Operational Security Coordination Team

Romain Wartel
OSCT Chair

EGEE'07 Conference, Budapest, Hungary

www.eu-egee.org

Information Society and Media

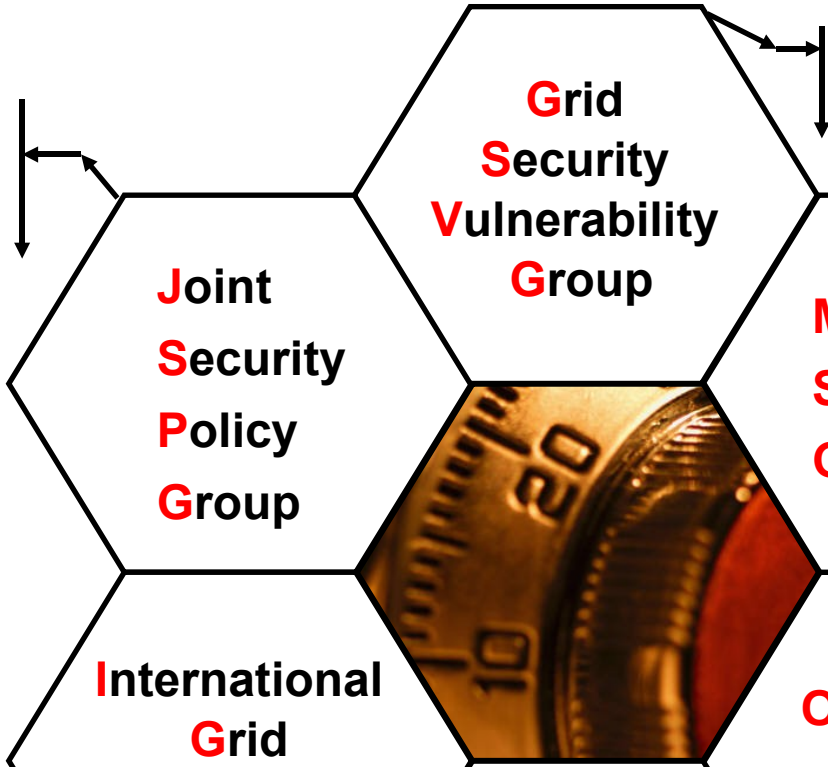
The Risks

- **Impact on the reputation of the project and of the partners**
- **Launch attacks on other sites (DDoS, Spam, ...)**
  - Large distributed farms of machines
- **Damage caused by viruses, worms, etc.**
  - Highly interconnected and novel infrastructure
- **Service disruption by exploitation of security holes**
  - Complex, heterogeneous and dynamic environment
- **Illegal or inappropriate distribution or sharing of data**
  - Massive distributed storage capacity

Exposure

- **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 the other
  - Large number of identical hosts
  - Heterogeneous skills, staffing and security standards
- **A few incidents happen per year within Grids**
- **So far no "grid incident" ... but will happen**
  (= where the grid is the attack vector)

