

## Handling Security Incidents

EGEE'08 Conference  
23 September 2008  
Harbiye Askeri Museum, Istanbul

Carlos Fuentes <carlos.fuentes@rediris.es>  
IRIS-CERT, RedIRIS  
SWE Security Officer

www.eu-egee.org

---

---

---

---

---

---

---

---

## Contents

- Review EGEE Procedures and Recommendations
- Handling a Security Incident

2

---

---

---

---

---

---

---

---

## Procedures & Recommendations

What should we have in our institution?

- **Security Policy**
  - Define what is require/allowed/acceptable
  - Define responsibilities and authorities
- **Security Plan**
  - What is provided, who receives it and who provides it
- **Incident Response Policy/Plan**
  - Documented steps to keep control of incident
  - What will respond to and when. How will we respond
  - RFC 2350 – format part of Incident Response Plan
- **These must link together**

3

---

---

---

---

---


---

---

---

**EGEE** Enabling Grids for E-science **Procedures and Recommendations**

- **Aims: ensure consistency, reduce stress**
  - Mid-incident is a bad time to make decisions!
    - Much easier to read a document you wrote earlier



4

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Procedures & Recommendations**

- **Aims: ensure consistency, reduce stress**
  - Make as many decisions as possible beforehand
    - Incidents differ in details; often same stages apply



5

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Procedures & Recommendations**

- **Aims: ensure consistency, reduce stress**
  - Be sure your team has read the IH procedure
    - Don't disturb me when I am on the beach, please read the doc!!!



6

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Procedures & Recommendations**

- If possible try out plans as exercises
  - Modify procedures as you learn from experience
  - Security Service Challenge
    - <https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge>

Procedures and policies are alive, keep them going/reading on

<https://edms.cern.ch/document/867454>

7

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Incident response policy**

- Grid participants are bound to (at least) two different incident response policies:
  - Local incident response policy
  - “LCG/EGEE Incident Handling and Response Guide” (JSPG) Base on the Open Science Grid, Approved by WLCG Management Board on 28th November 2005:
    - [http://cern.ch/proj-lcg-security-docs/LCG\\_Incident\\_Response.asp](http://cern.ch/proj-lcg-security-docs/LCG_Incident_Response.asp)
  - May apply the NREN security policy (are you directly connected to the NREN?) or your institution security policy

8

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Incident Handling**

- What is a computer incident?
  - Adverse event in information system infrastructure
  - Threat of the occurrence of adverse event
  - A security incident is the act of violating an explicit or implied security policy (ex: your local security policy, EGEE Acceptable Use Policy - <https://edms.cern.ch/document/428036/3>).
- What is an event?
  - Any observable occurrence in a system or network
  - Sometimes indicates an incident is occurring

9

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Incident Handling**

- **What is Incident Management?**
  - Process of managing the lifecycle of an incident

10

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Incident Handling**

- **Aims of Incident Management:**
  - Restore normal service as quickly as possible
  - Minimize adverse impact on business
  - Ensure no incident goes undetected
  - Ensure incidents are handled with consistent processess
  - Reduce number of incidents in time
  - Build working relationships across organization with open communication

11

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Incident response procedure for grid hosts**

- This procedure is provided for guidance only and is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between the sites. It is based on the EGEE Incident Response policy (available at [https://edms.cern.ch/file/428035/LAST\\_RELEASED/Incident\\_response\\_Guide.pdf](https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_response_Guide.pdf)) and is intended for Grid site security contacts and site administrators.

12

---

---

---

---

---

---

---

---



**EGEE** Enabling Grids for E-science

### Handling an incident

- **NREN notifies your local security team**

```
Sep 16 12:50:13 avancia/avancia sshd[8104]: Failed password for root from 89.121.12.178 port 55652 ssh2
Sep 16 12:50:16 avancia/avancia sshd[8104]: Failed password for root from 89.121.12.178 port 55743 ssh2
Sep 16 12:50:18 avancia/avancia sshd[8213]: Failed password for root from 89.121.12.178 port 55767 ssh2
Sep 16 12:50:22 avancia/avancia sshd[8281]: Failed password for root from 89.121.12.178 port 55815 ssh2
Sep 16 12:50:20 avancia/avancia sshd[8286]: Failed password for root from 89.121.12.178 port 55791 ssh2
Sep 16 12:50:26 avancia/avancia sshd[8291]: Failed password for root from 89.121.12.178 port 55855 ssh2
Sep 16 12:50:24 avancia/avancia sshd[8277]: Failed password for root from 89.121.12.178 port 55837 ssh2
Sep 16 12:50:31 avancia/avancia sshd[8389]: Failed password for root from 89.121.12.178 port 55914 ssh2
Sep 16 12:50:29 avancia/avancia sshd[8370]: Failed password for root from 89.121.12.178 port 55894 ssh2
Sep 16 12:50:34 avancia/avancia sshd[8429]: Failed password for root from 89.121.12.178 port 55951 ssh2
Sep 16 12:50:33 avancia/avancia sshd[8415]: Failed password for root from 89.121.12.178 port 55932 ssh2
Sep 16 12:50:36 avancia/avancia sshd[8444]: Failed password for root from 89.121.12.178 port 55970 ssh2
Sep 16 12:50:38 avancia/avancia sshd[8457]: Failed password for root from 89.121.12.178 port 55988 ssh2
Sep 16 12:50:40 avancia/avancia sshd[8479]: Failed password for root from 89.121.12.178 port 56007 ssh2
Sep 16 12:50:41 avancia/avancia sshd[8489]: Failed password for root from 89.121.12.178 port 56025 ssh2
Sep 16 12:50:46 avancia/avancia sshd[8554]: Failed password for root from 89.121.12.178 port 56060 ssh2
Sep 16 12:50:49 avancia/avancia sshd[8599]: Failed password for root from 89.121.12.178 port 56097 ssh2
Sep 16 12:50:44 avancia/avancia sshd[8510]: Failed password for root from 89.121.12.178 port 56043 ssh2
Sep 16 12:50:53 avancia/avancia sshd[8637]: Failed password for root from 89.121.12.178 port 56134 ssh2
Sep 16 12:50:48 avancia/avancia sshd[8582]: Failed password for root from 89.121.12.178 port 56079 ssh2
Sep 16 12:50:55 avancia/avancia sshd[8652]: Failed password for root from 89.121.12.178 port 56152 ssh2
Sep 16 12:50:51 avancia/avancia sshd[8616]: Failed password for root from 89.121.12.178 port 56116 ssh2
Sep 16 12:51:00 avancia/avancia sshd[8703]: Failed password for root from 89.121.12.178 port 56989 ssh2
Sep 16 12:50:57 avancia/avancia sshd[8674]: Failed password for root from 89.121.12.178 port 56171 ssh2
```

