Grid Security – An Introduction

Mingchao Ma, STFC – RAL, UK
GridPP Security Officer
UKI ROC Security Contact
Operational Security Coordination Team

EGEE'08 Istanbul, 23 September 2008

Science & Technology Facilities Council

Information Society and Media

Contents

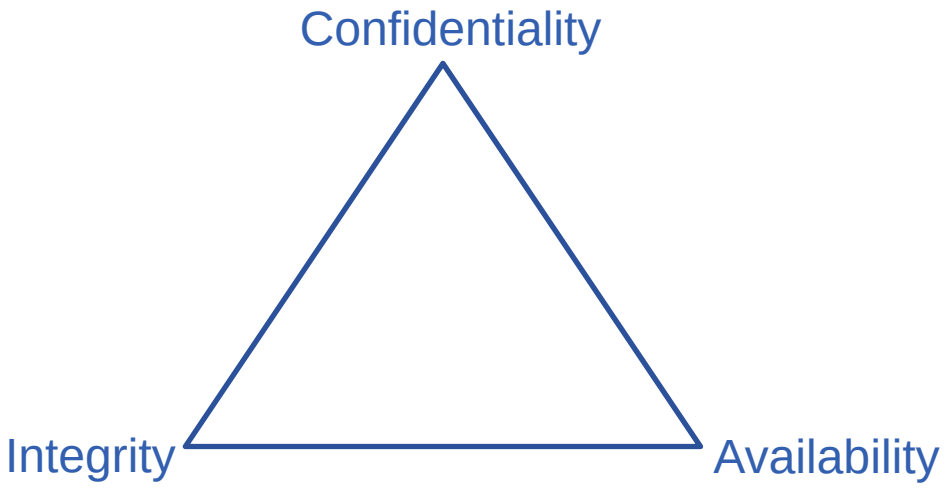
- Information Security in the context of Grid Computing
- The Risk
- The “Unique” Challenges
- EGEE Security Groups
- OSCT Activities
- Conclusion and Discussion

Information Security in the context of Grid Computing

Anything NEW?

Security Triad

- **Fundamental principle of security – AIC Triad**
- **Confidentiality**
- **Integrity**
- **Availability**



The “Unique” Challenges?

The “Unique” Challenges

- **Communication**
  - How to create and maintain a clear & up-to-date communication channel?
- **Blur Security Domain Boundary/Perimeter**
  - Transparent access to Grid resources
- **Security Monitoring at different levels (Site, ROC and Grid)**
  - Security events such as vulnerability, patch, log, scanning, attack and intrusion etc;
  - Balance of Privacy & Security – how to share sensitive information among sites, ROCs across the Grid?
- **Security Assessment/Audit**
  - Determine/verify that security controls are implemented correctly and operated as intended, but HOW?
- ... ...

The Risk?

The Risk

- **Attacks against other sites (ex: DDoS)**
- **Storage, distribution or sharing of illegal/inappropriate material**
- **Disruption of service, damage/lose of user data:**
  - Damage to the project/sites reputation;
  - Legal/financial actions against participants;
- **And more … …**

