Status of and prospects for Worldwide Cyberinfrasructure: Security and Cyberinfrastructure

John R. Hover
jhover@bnl.gov
Brookhaven National Laboratory

March 5, 2008

My Perspective

- Brookhaven National Laboratory: Large site.
- ATLAS: Pilot-based workload management, data intensive science.
- A relative newcomer to the Grid: 2 years.
- UNIX sysadmin.
- GUMS developer.
- Supporter of both OSG and EGEE middleware stacks.

Baseline Global Security Infrastructure

- X509 SSL Host and User Certificates: User and host authentication.
- International Grid Trust Federations: CA Consortium.
- VOMS/VOMRS, VOMS proxies: VOs, groups, and roles. Authorization framework.
- MyProxy for proxy delegation and retrieval.
- Globus Security Interface (GSI)
- All valid/used across grids (OSG, EGEE, Nordugrid, etc.)

Near-Term Issues and Challenges: Large-scale security infrastructure management.

- E.g. Sites w/ 500+ hosts that need certs. Automated renewal/request systems themselves become vital/vulnerable components of the infrastructure, e.g. "Certify".
- VOs with thousands of users: cert expiration, VO membership renewals become tedious.
- Site-level CA, CRL management.

Near Term Issues and Challenges: Site<-> VO scalability

- In EGEE, this has been mostly handled: 50 rapidly recyclable pool accounts per VO. VOMS proxies are mandatory.
- In OSG, all members of each VO must be pre-mapped to UNIX accounts, therefore thousands of pool accounts are required.

Near-Term Issues and Challenges: VOMS Auth and Proxy handling.

- OSG need to deprecate vanilla grid proxies. EGEE has already done this.
- Need easy, end-to-end proxy generation, delegation, renewal, and retrieval. With VOMS extensions. Still tricky and new.
- Need easy way for VO software to interact with and handle VOMS and proxies. If not, VO developers won't use it well.

Near-Term Issues and Challenges: Pilot-based systems

- (ATLAS, CMS, CDF, Minos, more...)
- glExec goes a long way toward bringing pilot-based systems back under Grid infrastructure (logging, accounting). Available OSG + EGEE/gLite.
- Pilot system itself becomes an entry point requiring security, authentication and authorization.

Near-Term Issues and Challenges: Incident response infrastructure.

- Technical: e.g. SAZ, CRL updates.
- Policy: privacy, incident policy, distributed trust model.
- Coordination and communcation across Grids.

Long Term Challenges:
Grid <-> UNIX

- Grid/UNIX interface (e.g. GUMS) is complicated and leads to "leaky abstractions", with security implications.
- Underlying software providing Grid services should natively understand X.509 identities, e.g. dCache, JobManagers,etc. (Batch systems?)
- This would allow Grid services to run as unprivileged service accounts rather than UNIX accounts representing individual Grid users.

Long Term Challenges: Complexity

- Greater complexity -> greater vulnerability. (Also less reliability, maintainability, and harder troubleshooting, but this is about security.)
- Environment variables considered harmful. As systems are layered (e.g. pilots -> Condor-g ->Globus -> UNIX -> LBMS -> userjob on WN.) Each layer may have different UNIX shell environment.
- E.g. Namespace collision in environments between OSG and gLite software.

Long Term Challenges: Scalability

- How to handle security in a global multi-grid environment with hundreds or thousands of VOs with hundreds of thousands of users..
- ...and where there may be incidents per day rather than incidents per month.
- VOMS replication and VOMSAdmin HA-- thousands of queries per minute.
- Distributed error/fault handling and logging for forensics.

Long Term Challenges: Compatibility

- Difficult to draft and maintain standards. Again, a general problem that has security implications.
- Ever present tension between VOs and Grids: Quick custom solutions vs. standard, general solutions.
- This tension is also mirrored between Grid middleware stacks, e.g. OSG vs. EGEE/gLite
- No final resolution, just ongoing negotiation: communication, coordination, joint projects.