JRA3 Security

Ake Edlund

on behalf of the JRA3 team

Contents

- Status of deployment of security solution in gLite services
- Security testing on gLite
- MJRA3.5 plans

Status of deployment of security solution in gLite services

Deployed on the prototype (released in gLite)

CE:

- globus gatekeeper with callouts to LCAS (authorization) and LCMAPS (credential mapping, identity switching). Uses GRAM protocol (GSI security)
- Globus Workspace service (WSS) with LCMAPS as a backend. Provides a management interface for local accounts (poolaccounts in practice). Currently stand-alone; not integrated with job submission services.

SE (in LCG-2):

- gridFTP server with callouts to LCAS + LCMAPS. Uses gsiftp protocol.

Status of deployment of security solution in gLite services

Deployed on the prototype (released in gLite) - cont.

- WMS: proxyrenewal service (IT/CZ)
- VOMS core (IT/CZ) + voms admin (LCG)
- myproxy server: online secure credential storage.
- DM: secure implementations exist but with some problems that are being sorted out. Note: Security model under discussion.

Status of deployment of security solution in gLite services

Work ahead - prioritized work (more details in 'Appendix')

- Support SA1/LCG deployment
- bug fixing
- WorkSpace Service integration
- fork/set-uid service
  - CE: su-exec wrapper/program - to be used by/integrated with gt4 GRAM, CREAM, Condor-C, gridsite. This provides a thin setuid layer for services running in unprivileged mode. Uses LCMAPS and the WSS on the inside.
- Encrypted storage
  - Started. Earlier: Data Key Mgmt
- Job repository
  - CE (and SE) job repository: site-local auditing and logging tool.
- Delegation
  - the libraries and first WS interface exist and are ready to be included to R1.2. Will probably also need a standalone service and client for non-WS services (e.g. for JRA4, BAR). WS-Trust version - ongoing work on standardizing.

Status of deployment of security solution in gLite services

Being integrated:

- WMS: WMproxy (IT/CZ), uses gridsite + LCMAPS
- authZ-framework-java. Used via the "authorization handler" by java services on the CE: CEMON.

Security testing on gLite

Planning for functional tests of some security requirements. Will be implemented as part of the JRA1 test suite and distributed with a gLite release.

Plans for the functional tests:

- The tests will initially be implemented using the command-line tools.
- Web browser-based tests will not be essential
- Will try to test functionality that is expected to fail so long as the error condition can be caught. This is important for AuthN and AuthZ (AA) so the user can see why their attempt is failing.
- Stress and stability tests should be made on the basic AA engines (org.glite.security.authz-framework-java and gridsite).

Candidates - Security components that can be tested:

- Gridsite Authentication and Authorization server.
- Encrypted storage
- VOMS testing is handled as a separate case.
- Data management (DM) File Transfer service (FTS)

Security testing on gLite

Comments on the current VOMS testing:

Some VOMS version difficulties lead to some tests being 'not visible' but essentially they are done and soon as a longer test-suite.

About testing gLite security software:

Much of the security software constists of libraries and APIs. After consulting JRA1 (Maite, Akos) we have selected FTS - as being the most complete DM component (see next slide).

Security testing on gLite

Detailed - Data management (DM) File Transfer service (FTS):

The data transfer jobs are authenticated and authorized using user proxy certificates but are submitted using the server credential.

The user proxies are held by the C++ submitter daemon. The web service (referred to as the portal) of the FTS system communicates with the Oracle database server and performs the authentication (AuthN) and authorization (AuthZ).

The AuthZ is based on a VOMS role or a mapfile, similar to a gridmapfile.

- **Check the authorization (AuthZ) mechanism**. Present the FTS web service with a series of ‘good’ and ‘bad’ proxies and make sure the correct AuthZresult is returned.

Security testing on gLite

Detailed - Data management (DM) File Transfer service (FTS) - cont.

- **Check that the connection between the service** running inside Tomcat (referred to as the portal) and the Oracle database is secure.

- **Check that the connections between the Oracle database** (server) and the C++ daemon are secure.

