Security aspects

(based on Romain Wartel's slides at ISGC Taiwan 2008)

David Bouvet – IN2P3-CC

Planning for Grid Deployment and Usage in South Africa
Meraka Institute, CSIR campus, Pretoria
12-13 may 2008

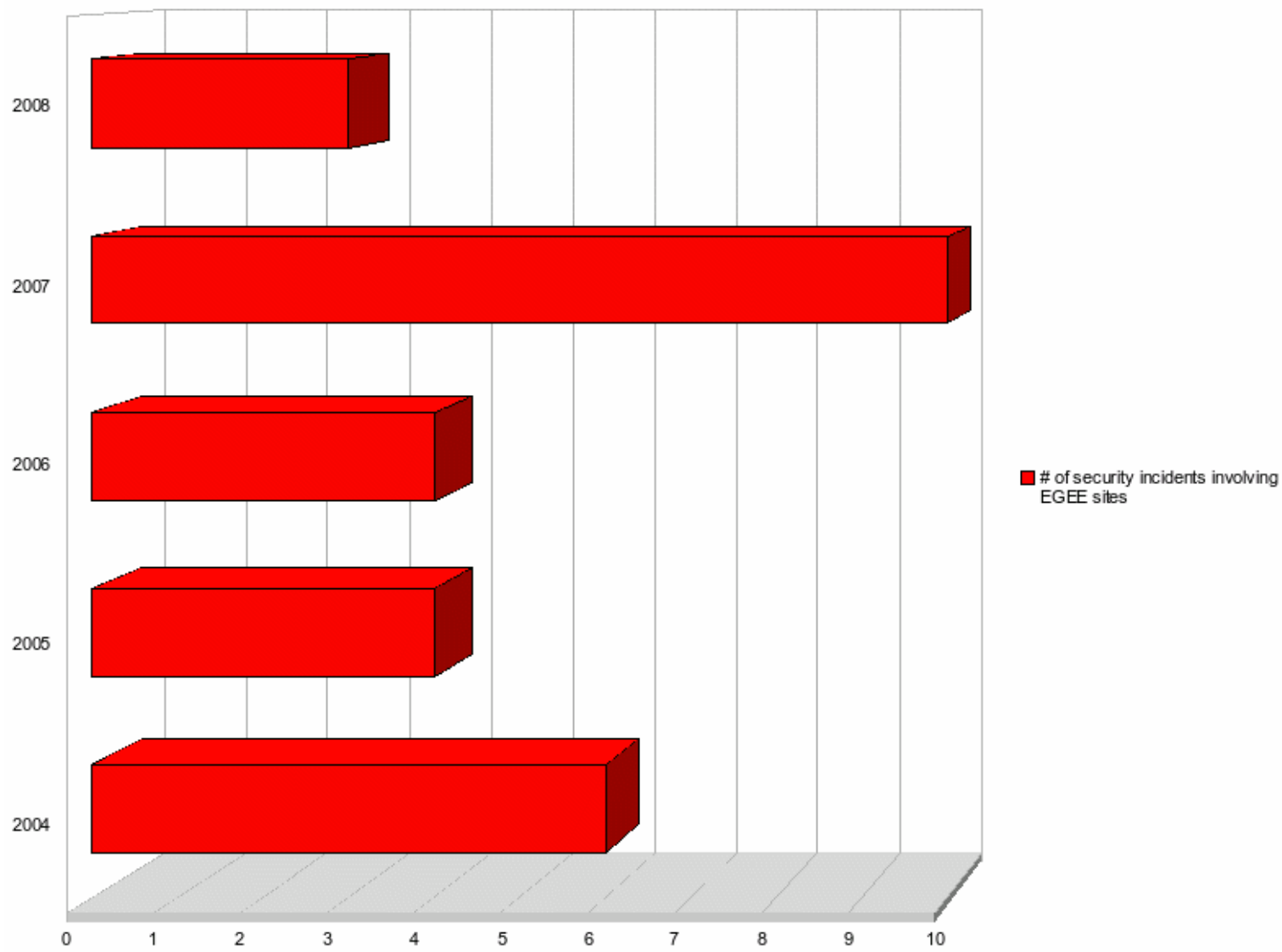
www.eu-egee.org

Information Society and Media

Computer security incident

- **What is a “Security Incident”?**
  - A security incident is the act of violating an explicit or implied security policy
- **What can motivate attackers?**
  - Money (and little risk of being caught)
  - Less likely: political motivation, challenge, ego, fame, etc.
- **How do attackers often proceed?**
  - Most attacks are partly/fully automated
  - First find an entry point (weak network service, stolen credentials, etc.)
  - Install necessary toolkit to maintain a 'quiet' access
  - Implant payload (DDOS, Botnet, SPAM engine, etc.)
  - Harvest additional credentials

