TSA1.2: A Security Infrastructure

Mingchao Ma
STFC – RAL, UK

TSA 1.2

- TSA1.2: A Secure Infrastructure

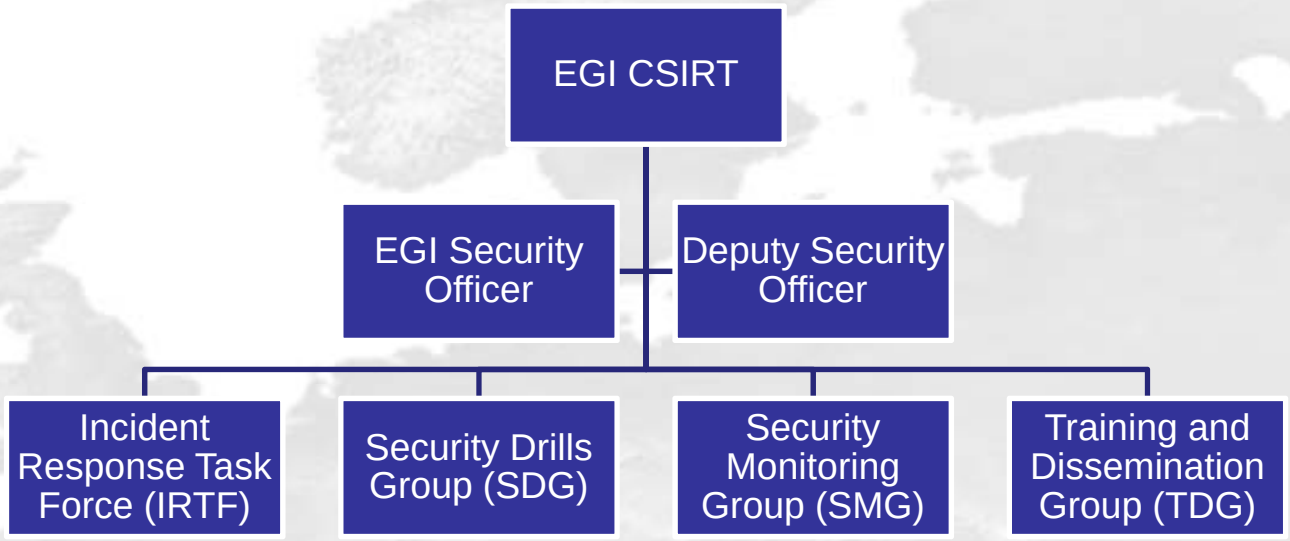
- “The aim of this task is to address the various operational security-related risks and to maintain the availability of EGI services. This task covers all aspects of **operational security** including Security Incident Coordination and **security vulnerability handling**. … … the **security related policy** work done under NA2. ”

TSA 1.2

- TSA1.2: A Secure Infrastructure

- The EGI Computer Security and Incident Response Team (EGI CSIRT)
  - coordinating the **operational security activities** in the infrastructure, in particular the response to security incidents
  - EGI CSIRT team combine efforts and resources from NGIs, each NGI must appoint a NGI security officer and provide NGI CSIRT function
  - Led and coordinated by the EGI Security Officer;
  - To replace EGEE OSCT team
- The EGI Software Vulnerabilities Group (SVG)
  - “The main purpose is to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents”
  - Led by SVG chair
  - To replace EGEE GSVG group

EGI CSIRT – Internal structure



- EGI CSIRT team is composed of NGI security officers
- A group coordinator has been appointed to each group
- https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

EGI CSIRT Activties

- Incident Response Task Force (IRTF)
  - EGI CSIRT duty contact rota
  - Security incident reponse
  - Security incident management
    - **Communication channels**
    - **Incident response tools development, evaluation and adaptation**
    - **Incident handling procedures update/maintenance**
  - vulnerability assessment

- Security Monitoring Group (SMG)
  - Pakiti development and maintenance
    - **https://pakiti.cern.ch/**
  - Nagios-based security monitoring framework development
    - **https://srv-102.afroditi.hellasgrid.gr/nagios/**
  - Explore other security monitoring tools
    - **E.g. user activites tracing tools**

EGI CSIRT Activties

- Security Drills Group (SDG)
  - Design and set-up realistic simulations of computer security incident scenarios.
  - Run/evaluate/disseminate the security drills at the project level
  - Provide a framework so that NGIs can run a particular security drill at some or all of their sites
  - Set up a "Sites-Readiness" web page where the results of the security drills are collected
  - Security Service Challenge 4 is ongoing, will finish in late June
- Training and Dissemination Group (TDG)
  - Plan and organize training events
  - Collect and archive training materials used in past events.
  - Support NGIs setting up local training events.
  - Develop training material
  - Setup and maintain EGI CSIRT public and internal wiki
  - Planning a security training session at 1st EGI technical forum

