Open Science Grid

OSG Security

Kevin Hill
Mine Altunay
Anand Padmanabhan

OSG Security Team

Disclaimer:

- I didn’t know I was giving a talk until I got here this morning, so hopefully this all makes sense…
- Adapted from OSG All Hands meeting talk

Our Mission

- Protecting OSG users and resources from security breaches
- Preventing loss of effort and resources due to security problems
- Making OSG resources easily accessible to users without compromising their security
- Being a security hub; disseminate security knowledge, best practices, and education

Security Incidents

- No new major OSG security incidents.
- Concerns from other grids:
  - Password compromises
  - Bitcoin mining

Password Security

- Move to SSH access instead of x509 access.
- Password re-use in combination with phishing and/or browser compromises biggest threat right now.
- Large news making compromises add all username/passwords to bad guys dictionaries.
- Recommending two-factor auth where practical.

Bitcoin Mining

- Bitcoin is a digital currency, which pays bitcoins for the effort to calculate complex hashes to log transactions.
- Designed so should always take about 10 minutes for current generation of hardware.
- Expected to cost more in electricity than payback for mining on conventional hardware.
- Could maybe possibly be legit research, but please don’t try it.

Security Vulnerabilities

- Heartbleed – major defect in OpenSSL. Most systems quickly patched. Important systems got certificates replaced as a precaution.
- A couple other new SSL vulnerabities in GnuTLS and OpenSSL. Not as serious as Heartbleed, but still good to keep up to date with patches.

SHA-2 Transition

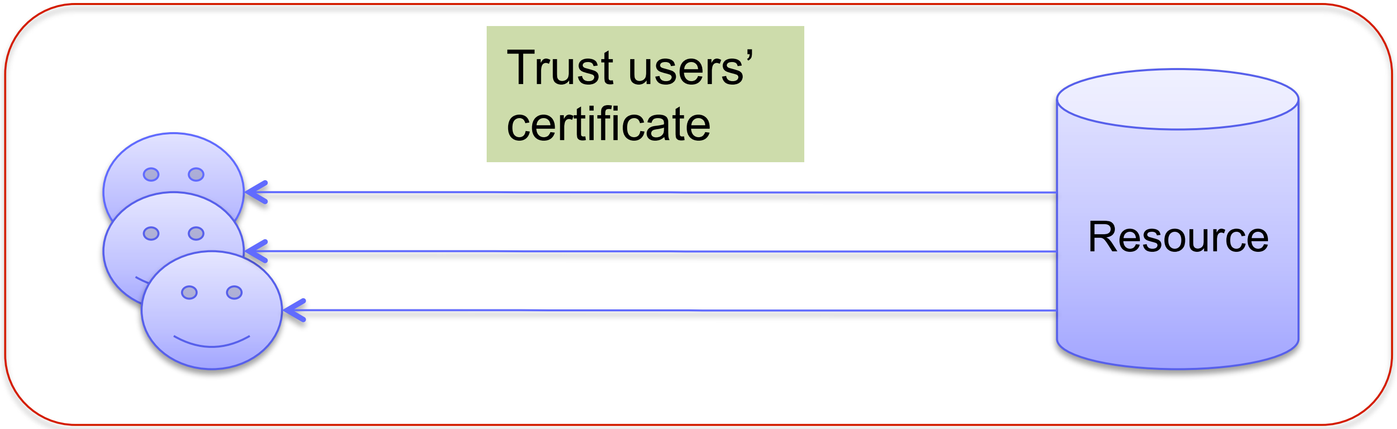
- SHA-1 certificates are nearing the point where processing power to generate collisions won't be unreachable
- SHA-2 certs now being issued by default
- Only a few issues.
- Digicert will be switching to a SHA-2 signed signing cert shortly.

Traceability Project

- Traditionally user jobs identified by certificate that accompanied jobs.
- Jobs should be able to be traced to individual users via condor/Glidein log files, even without end user certificates.
- VOMS servers no longer contain all end users, so user management practices of the VO more important.

