EGEE Security

Ake Edlund for JRA3

EGEE EU Review (CERN)

May 23-24, 2006

www.eu-egee.org

Information Society and Media

Outline

- Major JRA3 achievements since the 2nd EGEE Review
- Answers to recommendations at the 2nd EGEE Review
- Summary

EGEE-I security since the last review

- **gLite 3.0 work**
  - Updates of Job Repository, Trustmanager, Encrypted storage, Delegation and glexec, Enhancements to the LCAS and LCMAPS libraries, and LCAS/LCMAPS plugins, VOMS PDP for the java authorization framework

- **DJRA3.4, Assessment of security infrastructure report**
  - EGEE security architecture is well positioned and aligned with current thinking at a global scale
  - Identified a number of issues to be addressed in future work
  - This together will be a good input for analysing/monitoring future security efforts.

EGEE-I security since the last review

- **Interoperability efforts:**
  - Grid Authorization - Interoperability Here & Now workshop - GGF16, Athens, Feb 16
    - Outcome of this kick-off meeting was a proposal of a subgroup of GIN (Grid Interop Here and Now) the TONIC - Taskforce Organizing Nearterm Interoperation for Credentials – initiative.
  - EGEE/NAREGI Interoperability meeting – CERN, March 20-22
  - 8th Middleware Security Group (MWSG) meeting
- **EUGridPMA and IGTF work**
  - 1st TAGPMA was held in Rio in end of March, with participation from JRA3 (chair IGTF)

Overview - Security services

Enabling Grids for E-sciencE

Requirement	In architecture	Solution/ Technology/Service	Component Available	Implemented	Integrated
Single sign-on	Yes	Proxy certificates and a global authentication infrastructure	Yes	Yes	Yes
User Privacy	Partially	Pseudonymity services	No	No	No
Data Privacy	Partially	Encrypted Storage	Yes	Yes	Yes
Audit ability	Partially	Meaningful log information	Yes	Yes	Yes
Accountability	Yes	All system interactions can be traced back to a user	Yes	Yes	Yes
Combining policy from different administrative domains	Partially	Authorization framework	Yes	Yes	Yes
VO managed access control	Yes	VOMS	Yes	Yes	Yes
Support for legacy and non-WS based software components	Yes	Modular authentication and authorization sofware suitable for integration	Yes	No	No
Non-homogeneous network access	Yes	Dynamic Connectivity Service	No	No	No

Overview - 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

Answers to the reviewers' comments

- **Recommendation 34: Prioritize the various security related tasks and requirements at the user and system level in order to come up with a list of intermediate goals towards a fortified Grid suitable for commercial deployment.**

- **Response: The way JRA3 fulfills this is through the Technical Coordination Group (TCG), where the security requirements are - since start of EGEE and with input from previous projects and current collaborating projects - continuously collected, and prioritized with the overall goal towards an industry standard service.**

Answers to the reviewers' comments

- **Recommendation 35: Spearhead the effort of prioritizing the security requirements via the industrial partners starting with their own requirements and with their experience interacting with others.**

- **Response: This is input given by the EGEE Industry Forum representative, as well as direct meeting with industrial interest groups. E.g. JRA3 participated in February 2006 actively in the Grid in Finance workgroup. From Life Sciences, input are given through the security knowledgeable NA4 representatives in the Middleware Security Group. Later at GGF16 EGEE, in February 2006, security representatives organized a half-day workshop especially inviting the Life Sciences WG.**

Answers to the reviewers' comments

- **Recommendation 36: Track and actively contribute to the activities of the newly established IGTF (International Grid Trust Federation), conveying their experiences about prioritization of the security requirements.**

- **Response: This is one of JRA3's main tasks and through the EUGridPMA, JRA3 was one of the main contributors in the launching of IGTF together with APGridPMA, TAGPMA. David Groep (JRA3) is the first chair of IGTF.**

Answers to the reviewers' comments

- **Recommendation 37: Outline and plan a series of stress tests of the security infrastructure." and "Conduct deliberate external attacks by 3rd party contractors.**

- **Response: This will be one of the deliverables of JRA2/Security Coordination in EGEE-II. First investigations and meetings with such 3rd party contractors have been initiated, together with SA1/OSCT manager Ian Neilson.**

Answers to the reviewers' comments

- **Recommedation 38: Address the interoperability of the various Grid security mechanisms, existent and planned, with established security procedures.**

- **Response: Interoperability was, and is, one of the main goals of the Middleware Security Group (MWSG). This has been very successful between EGEE and OSG, and has been promoted by GGF to be used as an example of pair-wise interoperability of Grids. To extend the interoperability effort, MWSG now includes DILIGENT, DEISA, SEEGRID and GRIDCC as members. NAREGI Japan is also in close contact with MWSG and have met regularly the last year. New meeting focusing especially on NAREGI needs was conducted in March 20-23, 2006.**

Example of interoperability workshops co-organized respectively organized by EGEE:

- GGF16, "Grid Authorization - Interoperability Here & Now"
- HPDC15, "EGEE Workshop on Management of Rights in Production Grids".

Summary

- **EGEE-I Security objective was to “**Enable secure operation of a European Grid infrastructure by developing security architectures, frameworks and policies to allow deployment of Grid on a production scale”.

- **Together with JRA1, SA1, NA4, and international collaboration parties, esp. OSG, this is in place. BUT - as pointed out by the Security Assessment document - there is a continous work on improvements ahead:**

  ”Security is a continuous arms race: new threats trigger new countermeasures, and the bar is continuously raised. As such, our global security architecture is also subject to constant change and evolution” (From the EGEE Security Arch. document)

Q&A