Interactions between OSCT and MWSG

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

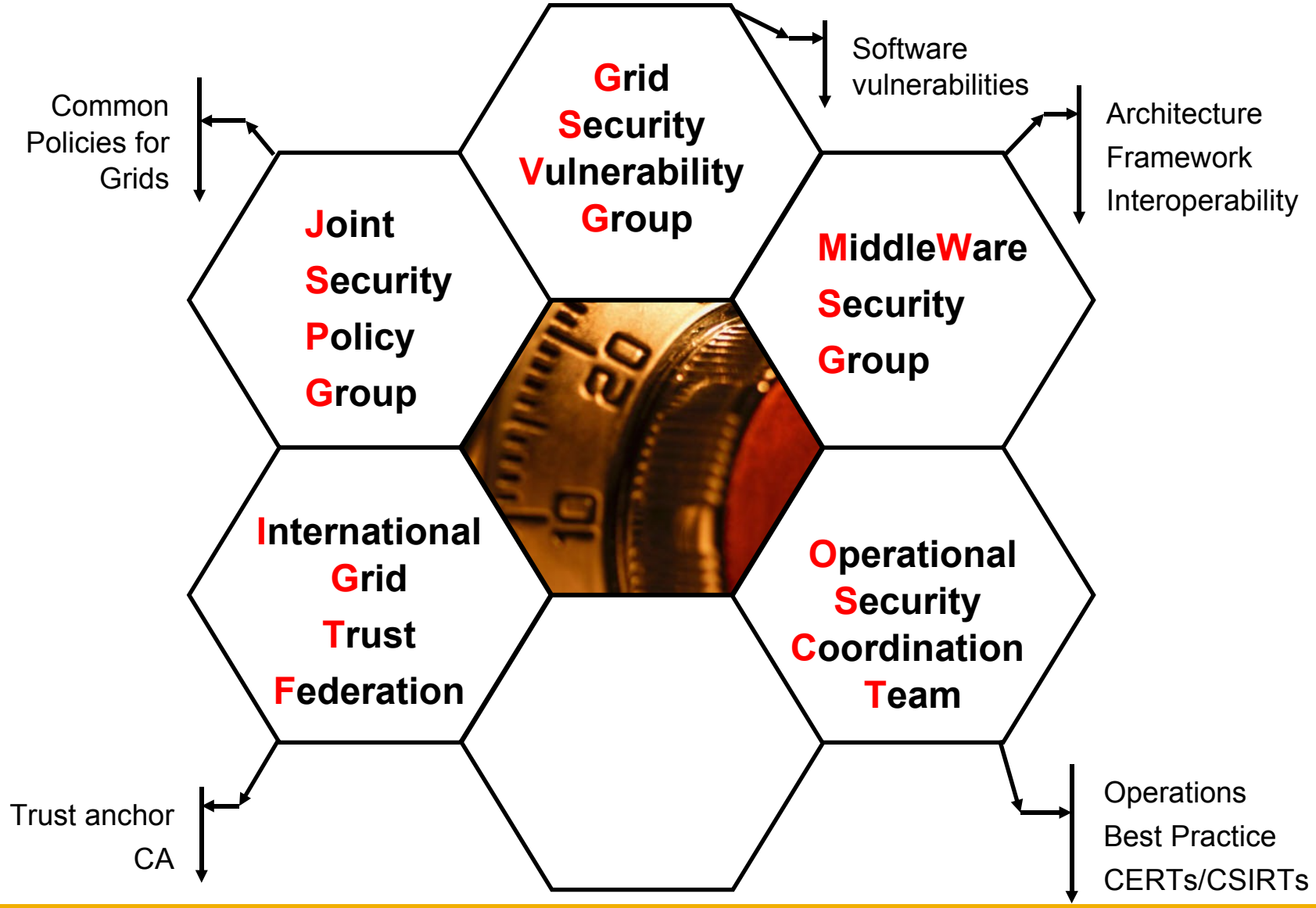
MWSG meeting, 27-28 March 2008

www.eu-egee.org

Information Society and Media

EGEE and gLite are registered trademarks

EGEE Security groups



(Initial picture by Ake Edlund)

