gMOC

GENI META-OPERATIONS CENTER

Spiral 1 Security & Privacy Strategy for Operational Data

Summary

The GMOC will be an important collector, aggregator, and provider of operational data to the GENI community and beyond. While we will not be developing policies and systems to classify this data, or to authenticate and authorize parties wishing to view or alter it, we will be working closely with any system developed by others in GENI to handle this.

General strategies, both for the immediate future, and the medium-term, have been discussed with Steve Schwab, and we believe that we will continue to work closely with GENI Security as we move forward to help develop security policy and integrate with GENI security systems as they become available.

Data Collection & Storage Strategy (inbound from projects)

Authentication/Authorization of GMOC for Data Collection

Since GMOC has been focusing on working with projects (particularly control frameworks) within each cluster and collecting data in whatever format is available at the project instead of asking the clusters to push data to GMOC, we have handled Authentication & Authorization of the data on a case-by-case basis, getting credentials using whatever method the individual projects have.

Protection of Operational Data Collected by GMOC

GMOC follows common security best practices to protect our systems from unauthorized access, attacks, etc. GMOC engineers have extensive security analysis and implementation experience. Access to GMOC data is protected by a variety of measures, including restricting access to servers by use of two-factor authenticated bastion hosts, encrypted communications channels, etc.

Planned Future Strategy for Security Characterization for Data being Provided to GMOC by GENI Projects

Moving forward (most likely later than Spiral 1), with the emphasis of leaving control of the sharing of data or pointers to data with the sources of that data, it will be important to have a system projects may use when sharing data to classify this data appropriately. For example, projects must be able to make measurements or data about a particular slice to be kept private, visible in both content and existence only to the slice owner. They must also be able to change this characterization at any point. For example, the slice data may be private until results are published, at which point the researcher would want the slice data to be widely visible for purposes of verification and repeatability.

The GMOC will integrate any security characterization methods developed by GENI into our data collection process, and will provide the interface needed to alter characterizations by authorized parties for data at any point. The GMOC will also integrate with any auditing of this process, for example, providing security characterization reports as needed.

The bulk of the development for this has not been completed, and the details of an appropriate characterization system, such as what types of classes and how many options for each type are necessary, have not been defined. The GMOC will participate and offer opinions on this discussion as it happens. The GMOC will not develop our own characterization schema or system to authorize and authenticate parties for characterization change purposes.

Data Sharing Strategy (outbound to consumers of operational data)

Initial Expectations for Privacy of Data Provided to GMOC by GENI Projects

GMOC has been explicit in our discussions with GENI projects that any data provided to GMOC is assumed to be public. So far, all projects providing data have been providing data that is unrestricted already.

Potential Early Methods for Authentication/Authorization for Consumers of Operational Data collected by GMOC

If the issue of privacy of operational data becomes an issue, if a project has data to share that must be kept private, GMOC will work with those projects to stand up an authentication/authorization system to protect that data, or use a system already in place.

For instance, we could use simple password protection for some data, and require sign-off from project data providers before providing access to parties who request it. Such a system would be expected to be useful in early spirals of GENI, before a more fully integrated Security system is in place.

Planned Future Architecture for Integration with GENI Security Services for Authentication/Authorization of Data Views and Sharing of Operational Data

In future spirals, as we begin to collect more data, and GENI brings active experimenters online, we will focus on following policies and security characterization schemas developed by GENI and on integrating our systems with a GENI Security service who would provide AAA services. We don't anticipate deploying any AAA infrastructure of our own. Rather, we believe that we will provide the hooks from our operational data tools into an external GENI Security Service to provide the authorization processing.