16

---

---

---

---

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science

### Handling an incident

- **OSCT notifies a local security team**

```
It was reported that any activity by
/DN=ch/DC=cern/OU=OrganicUnits/OU=Users/CN=mgrnygiel/CN=462927/CN=Monique
Grygiel
should be considered malicious.
RAL has so far found one job currently running under this DN.
We are still investigating the activity of the offending job but have so far taken the
following action:
1)The job is SIGSTOP'd
2) Access by the user has been blocked at our CE, dcache SE and FTS.
We are still working on CASTOR and the RB. More details will follow as we get
them. Regards Andrew
```

17

---

---

---

---

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science

### Handling an incident

**Time 1s**

- **What to do now?**
  - Don't get stressed & Calm down
  - Take your security plan, it's time to use it
  - Inform your local security team and your ROC Security Contact
    - No needed a long mail with too deep explanations
    - Just tell them what it's going on
      - Logs/information/evidences you did gather/receive
      - Actions you did take before sending the message
      - Very important the timing

18

---

---

---

---

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Handling an incident**

**Time 2s**

- **Take some actions**
  - Ask for help if you need to your local security team or your ROC security contact
  - Review carefully the complaint
    - Reject a false positive
    - To know the malicious activity
    - To get the timing
    - Users probably compromised
  - Assist your local security team and your ROC Security Contact to confirm and then announce the incident to all the sites via [project-egee-security-csirts@cern.ch](mailto:project-egee-security-csirts@cern.ch).
  - Alert to the VO Manager
  - Notify the responsible CA

19

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Handling an incident**

**Time 3s**

- Contain the problem
  - Isolate the machine from the network
  - NEVER SWITCH OFF or RESET the host
  - If appropriate:
    - *Report a downtime for the affected hosts on the GOCDB*
    - *Send an EGEE broadcast announcing the downtime for the affected hosts*
    - *Use "Security operations in progress" as the reason with no additional detail both for the broadcast and the GOCDB.*
  - Finding malicious Jobs and killing them
  - Suspending the user at the Site

20

---

---

---

---

---

---

---

---

**EGEE** Enabling Grids for E-science **Handling an incident**

**Time 4s**

- **Perform appropriate forensics and take necessary corrective actions**
  - If needed, seek for help from your local security team or from your ROC Security Contact or from [project-security-support@cern.ch](mailto:project-security-support@cern.ch)
  - Analysis of network traffic
  - Analysis of the submitted binaries
  - If relevant, send additional reports containing suspicious patterns, files or evidence that may be of use to other Grid participants to [project-egee-security-contacts@cern.ch](mailto:project-egee-security-contacts@cern.ch). NEVER send potentially sensitive information (hosts, IP addresses, usernames) without clearance from your local security team and/or your ROC Security Contact.

21

---

---

---

---

---

---

---

---

**egee** Enabling Grids for E-scienceE

Time 5s

- Restore the service
- Send an EGEE broadcast, if needed
- Update the GOCDB
- Service documentation and procedures to prevent recurrence as necessary.

23

---

---

---

---

---

---

---

---

**egee** Enabling Grids for E-scienceE

### Handling an incident

- Lesson learned
- The warning came through the appropriated channels
  - Do you keep updated your contact information?
  - Was your procedure enough accurate for giving a quick and good answer?
  - Were your actions enough for containing the problem?
- Coordinate with your local security team and your ROC Security Contact to send an incident closure report within 1 month following the incident, to all the sites via [project-egee-security-contacts@cern.ch](mailto:project-egee-security-contacts@cern.ch), including lessons learnt and resolution.

23

---

---

---

---

---

---

---

---

**egee** Enabling Grids for E-scienceE



[www.eu-egee.org](http://www.eu-egee.org)



---

---

---

---

---

---

---

---