# Introduction to OSG Security

Suchandra Thapa

Computation Institute

University of Chicago

# Overview

- Discussion of basic security infrastructure used by OSG
- Will discuss certificates
- Will discuss procedures and policies for OSG
- Will discuss some of the tools available
- Q&A time afterwards

# Certificates Used

- OSG uses X.509 certificates for authentication and authorization
- Most certificates in DOEGrids certificate chain
- Obtained from GOC / Need someone to "vouch" for you
- All tools use and verify using certificates
  - User submissions (job submission, gsiftp) use proxies signed by user's X.509 certificate
  - Sites and services have host certificates which are verified by user tools

# CA Certificates

- What are they?
  - – Public certificate for certificate authorities
  - – Used to verify authenticity of user certificates
- Why do you care?
  - – If you don’t have them, users can’t access your site

# Installing CA Certificates

- The OSG installation will **not** install CA certificates by default
  - Users will not be able to access your site!
- To install CA certificates
  - Edit a configuration file to select what CA distribution you want

```
vdt-update-certs.conf
```

  - Run a script

```
vdt-setup-ca-certificates
```

# Choices for CA certificates

- You have two choices:
  - Recommended: OSG CA distribution
    - IGTF + TeraGrid-only
  - Optional: VDT CA distribution
    - IGTF only (Eventually)
    - Same as OSG CA (Today)
- IGTF: Policy organization that makes sure that CAs are trustworthy
- You can make your own CA distribution
- You can add or remove CAs

# Why all this effort for CAs?

- Certificate authentication is the first hurdle for a user to jump through
- Do you trust all CAs to certify users?
  - Does your site have a policy about user access?
  - Do you only trust US CAs? European CAs?
  - Do you trust the IGTF-accredited Iranian CA?
    - Does the head of your institution?

# Updating CAs

- CAs are regularly updated
  - New CAs added
  - Old CAs removed
  - Tweaks to existing CAs
- If you don't keep up to date:
  - May be unable to authenticate some user
  - May incorrectly accept some users
- Easy to keep up to date
  - vdt-update-certs
    - Runs once a day, gets latest CA certs

# CA Certificate RPM

- There is an alternative for CA Certificate installation: RPM
  - We have an RPM for each CA cert distribution
  - No deb package yet
  - Install and keep up to date with yum
  - Some details not discussed here: read the docs

# Certificate Revocation Lists (CRLs)

- It’s not enough to have the CAs
- CAs publish CRLs: lists of certificates that have been revoked
  - Sometimes revoked for administrative reasons
  - Sometimes revoked for security reasons
- You really want up to date CRLs
- CE provides periodic update of CRLs
  - Program called fetch-cr
  - Runs once a day (today)
  - Will run four times a day (soon)

# Authorization

- Done by gridmap files or GUMS
- Gridmap files are fairly simple
  - Text file with DN followed by local account
- Will look at GUMS

# GUMS

- The GUMS service performs one function: it maps users' grid certificates/credentials to site-specific identities/ credentials (e.g., UNIX accounts or Kerberos principals) in accordance with the site's grid resource usage policy.
- The GUMS interface for the callout implements two standards, the older OSGA OpenSAML 1.1 AuthZ format and the new OSGA OpenSAML-XACML 2.1 AuthZ format. The existence of these interfaces means that any kind of client that implements one of these standards is able to contact GUMS. Existing clients are GT2/Prima, GT4, gPlazma/dCache, and glexec.
- Command line client too
- Allows blacklisting of users/DNs

# Security Team

- Mine Altunay (maltunay@fnal.gov)
  - Security Officer
- Doug Olson (dlolson@lbl.gov)
  - Deputy Security Officer
- Jim Basney (jbasney@ncsa.uiuc.edu)
- Ron Cudzewicz (cudzewicz@fnal.gov)

# Policies

- Site Registration Database
  - OSG Information Management – site manager, site security, site operations, site incident response
  - Names, email, address, phone
  - Old stale info needs to be uptaded
  - OIM is maintained at GOC
  - We currently check once year, but will the frequency increase once OIM sends automated emails

# Site Operations Policy: how to be a good citizen

- https://osg-docdb.opensciencegrid.org:440/cgi-bin/RetrieveFile?docid=676,
- Must support at least one VO: MIS
  - We are doing drills, tests are coming up – not perfect but getting there
  - Update your gums template
  - Let us know if you suspend a VO
- Apply patches announced asap
  - Let us know if you cannot
- Make sure published site info is accurate

# Incident Response Policy

- Incident: *any real or suspected event that poses a* real or potential threat
- You MUST Report and Respond
  - Report: email security@opensciencegrid.org
  - abuse@opensciencegrid.org
  - +1 317-278-9699
  - https://twiki.grid.iu.edu/twiki/bin/view/Security/IncidentDiscoveryReporting
  - Respond: follow this policy in collaboration with OSG

- When contacting OSG, let us know:
  - If any certs are compromised, or suspicious
  - If any VO accounts are affected
  - Have you informed any CA for revocation ?
  - Have you shut down the node ? Will you ?
  - Any suspicious connection out of your node to another grid resource ?
  - Any corrupted data
  - Please KEEP US INFORMED, keep emailing during your forensics, even if you think it is embarrassing – We are ALL in this together

# VDT Security Tools

- CA hygiene: run fetch-crl to update CRLs
  - How can we improve the tools
- Run vdt-cert-update to update CA directory
- Update your GUMS template
  - Subscribe to RSS feed at GOC
  - www.grid.iu.edu/news
  - http://software.grid.iu.edu/pacman/tarballs/vo-version/gums.template
  - http://vdt.cs.wisc.edu/components/gums.html

# Example of a security incident

- Will outline an example of how to deal with a security incident
- Four major steps
  - Stop further exposure
  - Find out if your site was exposed and to what extent
  - Conduct basic forensics
  - Clean up suspect jobs

# Stopping further exposure

- Just ban the user’s DN
- How?

# Sites using gridmap

- 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
- Repeat for any other hosts using gridmap files

# If Using 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

# GUMS Part 2

- 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

# Determining Exposure

- Need to check logs
- 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?

# Checking Exposure 2

- 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 same account?

# Need to continue?

- 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

# Forensics

- Conduct basic forensics to identify what the DN has run
  - Check the logs to see what jobmanager(s) were used
  - Check your batch system logs
  - Log into nodes and/or CE and see which processes are owned by the user
  - Use lsof and netstat to find any open files or ports that the DN is running
  - Check scripts, run strings to see if any hostnames or contact information appears

# Cleanup

- Use batch manager to remove any remaining jobs
  - condor_rm cluster_id
  - qdel job_id
  - kill -9 any remaining processes
  - If all VO DNs mapped to same account, can delete all jobs for that account

# Escalations / Followup

- Follow home institution policies for security incidents
- If the DN may have been able to access or obtain other user DNs contact security@opensciencegrid.org immediately

# Security Best Practices

- Best Practices • https://twiki.grid.iu.edu/bin/view/Security/Be stPractices

# Acknowledgements

- Mine Altunay
- Jim Blasney
- Alain Roy
- Anand Padmanabhan