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

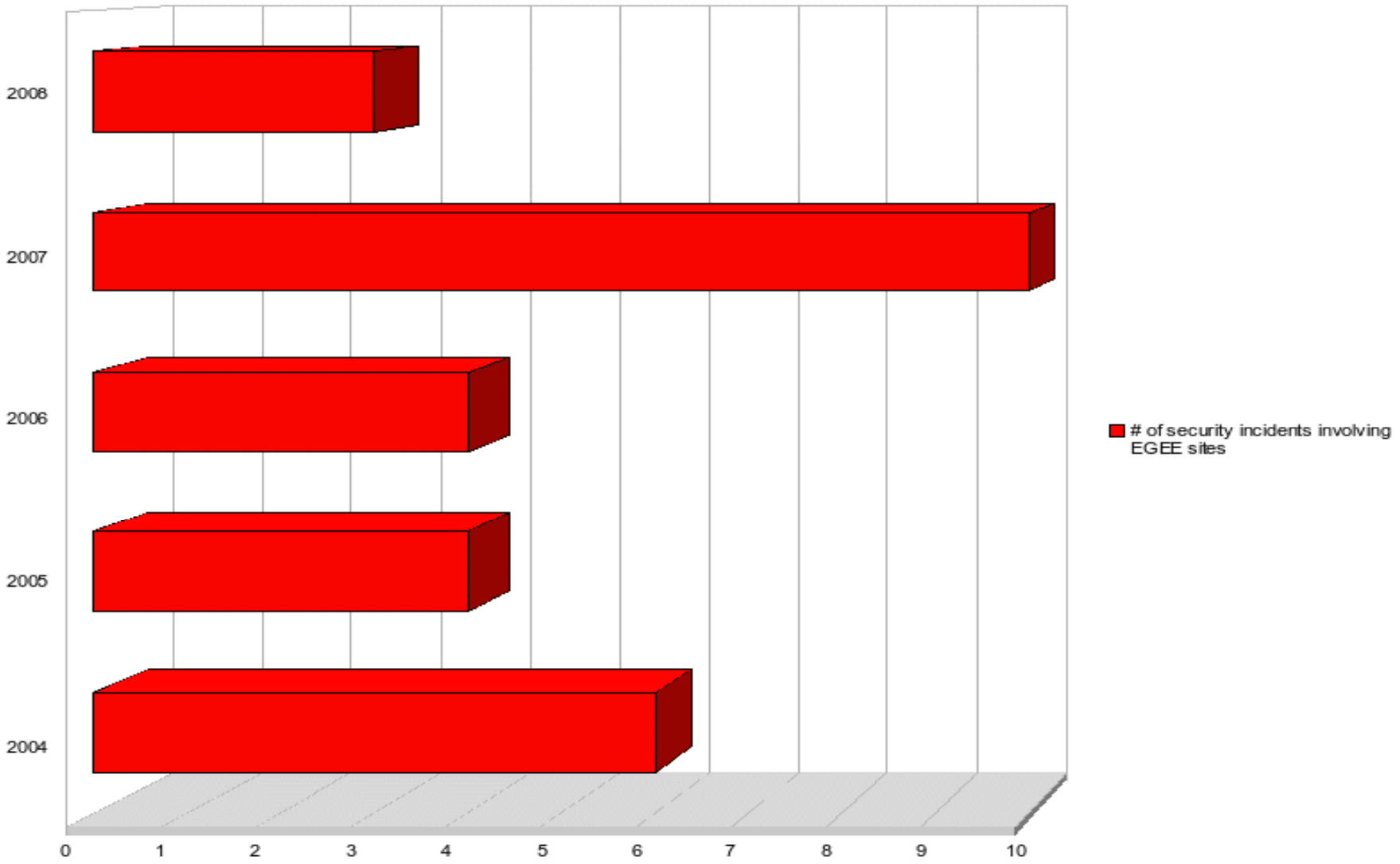
The Threat

- **Attacks from individuals**
  - motivated by fame, ego, self-satisfaction: scripting kids
  - Hacker for financial benefit or political motivation
- **Organised crime syndicate**
  - motivated by money
  - large-scale attacks
  - professional attackers
  - better-designed and smarter malicious code
- **Spams and Botnet is part of underground economy**
  - Top 11 Botnets sending SPAM (RSA conf, April 2008):
    - ~ 1 Million hosts
    - > 100 Billion SPAM emails per day
    - One SPAM message may be tied to up to 10 different organisations

The Grid

- **Grids are not (yet) a primary target**
  - Currently ADSL hosts are the easy/popular target (Botnets)
  - But this may change soon
- **Grids are valuable to attackers:**
  - **Large numbers of distributed hosts**
  - **High availability**
  - **High throughput network**
- **Grids are also particularly exposed**
  - **Transparent access/attack propagation from one site to another**
  - **Large number of identical hosts**
  - **Heterogeneous skills, staffing and security standards**
- **So far no "grid incident" ... but will happen (where the grid is the attack vector)**
- **A few incidents per year within the grids (see next slide)**

Grid Incident Statistic



Common Cause

- **From a site perspective, the incidents are often caused by:**
  - **Failure to apply security patches provided by vendors**
  - **Poor access control management (ex: root password)**
  - **Incidents at other sites**
  - **Unresolved past security incidents (lack of traceability)**
  - **Incorrect risk assessment (threats were not correctly identified)**
  - Shared user community, staff and computing resources between grids and HEP sites make propagation easier