- The C++ daemon forks a process for each job and stores relevant files (user proxy for instance) for further use. **The permissions on these files should be checked.** For a stored proxy only owner have permission to read/write the file.

MJRA3.5 plans(Jeremy Cook, UiB)

PM15, Secure Credential Storage procedures (recommendations document)

TOC to PEB	Done, same as in phase 1
Internal review starts **(JSPG early contact)**	May 20, 2005
Send EDMS link to JSPG, MWSG	June 10, 2005
Send EDMS link to Moderator	June 30, 2005
Moderator to send final decision to PEB	July 28, 2005

Review Credential storage methods, security considerations wrt compromise, physical security, etc.

Hardware devices	**Software credential storage**
USB memory sticks	Online CA
Biometric solutions	Kerberized CA
Smart card solutions	MyProxy

Illustrative case study: Web portal

- Touches several layers of grid middleware
- Requires user credentials
- Highlight any weaknesses

One more slide - from Olle

Proxy certificate issues

- **Only OpenSSL 0.9.7g+ and GT4.0 use RFC3820**
  - GT<4.0 (also 3.9.x) are NOT RFC3820 compatible (bug)
    - Globus libs are backwards compatible
    - GridSite currently supports a single (older) format
    - TrustManager supports both formats
  - Fixing this is important for the future
  - We need a date / release when to move to the RFC3820 format
    - Coordinated addition of support in all the middleware components
    - Possibly breaking backwards compatibility in the process

- **Side note: OCSP support faces the same inclusion coordination problem**

Appendix - workplan details

Appendix - workplan details

1. Delegation service (NC, a)

This service is essential for all other services.
gLite delegation components will be reimplemented to comply with a new/common interface which harmonizes delegation mechanism between other projects who are leveraging delegation in their products.

These new set of libraries use a single set of syntax and semantics of Delegation based on WS-Trust specification. We describe delegation as a standalone Web Services portType, and then we provide a set of ready-to-use library implementations of this portType based on WS-trust.

Appendix - workplan details

2. Data key management (NC, a) - NEW NAME: Encrypted Storage

Sensitive applications, for example Biomed, have strict security requirements for data. The data has to be encrypted not only during transfer, but also on storageto prevent data exposure in event of theft or compromise of the storage.

To facilitate this the data key management system will offer functionality (based where possible on Data Management modules) to encrypt the data where it is generated, to store the data and encryption secret, to retrieve these and to decrypt the data where the data is needed. This system in addition to protecting the data on storage also makes it harder for malicious system admins to acquire the encryption secret by spreading the secret over several servers.

Appendix - workplan details

3. Job repository for auditing (NC, a)

Any action taken on a resource via the grid interfaces must be audited and logged. The Job Repository will record all information relevant to the mapping of credentials, the credentials created or linked, and the associated attributes (VOMS groups, roles and capabilities). It is a local component, and does not communicate with and is not intended to be used from outside the site.

Appendix - workplan details

4. The following extensions to the security mechanisms, in particular available on the CE, are planned in collaboration with ANL:

a. su-exec wrapper for setuid services. Needs to work together with Condor-C, WorkSpace Service, Cream CE, gridsite apache servers (NC, a) Services/code running with privileges should be avoided as much as possible. For services that need to switch user identity (setuid, setgid) this can be done implementing a light-weight wrapper program that is easily auditable at the source level, that will always execute with elevated privileges, and will subsequently change user identity. This wrapper will execute a service-determined executable with local credentials that are derived from the user's identity and any accompanying authorization assertions (VOMS attributes). This component will interact with Condor-C, WorkSpace Service, Cream CE, gridsite apache server.

Appendix - workplan details

4. cont.

b. Interoperability: add globus (>gt3) authZ callout interface to LCAS and LCMAPS (to be defined) (NC, a). The globus code (gt3 and higher) contains hooks to make callouts to authorization libraries, such as LCAS. LCAS and LCMAPs have to implement this callout interface. Note that the hooks for LCMAPS still have to be added to the globus code.