Security Service Challenges

Edited by Pål S. Anderssen

OSCT-5, Lyon, 2008-03-18

Information Society and Media

SSC recap.

- **SSC level 1**
  - Challenged the Workload Management System (WMS) on the Resource Broker (RB) and the Compute Elements (CE);
  - Did not address the Security Incident Response Procedure;
  - Used Savannah as the vehicle for communication between the Test Operator (TOP) and the Target sites;
  - The Regional Operation Centres (ROC) challenged the Sites within their ROC;
  - Completed in 2006.

SSC recap.

- **SSC level 2**
  - Challenged the Storage Elements (SE);
  - Did not address the Security Incident Response Procedure;
  - Used the Global Grid User Support (GGUS) as the vehicle for communication between the Test Operator and the Target Sites;
  - The Regional Operation Centres (ROC) challenged the Sites within their ROC;
  - Completed in 2007.

SSC_3 the next step

- **SSC level 3, Outline**
  - Will challenge the Diligence of Security Operation at the Sites;
  - Crafted on the approved model for Grid Security Incident Response;
  - Security at the challenged Site is alerted about suspicious activity emanating from an identified user;
    - Note: The alert is clearly identified as a test.
  - Security operation is asked to follow normal incident response procedures and to report, albeit to a limited audience.

SSC_3 the Job and the Alert

- The Job is launched from a User Interface (UI);
  - It runs with valid credentials;
  - It is assigned to a Worker Node (WN) by the normal WN management system;
  - Once running, it will exploit its environment to conceal its activities;
  - Sign of life will be reported through an out-of-band channel.
- The Alert is sent to the CSIRT e-mail address registered in the Grid Operations Centre Data Base (GOCDB);
  - The text clearly identifies the alert as a test;
  - The Grid identity of the submitting user is indicated;
  - The Site is asked to deal with the Alert following approved Incident Response Procedures;
  - However, an alternative e-mail address is indicated to replace the normal multi-destination addresses.

SSC_3 the Response

- **The Incident Response is broken up in three activities:**
  - Communication
    - Acknowledgement/Heads-up report to the indicated e-mail address;
    - Alert to the VO manager;
    - Verification that the responsible Certification authority has been notified;
    - Filing of the final report.
  - Containment
    - Identification of the Job and killing of its processes;
    - Suspension of the offending user at the challenged Site.
  - Forensics
    - Discovery of emitting Site and contact to the Site's CSIRT;
    - Analysis of network traffic;
    - Analysis of the submitted binaries.

SSC_3 the Evaluation

- **The challenged Site's response will be evaluated by OSCT**
  - For the completeness and timeliness in terms of:
    - Filing and distribution of the reports;
    - Alerting of the cooperating bodies.
  - For the demonstrated technical abilities:
    - To disentangle the Job;
    - To execute managerial tasks on Grid elements;
    - To preserve and analyze the evidence.

SSC_3 target deadlines(1)

- **Communication**
  - Acknowledge/Heads-up report to “CSIRT” list: – 4 hours
  - Alert to the VO Manager: – 24 hours
  - Verification of notification of responsible CA: – 144 hours
  - Final report to “CSIRT” list: – 144 hours

SSC_3 target deadlines (2)

- **Containment**
  - Finding Jobs and killing them:
    - 4 hours
  - Suspending the user at the Site:
    - 4 hours

SSC_3 target deadlines(3)

- **Forensics**
  - Discovery of the submitting UI and contact with that Site's CSIRT:
    -
    - 24 hours
  - Analysis of network traffic:
    - 48 hours
  - Analysis of the submitted binaries:
    - 48 hours

SSC_3 evaluation

- **Your comments are welcome -**
  - With respect to the execution of the challenge;
  - To the relevance of the individual items;
  - To the target deadline.
- **But perhaps we should first review the results from the eight Sites that have participated in the pilot test -**