Security Best Practices

Anand Padmanabhan

Jim Basney

Open Science Grid

What to expect?

- A hands-on session
- You will learn
  - How to respond to a security incident
  - How to ban a user DN from your site
  - How to track down jobs submitted by a DN
  - How to locate relevant log files
  - Basic forensics steps for incident response
- Open discussion on security best practices used by the sites

Open Science Grid

Scenario Overview

- OSG Security Team contacts you about a “bad DN”
- We're submitting jobs using the “bad DN”
- In a real incident
  - Contact security@opensciencegrid.org and local security response
  - Security team will send you a signed email indicating the action to be taken
  - Take actions identified in the email ASAP

Open Science Grid

Have you signed up?

- Provide gatekeeper/jobmanager contact you want us to send jobs to
- DN used:
  - "/DC=org/DC=doegrids/OU=People/CN=James Alan Basney 710056"
- Make sure MIS VO (and this DN) are accepted on your site

Open Science Grid

We submit jobs now!

Open Science Grid

Four Major Steps

- Stop further exposure
- Find out if your site was exposed and to what extent
- Conduct basic forensics
- Clean up suspect jobs

Open Science Grid

How to stop further exposure of your site?

Open Science Grid

Ban the “bad user DN”

How?

Open Science Grid

Does your site use GUMS?

- Go to the GUMS interface
  - https://gums-host:8443/gums/
- Add new manual group called banned
  - Configuration -> User Groups -> Add
  - Select type = manual and provide name, description. Then save
- Add this group to a “banned user group”
  - Click on Configuration
  - Select the group from drop down menu and save

Open Science Grid

Does your site use GUMS?

- Add user DN to the banned group
  - Click on “Manual User Group Members” in “User Management” section
  - Click Add, select the appropriate “user group”
  - Add the user DN and save
- Test the mapping from your CE
  - %gums-host mapUser "DN" (as su)
  - Only if the mapping returns null, the user is banned

Open Science Grid

Does your site use edg-mkgridmap?

- Update the edg/etc/edg-mkgridmap.conf
  - Add a line 'deny “DN”'
  - Wild cards are also accepted
  - Regenerate grid-mapfile executing edg/sbin/edg-mkgridmap
  - Log file can be generally found at edg/log/edg-mkgridmap.log
- Check your grid-mapfile and confirm that the DN has indeed been removed

Open Science Grid

Best Practices

- Keep CAs and CRLs upto date
  - Ensure that tools like vdt-update-certs and fetch-CRL have been enabled
- Keep the VO list updated
  - Check if GUMS is contacting the VOMS server periodically and gums-host-cron service from VDT is enabled on CE
  - If using end-mkgridmap ensure that the edg-mkgridmap service is enabled in VDT
- Watch the logs

Open Science Grid

What ifs?

- I am running GUMS 1.2.x which does not support banning user DN? What should I do?
  - Ensure your site should follow the best practices.
  - If critical security problem has been reported, you may choose to ban all the VOs the DN is a member of for a short period till the VO membership/CRL has been updated
  - Disable the unix account the user is getting mapped to

Open Science Grid

What have we accomplished?

- User will not be able to submit new jobs (or get authorized in the future) to your site.
- Existing jobs will continue to run.

How to find out if your site was exposed?

Look at log files!

What logs did you look at?

- Examples
  - Globus gatekeeper and accounting logs
  - GUMS log can provide a centralized place to check multiple gatekeepers
  - Check syslogs
- Location of some log files can be found at
  - https://twiki.grid.iu.edu/bin/view/Integration/ITB092/ComputeElementLogFiles
- What did you find?

Open Science Grid

- Has the “bad DN” run on your site?
- What IP address did the job originate from?
- When (timestamps)?
- What unix account did the user map to?
- Did the mapping use a pool account or were all users from VO mapped to the same account?

Open Science Grid

What to do next?

- If the site had no record of the activity from the user, then Hurray!! No exposure and you are done!
  - Please make sure that none of your grid resources were exposed
- If you see activity related to that DN, more action is needed

Perform Forensics

What processes are running for this user? and Where?

Open Science Grid

Inspect batch system

- Where did the job run?
  - Fork jobmanager or batch system
  - If batch system, which node
  - For Condor
    - % condor_q -l job_id
    - % condor_q –l userid
  - For PBS
    - % qstat -f job_identifier
  - Review your batch system logs

Open Science Grid

Locate user processes

- What processes are running for that user?
  - % ps -u mis -U mis uwww
  - Locate processes on both CE and WN
  - Other suggestions?

Open Science Grid

Does the job have any open files or ports?

- Use lsof and/or netstat
  - % lsof -u mis -P
  - % netstat -ap
- Did you find them?
  - An open hidden file (in /tmp)
  - An open TCP connection
- Any other tools you recommend?

What does the job do?

Open Science Grid

Review the user scripts

- The earlier ps should reveal the user scripts
- Did you see we were sending out data to a remote gsiftp server periodically?

Open Science Grid

What ifs?

- The executables were binary files?
  - Use strings command
    - Look for hostnames, email addresses, usernames, passwords, and other clues

Open Science Grid

Clean up

Lets kill the suspicious jobs!

Open Science Grid

What should we kill?

- Remove job from batch system
  - Condor: % condor_rm cluster_id
  - PBS: % qdel job_id
- Kill any lingering processes associated with the suspicious user
  - % kill -9 process_id
  - % killall process_name
- Make sure all the suspicious user processes have been terminated

Open Science Grid

What ifs?

- All DNs from the VO are getting mapped to the same user DN.
  - Killing all the user process on the CE
    - Kills Condor-G grid-manager and Globus jobmanager processes of other users in the VO
    - VO should be able to recover from these failures
  - Selective killing of jobs associated with user DN
    - Possible by looking at logfiles, process timestamps
    - Will be tedious
    - Decision at the discretion of the sites
    - VOs will appreciate it

Open Science Grid

What ifs?

- User process is aggressively forking?
  - After killing suspicious processes, check for new processes using ps
  - Node shutdown/reboot may be required
  - Beware of lingering effects (example: cron)

Open Science Grid

Any escalations?

- Investigate the incident (in case of a real incident)
  - Follow your home organization's security procedures and policies
  - Determine if there were any compromises arising from the incident
- If you suspect that any other user accounts, certificates, proxies have been compromised due to this incident immediately notify security@opensciencegrid.org

Open Science Grid

Any escalations?

- Any other policies/procedures for sites to follow?

We will check if we are still getting pings (data files) from our jobs!

Open Science Grid

Let us un-ban “bad DN” used for this session!

Additional Slides

Open Science Grid

Best Practices

- https://twiki.grid.iu.edu/bin/view/Security/BestPractices