Security Incidents Statistics



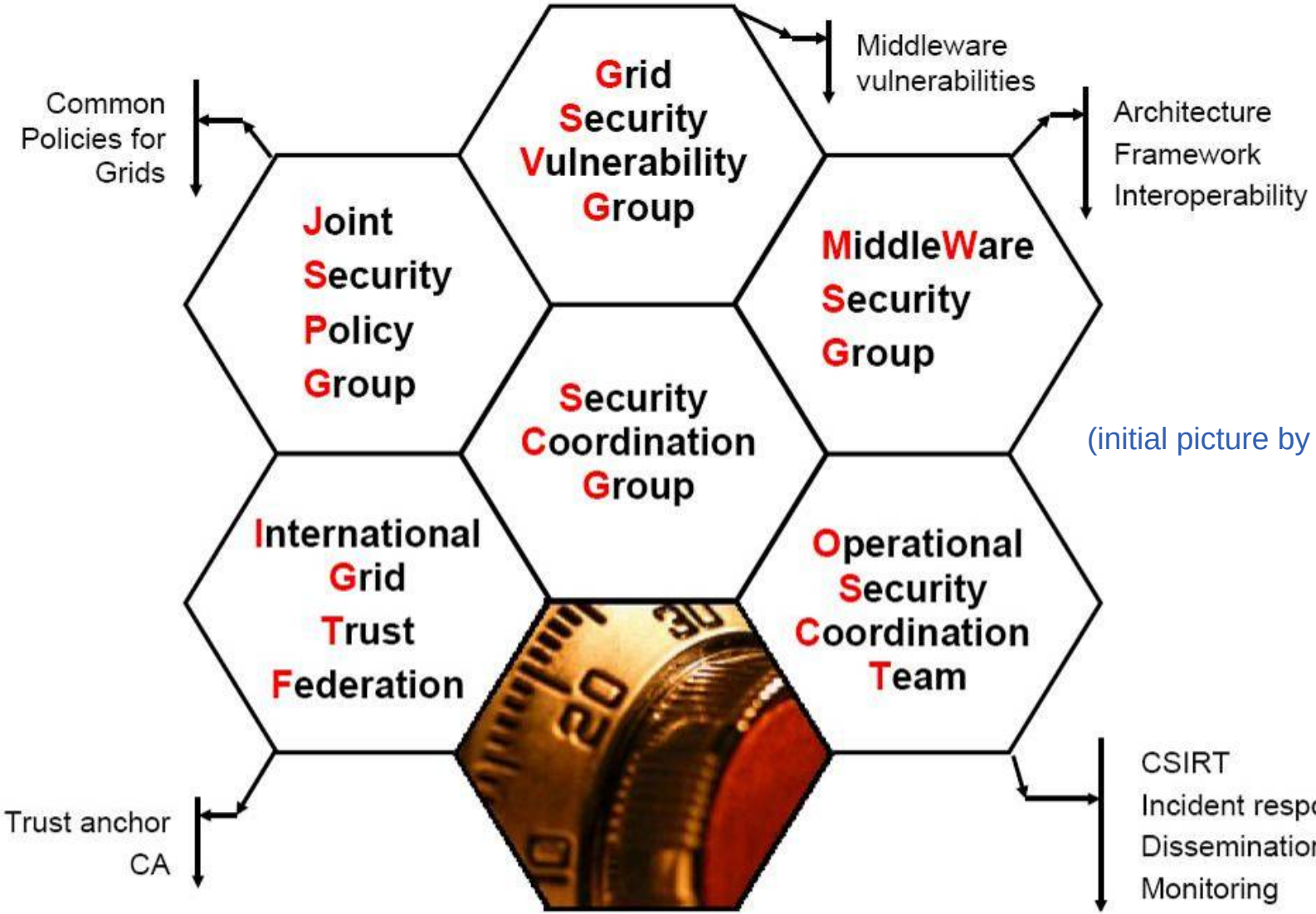
Top risks for the grid

- 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



(initial picture by Ake Edlund)