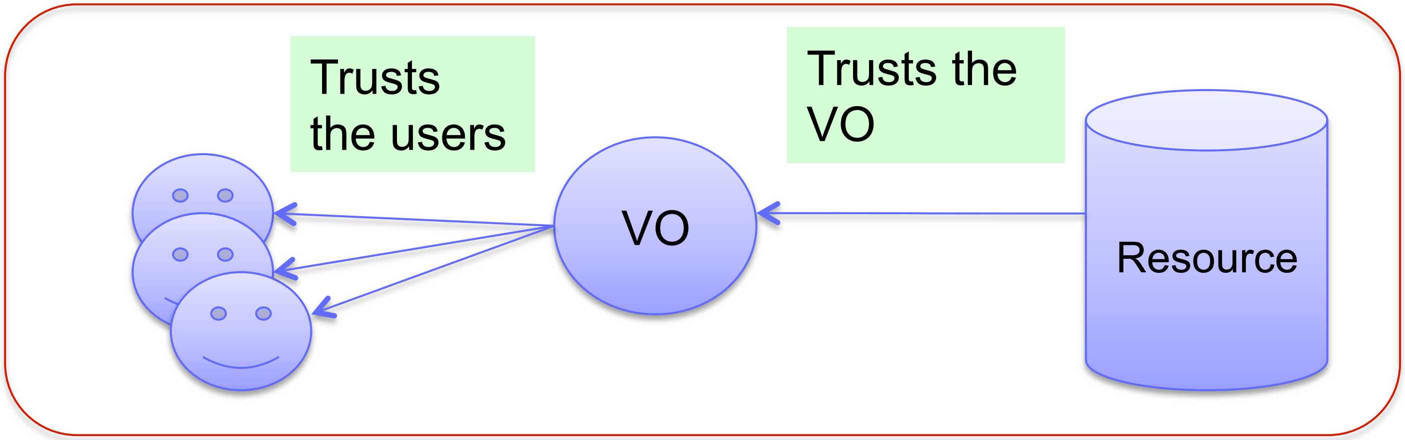
Open Science Grid

Traceability Project: Changing Trust Relationships


Trust users' certificate

Resource

OLD MODEL


Trusts the users

VO

Trusts the VO

Resource

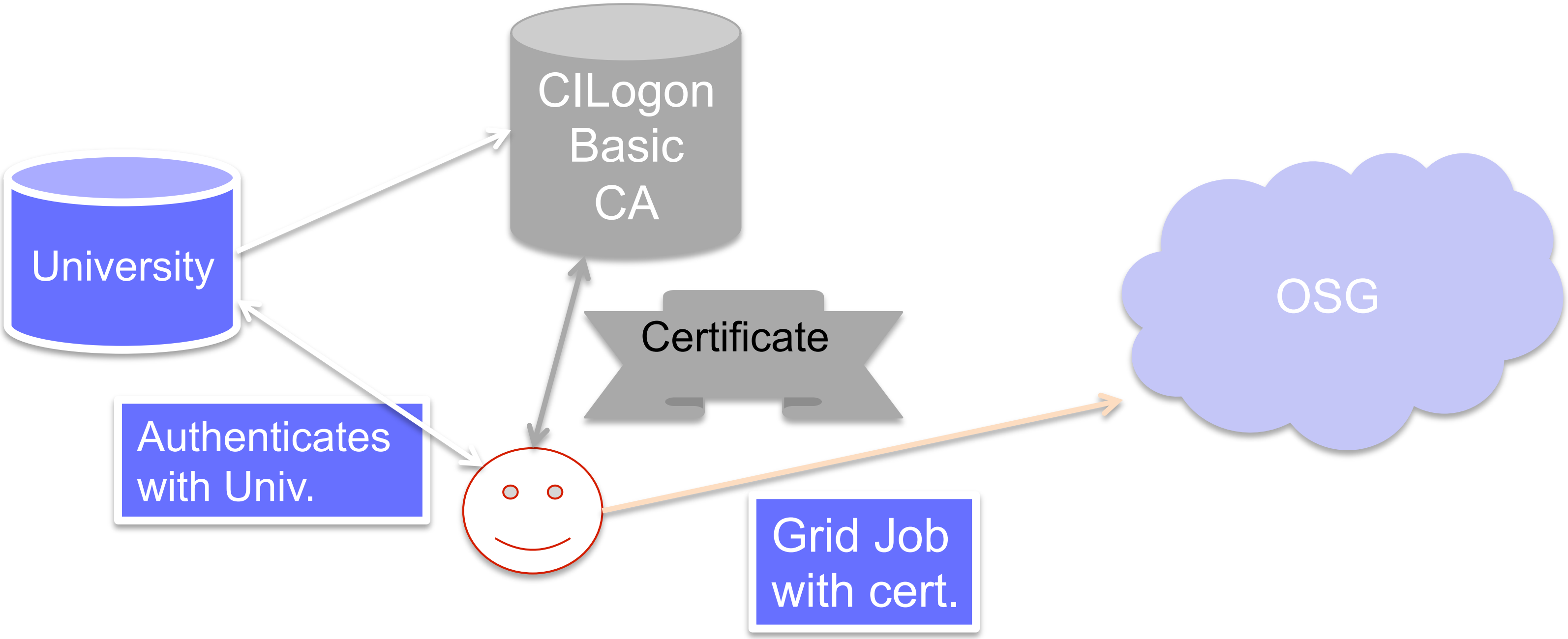
NEW MODEL

Traceability

- Goal is eliminating certificates for end users
  - Traceability = associating users with their jobs
  - Who owns this job? Can we answer this question without certificates?
  - Proved that GlideinWMS system can trace user jobs even without certificates.
  - OSG-XSEDE VO and GLOW VO are the first beneficiaries. Evaluated their user management practices and job submission systems

Federated Identities

- Federated Identities for access
  - For those users, who still need certificates
  - Providing certificates via their home organization
  - No need to get vetted by OSG to get a cert, users utilize their university accounts



CILogon Basic CA Advantages

- Quick for users to get certificates
- Replaces the RA->Sponsor manual verification step in the OSG CA workflow a federated authentication check via InCommon federation.

Future CILogon Basic usage

- Currently looking for more sites to accept certs, so more users can use them.
- Some sites have issue with certain IdPs, which effectively lets everyone with a valid email account sign up.
  - Can be limited via modified signing_policy file.
  - Care needed in case of updates to cilogon ca cert package.
- Really not that different than regional CA or large university.
- VO registration is an added authentication step.

Federated Identities

- CILogon Basic CA is accepted at 6 OSG sites, Fermilab, Nebraska, UCSD and more, representing 40% of total wall clock hours available in OSG.
- Goal is to reach out to more sites.
- The challenges are that
  - CILogon Basic CA is not an accredited CA (yet)
  - It has a slightly different risk model
- So, sites are slower to adopt this CA and the federated identities represented by that.
- Helping sites by explaining the new risk model behind CILogon Basic CA.

Next Challenge: Storage

- Can we provide access to storage without certificates?
- We've gotten requests to provide individual user access to storage, vs. group accounts normally used for job execution
- Will need some sort of session token for authentication/authorization
- Perhaps we can hide certs/proxies in the background?

Challenges/ What Lies Ahead

- Goal is to shield users from certificates and offer more user friendly access control technologies.
- Certificate-free jobs was a big success, we want to repeat it for accessing storage
- Get more VOs to submit jobs without certificates
- Campus grid and federated identities. Utilize campus identities seamlessly in OSG.
- Further reducing the number of host certificates. Optimizations on osg software stack.
  - Can we completely get rid of them?

Questions?