The Risks

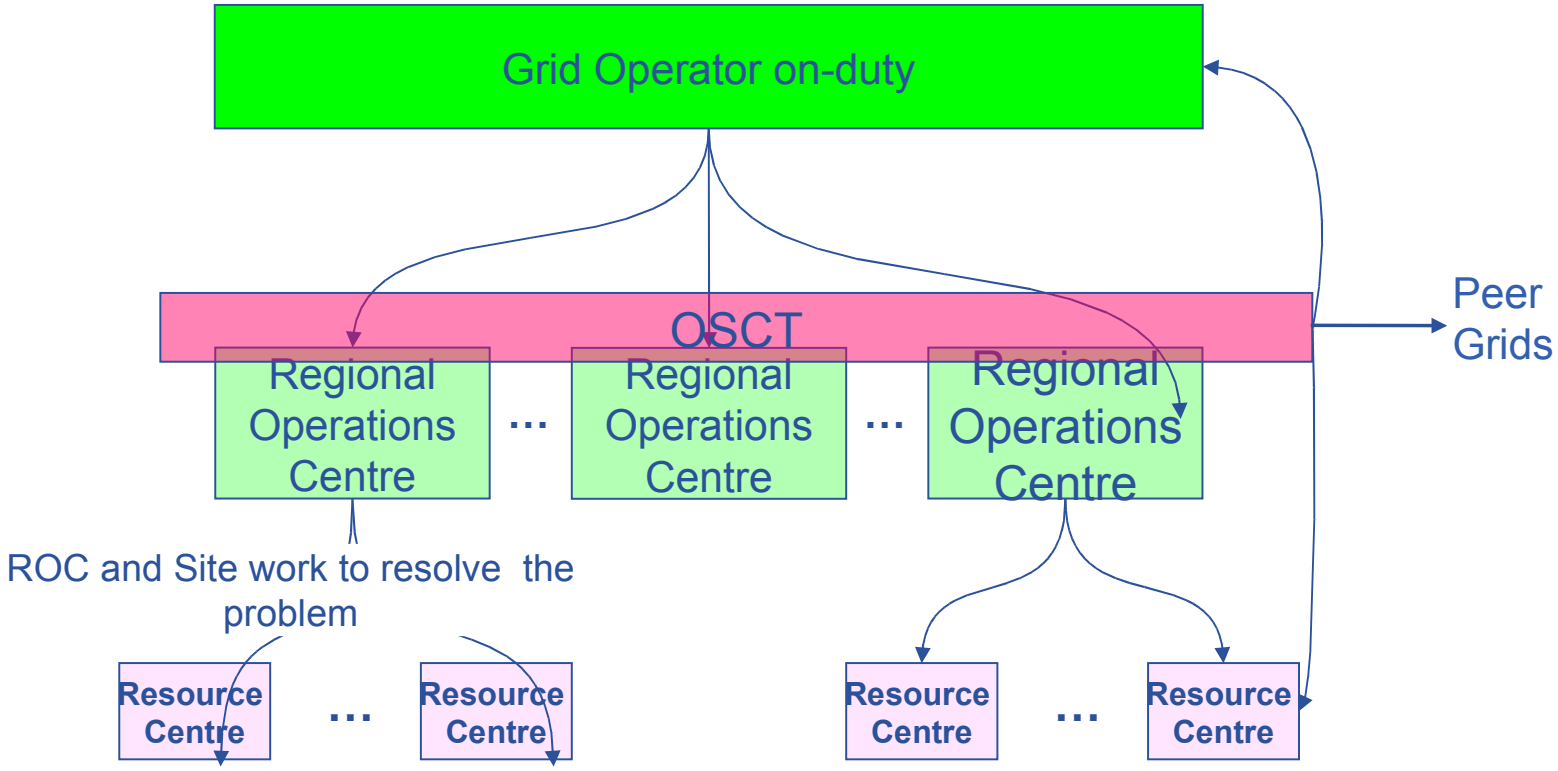
- **Top risks from Security Risk Analysis**
  - *http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html*
  - Launch attacks on other sites
    - Large distributed farms of machines
  - Illegal or inappropriate distribution or sharing of data
    - Massive distributed storage capacity
  - Disruption by exploit of security holes
    - Complex, heterogeneous and dynamic environment
  - Damage caused by viruses, worms etc.
    - Highly connected and novel infrastructure

slide from Ian Neilson

Policies

- **JSPG is producing a set of security policies**
- **The following policies have been approved by the EGEE PEB and the WLCG GDB**
  - Grid Security Policy (= top level policy)
    - Grid Acceptable Use Policy
    - Grid Site Operations Policy
      - *Site Registration Policy*
      - *Audit Requirements Policy*
      - *Grid Security Incident Response Policy*
    - VO Security Policy
      - *VO Operations Policy*
      - *User Registration Policy*
    - Approval of Certification Authorities

OSCT



slide from Ian Neilson

OSCT activities

- **Incident response improvement**
  (ex: Procedures, likely scenarios, Security Service Challenges, Incident tracking, reporting channels, etc.)

- **Training and dissemination**
  (ex: OSCT websites, Security RSS feed, training events, etc.)

- **Security tools (monitoring, detection, prevention)**
  (ex: Pakiti, SAM Security tests, etc.)