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

Certification Authorities

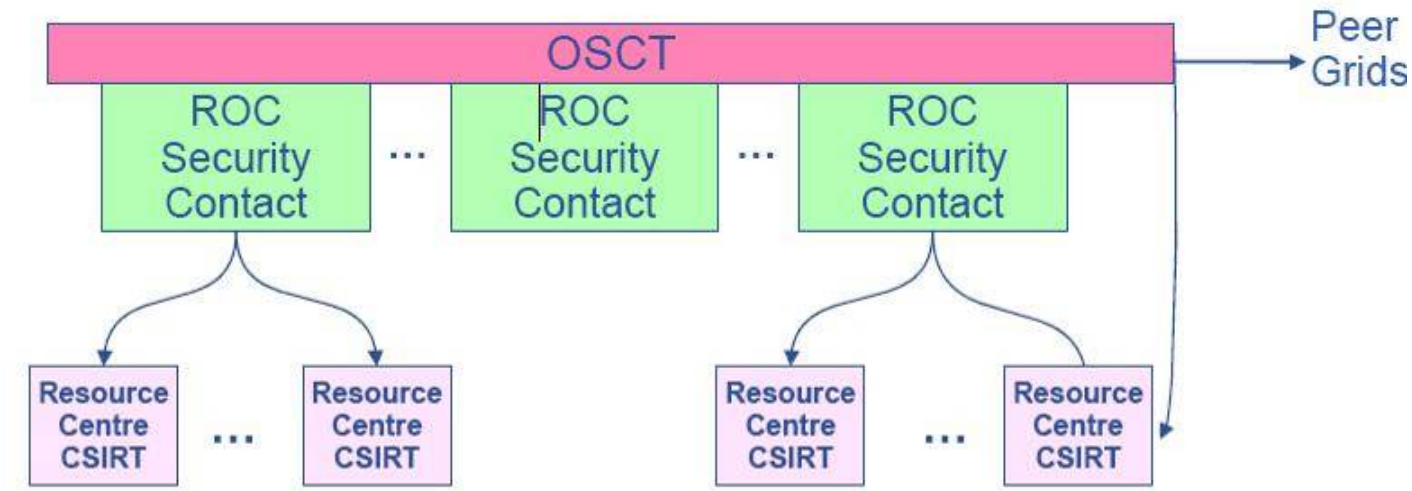
- **IGTF (International Grid Trust Federation) is a body to establish common policies and guidelines between its Policy Management Authorities (PMAs) members.**
  - current PMAs :
    - Europe: EUGridPMA
    - Asia-Pacific: APGridPMA
    - Latin America, Carribean, North America: TAGPMA
- **To create a new PMA, see http://www.gridpma.org/ or contact David Groep (davidg@nikhef.nl) to get more information on the procedures.**

- **In EGEE, there is the possibility to use "catch-all" CA**
  - France (CNRS) for all non HEP VOs
  - CERN for HEP VOs

  ⇨ **African users can ask CNRS or CERN to get their certificates (need to have a minimal structure about identity verification on new certificate request: one person per lab)**

Incident response - coordination

- ROC Security Contacts are part of the EGEE Operational Security Coordination Team (OSCT)
- Incidents coordination: ROC Security Contact on duty



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)
      - *http://cern.ch/grid-deployment/ssc/SSC_2/SSC_2_google.html*
    - IR channels (lists, IM)
    - IR scenarios
  - Incident detection and containment (=monitoring)
    - Several monitoring tools available to the sites
    - Central security tests (SAM)
  - Incident prevention
    - Best practice
      ex: https://cic.gridops.org/index.php?section=roc&page=securityissues
    - Training events

Incident response - coordination

- **A large part of the incident response coordination consists in managing the flow of information**

