MAGIC Meeting Minutes
August 5, 2015

Attendees

Ilya Baldin	RENCI
Richard Carlson	Richard.carlson@science.doe.gov
Jeff Chase	Duke U.
Shantenu Jha	Rutgers Un.
Dan Katz	NSF
Grant Miller	NCO
Rajiv Ram	NSF
Don Riley	U. Md
Derek Simmel	PSC

Action Items

1. Grant Miller will send out proposed MAGIC FY16 tasking from the LSN to the MAGIC members

Proceedings

The meeting was chaired by Rich Carlson, DOE and Dan Katz, NSF.

ExoGENI, ORCA, SAFE: Jeff Chase

The GENI federation supports the development, management, and functioning of distributed resources. It enables users to request slices of resources, an end-to-end virtual execution context with configurable properties including containment and isolation. GENI uses the Open Resource Control Architecture (ORCA) to instantiate VMs and VLANs to link sites via circuits and to enable an external SDN controller. Building a GENI platform entails a sequence of joins of a hub and a spoke. Each binding operation is a stitch which has values (label, tag, LUN, flowspace). Slivers include nodes and links. Nodes run programs, links connect nodes.

ExoGENI provides an infrastructure as a service (IaaS) that includes:

- Open substrate
- Off-the-shelf back-ends
- Provider auton0omy
- Federated coordination
- Dynamic contracts
- Resource visibility

ORCA Aggregate Manager (AM) structure provides:

- Off-the-shelf AM shell
- Plug-in setup scripts
- Substrate specific back-end code
- API messages carry declarative semantic resource descriptions, e.g., NDL/OWL

GENI AMs are proxies for authZ and resource control. AMs delegate some policy control to GENI Authority servers. The coordinator authorities act for the federation to vet identity, access control, kill switch, etc. Policies are described in logic. The GENI clearinghouse provides coordination among the GENI root participants so that:

- Each entity can speak with its own keypair

- Wield credentials
- Produce and consume credentials

There are limited trust relationships among them. Trust reflects agreements. Credentials capture this trust. Trust may be transitive. Transitive trust is inferred from facts and policy rules.

Under AuthZ a user with an identity is authenticated with PKI/SSL/MAC and is issued credentials that enable them to request resources. The GENI central authority then authorizes the use of the requested resources. Authentication => Identity=> Attributes=> Policy=> Rights=> Authorization.

Secure Authorization for Federated Environments (SAFE) is a practical minimalist trust logic with a custom datalog+says inference engine. It composes policies and statements easily in plain text. SAFE certificates are a building block for secure networked systems. Knowledge about principals is represented as logic statements. Principals have secure names (public key/hash, e.g., SPKI/SDSI). Predicates/atoms represent roles, attributes, and capabilities. Statements are authenticated and may be shared over the network.

GENI enables chains of trust:

- Member Authority: A user registers. GENI checks the user identity, obtains user attributes, checks that the user is qualified, and executes an agreement
- Project Authority: Verifies that the user is authorized to create a project and act as a project leader. Project membership can be delegated
- Slice Authority: Verifies that project is valid and user is authorized to create a slice in the project. It verifies that the4 slice created is valid and the user is authorized to request resources for the slice.

SAFE GENI is/has:

- A multi-provider cloud with evolving trust structure
- Cloud/transport providers provide local trust policies governing interactions with peers
- Delegatable access control for Global Objects with Policy Mobility: policy is applied wherever the object is used
- Federated Identity
- Flexible federation
- Secure SDN within/across/to/from slices

For the complete briefing, please see:
http://www.cs.duke.edu/~chase/chase-magic-080515.pdf

Potential MAGIC tasking form the LSN

Discussion among the MAGIC members identified a number of topics that MAGIC would like to focus on in the upcoming year. These topics include:

- OSG growth and evolution; XSEDE components: Wrangler (data intensive computing), COMET infrastructure, JETSTREAM Infrastructure
- Advanced computational modeling and cloud computing: Radically new techniques and standards. Invite involved organizations to talk.
- Federation of repositories across federal agencies. Current applications of iRODS include NASA, NOAA, NOAO, NSF projects. Keith Marzullo potential speaker
- E2E encryption in the cloud
- Identity management and access control in virtual environments and clouds

Meetings:

August 13-14: BER virtual laboratory meeting, Washington DC: How to design a virtual laboratory
September 28-29, WSSPE meeting, Boulder, CO: Software sustainability
October 15-16: Software management workshop, Washington DC

Next MAGIC Meeting
September 2, 2015, NSF, Room TBD.