OSG Security Review Report

DRAFT

Jim Marsteller, PSC
Todd Tannebaum, UWisc
Romain Wartel, CERN
Von Welch, NCSA
2/27/2009

Context

This review is requested by the Executive Director. The report will be delivered to OSG ED. The ED is asking for more discussion and less presentation. I want to use the existing information available and improve it and the formatting as preparation for the review.

Charge

The charge of the review is to assess the effectiveness of the Open Science Grid computer security program. This would: Assess our program and that we are minimizing as far as possible loss of scientific opportunity due to security issues; Assess our assertion in striving to maintaining an open, self-administered environment that does not in fact introduce "high cost" risk; Give us advice on areas of our program that would benefit from change/clarification/rethink.

There are several other issues inherent in the charge:

- Is the effort assigned to the OSG security program appropriate given the impact of potential disruptions?
- Is the OSG security program scoped appropriately and evolving in the right direction both operationally and technically ?
- Are the principles of the OSG security program appropriate in terms of the division of responsibilities and authorities between the members of the OSG Consortium.

Answers to Charge Questions

Is the effort assigned to the OSG security program appropriate given the impact of potential disruptions?

From the information presented at the security review we believe that the current security staffing of 2.05 FTE is appropriate. However, while this level of staffing is sufficient for supporting day to day tasks to promote the security program, it is not capable to adequately handle security emergencies.

The response to a security emergency will require the assistance of many members of the OSG program, sites and VOs under the coordination of the the OSG security staff. In order to minimize potential service disruptions, a clearly pre-defined response plan that outlines roles and responsibilities

must be communicated to all responders. Some things this plan would include are: instructions for responders such as when is it appropriate to take a service offline, coordinating communications during the emergency as well as contingency plans for service outages.

In summary, the amount of effort assigned to the OSG security program is adequate excluding security emergencies. The ability the to organize and effective response team and preparedness plan beyond the dedicated OSG security staff must not be overlooked.

Is the OSG security program scoped appropriately and evolving in the right direction both operationally and technically ?

The OSG program has incorporated the different elements necessary to ensure an appropriate response to the security threats faced by the grid infrastructure.

It has also managed to adapt to new risks and to collaborate with additional partners when needed. Establishing communication channels with communities and infrastructures linked to OSG has also been correctly identified in the OSG security program. Effort to continue in this direction is highly encouraged, in particular to ensure collaboration in the operational security area with peer-grids and other partners involved with OSG. The use of common standards,like policies, procedures or tools is perceived to be an important asset.

In order to provide additional structuring to the OSG security program and to ensure that an appropriate level of priority is given to the most important security threats, a process should be implemented to periodically review and update the OSG risk assessment. That risk assessment should then be used as the basis for the work plan (WBS) for the upcoming year. A number of metrics should be identified in order to measure the progress of the sites and of the infrastructure to respond to identified security threats. Such metrics should be used to adapt the priorities of the security team to emerging threats or possibly weak areas.

The security of the software has also been identified as a possible risk for the infrastructure and should be incorporated to the risk assessment. A particular emphasis should be given to review security risks linked to the software release process itself, for instance access control to the source code or the management of security vulnerabilities.

A significant amount of work has been dedicated to incident response, which has proven fruitful. However, in order to improve the overall security of the infrastructure, security training and dissemination should also become a priority. Ultimately, the objective is to improve and leverage the security standards of the different participating sites. Whenever possible, sites should be given the opportunity and encouraged to be involved in security activities, for instance to provide feedback on security procedures and policies, to organize local security training events or to report possible security vulnerabilities.

As the infrastructure is believed to have reached maturity and a phase of stable operations, some effort should be made to ease the day-to-day security operations by automating a number of manual tasks (for instance, monitoring, or identifying the source of suspicious grid jobs).

Are the principles of the OSG security program appropriate in terms of the division of responsibilities and authorities between the members of the OSG Consortium?

The principles of the OSG Security Program are:

- Autonomy of OSG members
- Integrated Security Management

In practice, these principals equate to a responsibility on the security program to communicate heavily with the sites, VOs, users, software providers, etc. that make up the OSG. It puts the program in the role of requirements gathering, coordinating with and educating these members, in order to understand the needs of the members, reach a agreeable compromise, set expectations, and make sure each member has the knowledge to fullfill those expectations. It often puts the program in a mediation role when there are conflicts between different members, eventually such conflicts will tend to get escalated to the executive level, but that tends to be after efforts at the level of the security progam prove fruitless.

These principles are in line with a "bottom-up" philosophy that is not uncommon in distributed collaborations and the overheads introduced are also not uncommon in such collaborations. Generally as long as there is a understanding in the program and its management of the added overhead, these principles should not pose a major problem.

Questions for the Security Team

1. What were priorities last year, how well did they do in meeting them?
2. What are the priorities for next year?
3. How will you go about updating the Risk Assessment plan?
4. What is the relationship between the EB and the security team? What authority, if any, has been delegated from the EB to the security team?
5. How does OSG manage the different security standards between the sites?
6. What is the goal of OSG's security training? What is the audience? What is the objective? What problems are you solving? Is it within the scope of OSG itself?
7. What metrics are in place and/or planned to measure security progress?
8. What metrics are in place and/or planned to measure how security obstructs users from their scientific mission (Example: Dzero production impacted by INFN shutdown)
9. What plans, if any, are in place to digest logs from grid services?
10. How is the gap between high-level policies and specific procedural guidelines filled? Example: One hour response time to GOC security alerts.
11. What could be automated?
12. What is your procedure for auditing the software and what do you expect/hope to find?
13. OSG is community; how does the security team incorporate help/effort from 3rd parties? (software providers, site admins, VO admins, users)
14. Who are the stakeholders in the OSG program? And what are the responsibilities the OSG has to them?

Recommendations for Security Team

- OSG Security Team priories should focus on issues that
    - Sites cannot do by themselves. Example: Only OSG has a "global" view of auditing data to enable detection that user XXX only used 2 sites for the past year, but now all of the sudden is using 50 sites.
    - Risks that sites would otherwise not encounter except that they joined OSG. E.g. Focus on worrying about how adding an OSG CE increases a site's attack surface –vs- worrying about teaching sites about ssh security (something they would need to deal w/ regardless of OSG involvement).
- Is there a possibility of developing a volunteer community of security-interested people from sites and VOs to help?
- Define a set of metrics for the security program.
- There is a gap between light, high level security policies, and actual procedure (= guidelines). It may be necessary to fill this gap with operational requirements for the sites like "operational policies", whose approval process would be lightweight, yet describing actual requirements on the participants (as opposed to guidelines)?
- Dealing with the press during a disaster: Should this be incorporated in the OSG security

program? Send somebody to a "dealing with the media" training? Talk to the HEP press office network in the US?

- In OSG, a "security vulnerability" is identical to a "security incident", which is quite non standard as most people make a different between a security threat and its actual exploitation, perhaps the definitions could be clarified?
- VDT vulnerabilities management: perhaps a clear process should be produced (including timeline for disclosure, so called "quarantine") with the stakeholders?
- The risks linked to dependences in the VDT software should be incorporated, for instance by implementing a process to monitor security announcements from the relevant vendors.
- 24/7 coverage: the cost is rather cheap, but have the actual objectives and impact for the OSG security team being clarified?
- The security team uses accounting information for incident response, which is good. But should this be complemented with actual logs from grid services?
- Sites have their own monitoring, can it be complemented by grid-level monitoring? The aim would be to provide monitoring tools using information that is not available to sites alone.