SA1 – Grid Security

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

http://www.eu-egee.org/security/

SA1 Transition Meeting

www.eu-egee.org

Information Society and Media

Top risks for the grid

- Attacks against other sites (ex: DDoS)
- Storage, distribution or sharing of illegal/inappropriate material
- Disruption of service, damage to user data

This can involve:

- Damage to the project/sites reputation
- Legal/financial actions against participants

http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html

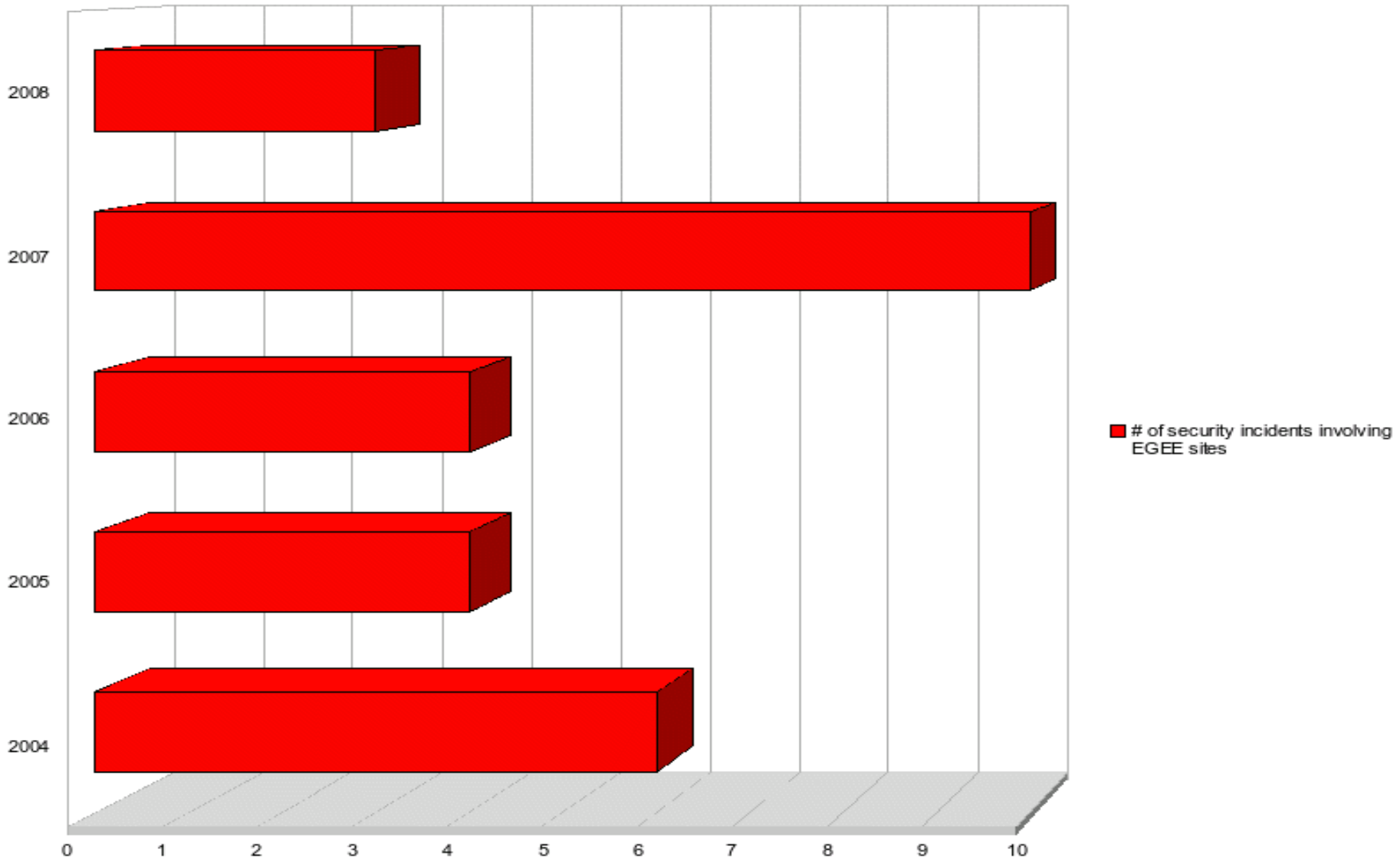
SA1 Security – Main Objectives

- **Provide a security framework to grid operations to:**