These activities have been divided into different tasks, which are spanned across the ROCs

Objective: reducing the likelihood and impact of security incidents

Impact on MWSG

EGEE and gLite are registered trademarks

Key policy for MWSG

- **"Grid Security Traceability and Logging Policy" (draft)**

  https://edms.cern.ch/file/428037/2/Traceability-Logging-v

- **In particular Section 3 and 4:**
  - "Identifying the cause of incidents is essential to prevent them from re-occurring"
  - "it is a goal to contain the impact of an incident while keeping services operational"
  - "The minimum level of traceability[..] is to identify the source of all actions [..] and the individual who initiated them"
  - "sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational"
    "It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user"
  - **"In order to satisfy the traceability requirements, software deployed in the Grid MUST produce sufficient and relevant logging. The software SHOULD follow the Grid security guidelines on logging but MUST include the ability for a Site to collect logs centrally."**

Incident response - Traceability

- **Sites must have the ability to trace the activity from the WN back to the originating UI**
- **Usual questions include:**
  - What are the 10 last jobs executed on CE foo.bar?
  - When have been executed the 5 last jobs from DN /C=CH/O=CERN/OU=GRID/CN=John Doe 0001?
  - Where have been executed the 10 last jobs scheduled by RB foo.bar
  - What executables have been run on CE foo.bar since yesterday?
  - How many distinct certificates have been using myproxy server foo.bar (and list them)?
  - What DNs have been mapped to UID 11111 on CE foo.bar in the past week?
  - When and where did we first see this DN (from where and what did to do)?
- **Several weeks/months may happen between the incident and its discovery**
- **There is currently a major problem with logging and traceability**

Incident response - Controls

- Sites must have the ability to suspend a user or a group of users centrally
- Grid operations should have the same ability
- The job or credential status (proxy, renewal) is irrelevant
- Several VOs use one week long proxies.
  The concept of 24h proxies is no longer true, major discrepency with the initial security design
- Often loose several/many credentials at once (sometimes > 1000), exposed or compromised and that may need to be blocked at all sites
- Sites must be provided with clear documentation on how to ban users on their services (WMS, CE, SE, etc.)
- There is currently a major problem with access control

Monitoring

- **There is currently very little Grid-specific security monitoring**
  - SAM Security tests (private)
  - Pakiti
- **Objectives:**
  - Check if the sites are following basic security principles
    - *patching*
    - *software configuration*
    - *etc.*
  - Detect incidents before they happen (data mining)
    - *Record all job submissions patterns*
    - *Detect suspicious changes*
- **Problems faced:**
  - Provide monitoring tools as third parties 'adds-on' does not work well
  - Functionalities offered by existing frameworks like SAM are limited
  - We do not have the ressources to provide monitoring features in gLite
- **MWSG view on this?**

Training and dissemination

- **Clear documentation for the sites is needed**
  - How to improve the configuration their services in terms of security
  - Ideal configurations, common mistakes, etc.
  - Node types that should not be mixed
  - etc.

- **Clear procedures are needed:**
  - How to suspend users
  - How to suspend a site
  - How to disable a particular service
  - How to remove services from the information system
  - etc.

Operational experience - Theory

- **Typical incident (theory)**
  - Incident is reported to the EGEE CSIRTs
  - All sites investigate locally
  - An incident coordinator manage the incident (from the OSCT)
  - Affected sites communicate with the coordinator and the other sites
  - The coordinator ensure a sufficient and relevant information flow between the sites and other participants (projects, peer grids, etc.), and aims at understanding the exact cause of the incident
  - Incident understood, corrective actions taken

- **Sites are bound by**
  - the incident response policy (JSPG)
  - the EGEE/LCG incident response procedure (OSCT).

