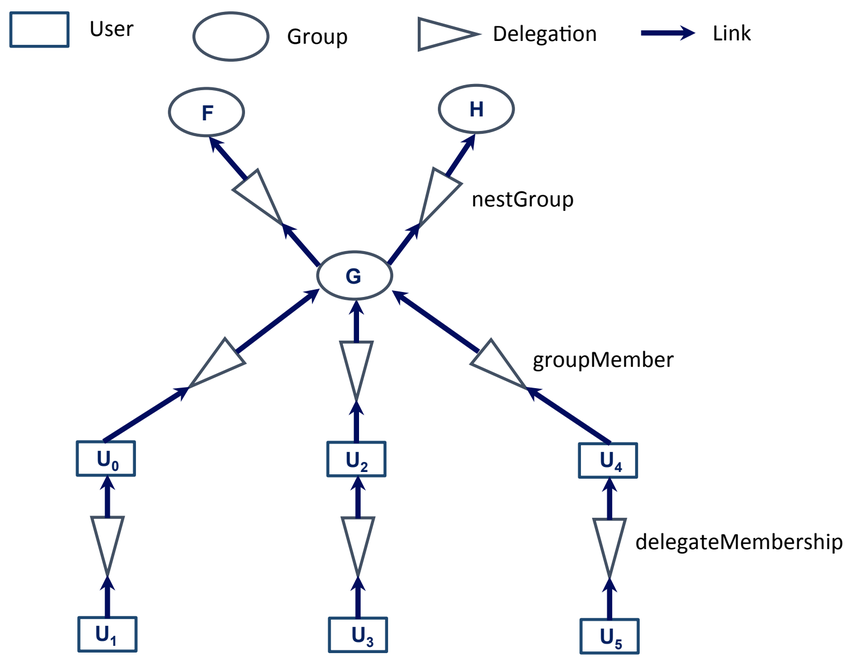
SAFE: simple and powerful authorization with logical trust

- Logic-based declarative trust language (datalog with *says* and ranges)
- User-defined predicates capture trust assertions and credentials.
- User-defined inference rules capture policies.
- Off-the-shelf logic engine checks policy compliance.

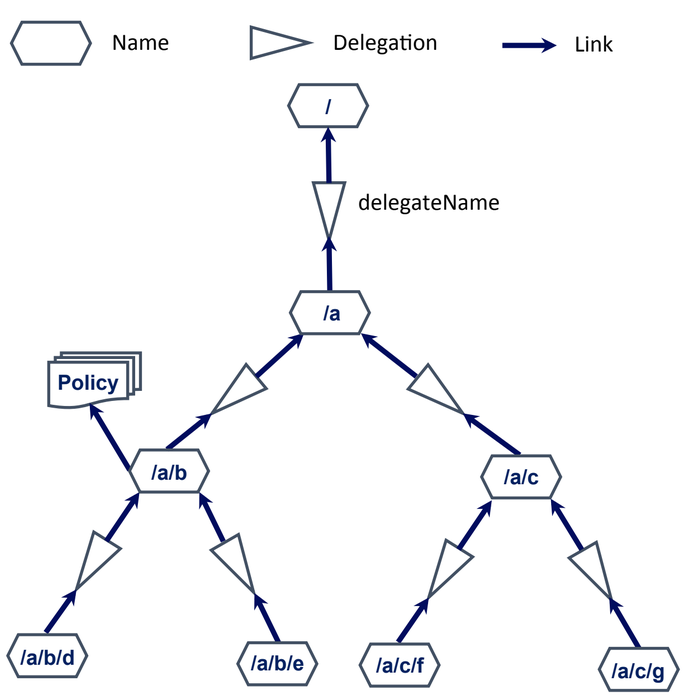
System framework for scalable trust logic in federated systems

- Cryptographically self-certifying names for principals and objects
- Logic sets are stored as certificates in a shared key-value store (Riak).
- Sets are named by secure tokens: pass-by-reference, fetch, and cache.
- Sets are linked to match delegation patterns in the application.
- → Easy retrieval/pruning of relevant content for each check.
- Scripting language simplifies management and linking of logic sets; isolates logic and trust concerns behind an application-defined API.

