Operational Security in EGEE

Romain Wartel, CERN IT
EGEE Operational Security Coordination Team
http://www.eu-egee.org/security/

International Symposium on Grid Computing (ISGC) 2008
Academia Sinica, Taipei, 7 - 11 April 2008
• 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
Money, money, money

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

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
Incident response coordination

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

- **Incident detection and containment (=monitoring)**
  - Several monitoring tools available to the sites
  - Central security tests (SAM)

- **Incident prevention**
  - Best practice
  - Training events
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
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.)
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
Discussion