EGEE-III SA1 Security Tasks Transition to EGI

David Kelsey (STFC)

SA1 meeting, Amsterdam, 1 Feb 2010

Security - EGEE-III to EGI

- **SA1 Grid Security today (TSA1.4)**
  - Operational Security Coordination Team (OSCT) - CERN
  - Grid Security Vulnerability Group (GSVG) - UK
  - Joint Security Policy Group (JSPG) - UK
  - Authentication Coordination (EUGridPMA and IGTF) - NL
- **Transition to EGI-InSPIRE**
  - TNA2.3 – Policy Development (**O-E-15** – UK/NL)
    - Security Policy Group (SPG) - UK
    - IGTF and EUGridPMA - NL
  - TSA1.2 - A Secure Infrastructure
    - EGI CSIRT (Old OSCT) – **O-E-16** - UK & NL
    - Software Vulnerability Group (SVG)
    - EGI Certificate Authorities – Distributions - NL

Policy Development

- **Build on EGEE-III successes**
  - Both under same leadership in EGI as in EGEE-III
  - No major issues
- **Security Policy Group (SPG)**
  - All security policies (will) have been revised during EGEE-III
    - These will be the policies for start of EGI
  - Transition well under way – meeting 25/26 March - NIKHEF
  - Future processes to be defined during first year of EGI
    - Likely to continue with relatively small (editorial) group
    - Already expanded JSPG to include more NGIs
    - More representation of users and sites welcome
    - Wider consultation for any new policies with all stakeholders
- **IGTF & EUGridPMA**
  - Build on strong starting point
  - EGI to become official RP member of EUGridPMA early on

EGI CSIRT

- **Today OSCT activities include:**
  - Security Incident Prevention and Handling
    - Security Service Challenges and Incident Response
  - Security Duty Coordinator (weekly rota)
  - Security Monitoring (SAM, Pakiti, Nagios, …)
    - *Not funded in EGI*
  - Security training and dissemination
  - Security advice and other issues
- **EGI CSIRT**
  - O-E-16 (UK and NL)
  - Individuals already playing leading roles in EGEE-III
  - Transition should be smooth – “business as usual”
  - Build on established trust relationships with NRENs and other CSIRTS
- **OSCT transition meeting – 22/23 March – Amsterdam**
  - NGI security officers can join now

Software Vulnerabilities Group

- **Included in EGI-InSPIRE TSA1.2**
  - But currently no explicit funding (or is just part of EGI CSIRT?)
  - There is no identified future funding for leadership of this activity
- **Main aims of SVG**
  - Eliminate existing vulnerabilities
    - Primarily in deployed middleware
  - Prevent introduction of new vulnerabilities
  - Prevent security incidents
- **Risk Assessment Team**
  - Assesses new vulnerabilities
  - Classifies according to risk, which defines urgency and timetable
- **Must work closely with middleware providers**
  - SLD between EGI and EMI (and others) will require participation in and acceptance of SVG
- **Draft EGI transition plan exists**
  - https://edms.cern.ch/document/1059512/1

Security - EGI transition issues

- **EGI CSIRT**
  - No explicit task/funding for development of Security Monitoring
    - A separate EU bid has been submitted by some partners
    - What happens if this does not succeed?
  - NGI funding is (of course) required to provide the effort
    - Will we achieve this?
  - Move from ROCs to NGIs
    - NGIs who do not have a security officer on day 1?
    - Assuming all ROC security contacts continue they should be able to provide initial cover
- **SVG**
  - No explicit funding for this activity
  - In particular, funding is required for SVG leadership