

# Security Services Challenge @ Uni Bonn

Detlef Bartsch, Robert Zimmerman  
University of Bonn

- The Grid cluster in Bonn
- Procedure during SSC
- Remarks



GridKa school 2009  
04.09.2009

# My personal status in the Grid Bonn

During the SSC I was working for the Grid since one week.

→ I did not know anything! (and still don't know much)

The real work was done by Robert Zimmermann;

My role was and still is to learn from him.

# The Grid-cluster in Bonn

We have a very small grid cluster running in Bonn:

- 12(6) worker nodes
- storage element using dcache (configuration from DESY)
- using gLite 3.1

... nothing special ...

Network supported by computing center  
→ we do not have access to network logs

What did we do in the SSC?

Follow the rules!

# What we did in the SSC

Most important input for our procedure:

- the EGEE incident response procedure

[https://edms.cern.ch/file/867454/2/EGEE\\_Incident\\_Response\\_Procedure.pdf](https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf)

- useful to know what to do
- many links given in these instructions
- mail templates are good guides to know what should be reported

- the SSC evaluation form

<https://twiki.cern.ch/twiki/bin/view/LCG/NorthernEurope>

- useful to build a priority list according to the response times

# What we did in the SSC: first steps

Highest priority: stop activity of the user:

- banned user in `/opt/glite/etc/lcas/ban_users.db`
- identified local user name in log file
- search for jobs: `qselect -u dteam016`
- froze job: `qsig -s STOP 18746.batch.grid.physik.uni-bonn.de`
- checked it: `qstat -n 18746.batch.grid.physik.uni-bonn.de`
- excluded wn: `pbsnodes -o wn008.grid.physik.uni-bonn.de`
- check for 'future' jobs: `crontab -l -u dteam016; atq`
- check network connections: `netstat -anp`
- unplug network cable

Our main fault in these steps:

- We stopped only the main process tree, ignoring the job running in a separate process tree. The latter one was stopped several hours later. So, search for all processes (including hidden ones).
- For convenience reasons we kept the network connection of the worker node up for the first 7 hours. Afterwards we disconnected the node.

# What we did in the SSC: other activities

- **rootkits:** `chkrootkit`; `rkhunter --update`; `rkhunter --check --nomow`
- If attacker used scripts, find out what they try to do and see if they were successful.
- Try running attacker's binaries on an isolated machine and see what they do.  
E.g. use a system without disk and network and a live CD/DVD and run binaries with `strace` or in `gdb` and make directory snapshots before (`find <dir> -ls > before.log`) and after, etc...
- see if attacker tried to exploit known vulnerabilities  
<http://cve.mitre.org/>
- implement lessons learned at local site

# What we did in the SSC: data preservation

Try so save all information which might be useful for forensics:

- save list of running jobs: `ps auxf > ps_logfile`
- save list of open files: `lsof -u <USERNAME> > lsof_logfile`
- save core dump: `gcore`
- save image of WN
- save log files of WN, CE and batch system

special feature in Bonn:

WN and CE run with different local time.

Important to know for comparing the log files!

- :

Always a good idea:

Write private log about your activities, including all relevant information.

# What we did in the SSC: communication

Keep the rest of the grid community informed.

Send mails according to the EGEE incident response procedure.

Keep ROC Security Contact and EGEE CSIRT list informed about the status of the incident and the investigation:

- Send mails according to the EGEE incident response procedure.
- Keep ROC Security Contact and EGEE CSIRT list informed about the status.

# My big question

How does the whole procedure start  
if we do not get an email from Ursula Epting, telling

This e-mail is an alert about a TEST incident...

?

# Remarks about the SSC

- I learned a lot about our Grid cluster.
- The SSC helped to build a strategy of how to proceed in such accidents.
- In a real attack we will be able to react faster and more goal oriented than before the challenge.
- The challenge was very time consuming (main task for 3 working days for one person plus one investigator).
- The checklist for the SSC rating is
  - a good guide what to do in which order (due to the target times)
  - might limit the view to only what is written in this checklist
  - triggers to delay actions up to the target time
- Some confusion about the procedure of the SSC itself:  
Which mails should have been sent to their 'original' destination, which to the 'multi destination SSC mail address'?
- The draft for final reports is a helpful tool, giving a guideline for what to report about.