EGEE Security

Joni Hahkala, UH-HIP
On behalf of JRA3

JRA1 AH
March 22-24, 2006
CERN, Switzerland

www.eu-egee.org
www.glite.org

Information Society and Media

Released gLite Security Modules

Authz framework (java)
Generic, pluggable policy-engine chaining infrastructure.

Encrypted storage (C++ and Script)
File encryption and secret sharing library and example of usage.

Grid enhancements for OpenSSL
Implemented support for Grid proxies. Added to OpenSSL main line.

glexec
Designed to switch identity from the grid user to a local user, “sudo for grids”.

Jobrepository
Stores all known information about the user-mapping

Security test utils
Simplifying testing of security modules. Used widely in gLite standard testing procedures.

Trustmanager
Grid proxy support and enhancement for java SSL.

Delegation
Delegation of credentials from client to server.

LCAS - Local Centre Authorization Service
Handles the authorization to the local fabric based on the user's proxy certificate and the job description in RSL format.

LCMAPS - Local Credential Mapping Service
Provides the local credentials needed for jobs allowed into th local fabric, in particular the unix uid and gids.

Gatekeeper
Globus gatekeeper, extended with call-outs to LCAS and LCMAPS.

Util (java)
Security utilities for java.

Mutual Authorization
Authorization of the server

gsoap plugin
Grid proxy support and ssl for gSOAP SOAP library

VOMS
VO management

proxyrenewal
Grid proxy support and ssl for gSOAP SOAP library

Summary - Security modules

Module	Component available	Implemented	Integrated
AuthZ framwork (java)	Yes	gLite1.0	Yes
Grid enhancement for OpenSSL	Yes	No	Yes, in openssl-0.9.7g
glexec	Yes	gLite3.0	No
Jobrepository	Yes	gLite1.5	No
Security test utils	Yes	gLite1.3	Yes
Trustmanager	Yes	gLite1.0	Yes
LCAS	Yes	gLite1.0	Yes
LCMAPS	Yes	gLite1.0	Yes
Gatekeeper	Yes	gLite1.0	Yes
Delegation	Yes	gLite1.2/1.5	Yes
gsoap plugin	Yes	gLite1.2(not JRA3)	Yes

Security Assessment

DJRA3.4 EGEE Security Architecture assessment

https://edms.cern.ch/document/686044

Describes the PM18 status of EGEE Security, including comparison with other Grid initiatives.

Glexec

- **In gLite 3.0**
- **Not yet ready for deployment on WNs**
- **Some details of deployment on WNs still need discussion**
  - Sites don't like setuid executables in WNs
- **Configuration improvements**

TODO

- **Chown support**
- **Better error codes**
- **Condor integration**
- **(Authz callout to WSS, GUMS…)**

LCAS/LCMAPS, Job Repository

LCAS/LCMAPS

- Better wildcards in configuration files
- Proxy verification and lifetime checking (glexec)

TODO

- Finer grained error codes
- Authz callout for GT3,4 authz routines
- Advanced proxy lifetime limitations
- Site Central Mapping Service
  - Through a SAML interface to interop with GUMS

Jobrep

- Being integrated with gLite 3.0 components

TODO

- WS interface to the DB for site central audit trailing

Delegation

- **Most current development done by DM cluster**
- **New interface**
  - Adds methods found in GT4 (destroy, renew…)
- **Two backends**
  - Filesystem
  - DB
- **Java implementation finished**
  - In gLite 3.1
- **GridSite implementation being committed to CVS**
- **Integration**
  - CREAM (filesystem backend)
  - FTS (DB backend)

Encrypted storage

- **C++ libraries**
  - Encryption, decryption
  - Key splitting (trivial, Shamir's secret sharing)
  - Being translated into C
- **Hydra key server up and running**
  - Client code to manage ACLs being integrated
  - Current ACL restricts access to original user
- **Currently integrated into gLite I/O**
  - Move to FTS planned
  - No key splitting yet, waiting for C lib

Trustmanager, Mutual Authz

Trustmanager

- Timeout support added, Thanks to Steve Hicks

TODO

- Namespace restrictions
  - Both old and new format configuration files
- Per thread/message security context configuration

Future

- OCSP support

Mutual Authz

- Initial interface defined
- Implementation ongoing

Proxy renewal/Myproxy

- **Two stage system exists and is deployed**
  - First renew the plain proxy from MyProxy
  - Then renew VOMS AC from VOMS
- **IT/CZ working on adding VOMS support to MyProxy to ease configuration**
  - VOMS groups in MyProxy configuration file
    - Services need to register to VOMS and get VOMS proxy
  - Also VOMS AC renewal inside MyProxy is considered
    - Would improve security
- **Separate library being produced**

VOMS

- **Lots of bugs fixed**
- **VOMS, VOMS admin seem stable now**
- **New way of distributing VOMS server certs**
  - Inside VOMS AC
  - Compare to a DN within the system
  - No need to update server certs every time it is renewed
- **Works better with Oracle**
  - New Oracle lib caused some problems because of undocumented changes
- **Development concentrated in CNAF**
  - Other developers still participating

8th MWSG (cont.)

MWSG decision on glexec on WN

”The gLite software will support a deployment model where glexec is run on worker nodes. Although technically possible today, enhancements towards centralised policy coordination are needed for scalable deployment, that and should be ready by July '06.

Glexec can then be deployed on the head node (as today), and on the worker nodes. A "null" operational mode will be provided for glexec, so that is can be run without setuid capability. In that case, running glexec will of course not enable discrimination of the different users' actions.

Deployment of a setuid-capable glexec on the worker nodes is objected to by Ruth (from OSG) as it makes the setup unneccesarily complicated.
The conclusion was to get some more comments from the site operations side. Ian Neilson sent a request for comments to some people in SA1/3, but hadn't received any last time I talked to him.

In a future model, job requests can have to be signed - together with the sandbox (in/out) - to give additional confirmation of the users intent to run a job.”

MWSG decision on VO naming

”The VO name is a string, used to represent the VO in all interactions with grid software, such as in expressions of policy and access rights.

The VO name MUST be formatted as a subdomain name as specified in RFC 1034 section 3.5. The VO Manager of a VO using a thus-formatted name MUST be entitled to the use of this name, when interpreted as a name in the Internet Domain Name System.
This entitlement MUST stem either from a direct delegation of the corresponding name in the Domain Name System by an accredited registrar for the next-higher level subdomain, or from a direct delegation of the equivalent name in the Domain Name System by ICANN, or from the consent of the administrative or operational contact of the next-higher equivalent subdomain name for that VO name that itself is registered with such an accredited registrar.

Considering that RFC1034 section 3.5 states that both upper case and lower case letters are allowed, but no significance is to be attached to the case, but that today the software handling VO names may still be case sensisitive, all VO names MUST be entirely in lower case.”

Questions and Answers