SA1 – Grid Security

Romain Wartel

EGEE08 Conference, Istanbul, 23rd September 2008

Top risks for the grid

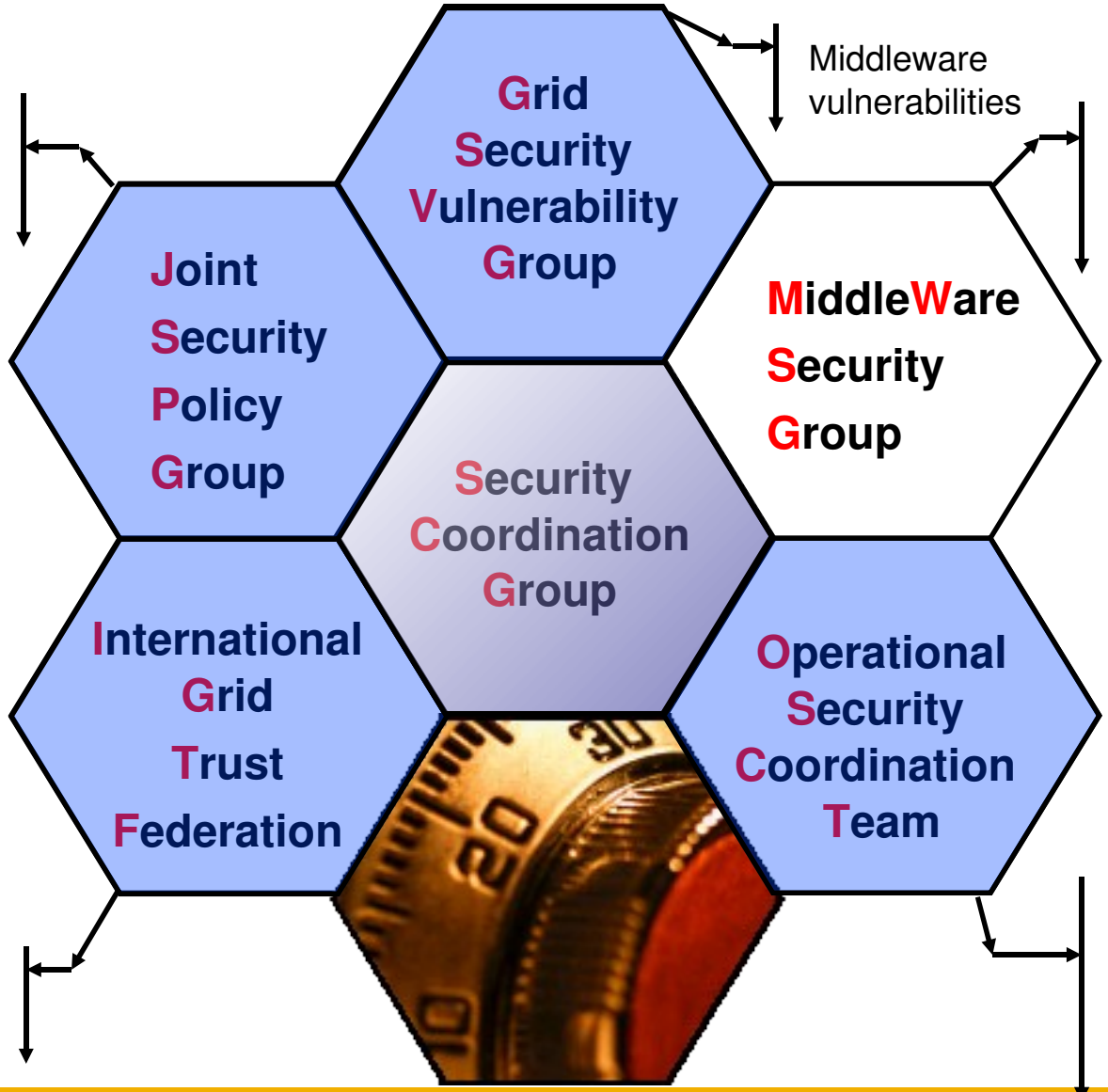
- Attacks against other sites (ex: DDoS)
- Storage, distribution or sharing of illegal/inappropriate material
- Disruption of service, damage to user data

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

EGEE Security groups



Middleware vulnerabilities

Common Policies for Grids

Architecture
Framework
Interoperability

Trust anchor
CA

CSIRT
Incident response
Dissemination / training
Monitoring

(Initial picture by Ake Edlund)

