EGEE III: Main challenges in the operational security area

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

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

http://cern.ch/osct

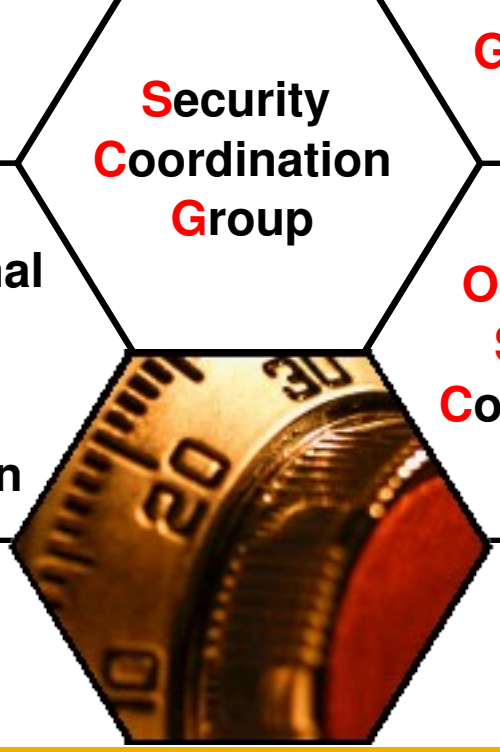
WLCG GDB

CERN, 11 June 2008

www.eu-egee.org

Information Society and Media

EGEE Security Groups



Grid Security Vulnerability Group

Middleware vulnerabilities

Common Policies for Grids

Joint Security Policy Group

Architecture Framework Interoperability

MiddleWare Security Group

Security Coordination Group

International Grid Trust Federation

Operational Security Coordination Team

Trust anchor CA

CSIRT
Incident response
Dissemination / training
Monitoring

(Initial picture by Ake Edlund)

EGEE-II: issues and successes

- **Successes:**
  - No major disruption caused by security incidents
  - Gained additional security expertise
    - *More/better documentation to deal with incidents*
    - *Experience with multi-site incidents, built-up expertise in the OSCT*
    - *Roles and responsibilities is now clearer*
  - Improved collaboration with peer grids, including OSG and NDGF
  - Improved collaboration with the VOs
    - *Ex: LHCb/OSCT worked together for Security Service Challenge 3*
  - Progress in security monitoring also enabled the detection of a number of insecure configurations

- **Issues:**
  - Most ROCs unable to deliver agreed effort
  - Still observe very heterogeneous security standards
  - Several concerns related to the infrastructure need to be addressed

Security trends

- **Change in the attack patterns:**
  - More sophisticated attacks and malicious software, targeted attacks
  - Web applications are now also a target
- **Attacks and malware becoming professional**
  - SPAM, extortion, phishing, identity theft, click fraud, Warez, etc.
  - ADSL hosts are the easy/popular target (Botnets)
  - Attackers go for the easiest target
- **Grids are not (yet?) a primary target, but are valuable:**
  - 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

Challenges for EGEE III

Security Monitoring

"Still observe very heterogeneous security standards"

- **Current model to detect insecure configurations:**
  - Promote the use of helpful security tools (dissemination)
  - Use a small number of SAM tests to monitor all sites
- **Need more security tests**
  - Effort needed from the ROCs
  - More advanced checks
    - Ex: patching status
- **Need to adapt to popular monitoring tools/frameworks/standards**
  - Nagios
- **Need further discussions with the Operations Automation Team**

Targeted training

"Still observe very heterogeneous security standards"

- **Organise more training events**
  - Held a successful training event at EGEE07
  - Another event planned for EGEE08
  - Needs further discussion with NA3
- **Better operational procedures for the sites**
  - Clearer security procedures needed
    - Ex: how to suspend a user
  - Better integration within existing operational procedures
- **Better documentation, more grid-specific**
  - Currently seeking contributions from middleware/security experts
    - Ex: Local firewall configuration, important log files, etc.
  - Restructuring of existing training material would help

Traceability and Logging

- **It is essential to understand the cause of security incident in order to:**
  - Contain and resolve the incident
  - Unblock users/sites/VOs
  - Prevent re-occurrence of the incident

- **Updated "Grid Security Traceability and Logging Policy"**
  - https://edms.cern.ch/document/428037/
  - The middleware must produce relevant logs
  - It must enable central collection (at the site) of the logs

- **Impact for the sites**
  - Grid logs must be collected centrally (=central site syslog)
  - 90 days minimal retention period
  - Longer retention period needed for "core" grid services

Central Authorization

- **Applying controls is essential for security operations**

- **However banning users is problematic**
  - Difficult to ensure all WLCG sites have taken appropriate action
  - Current model is not easily scalable:
    - Requires expertise of the services
    - Cannot easily implement site-wide banning
    - etc.
  - Recent SSC: 1/3 of the Tier1s unable to block a malicious DN

- **Improved central authorization mechanisms needed**
  - Work in progress in the MWSG
  - Seen as a priority

Cross Site Request Forgery

- **CSRF - Cross-Site Request Forgery**
  - The attacker uses the identity of the currently logged in victim to interact with websites (ex: e-banking)
  - Becoming more and more popular (Google, Amazon, etc. have been successfully attacked)
  - Most grid-related Web applications use X509 authentication
  - Once the user has typed its passphrase, the certificate can be used transparently to access vulnerable portals

- **Need to adapt our code**
  - Implement “Double Submit Cookie” technique
  - Carefully check all user input
  - MWSG is actively following this up

EGI/NGI

- **Need to prepare for post-EGEE III**
  - All ROCs have been asked to allocate some efforts
- **Where will global security incident coordination happen?**
  - NGI security officers?
  - EGEE NOCs (EGEE Network Operations Centres / ENOC)?
  - Integrated with existing CSIRTs (ex: TF-CSIRT)?
  - A mix of all? (likely)
- **Lots of discussions ahead!**

Conclusion

- **Clear progress was made during EGEE-II**
  - More security expertise and know-how
  - Better procedures
- **Need to continue to improve sites security in EGEE III**
  - Improved security monitoring
  - More targeted and structured documentation and training material
- **Some issues need to be addressed during EGEE-III, in particular:**
  - Central Authorization
  - Logging and traceability
- **Also need to adapt to new threats**
  - more sophisticated attacks and malware
- **Agreed effort must be delivered by the partners to achieve this**

Questions