Security Collaboration in the LHC Grid



Grid Security Vulnerability Group

Joint Security Policy Group

MiddleWare Security Group

International Grid Trust Federation

Operational Security Coordination Team

Software vulnerabilities

Common Policies for Grids

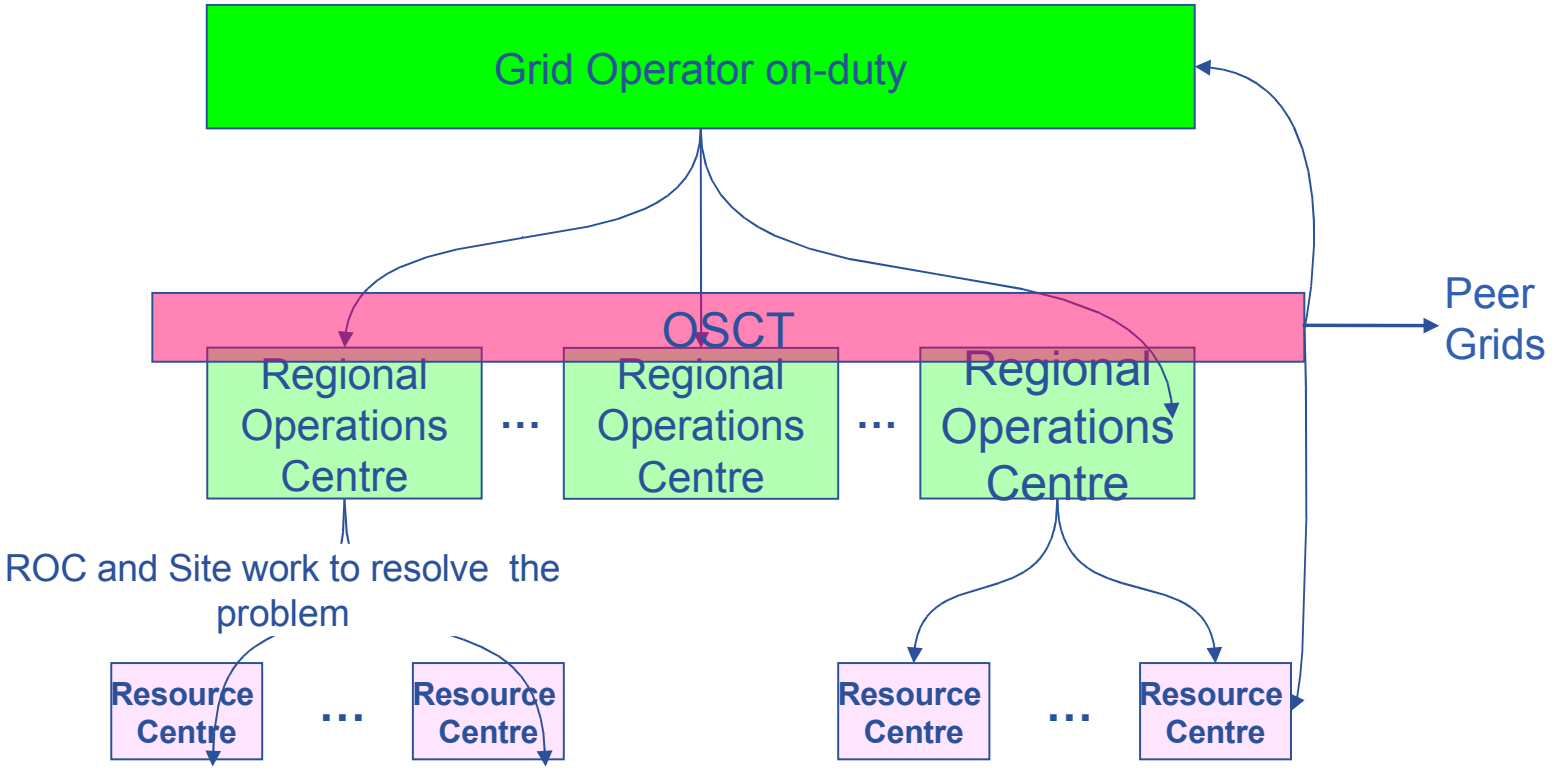
Architecture
Framework
Interoperability

Trust anchor
CA

Operations
Best Practice
CERTs/CSIRTs

(Initial picture by Ake Edlund)

Operations Support Model



slide from Ian Neilson

Security incident prevention

The EGEE Operational Security Coordination Team has three main activities:

- **Incident Response improvement**
  - Security service challenges (SSC)
    SSC1, SSC2, *SSC3 (in work)*
  - IR channels (lists, IM)
  - IR Scenarios

- **Security Monitoring**
  - Several monitoring tools available to the sites
  - SAM Security Tests (pilot stage)

- **Incident prevention**
  - Recommendations and dissemination
    ex: https://cic.gridops.org/index.php?section=roc&page=securityissues
  - Training (2 sessions for site admins at EGEE 07!)

Progress review

- **Main improvements during EGEE-II**
  - Team members are on rota to ensure timely response to operational issues
  - ROCs are more involved in pan-regional activities (ex: training, IR procedure)
  - Security Service Challenges (SSC) remain very useful. All the ROCs have performed a SSC
  - The team is now more cohesive
  - Good participation to meetings
- **But:**
  - Most ROCs are unable to deliver agreed efforts (TSA 1.4.1)
  - Several ROCs are unable to contribute to any activity other than the rota

Objectives

- **Objectives before the end of EGEE II**
  - Continue to handle day-to-day security operations
  - Integrate (sensors, alerts, tickets) more (relevant) security tests in SAM
  - Provide a coherent set of recommendations
  - Provide a set of training modules
  - Complete Security Service Challenge 3
  - Gather more expertise within the team (volunteers welcome!)

Conclusion

- Important milestones have been achieved
- Several key objectives for EGEE II
- Need to gather more expertise in the team
- But support from the ROCs is essential to do this
- 2nd training event on Thursday (Roma: 11:00 – 12:30)

Thanks to all the speakers!

Questions / discussions