LCG/EGEE SECURITY SERVICE CHALLENGE, LEVEL 1 DEBRIEFING REPORT

2006-04-18

OBJECTIVE

The goal of the LCG/EGEE Security Service Challenge is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.

OUTLINE

The Security Service Challenge level 1 (SSC_1) was launched in October 2005. The goal was that each of the 11 Regional Operation Centers (ROC) would submit a Grid job to their respective Grid Sites, and subsequently ask the Security Contact at the target Site for some specific details about the execution of the job. SSC_1 challenged the Workload Management System (WMS) of the Grid, i.e. the Resource Broker (RB) and the Compute Element (CE).

The original deadline for the completion was intended to be the end of November 2005. However, by the end of 2005, only five ROCs were ready with their report. A first reminder was sent in January 2006, and an escalation reminder was sent early February 2006. By mid-March 2006, three additional ROCs had reported. The eight responding ROCs were:

- AsiaPacific
- CentralEurope
- CERN
- GermanySwitzerland
- Italy
- NorthernEurope
- SouthEasternEurope
- UKI

The report from the January/February execution at the Russian ROC was filed in April 2006.

The responding ROCs represented 129 (out of a total of ~190) participating Grid Sites.

To date, three ROCs have not filed a response:

- France
- SouthWesternEurope

The Test OPerator (TOP) would normally be the Security Contact at the primary Grid Site of each ROC. The TOPs were asked to provide feedback from the exercise. The feedback helps us evaluate the results and to improve the procedure in view of future challenges.

The points raised below have been extracted from the feedback received.

WAS THE CHALLENGE USEFUL?

The majority of the participating TOPs deemed the exercise to be useful and not too time consuming. The experienced Security Contacts solved the exercise easily, while the less experienced found it difficult and perhaps de-motivating.

A relatively heavy workload fell on the shoulders of the system administrators of the Resource Brokers (RB). Most ROCs would submit the challenges via a small selection of RBs. On request from the target Sites, the RB staff repeatedly had to plough through large volumes of log-files in order to provide the information.

OBSERVATIONS

Alerting

Some Sites did not respond to the alert. Some reasons for this have indeed transpired:

- The Security Contact list was not up-to-date, i.e. the alert went to the wrong person;
- The Security Contact was overloaded and did not read the alert e-mail;
- The Security Contact was overloaded and quietly chose to drop the challenge;
- The Security Contact did not understand or realize the purpose and context of the alert e-mail;
- The Security Contact had not received guidance or was not sufficiently trained for his/her assignment.

Following the reminder or the further escalation, at times, the TOPs indeed succeeded in prompting the target Site to provide a response.

Reporting

The instructions strongly suggested that the participating parties use the Savannah reporting tool for the follow-up of the challenge procedure. Five TOPs chose not to follow this recommendation. The main reason for this was that the ROCs already had other reporting tools in operation. Thus did not want to make an exception for the SSC. Some Sites, that actually used Savannah, suffered because their Sites' e-mail filtering process rejected e-mails relayed by Savannah. Ticketing systems appear to be labor intensive, and mass production of tickets was reported inefficient.

Availability of logged information

The retention period for log files was not sufficiently long on all sites. In a few cases the required information had already been purged as a consequence of adopting the defaults of the distributed software.

Lines of communication

Not all challenged Sites contain a Resource Broker (RB). Challenges targeting these Sites were configured to use an off-Site RB (or even an off-ROC RB). An implication was that the target Site then had to contact the foreign RB site and enquire about the particularities of the challenging job.

Some Sites reported missing contact information or lack of responsiveness in this process. However, at least one ROC lauded the efficiency of the RB staff. Perhaps the diverging statements reveal an organizational difference between the regions.

On the other hand, one ROC considered the need to communicate off-Site as a premium and valuable learning point for the system administrators of the targeted Site.

Service availability

There will generally be some Site within a ROC which is unable to accept job submission at any given time. There can be many reasons: facility changes, hardware and software upgrades, incompatible and also incorrect configurations of the services. If the unavailability persists, it may cover the test window of the TOP, and the Site will be noted as incomplete for the purpose of the SSC.

Confidentiality concerns

Two ROC managers raised the question of confidentiality. Should the procedure followed by the SSC_1 be a model for real security alerts? Helpdesk staff and many other people are involved in providing the requested information, and they have access to an extensive collection of potentially confidential information.

Software

A software package was distributed to the TOPs. The software, the example Site configurations and the companion instructions were really beta release, but this did not raise much concern, apart from being somewhat too dependent on the development environment of the package creator. At a second, minor release, this dependency was relaxed.

Several TOPs complained about the time consumed in the execution phase of the challenge, and one TOP asked for a more asynchronous submission model.

RECOMMENDATIONS

The recommendations listed below, attempt to take into account the specific suggestions made by the TOPs, and, in addition, to respond to the major grievances that have been expressed.

Alerting and Reporting

A single comprehensive reporting tool with adequate access right granularity would greatly enhance both the efficiency and the transparency of the reporting and follow-up process.

Communication contacts

The relationships between a Site’s CSIRT, Security Contact and system administrators need to be clarified. The role and responsibility of each party must be clearly defined, at least in the context of the Security Service.

Learning material

Only skeleton recipes were available to help the sysAdmins of the target Sites through the information gathering process. The availability more guidance, perhaps in the form of a selftraining kit would help give the confidence needed.

Extraction of information

The three recipes illustrate the complexity of analyzing the available log files. There are at least two operational issues in this context:

- The amount of time required for the extraction process;
- The quality assurance of the information extraction process.

We recommend that these issues are taken into account when logging and accounting of Grid information is reviewed in the future.

Confidentiality of information

The confidentiality level which protects personal information stored in the Grid accounting systems must emanate from an approved policy definition. Confidentiality is a component of the approved Acceptable User Policy (AUP) documents. However, in view of the global nature of the Grid with the multiple national legislations involved, we recommend that the Joint Security Policy Group (JSPG) considers a specific policy agreement addressing the issue of confidentiality of personal information.

Software

The software for future SSC will be designed to work in a production environment. It will assume that TOP, when working with the User Interface (UI) of the SSC, has a fully authenticated and valid Grid environment already set up. The software will have the capability to select the target Site and to execute a challenge, and TOP will no longer have to wait for the completion of each submission before the next is submitted.