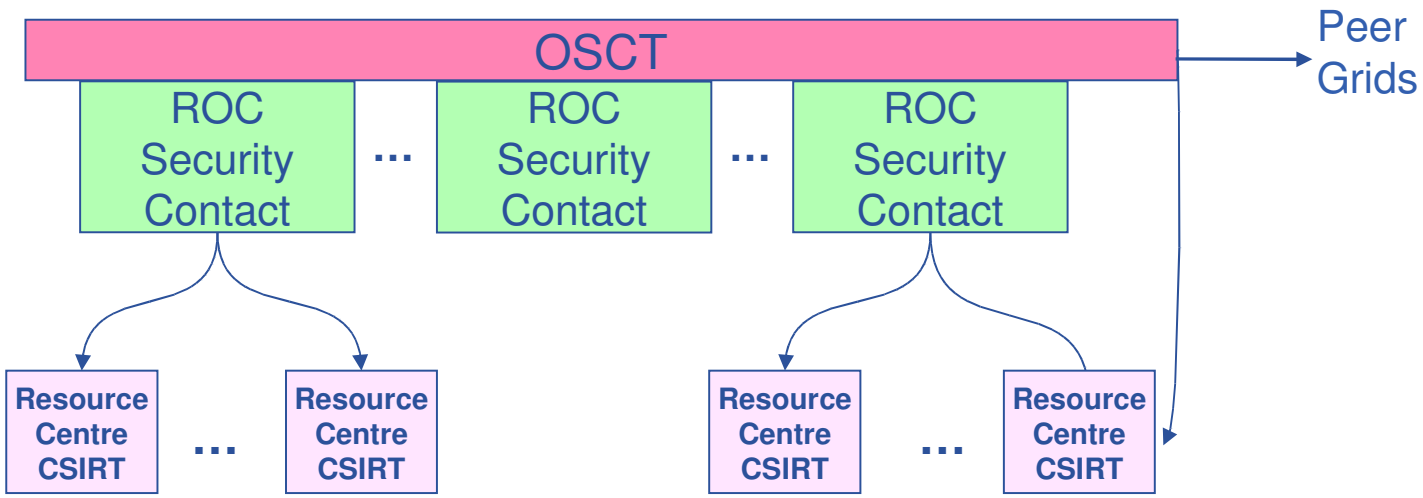
Operational Security Coordination Team (OSCT)

-

Chair: Romain Wartel

OSCT 1/4

- **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



OSCT 2/4

The EGEE Operational Security Coordination Team has three main activities:

- **Incident response** (activity lead: SWE ROC)
  - Security service challenges (SSC) (Activity lead: NE and CE ROC) SSC1, SSC2, SSC3
  - IR channels (lists, IM)
  - IR Scenarios

- **Monitoring** (activity lead: CE ROC)
  - Several monitoring tools available to the sites
  - Central security Tests

- **Dissemination and training** (activity lead: UK and AP ROC)
  - Best practice

  ex: https://cic.gridops.org/index.php?section=roc&page=securityissues
  - Training events

OSCT 3/4

- **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

OSCT 4/4

Progress and future:

- **Main activities being distributed in the ROCs**
- **But the team still suffers from lack of expected resources from several ROCs**
- **Incidents Response:**
  - Still no grid-based incidents
  - Effective incident handling structure (used for non-grids incidents so far)
  - Accumulated valuable experience
  - Need more specific guidance/metrics to improve (based on SSC)
  - Our model needs to scale (involve peer-grids, and NGIs)
- **Monitoring / Security Service Challenges**
  - Coordination with the OAT should help
  - SSC3 completed. Now being run within several regions
- **Training and dissemination**
  - Full review of our material in progress
  - Need to improve both the content and structure of the information
    - Objective: ease understanding and adoption by the sites

Grid Security Vulnerability Group (GSVG)

-

Chair: Linda Cornwall

The Grid Security Vulnerability Group (GSVG)

- **This was established in EGEE-II, continuing in EGEE-III**
- **Largest part of the work is the handling of specific Grid Security Vulnerability issues as they are found**
- **Process was set up, agreed and approved by the project**
  - Issues may be reported by anyone
  - Risk Assessment team Investigates the issue and places the issue (if valid) into 1 of 4 risk categories
    - Extremely critical, High, Moderate, or Low
  - Target Date (TD) for resolution set according to risk
  - Advisory released when patch issued, or on TD, whichever is the sooner
  - Release notes refer to advisory, advisory refers to the release notes
- **144 issues submitted since work started in**
  - 93 closed (49 fixed, 15 invalid, 5 duplicates, 5 software no longer in use, 10 general concerns, 9 OSCT informed)
  - 51 open (Including 3 before TD, 15 general concerns/missing functionality, 14 disclosed (still open)

GSVG - future

- **Issue handling will continue to be a largest activity**
  - 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
- **Anticipation of Vulnerabilities**
  - 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**
  - 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
- **GSVG web page (including advisories) at http://www.gridpp.ac.uk/gsvg**

Plan for EGEE III

-

JSPG

-

Chair: Dave Kelsey

Joint Security Policy Group

- **JSPG mandate (http://www.jspg.org/)**
  - 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 policy matter
- **Four policies recently approved**
  - CA Approval, VO Operations, Pilot Jobs, Traceability and Logging
- **Vision for rest of EGEE-III**
  - 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)
- **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

- **The European Policy Management Authority is a body to:**
  - establish requirements and best practices for grid identity providers
  - 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**
  - So far the grid actually made the sites **more** secure!
- **A change in our incident response model will be needed to scale**
- **Difficult to improve security practices at the sites**
- **Security groups help the project to deal with security issues**

...but they can't “solve security” by themselves

- **Need contributions and support from all, and in particular from the ROCs**

Discussion