  - Understand the security threats faced by the infrastructure
  - Establish a common set of policies and requirements
  - Enable reliable authentication of the grid users and resources
  - Manage middleware security vulnerabilities identified in our infrastructure
  - Provide incident response capabilities for the participants
  - Promote security best practices at the sites
  - Monitor the infrastructure to detect possible security issues
  - Coordinate and resolve security incident
  - Provide guidance or expertise as part of day-to-day operations

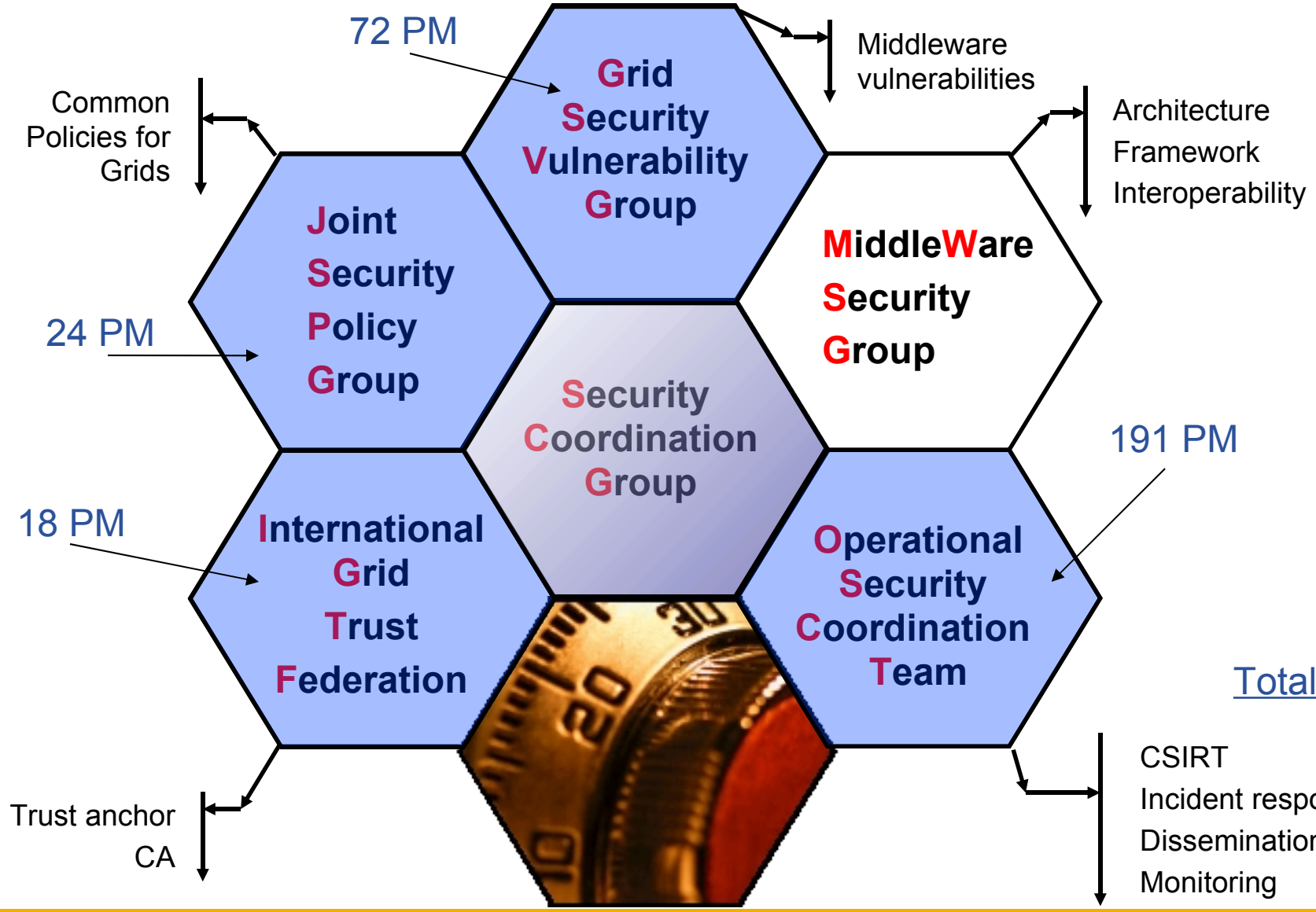
  etc.