Linked logic sets for nested groups



Secure hierarchical names in a multi-rooted name space



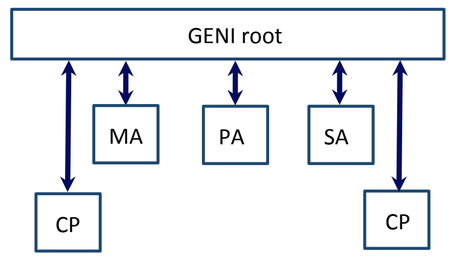
Applications

STRONG identity and access management in cloud

- Secure hierarchical names for objects and principals (SRNs)
- Attach policies to subjects, objects, and name spaces
- Nested groups
- Equivalent in power to AWS IAM, but for a federated system
- <300 lines of SAFE logic and scripting

GENI multi-domain cloud using STRONG groups ("projects"), federated identity, and multiple object authorities

- Federation of multiple cloud providers (CP)
- CPs and authority servers for user identity (MA), projects (PA), and resource slice approval (SA) endorsed by federation trust root
- Rich delegation of project membership and slice capabilities

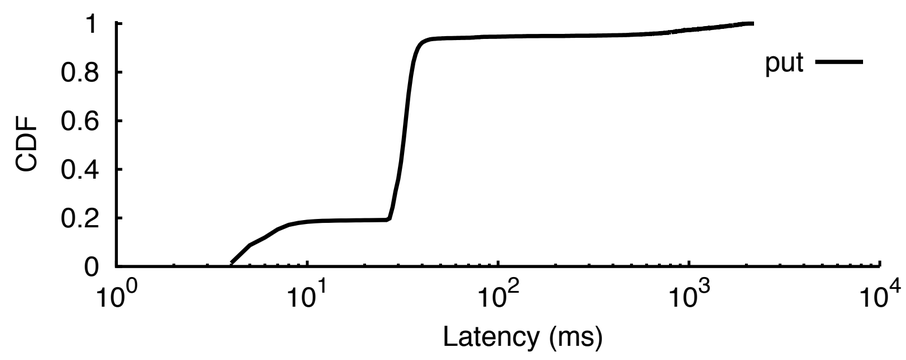


Some Results

GENI Workload mix:

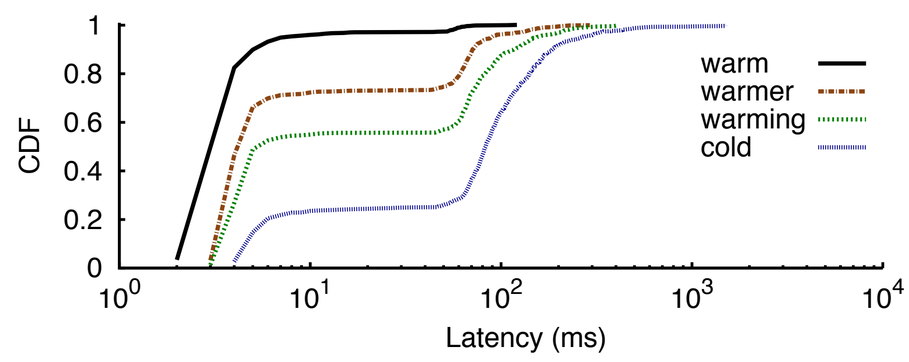
Phase I: put-only operations

- Create project and slice objects and delegate rights
- Policy compliance checks for object creation



Phase II: query-only operations

- Perform authorization checks
- Cold start: direct query loads to different VM(s)



Phase III: update+query operations

- updateThenQuery: a delegation update is immediately followed by a query that uses the delegation
- Cache misses result in prolonged latency