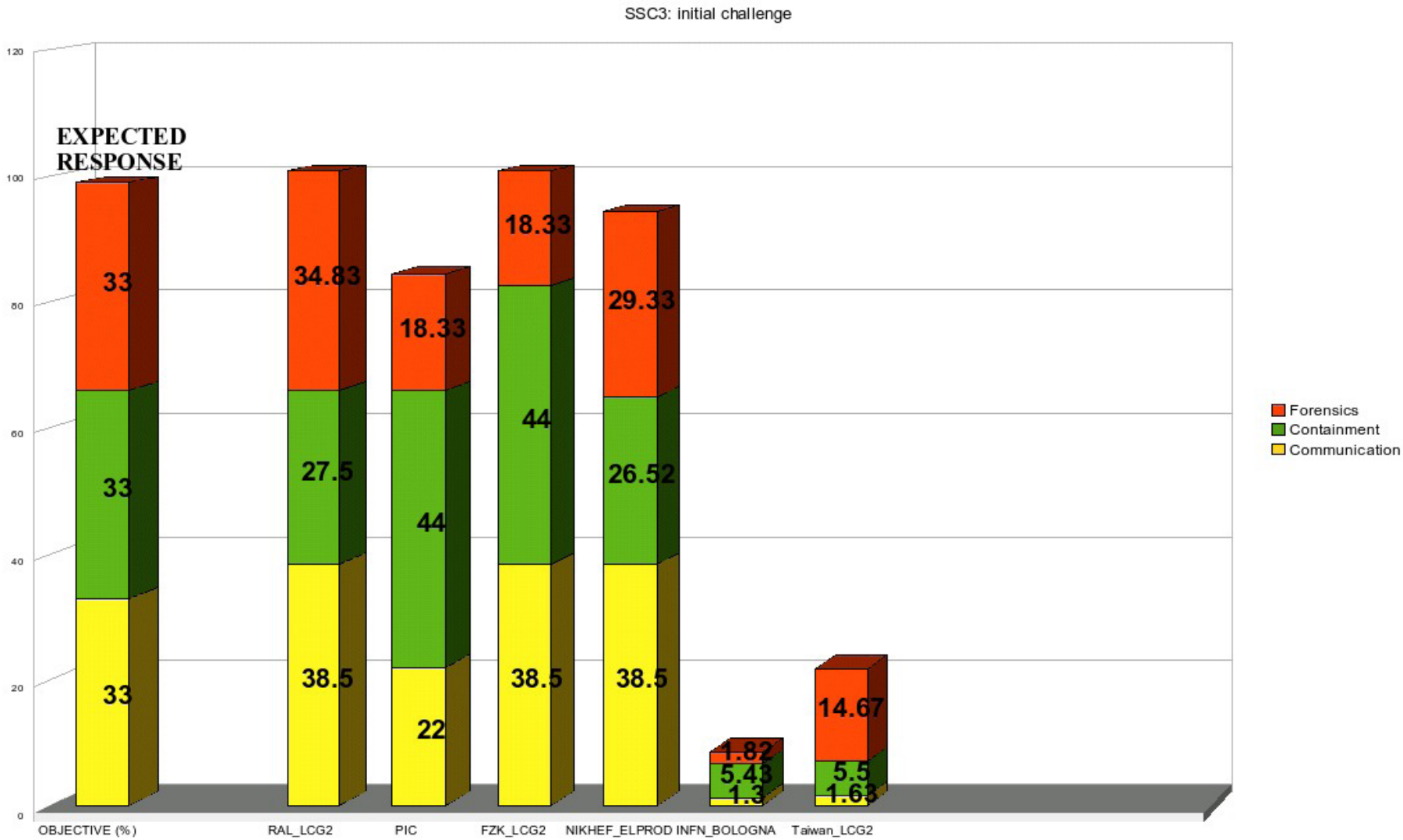
- **The role of the coordinator is to:**
  - Process the available information as soon as possible and follow the most likely leads
  - Provide accurate information to the sites
  - Contact and follow up with the relevant CERTs/CSIRTs
  - Ensure the process does not stall

- **The objective is to:**
  - Understand what was the vector of attack (ex: entry point)
  - Ensure the incident is contained
  - Establish a detailed list of what has been lost (ex: credentials, data)
  - Take corrective action to prevent re-occurrence

Incident response – main issues

- **Main issues:**
  - It is essential to establish and maintain trust between the sites
  - Obtain relevant and accurate information and collaboration from all possibly affected sites
  - Cope with the information flow (large incidents)
    (during a multi-site incident, the coordinator had to process 500+ incoming emails during the first 5 days, including 280 at day 3)
  - Redistribute the information with an appropriate level of details
  - Prevent information leaks, which are a serious problem.
    They can discourage other sites from sharing their findings in the future and expose sensitive information (personal details, etc.)

SSC3 – Early results



Conclusion

- Training and dissemination requires significant efforts, as it is difficult to improve security practices at the sites
- Tests (security service challenges) are extremely useful
- Increased expertise in the team to manage multi-sites security incidents
- Need to build and maintain trust between the participants
- Cooperation and sharing with peer grids (ex: OSG) and with other involved parties (ex: NRENs) is essential

Links

- IGTF web site: http://www.gridpma.org/
- OSCT web site: https://twiki.cern.ch/twiki/bin/view/LCG/OSCT
- OSCT web site: http://cern.ch/osct
- Incident response guide: https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf

Security aspects

Discussion