From: William E Johnston <wejohnston@lbl.gov>
Subject: **possible issue for discussion at the OSG Council Meeting**
Date: August 9, 2009 5:41:52 PM PDT
To: osg-council <osg-council@OPENSCIENCEGRID.ORG>

OSG Council;

I would like to propose the following for discussion.

At a recent meeting in Berkeley with Miron, Ruth, Mike Helm, and others, there was a discussion about the existence of risks associate with the authentication and authorization systems that act as gatekeepers to the LHC computing and storage resources.

The functioning of the LHC data analysis systems depends, at a fairly intimate level, on the certificates issued by one or more CAs (mostly the DOEGrids CA at this point in the US) and on the authorization systems that use those certificates, together with information about resource policy and user characteristics, to grant access to the underlying compute and storage systems.

While a lot of attention is paid to the functioning, and adequacy of behavior under extreme loads of the analysis systems, including the authentication and authorization systems, with at-scale testing used to identify and correct load-based failure modes that could negatively impact operation in the production data analysis environment, rather less attention has been paid to the possible cybersecurity failure modes of the authN and authZ systems that are the access gatekeepers for the resources.

What are the vulnerabilities associated with these systems? What are the threats / attack modes that could exploit the vulnerabilities? What is the likelihood of successful exploits? What are the consequences and thus the risks of exploited vulnerabilities? How is recovery accomplished and with what impact on the operation of the systems that depend on authN and authZ?

With respect to the ESnet operated DOEGrids CA, this is operated according to current best practices for securing the CA infrastructure (off-line root CA kept in vault, hardware crypto modules for managing DOEGrids CA keys, single-purpose CA servers in locked machine room in alarmed, locked racks, etc., etc.). However, while ESnet undergoes a periodic external review of its internal security stance, none of the review committees have really had reviewers who were familiar with the subtleties of PKI infrastructure. (A recent IGTF audit focused on operation and record keeping of the sort related to PKI based trust standards rather than cyber threat issues.)

An evaluation is needed of the vulnerabilities and threats, risks and consequences and mitigation procedures for authN and authZ systems that support the LHC and other OSG projects. There are probably not a lot of surprises lurking in the DOEGrids infranstructure itself, but, but the situation must be documented so that the LHC community knows exactly where it stands in its use of this infrastructure, how it could fail, the likelihood of failure, the consequences of failure, the recovery process, etc.

Probably the more important issue is the cybersecurity robustness of the authZ systems that the LHC community uses, their interaction with the PKI CA, and the vulnerabilities and risks/consequences inherent in those systems and interactions. Because if there are major breakdowns in the authZ systems, this could easily disrupt the data analysis for the production LHC data.

Examining the authZ system is harder than examining the DOEGrids CA because they are more complex and are intertwined with the analysis systems.

So, the issue here is to develop a methodology for such an analysis and then to figure out how to actually accomplish the analysis and document the results in such a way that 1) the community will have a clear understanding of the situation, and 2) so that any serious vulnerabilities are identified in such a way that they can be addressed, and 3) risks and consequences are recognized and mitigation strategies are developed and documented.

I had hoped to have some external input on the availability of cybersecurity expertise in the PKI arena, but I have not yet been successful in this quest.

Bill

```
--
  William E. Johnston
  ESnet Senior Scientist and Adviser
  Lawrence Berkeley National Laboratory
  PGP: EF 39 DD 5E 42 A3 B4 09  BD 51 82 88 DE 66 6F 44  46 78 3E C7
```