Transition

- Aim at maintaining normal day to day operation during transition period
  - Weekly duty contact rota
- Build up the team and restructure internal groups
- Setup communication channels
  - csirt@mailman.egi.eu with alias csirt@egi.eu and abuse@egi.eu
    - **For incident report**
  - EGI-CSIRT-Team@mailman.egi.eu
    - **EGI CSIRT team mailing list**
  - ngi-security-contacts@mailman.egi.eu
    - **NGI security officers/backups**
  - site-security-contacts@mailman.egi.eu
    - **Site CSIRTs**
- Setup EGI CSIRT wikis
  - Public wiki: https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
  - Private wiki: https://wiki.egi.eu/csirt/
- Updating security incident handling procedure
- SSC 4 is ongoing

Y1 Milestones

- MS405 Operational Security Procedures PM3
  - Updating EGI Security Incident Handling Procedure
  - Based on current EGEE incident handling procedure
  - Expect to finalise the first version by end of June 2010
  - All NGIs should follow the procedure to report and handle security incident
- OMB should approve the procedure on behalf of EGI?
- EGI Security Policy?

Roadmap for Y1

- Maintain normal operation
- Finalise operational security procedures
  - Incident handling
  - Vulnerability assessment
- Setup communications
  - NGIs
  - Other security groups such as SSG, SPG, EUGridPMA
  - Peer Grids
  - NREN CSIRTs
- Collaboration with peer Grids such as WLCG, OSG
- SSC, security monitoring tools development and training etc.

Issues

- Confusion about the concept of “NGI International task”
- Can we have enough committeemen and manpower from NGIs?
  - EGI global task: 48 PM
  - NGI international task: ~ 350 PM
  - Some NGIs only commite very small fraction of manpower such as 3 or 4 PM over 4 years
- NGI security contacts information?
  - GOCDB
- Escalation procedure?
- Authority of EGI CSIRT?
  - E.g. Site, user suspension
- EGI security policy
- Security monitoring tools development
  - Increased work, but less effort

The EGI Software Vulnerability Group (SVG)

- Part of Task TSA1.2 “A Secure Infrastructure”
- The main purpose is “To eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware, prevent the introduction of new ones and prevent security incidents”
- The main scope is to deal with software vulnerabilities in the EGI UMD software distribution
  - Plus the effect of vulnerabilities in dependencies
  - And will look at other vulnerabilities that effect EGI on a case by case basis
- This is a larger scope than the EGEE Grid Security Vulnerability group
  - Which mainly focussed on gLite

SVG – Issue Handling

- Anyone may report an issue
  - By e-mail to report-vulnerability@mailman.egi.eu
- NGIs should be aware that vulnerabilities should be reported to this list
  - Not discussed on publically archived mailing lists
  - Not entered into publically readable bug handling systems
- Issue is investigated by a collaboration between the reporter, the developers, and the Risk Assessment Team (RAT)
- If an issue is found to be valid, the places it in one of four risk categories
  - Extremely Critical, High, Moderate or Low
- Target Date is set according to the Risk

  EC – 2 days, High – 3 weeks, Moderate – 3 months, Low – 6 months

SVG – issue handling (contd)

- It is then up to the developers and release team to get a patch released by the Target Date
  - SVG will provide help and advise when appropriate
- Advisory issued when patch is available or on Target Date – whichever the sooner
- Details will be revised for SVG
  - By those participating in the EGI SVG
  - Which provides incentive to participate!

SVG – call for participation!

- Membership mainly drawn from NGIs and those providing software to the EGI UMD
- Most the EGEE RAT members wish to continue in EGI
- Increased scope means we will need more people
  - By participating influence the process
  - As well as helping to ensure the software is secure!
- What is needed
  - RAT members
    - **to carry out investigations and Risk Assessments for issues reported**
    - **Typically 10% of members time or less**
  - Deputies
    - **Others to run process in addition to task leader – to provide cover for as many working days as possible**
    - **Of order 10%**
  - Others
    - **Anyone to look at code for vulnerabilities**
    - **Educators – to help developers produce secure code are welcome**

SVG Contact details

- If interested, please contact Linda.Cornwall@stfc.ac.uk
- General discussion SVG list available SVG-discuss@mailman.egi.eu
  - Membership moderated but anyone in EGI can join if interested