EGEE Grid Security (JRA3)

Fredrik Hedman

hedman@pdc.kth.se

Objectives

Enable secure operation of a European Grid infrastructure by developing *security architectures, frameworks and policies*.

Includes a requirements cycle with:

- definition of incident response methods and authentication policies, and

- the consistent design of security mechanisms for all core Grid services.

Also, address production needs of resource providers with regard to identity integrity and protection.

JRA3: areas to be addressed

- Basic Security Policy and Incident Response

- CA Trust

- Establishment and Policy Management

- VO Definition, Rights Delegation, and Scalability

- OGSA Web services security and site service access

- Control and auditing

- Site Usage Control and Budgeting

- Secure Credential Storage

JRA3 is run by people from Finland, Holland, Norway and Sweden

Partners

- Amsterdam: UvA, FOM(NIKHEF) (2+2)

- Bergen: UiB (1+1)

- Helsinki: UH-HIP (1+1)

- Stockholm, KTH/PDC (2+2)

Tasks first 6 months

- [Stockholm] M03 MJRA3.1 User requirements survey

- [Amsterdam] M03 MJRA3.2 Set-up of the PMA for European CAs

- [Helsinki?] M04 MJRA3.3 OGSA SEC service initial recommendations for reenigneering

- [Stockholm] M05 DJRA3.1 Global security architecture

- [Amsterdam] M06 MJRA3.4 Security operational procedures and incident handling; definition of a common Grid incident format

- [Stockholm] M03 MJRA3.1 Completed user requirements survey defines effort redistribution over action lines.

  Collect and summarize already existing documents from EDG and LCG (others?). If necessary conduct survey.

  Summarize, define and clarify scope, prioritze.

  Circulate summary. Collect responses and take reactions into account.

First 6 months (II)

- [Amsterdam] M03 MJRA3.2 Set-up of the PMA for European CAs; liaison with the corresponding CAs outside of Europe;

  - What of the catch-all CA? (document + standing committee)

  - Setup PMA.

  - Define CA and EGEE interaction.

- [Helsinki?] M04 MJRA3.3 OGSA SEC service initial recommendations for reenigneering

Joni Hakkala?

More web services in general, rather than just OGSA specific. This milestone is rather hazy. Use survey to find out what is really needed. Items to include in manual: coding practices, experience from other sources, peformance tips (session or messag security)? FAQ/wiki.

- [Stockholm] M05 DJRA3.1 Global security architecture

  - Security is a process

  - Practical and concrete

  - Global as in "not tied to any specific site"

  - What should be protected ?

    - assets to protect?

    - what risks?

    - how well does the solution mitigate risks?

    - what other risks does the solution introduce?

    - what trade-offs does the solution require?

- [Amsterdam] M06 MJRA3.4 Security operational procedures and incident handling; definition of a common Grid incident format

  To what detail? Use existing documents (LCG, CERT).

  Define interactions with local CERT. What about

  intrusion detection systems (ids)? Incident response?

  Logging and system consistency; port scans, software integrity.

Training requirements

- TBD

-

Risk Analysis

- TBD

-

Issues related to other activities

- JRA3 and other JRAx

- JRA3 and SA1?

- EGEE and LCG?

- EGEE CA interaction?

Requested changes to TA

- None at the moment...

- people

- effort

- What tasks can start early?

- Visit with Bergen, Amsterdam, Helsinki

- Regular phone conf startup

- Web pages

- ?

Objectives of Security Activity (JRA3)

Enable secure operation of a European Grid infrastructure by proposing and developing:

- Overall security architecture and framework

- Policies to be adopted by other EGEE activities (mware, operations etc.)

to allow deployment of a secure Grid on a production scale.