- **Lots of tasks: structure and prioritisation needed**
- **Impossible to get agreed effort in EGEE-II: must to better in EGEE-III**

Security Incidents Statistics



EGEE Security groups



(Initial picture by Ake Edlund)

Plan for EGEE III

-

Operational Security Coordination Team (OSCT)

-

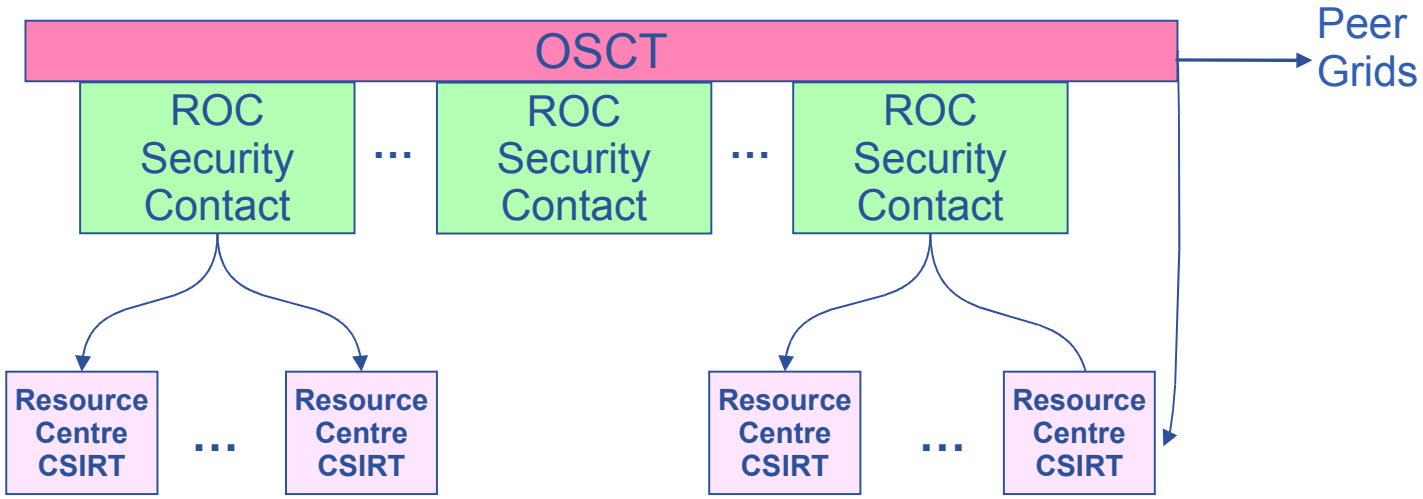
Chair: Romain Wartel

www.eu-egee.org

Information Society and Media

OSCT 1/8

- **ROC Security Contacts are part of the OSCT**
- **Chaired by the EGEE Security Officer**
- **ROCs provide resource for :**
  - Pan regional activities to improve security in the grid
  - OSCT-DC (Duty Contact) for day-to-day operations



The EGEE Operational Security Coordination Team has three main activities:

- **Incident response**
  - Security service challenges (SSC)
    SSC1, SSC2, *SSC3 (in work)*

    http://cern.ch/grid-deployment/ssc/SSC_2/SSC_2_google.html
  - IR channels (lists, IM)
  - IR Scenarios

- **Monitoring**
  - Several monitoring tools available to the sites
  - Central security Tests

