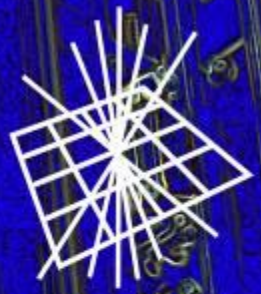

GridPP

UK Computing for Particle Physics

Security: Review and Plans

Ian Neilson STFC - RAL

Overview

- Review
  - Recent activity: CSIRT, SVG, SPG, EUGridPMA …..
- Plans
  - Communications Challenges
  - Certificate Banning Tests

Security Activity

- EGI CSIRT
  - 2 incidents
    - Compromised EGI FedCloud virtual machine - CESNET [EGI-20150514]
      - Weak root pw
    - Elasticsearch – Glasgow/Edinburgh [EGI-20150611-01]
      - Exploited through open firewall / lack of updates
  - 1 critical vuln - CVE-2015-3245 libuser
    - Vulnerability tickets
      - July 10 new cases 10 cases closed
      - August 95 new cases 85 cases closed
- Intention to run SSC against all FedCloud sites
  - Verification CSIRT (?if any) capability
  - Training for endorsers and operators

Security activity cont.

- SVG (from Linda Cornwall)
  - "Critical"
    - CVE-2015-1815 Setroubleshoot (Mar 2015)
    - CVE-2015-3456 VENOM (May 2015)
    - CVE-2015-3245, CVE-2015-3246 RedHat libuser (July 2015)
  - ~25 other reports including VM/cloud enabling
  - New vuln. handling procedure (see OMB slides) :
    - https://indico.egi.eu/indico/conferenceDisplay.py?confId=2378
- SPG (from Dave Kelsey)
  - Refreshing policy set
    - AUP, VM Endorsement, Long Tail of Science, Data Protection
  - Security for Collaborating Infrastructures (SCI)
    - joint meeting with GEANT SIG on Information Security Management in October 2015, working with PRACE and EUDAT
  - Security Incident Response Trust Framework for Federated Identity (SIRTFI)
    - defining best practice and trust mark of Federated Identity Providers (with AARC and REFEDS).

Security Activity

- EUGridPMA / IGTF
  - Business as usual –
    - auditing existing, reviewing candidate CAs (e.g Kenya)
    - CERN WebFTS service, hidden, “on-the-fly” certs using CERN SSO/EduGain + VO membership db for identity
  - Diversity of Credential Issuers & Identity Providers
    - How do Relying Parties decide to trust?
    - Level of Assurance generalisation
    - Separating Level of Assurance from (PKI) Technical Implementation
    - http://wiki.eugridpma.org/Main/IGTFLoAGeneralisation

SSC6 2013

- UK run of SSC6 (used for some CMS sites last summer [2012])
- Tested 11 UK sites
- Uses SSC framework developed by EGI Security Drills Group
  - Aram, Oscar, Sven, Carlos
- Attempt to make realistic within constraints
  - Payload Pinky_packed.sh, does “stuff” but …
  - No exploit dropped, single job/site, no external attack/dos
- Test for communication as well as technical response
  - EGI Incident Response Procedure
  - Measured times: Ack., “Malware” connection, DN ban, Report

SSC6 Report Conclusions

- **Common Issues and Recommendations (from John Green)**

  "Wide range in responses and approaches, key defensive actions were taken on all sites"

  - Security contact information and acknowledgement

    "A number of sites included their University CERT team … valuable at smaller sites … recommended as standard practice at all GridPP sites."

  - Banning

    "A considerable number of sites were unsuccessful at banning … on their first attempt ... Once fully deployed Argus is intended to provide ……"

  - Forensic first responder training

    "… Some sites were able to recover deleted files … no sites demonstrated the use of more technical forensic tools …"

  - Network monitoring

    "No sites demonstrated any network monitoring from their sites. … "

UK NGI Security

- Security contact information and acknowledgement
  - Communications “challenges”
  - Send a ticket then wait for ack. – can use EGI ticketing
  - Issues?
    - Want to really test CSIRT address but without raising alarms
    - How often?
      - Once or twice a year, repeated ……
      - ~15 sites -> ~30 challenges (automate it!)
      - Then make it more interesting.
- Banning
  - Ewan’s 2014/15 banning tests
    - Sites: 6 OK + 6 Some + 6 NOK
  - Repeat
    - Monitoring central Argus
    - Supplement with local banning tests

Security Plans

- Forensic first responder training
  - Hepsysman training days
  - Make use of EGI training and SSC activities
  - Image and VM forensics
- Network monitoring
  - Survey (and share) existing (best) practice
  - Interest in “Security Operations Centre”
  - IPv6 security best practice
- Misc
  - GridPP5 - risk analysis
  - Always ….. documentation “freshness”

Security: Review and Plans

Of course something unplanned might happen …..

PILOT JOB TRACEABILITY

Pilot job traceability

- gLExec
  - use OS to enforce pilot/payload separation (or logging-only)
  - call-outs to check banning (Argus)
  - logging
- WLCG MB meeting May, 2013 + Sec. Technical WG

  "…decided that the deployment of gLExec shall be ramped up for all WLCG sites"
    - https://twiki.cern.ch/twiki/bin/view/LCG/GlexecDeploymentTracking
    - http://research.cs.wisc.edu/mist/glexec/vuln_reports/
- WLCG now –

  ".. production: that would be the next step, foreseen for this autumn."
- GridPP Dirac now ….. multi-VO pilot?
  - Adds potential for cross-VO access