Security Management

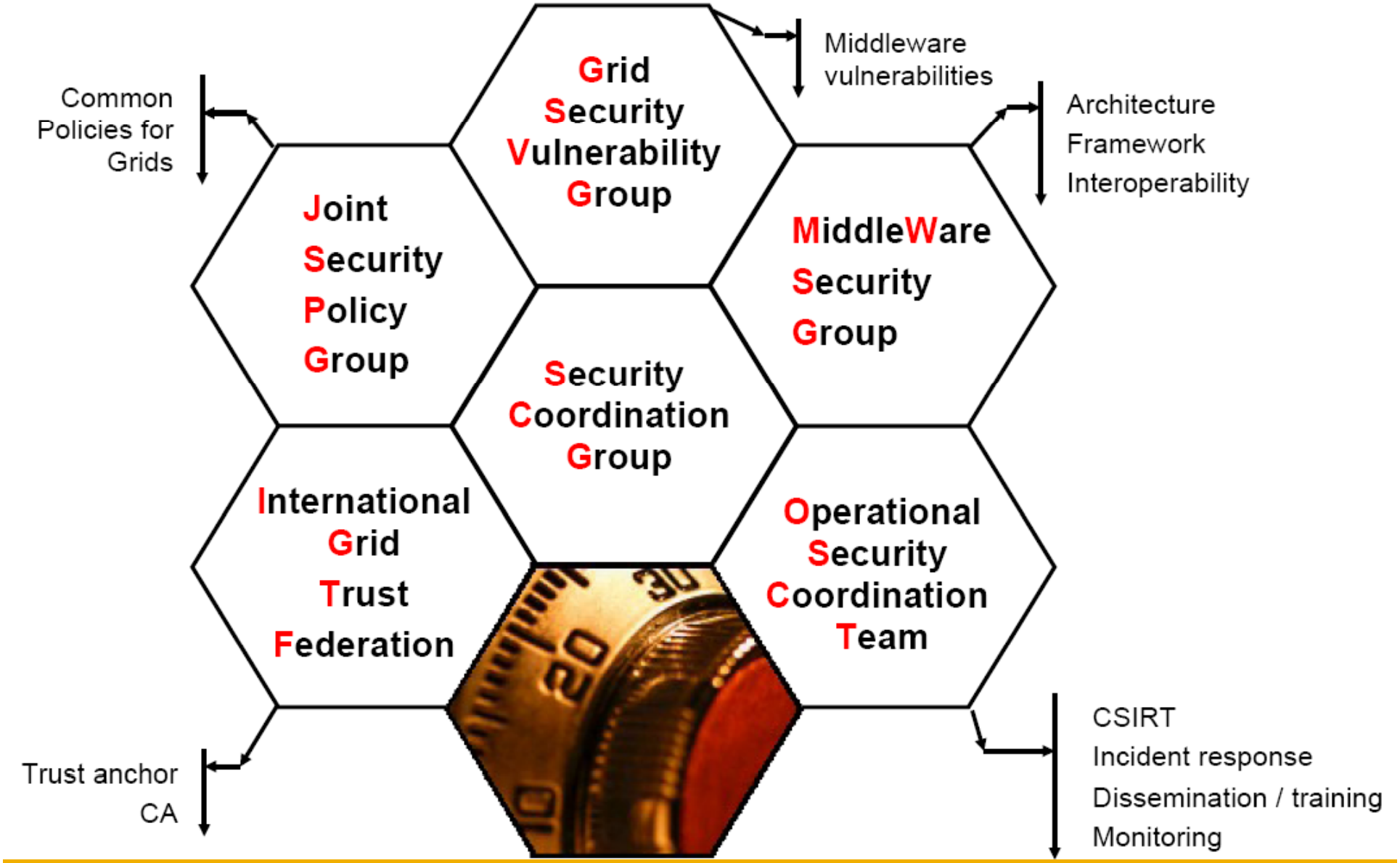
- **Risk management**
- **Security policy**
- **Security procedures, standards, guidelines, baselines**
- **Information classification**
- **Security education and awareness**