- **Dissemination and training**
  - Best practice
    ex: https://cic.gridops.org/index.php?section=roc&page=securityissues
  - Training events

OSCT 3/8

- **Incident response are day-to-day operations are covered by the OSCT-DC (Duty Contact)**

- **Following the CIC agenda, each weak a ROC Security Contact becomes the OSCT-DC:**
  - Ensure security incidents are coordinated (if possible in the originating region)
  - Ensure GGUS tickets are handled the appropriate ROC

- **The role of the coordinator is to:**
  - Actively stimulate and probe the affected participants to obtain accurate information in a timely manner
  - Aim at understanding the exact cause of the incident, what assets have been compromised (credentials, etc.), and how to resolve the incident
  - Help involved sites to resolve the incident, by providing recommendations, promoting collaboration with other sites and by periodically checking their status

EGEE III plan

- **Similar structure to EGEE II**
- **Main activities coordination will be in the ROCs**
- **Meetings:**
  - Face-to-face meeting 2/year, organised by the ROC
  - Ops meeting: 1/week
  - Status report meeting: 1/month
- **Based on the DoW, each ROC contributes between 12 PM and 24 PM**
  - Need firm commitment from the ROCs to reach objectives
- **It is essential that the ROCs deliver the effort in EGEE-III.**

OSCT 5/8

- **Base level of efforts estimate: 8 PM per ROC** (Total: 88 PM)
  - The workload should increase as EGI becomes closer and as the other activities mature
  - Day-to-day issues
  - OSCT-DC
  - Issues detected by the monitoring tools
  - Work in the region (challenges, local events, etc.)
  - Contributions to JSPG
  - Contributions to EGEE deliverables
  - Meeting organisation
  - EGI planning and organisation

OSCT 6/8

- **Pan regional activities** (total: 103 PM)
  - The workload should decrease as the activities mature
  - Monitoring - Estimated efforts, all ROCs: **38 PM**
    - Activity coordination (CE?)
    - Monitoring contributions (RUSSIA?, ITALY?)
    - Detect and escalate grid-wide SAM problems
  - Incident response - Estimated efforts, all ROCs: **20 PM**
    - Activity coordination (SWE?)
    - Incident response channels (FRANCE?)
    - Incident response scenarios
    - Security service challenges (CERN?)
  - Training and dissemination - Estimated efforts, all ROCs: **35 PM**
    - Activity coordination (UK?)
    - Training and dissemination contributions (ITALY?, SWE?)
    - Website, communication and outreach (RUSSIA?)
  - Global architecture security review (UK?): **5 PM**
  - Audit (VO scheduler, Web applications, etc.): **5 PM**

Plan for EGEE III

-

Grid Security Vulnerability Group (GSVG)

-

Chair: Linda Cornwall

www.eu-egee.org

Information Society and Media

The Grid Security Vulnerability Group (GSVG)

- **Beginning of EGEE-II - stated aim - "to incrementally make the Grid more secure and thus provide better availability and sustainability of the deployed infrastructure"**
  - This continues to be the aim for EGEE-III
- **Main activity in EGEE-II was to handle specific Grid Security Vulnerability issues reported**
- **This involved setting up, agreeing, and getting approval of the process which involves**
  - Investigation and Risk Assessment
  - Setting a Target Date for resolution according to Risk
  - Releasing an advisory when a patch is released (or on the target date)
- **Setting up the infrastructure and the Grid Security Vulnerability Group webpage at http://www.gridpp.ac.uk/gsvg**
- **The Issue handling has reached a reasonable level of maturity, is well established and accepted, but there is still room for improvement**
- **Other activities included code reviews and testing which identified problems that have been or are being resolved**

Some numbers (10th April 2008)

