# Area Coordinators

Mine Altunay

Security report

September 16, 2015

# Key Work Items

- OSG CA
  - IGTF review is going ok, but I am getting more nervous. Got the first review from Dave Kelsey. Mainly positive but lots of work. Already addressed all his comments and updated the CP/CPS.
  - The other reviewer, Irwin Gaines, did not send me any feedback. He truly understands our situation and wants to help us. But recent security hacks impacting DOE and government threw his schedule off. We cannot make the September IGTF release but I will do my best to get into October release. If Irwin's schedule is not changing, then I either ask him to delegate to someone on his team or ask for another reviewer.
  - OSG CA Testing.
    - OSG software stack thoroughly tested. Most OSG services are also tested. We have not tested OSG Connect and Stash Cache. Since we tested glideinwms, I am not very worried.

- OSG CA transition Plan. CMS and Atlas will start their tests as soon as the IGTF accreditation is approved.
  - CMS and Atlas confirmed that they will obtain user certs from CERN CA, but only use OSG for host certs.
  - We plan to transition these VOs right after testing period.
  - Already contacted 13 VOs and scheduled them for January/February 2016 for transition.
- We wrote and tested a script to add new cert DNs to VOMS servers. This means user certs will be automatically re-registered in VOMS. Please note that since CMS and Atlas are using CERN CA certs, this is not as big of a pain as it used to be.

# IF Access Control Model

- We are changing the IF access control model to integrate it with Federated Identities and the fully automated CILogon Basic CA certs.
- Demand from DUNE and other IF experiments.
- Currently, they are using Kerberos CA to obtain certificates. This is very cumbersome for non-FNAL or offsite collaborators.
- The ultimate goal is to get rid of end user certificates completely, but in the meantime we have to provide a workable, easier solution to IF experiments in a reasonable timeframe. Going completely cert-free will take 2-3 years.
- We decided to integrate with InCommon federation and CILogon Basic CA. We will create certificates for users automatically and transparently.
- Users will not have to manage their certificates.
- This is a very significant change to IF submission infrastructure.

# IF Access Control Model

- Created a new software architecture and defined the message flowcharts. Seeking approval from developers who will be impacted the most, SAM, IFDH, JobSub.
- This is the second round of creating an architecture. The first design evolved due to technical changes/problems.
- Currently waiting for Fermilab to change their IDP so that we can obtain CILogon Basic certs on the command line through the InCommon Federation.

# Key Work Items

- HEPCloud
  - Security assessment of the HEPCloud
  - For production jobs, there are no security issues.
  - If/When we move to end user jobs, the architecture needs to be changed significantly
  - Still needs some paperwork and document the risk assessment and security controls in place.
- Researched and compared the access control model of ALCF and OSG
  - The basic security models are similar.
  - ALCF has the concept of “Project” and “PI”, similar to XSEDE

# Key Work Items

- ALCF and OSG security models
  - The biggest difference is ALCF requires and extra audit for foreign nationals.
  - OSG does not even collect citizenship information
  - ALCF provides interactive access to its resources.
  - Requires 2-factor authentication. Crypto-cards and PIN
  - For data transfers, there is an internal ALCF CA that gives out certificates based on the 2-factor authentication. Very short term certificates.

# Security Goals for the Year

- OSG CA. We already talked about it.
- Fixing the security weaknesses found in certificate-free job submission system. We analyzed the problem, found a solution and wrote down a proposal. We need to send this to Miron for approval.
- Maintain Operational security. Will talk about it.
- Perform security controls and risk assessment. Completed.

# Operations

- Vulnerabilities
  - CVE-2015-3245, CVE-2015-3246. The vulnerabilities in libuser modules.
  - OpenSSL CVE-2015-1793. OpenSSL vulnerability. Thankfully did not make it to RedHat or Scientific Linux, so we were not impacted.
  - Vulnerability in dcache, just came out recently
  - OpenSSH vulnerability. Waiting for globus to weigh in on gsi-ssh.
  - Major vulnerability in GUMS. Software team released the fix very quickly. Thanks to Brian, Tim C and Tim T.
  - We tested the fix and confirmed it works. We want to test GUMS for other similar vulnerabilities. And, then to send it off to SWAMP for a thorough check. This was actually in our action items decided in the staff retreat.

# Operations

- Incidents
  - OSG main website got hacked. This is the news page that has updates from various OSG staff and contributors. The hacker placed various advertisements for Oakley eyeglasses.
  - The communication staff, Katherine, noticed the issue and promptly reported.
  - Cleaned up the spam.
  - Since there were very little logs, we could not exactly understand how they infiltrated.
  - One theory is we had a lot of dummy accounts, accounts created for guest authors so we can post articles under their name. But guest authors never use these accounts. There were quite a few of these accounts.
  - We also noticed there were a lot of attempts on Ruth's account. It is possible they broke her password.
  - We asked for 2 changes, more logs files and elimination of dummy accounts.
  - We also notified Ruth and asked her to change her passwords.
  - There was no other damage

# Operations

- DOS Attack on OIM ticketing service
  - The ticketing service went down for 2 hours.
  - No major damage to our systems.
  - We implemented max connection restrictions and timeout.
  - Also considering restricting access to certain domains. Still unclear.
  - Attack was coming from Russia.

# Operations

- WLCG-OSG security communications.
  - We have an incident sharing email list among OSG/ XSEDE/WLCG/EGI, grid-sec
  - Since Kevin left and Jeny started in July 1st, we are trying to get Jeny's membership established. It requires 2 members to vouch for her. We applied when she started but still have not finished it. Finally we found another non-FNAL non-OSG grid-sec member who can vouch for her.
  - Emailing Romain twice a week each week about this, but no resolution yet.

# Operations

- CVMFS security drill
  - Finally it is done ☺ Very happy that we did it.
  - The report is available at twiki.
  - We asked 2 repos to be blanked as part of our security practice.
  - The goal is to show that if we ever have malicious content in one of the repos we can pull it out quickly.
  - The GOC team were able to do this successfully for one of the repos, but the other one we found a bug. Luckily, Dave Dykstra as a new member of the security team diagnosed the problem and released a fix.
  - We are happy that we had a chance to practice this and identified a bug.

# Operations

- OSG Connect security assessment has started.
  - We are documenting the architecture
  - We will later submit jobs and do a traceability study.
- DigiCert intermediate CA transition to SHA-2
  - The end users have transitioned 2 years ago.
  - This is the CA itself transitioning.
  - We got the CA cert and generated couple certs and tested them. Everything seems fine.
  - We made announcement to the community and asked them to switch
  - The one big change is we no longer support v3.1 so no CA release for this version. There are still some resources on 3.1 but OSG polciy was not to support this version.

# Operations

- Risk assessment for OSG assets are completed
- New members into OSG team:
  - Jeny Teheran has started at the beginning of July
  - Dave is also a recently transitioned into security team.
  - Very happy with these new additions.