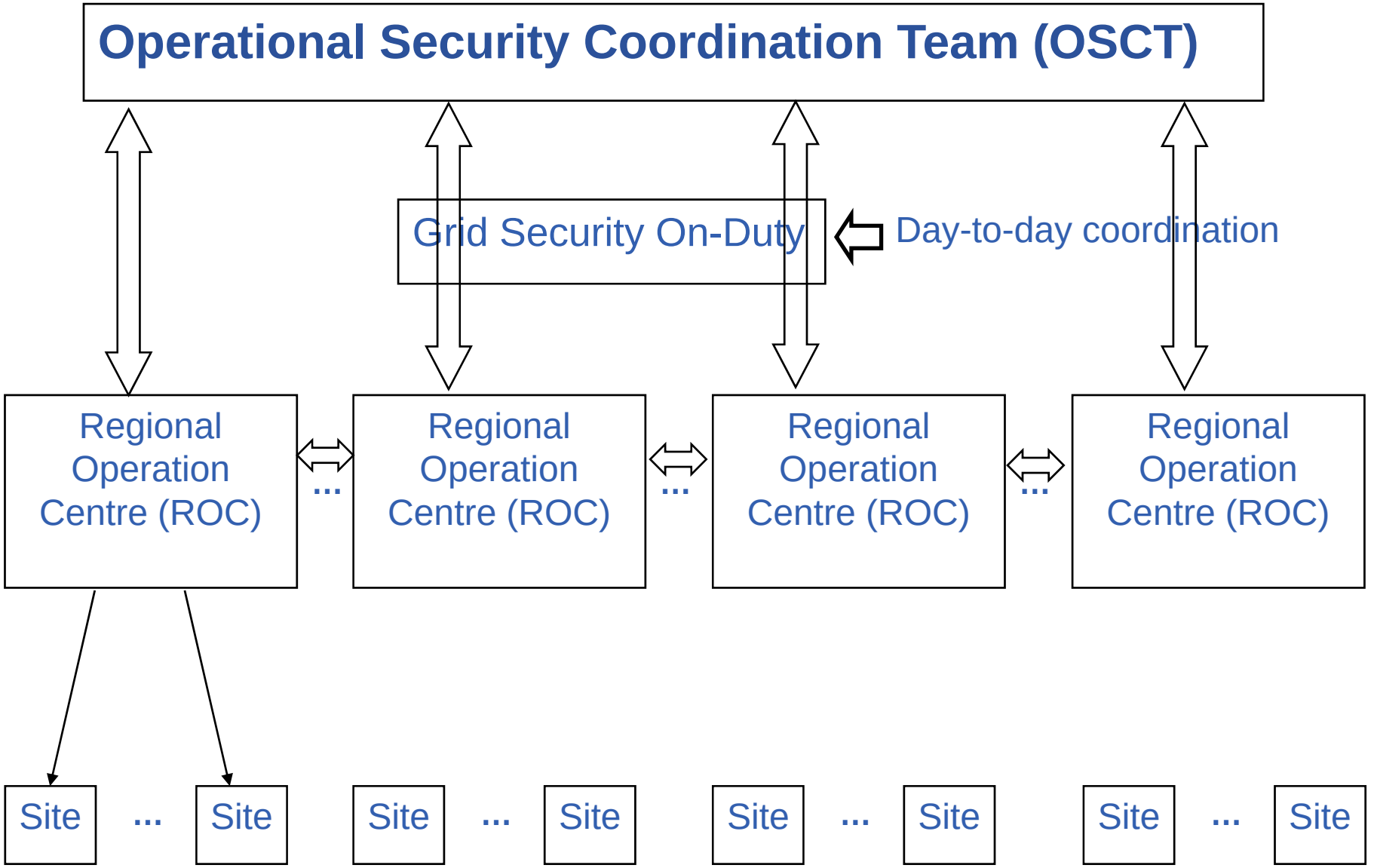
Risk Management

- **Computer Security is about understanding & managing the RISK**
- **Risk assessment**
  - Transfer
  - Avoid
  - Reduce
  - Accept
- **Balancing costs vs. benefits**

- **No perfect security**
- **The goal is to reduce the risk to an acceptable level**

EGEE Security Groups




Operational Security Coordination Team (OSCT)
Grid Security On-Duty
Day-to-day coordination
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
...
...
...
Site
...
Site
Site
...
Site
Site
...
Site
Site
...
Site

OSCT Activities

- **Weekly telephone meeting; Twice F2F meeting per year**
- **Work together with other security groups to improve Grid security;**
- **Provide security expertise to sites;**
- **Handling and mitigating Grid security incidents**
  - Procedures; Incident tracking; IR Channel (list, IM) and Security Service Challenges;
- **Best practice, training and dissemination**
  - Security RSS feed; OSCT website/Wiki; Training events
- **Security Tools (monitoring, detection and prevention)**
  - Pakiti; SAM security tests
- **Analysing and evaluating security risks/vulnerabilities (together with GSVG)**

Conclusion

- **Grid is a valuable target**
  - Lot of powerful, but distributed hosts
  - High bandwidth connection
- **Grid is also particularly exposed**
  - transparent access to resources & very well interconnected
  - Similar/identical systems (OS and Grid middleware)
- **Ways to improve:**
  - Training and dissemination (require significant efforts)
    - Both users and system administrators/site managers
  - Ability to test and monitor the Grid
  - Cooperation and sharing between sites and with peer grids
  - Building up expertise/experience in the team
  - Security management is the key

Links and Support Contacts

EGEE Security

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

OSCT website and Wiki

http://osct.web.cern.ch/osct/

https://twiki.cern.ch/twiki/bin/view/LCG/OSCT

Security RSS feed

http://rss-grid-security.cern.ch/rss.php

Vulnerability reporting

- grid-vulnerability-report@cern.ch

Incident reporting

- project-egee-security-support@cern.ch
- Incident response procedure
  - https://edms.cern.ch/document/867454/

Discussion