- **133 issues entered since we started in 2005**
- **55 open (39 s/w bugs, 16 more general)**
- **Most issues are software bugs –**
  - Ask developers to fix
- **Some more general issues**
  - Design, missing functionality
  - These raised with other parties in EGEE
- **78 closed (soon we close about 12 more when glite 3.1/code in head fully rolled out.)**
- **Risk – all those fully assessed with EGEE-II criteria**
  - 1 Extremely Critical, 11 High (2 open), 15 Moderate (9 open), 19 Low (14 open)
- **Risk – all open s/w bugs**
  - 2 High, 9 Moderate, 14 Low, 2 not applicable, 12 Pre-EGEE2, 2 n/a (software not yet certified)
  - Pre-EGEE2 sites informed according to pre-EGEE2 process
- **25 advisories put on the web since July 2007**
  - Before then advisories were included in the release notes

GSVG Plans for EGEE-III

- **Issue handling will continue to be a largest activity (46 PM)**
  - Fine tune the process and interaction with other parties
  - Improve the quality of advisories
    - *possibly include who is at risk*
  - Improve the handling of issues that are not straight forward bugs on EGEE/glite Middleware
    - *By raising them immediately with other parties*
  - Aim to be fully tuned where non-resolution of issues in a timely manner is a rarity by the end of EGEE-III
- **Security assessment of services (8 PM)**
  - Carry out code walkthroughs of EGEE/glite services
- **Anticipation of Vulnerabilities (4 PM)**
  - Greater awareness of new types of vulnerability as they are identified in the broader software community, how to detect them and avoid them
- **Developer education (8 PM)**
  - Developer guidelines to avoid the introduction of new vulnerabilities, including newer types of vulnerabilities as they are identified
  - Developers should be aware of how to write secure code hence introduce less new vulnerabilities
- **Security Co-ordination Group participation, EGEE milestones and deliverables (6 PM)**

Plan for EGEE III

-

JSPG

-

Chair: Dave Kelsey

Joint Security Policy Group

- **JSPG mandate**
  - Jointly owned by EGEE and WLCG
  - Prepare and maintain security policies
    - *to be approved and adopted by Grid management bodies*
  - May also advise on any security matter
- **Vision for next 2 years**
  - Aim for simple, general and interoperable policies of use to many Grids
  - To allow VOs to easily use resources in multiple Grids (as move to EGI)
  - The policy set which specifies the policy needs for global interoperation
- **Main goals**
  - Revise all current security policies – even simpler and more general!
  - Of interest to and potential use by NGIs as we approach EGI.
- **Main challenges**
  - Little directly funded effort in EGEE-III
  - Must involve more ROC security contacts
  - Need to develop simple policies which will not conflict with NGI policy
  - Essential to get more participation from others, NGIs in particular
- **Important points for SA1**
  - ROC security contacts need to be more involved than in EGEE-II
  - Please provide pointers to appropriate NGI security contacts

Plan for EGEE III

-

EUGridPMA

-

Chair: David Groep

EUGridPMA and IGTF

- **EUGridPMA and IGTF**
  - The European Policy Management Authority for Grid Authentication in e-Science (hereafter called EUGridPMA) is a body to
  - establish requirements and best practices for grid identity providers
  - to enable a common trust domain applicable to authentication of end-entities
  - IGTF is the ensemble of the EUGridPMA and its two peers in the Asia-Pacific and Americas
  - Fully project independent, with support from European Research Infrastructures
- **Goals and vision for EGEE-III time span**
  - Ensure sound authentication trust fabric
  - Make it easier to obtain trustworthy credentials for the grid (using national federation technologies and SLCS style CAs)
  - Consider applying the best practices learned to more areas where cross-organisational trust is needed
- **Main challenges**
  - Can we grow the user base to encompass new end-users and communities?
  - Dealing with varying levels of assurance and credential qualities
  - Ensure the hard lessons on trust building learnt in PKI are not forgotten when we move to new buzz-word compliant technologies
- **Important points for SA1**
  - Management of the trust anchor distribution in EGEE operations must improve
  - Work out new deployment models that are scalable and less error prone!

Conclusion

- Need to build and maintain trust between the participants
- Increased expertise on multi-sites security incidents
- Security groups help the project to deal with security issues
- ...but they can't “solve security” by themselves
- Difficult to improve security practices
- Need contributions and support from all, and in particular from the ROCs

Discussion