OSG Security review & plans

Dave Dykstra

OSG Staff Retreat

May 10, 2016

YEAR IN REVIEW

OSG Security review
May 2015 – May 2016 Accomplishments

- Switched to Digicert SHA2 CA
- Transitioned from Digicert to CILogon OSG CA
- Implemented general mechanism for auto-managing per-user certs from CILogon Basic CA
- Produced security risk assessment for HEP Cloud Facility
- Kept in touch with WLCG Privacy effort
- Engaged with WLCG Traceability & Isolation Working Group

Detailed review of these activities are in the backup slides

Security operations - vulnerabilities

- The usual vulnerabilities in O.S. software
  - libuser, glibc, 2 on NSS libraries
- The OSG's Wordpress-based news website was hacked & spammed
- A Cross-Site-Scripting problem found & fixed in GUMS administrator web access
  - Notable as this is software OSG maintains.
- Two developer-found dCache security bugs
- Potential perfSONAR problem if misconfigured

Assessments, drills

- OSG Connect assessment/drill was done
- Risk assessment for OSG assets were completed
- An OASIS security drill found that blanking worked for opensciencegrid.org repo but not egi.eu repo
  - Another drill scheduled in 2 weeks

Conferences

- NSF Cybersecurity conference
  - Lack of support for some critical open source tools is scary, e.g. ntpd. Even gpg almost died.
- Cyber & Information Security Research conference
  - Wrote & presented paper on project with FNAL stakeholder on transparent user certificate management and its integration with grid job submission.

YEAR 5 PLANS

Plans for the coming year

- Transition to new OSG security team leadership
  - Help them get up to speed
  - Figure out how team effort will be composed.
  - Probably only do evolutionary projects, no major changes this year.
- Collaboration with FNAL stakeholder: “touch point” is HEPCloud security improvements and usability.

Year 5 staffing

	FTE
Mine Altunay	0.7
Jeny Teheran	0.8
Susan Sons	0.5
Anand Padmanabhan	0.5
Dave Dykstra	0.25
Total	2.75

Security drills

- Planning a new round of site security drills.
  - Submit a job and ask the site to find it, kill it, and block the user
- Should perhaps also do drills on VOs that don't separate their users.
- Basic question: Do seasoned site and VO admins know how to perform the basic tasks from our training?

Simplifying VO Operations

- Host more VOMS servers.
  - If all are managed centrally, then this is *no longer a product* but a *service*. Makes later retirement of VOMS more straightforward.
- Investigate mechanisms for having pilots manage "trust environment" (CAs / CRLs) on worker nodes.
  - Eliminates the current, incorrect need for *sites* to manage this environment.

Simplifying Site Management: Automating host cert renewals

- The requirements/procedures for renewing host certificates should be reviewed
- For example, BNL is moving toward a more automated process:
  - Automation is good, but is it secure enough?
  - There are administrators that approve the requests: but could they recognize a bogus request?
    - Could a compromised host request a cert for an uncompromised host?
- Would like to make sure our admins remain covered by our policies.

Simplifying User Experience: Auto-managing user certs

- Refine cigetcert.
  - cigetcert is the command-line tool developed in 2015 to generate certificate from an institutional user / pass login.
- Continue to shield users from certificates.
  - For VOs that still think they need certificates, try to understand if cigetcert helps.
- Probably need general mechanism for registering users in VOMS using federated identity
  - Some VOs could benefit from VOMS getting its information from another source such as Grouper like LIGO uses

CILogon Relationship

- CILogon relationship is going well.
- Interesting challenge: CILogon Basic CA (used by LIGO, FNAL to transform institution credentials – user/pass - to X509 credentials) is not accepted in Europe.
  - EGI is working on a technical solution to their concerns.
  - **Not** an OSG policy problem, but it affects OSG stakeholders.
- Proposal: modify definition of CILogon Silver CA (accepted in Europe) to include OSG-approved institutions.
  - Does not require changes at the institution, but audit / documentation at the VO. Policy and organization: not code.
  - Similar to the approach we took with traceability project.
  - CILogon team is on-board.

Traceability/isolation

- **Isolation**: VOs – and some sites - still desire stronger isolation (such as Unix user isolation) that existed with traditional glexec:
  - Now that WLCG is exploring options outside traditional glexec, opportune time to revisit this with them. Goals:
    - No worker node customization necessary.
    - Does not rely on GUMS.
    - No user certificate necessary.
- **Traceability**: There's relatively little protection for pilot logs on the worker node from alteration by the payload:
  - Would like to make progress here.

CVMFS master key storage

- The CVMFS master key should be stored in secured hardware module
  - CERN has done this since the beginning
  - Prevents key from being stolen if signing host is compromised
  - Equivalent of a Certifying Authority

QUESTIONS?

BACKUP SLIDES

Digicert SHA2 CA

- Certs had been SHA2 for a couple of years, but not the CA
- Main issue discovered was that VOMS by default was checking CA's DN in addition to user DN
  - Passed along to VOMS & VOMS-admin administrators an IGTF request to change configuration to not require this
  - Required backporting a patch for VOMS-admin
  - This change should also be useful in the future as CA DNs change

CILogon OSG CA transition

- Took a long time to get approved by IGTF
- Certs issued by CILogon, but user DNs mention only opensciencegrid so changing CAs in the future won't have to change DNs
- VOs were transitioned in groups over 6 months, biggest VOs first, the last group today
  - 5 VOs deprecated, 44 transitioned
- Some fairly significant startup glitches happened, but only very minor issues later
- Added tool support for Subject Alternative Names
- Late change: user certs weren't suitable for signing email, changing today

Auto-managing user certs

- The most powerful way to submit to the grid without users having to manage certificates is to generate and manage certs for them
  - Enables per-user access control on storage
- We wrote a general tool 'cigetcert' for doing this
  - Uses CILogon Basic CA and federated identity to generate certs weekly
  - Uses Enhanced Client or Proxy (ECP) profile, designed for command line
  - Authenticates to the Identity Provider (IdP) with local institution's own kerberos, or password
  - Stores unencrypted week-long proxy for user in /tmp, and stores longer proxy (4 weeks is plenty) in a MyProxy server
  - Job submission client invokes cigetcert for users, then server accepts authentication from short-term proxies and renews certs out of MyProxy to send to jobs
  - Going into production for first Intensity Frontier project next month

HEPCloud security assessment

- Securing cloud resources has some harder challenges than grid
  - Continuous active attacks in the wild
  - Credentials have to be carefully protected
- Some gaps were identified in the assessment
- HEPCloud is not directly an OSG concern yet, but probably its experience will be relevant to OSG in the future

WLCG Privacy

- WLCG wrote a Data Protection Policy
  - No changes are expected to grid software
  - It just documents what is done with private data (including user names), why it is kept, and for how long
  - Mostly it's about clarifying to users what personal data is kept

WLCG Traceability & Isolation WG

- WLCG froze deployment of glexec in February
- First meeting of working group on alternatives today – previously the WG focused on VMs
- glexec's isolation is most needed when user certificates are sent to pilots for payload jobs to have access controls on storage
- Container-based isolation not mature enough
- Brian & I shared the recommendations that Mine talked about at last year's staff retreat