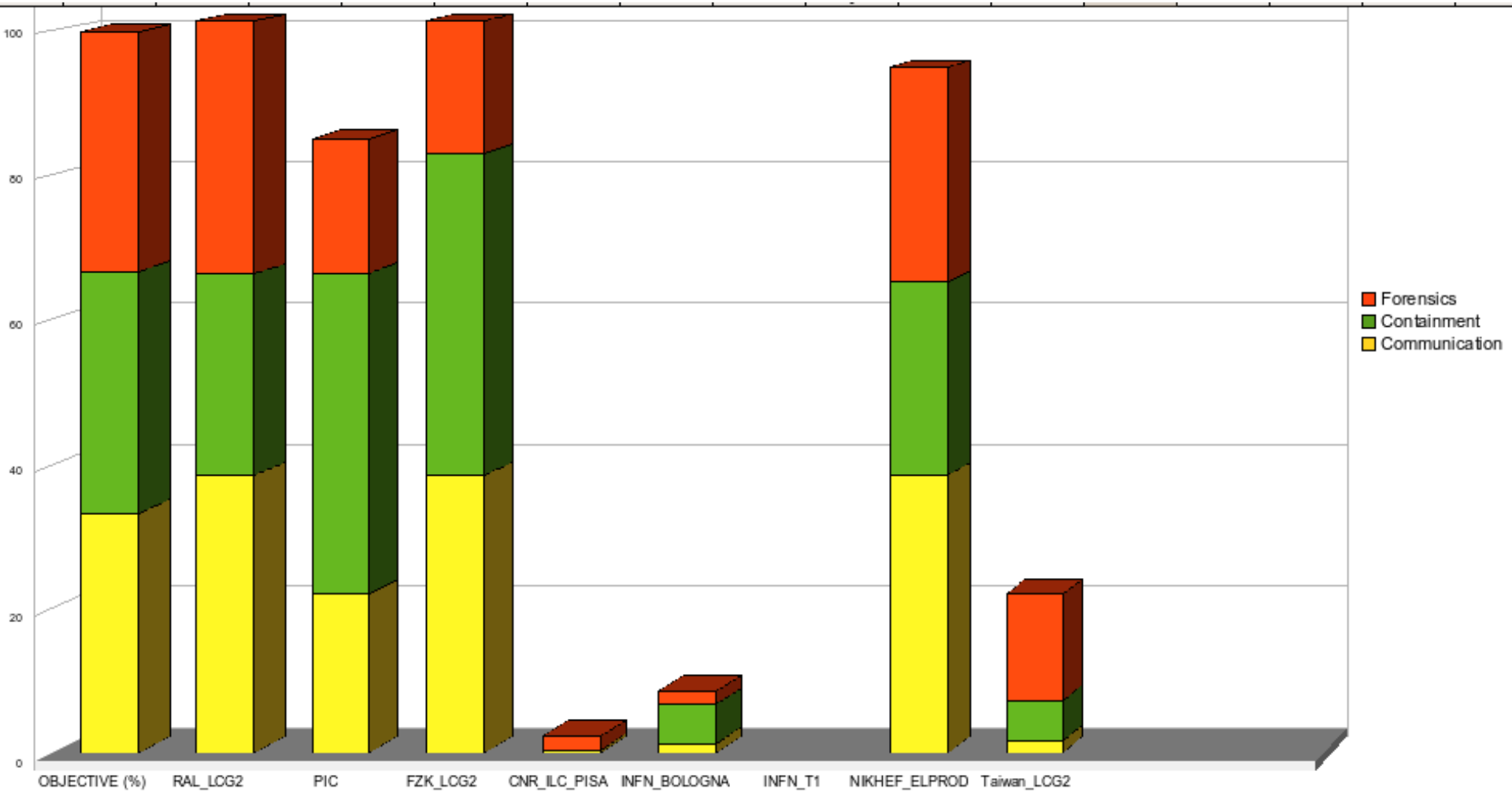
Typical incident (practice)

- Often a « special case », involving exotic/rare configuration (= very heterogenous environment)
- Site security contacts != Grid security contacts
- Involve different sites, and possibly a large number of people
- Lots of emails/communication. Information flow hard to manage
- A number of sites not responding/acting
- Often need to check several month-old logs
- Often information leaks
- Often see a number of credentials exposed (!= from compromised)
- Sometimes difficult to understand the extent and/or causes of the incident

Security Service Challenges

- **Training on-going for the sites, via the Security Service Challenges (SSC)**
- **Simple concept (SSC3):**
  - Send a job to a site
  - Contact them and ask them to treat it as malicious
- **This does not represent the reality...**
  - No production user is involved
  - Only one job is sent (reality: thousands)
  - Site needs to investigate readily available logs (reality: months old logs)
- **...but shows interesting results**
- **SSC3 has been prepared with the kind support of LHCb, launched so far at most of the EGEE Tier1s**

SSC3 (8 sites challenged on ~250)



Real incident

- **See:** http://indico.cern.ch/materialDisplay.py?sessionId=8&ma

Conclusion

- **Need to provide the sites with:**
  - improved traceability, improved controls
  - documentation, recommendations and procedures
- **Clear need for improved security monitoring**
- **Closer collaboration between MWSG and OSCT essential**
  - Joint meetings (probably at EGEE08)
  - Cross representation in the separate meetings
- **OSCT and MWSG have identical goals: provide a secure grid infrastructure**
- **OSCT needs more technical expertise, and better understanding of the possibilities/limitations of middleware**
- **MWSG needs a clear understanding of operational security problems and day-to-day issues**

Discussion

http://cern.ch/osct
https://twiki.cern.ch/twiki/bin/view/LCG/OSCT
https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurity

<*project-egee-osct@cern.ch*>

EGEE and gLite are registered trademarks