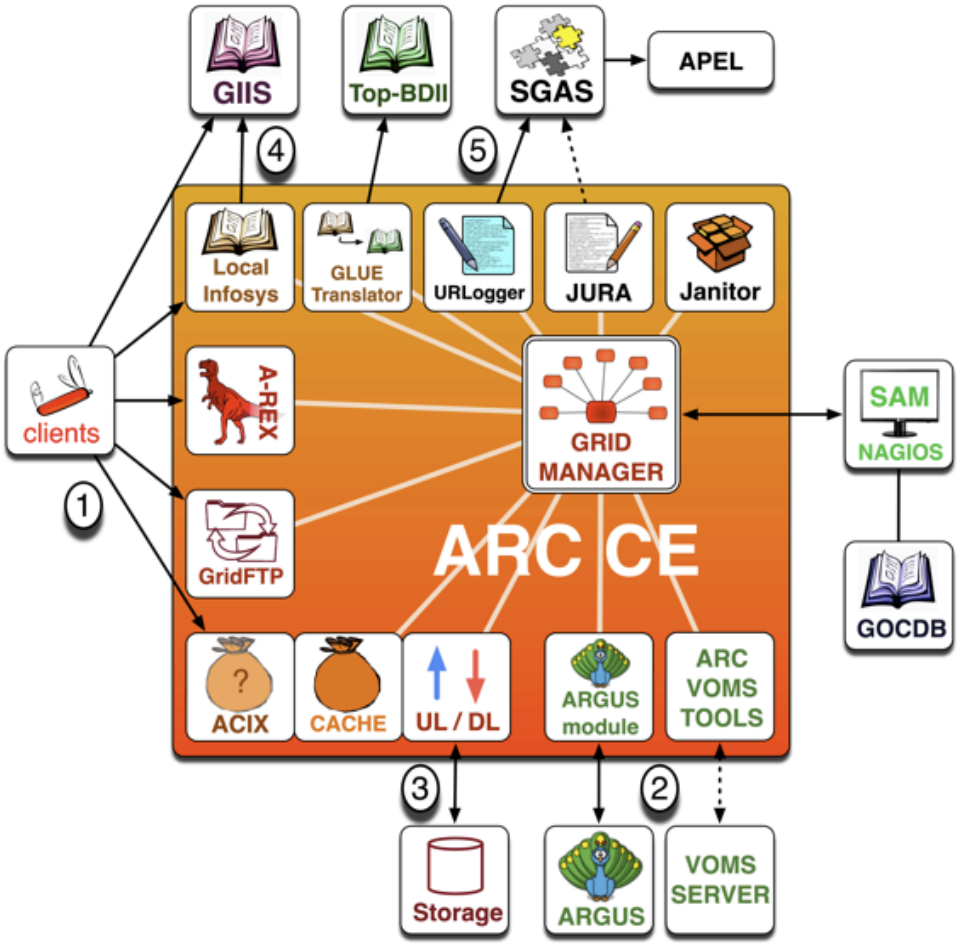
Security recommendations ARC CE

Andrej Filipčič
Jozef Stefan Institute
Ljubljana, Slovenia

ARC CE architecture



Main services (arc0):
gridftpd
grid-infosys
grid-manager

Service roles

- Gridftpd: clients use it to
  - Submit jobs
  - Retrieve output files
- Grid-infosys:
  - Resource Information index
  - Publishing to higher level indices
- Grid-manager:
  - Transferring input/output files
  - Job processing, batch submission
- Documentation:
  - http://www.nordugrid.org/papers.html

Services

- Single configuration file /etc/arc.conf
- All the 3 services started by init:
  - /etc/init.d/gridftpd
  - /etc/init.d/grid-infosys
  - /etc/init.d/grid-manager
- Standard distribution rules (chkconfig, …) to control the services

gridftpd

- Port 2811 (+ ftp transfer ports)
- Critical service: the single entry point to access the ARC CE
- Single (threaded) process, forked process per active session

```
# ps ax|grep gridftpd
23250 ?        Ss     2:57 /usr/sbin/gridftpd -c /etc/arc.conf -P /var/run/gridftpd.pid
```

- Logfile: /var/log/gridftpd.log (important lines)

```
Sep 16 13:38:12 [11957] Accepted connection from 194.249.156.100:54091
Sep 16 13:38:12 [11957] response: 220 Server ready\\
Sep 16 13:38:12 [11957] User subject: /C=SI/O=SiGNET/O=IJS/OU=F9/CN=Andrej Filipcic
Sep 16 13:38:12 Initially mapped to local user: griduser02
Sep 16 13:38:12 Remapped to local user: atlas001
Sep 16 13:38:12 Remapped to local id: 11001
Sep 16 13:38:12 Remapped to local group id: 11000
Sep 16 13:38:12 Accepting submission of new job: 119571284637092100853055 4
```

grid-infosys

- Port 2315 (+ 2170 if glue12 enabled)
- Several processes:
  - Arc-infoindex-server
  - slapd (local ports 2136, 2137 for bdii)
  - grid-info-soft-register
  - Periodic collection processes
- Logfiles:
  - /var/log/inforegistration.log
  - /var/log/infoprovider.log
  - /var/log/bdii4/*
- Not critical from security point of view, but providing information to outside world
- Ldap dump might provide additional information:

  # ldapsearch -x –h cluster.domain -p 2135 -b 'mds-vo-name=local,o=grid'
  for example: DN authorized to particular queue
  dn: nordugrid-authuser-name=Dejan Lesjak...373,nordugrid-info-group-name=users
  ,nordugrid-queue-name=gridlong,nordugrid-cluster-name=pikolit.ijs.si,Mds-Vo-name=local,o=Grid

Grid-manager

- Not listening on any port
- Logfiles:
  - /var/log/grid-manager.log (job state logs)
  - /var/log/gm-jobs.log (accounting records)
    - 16-09-2010 13:15:52 Finished - job id: 830212846378681244436156, unix user: 11001:11000, name: "ANA_3ac48d41-8928-415b-a7e3-978c5428dfa5",owner: "/C=SI/O=SiGNET/O=IJS/OU=F9/CN=Andrej Filipcic", lrms: pbs, queue: gridlong, lrmsid: 3697141.brenta.ijs.si
    - 16-09-2010 13:15:54 Started - job id: 223471284638273471059749, unix user 11001:11000, name: "ANA_3ac48d41-8928-415b-a7e3-978c5428dfa5", owner: "/C=SI/O=SiGNET/O=IJS/OU=F9/CN=Andrej Filipcic", lrms: pbs, queue: gridlong
  - Useful to look for previous attempts
- Transfer control (uploader, downloader):
  - 26717 ? Sl 0:14 /usr/libexec/nordugrid-arc/downloader -U 11001 -f -n 2 -c -i 300 -r srm://srm.ndgf.org|.si$|.se$ 246091284638356207624726 2 /var/spool/nordugrid/jobstatus /net/pikolit/d0/nfs/grid/sessions/246091284638356207624726 2

Job control

- /var/spool/nordugrid/jobstatus/
  - Several files per job: job.<jobid>.*
    - job.<jobid>.description: job in xrsl
    - job.<jobid>.errors: input preparation, batch submission, output transfer logs, for example:
- Grid-manager uses those files to process the jobs and move them through steps (ACCEPTED, PREPARING, INLRMS:R, FINISHED…)

/etc/arc.conf

```
# authorization groups
[group]
name="atlas-users”
voms="atlas * NULL *”

# sources for initial access, used for grid-mapfile creation
[vo]
id="vo_atlas-user"
vo="atlas-user”
source="vomss://voms.cern.ch:8443/voms/atlas”
mapped_unixid="griduser03”

# (re)mapping rules
[gridftpd]
# several mechanisms for mapping, one possibility
unixmap="atlassgm001 group atlas-lcgadmin"
unixgroup="atlas-users simplepool /var/spool/nordugrid/map/atlas-users”

# job workdir in sessiondir/<jobid>
[grid-manager]
sessiondir="/net/pikolit/d0/nfs/grid/sessions”
# local scratch dir on nodes, if used, workdir in scratchdir/<jobid>
scratchdir="/data0/grid"
```

Actions

- Stop gridftpd service
  - Grid-infosys + grid-manager not critical, but better to stop to disable grid job processing
- Identify the batch job from job.<jobid>.local file
- Kill or freeze the batch job, isolate or disable WN
  - Depending on type of attack, for unknown a deeper inspection of job activity needed
- Inspect logfiles for the relevant information

Dig the info

- /var/log/gridftpd.log:
  - Access host
  - Jobid
  - Timestamps of access
  - DN, mapped UID
- /var/spool/nordugrid/jobstatus/job.<jobid>.errors
  - Inspect input, output transfers
- sessiondir/jobid on CE, scratchdir/jobid on WN
  - Inspect job scripts, process activity on node
  - Generic procedure (ps, lsof, strace,…)

Banning

- Ban the DN:

  [gridftpd]

  #before any other mapping rule

  -subject=DN

  Followed by gridftpd restart

- Detailed description on
  - http://www.nordugrid.org/documents/Config_Auth.pdf
- Regenerate grid-mapfiles to update synchronize with VOMS servers
  - /etc/cron.d/nordugridmap.cron

Summary

- All the grid related information contained in few log and job files
- The exact procedure in case of an incident yet to be provided for ARC CE