Managing grid security incidents

Romain Wartel
CERN, IT Department
EGEE Operational Security Coordination Team

EGEE'09, Barcelona, Spain, 21-25 September 2009

www.eu-egee.org

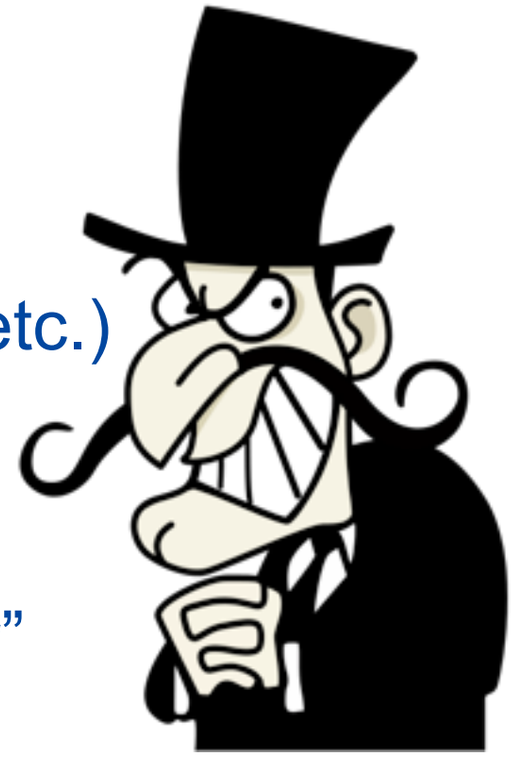
Exposure and motivation

- **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 another
  - Large number of identical hosts
  - Heterogeneous skills, staffing and security standards
- **ADSL hosts are the current easy/popular target**
- **Regular attacks against academic sites**
  - Often involve SSH or Web applications

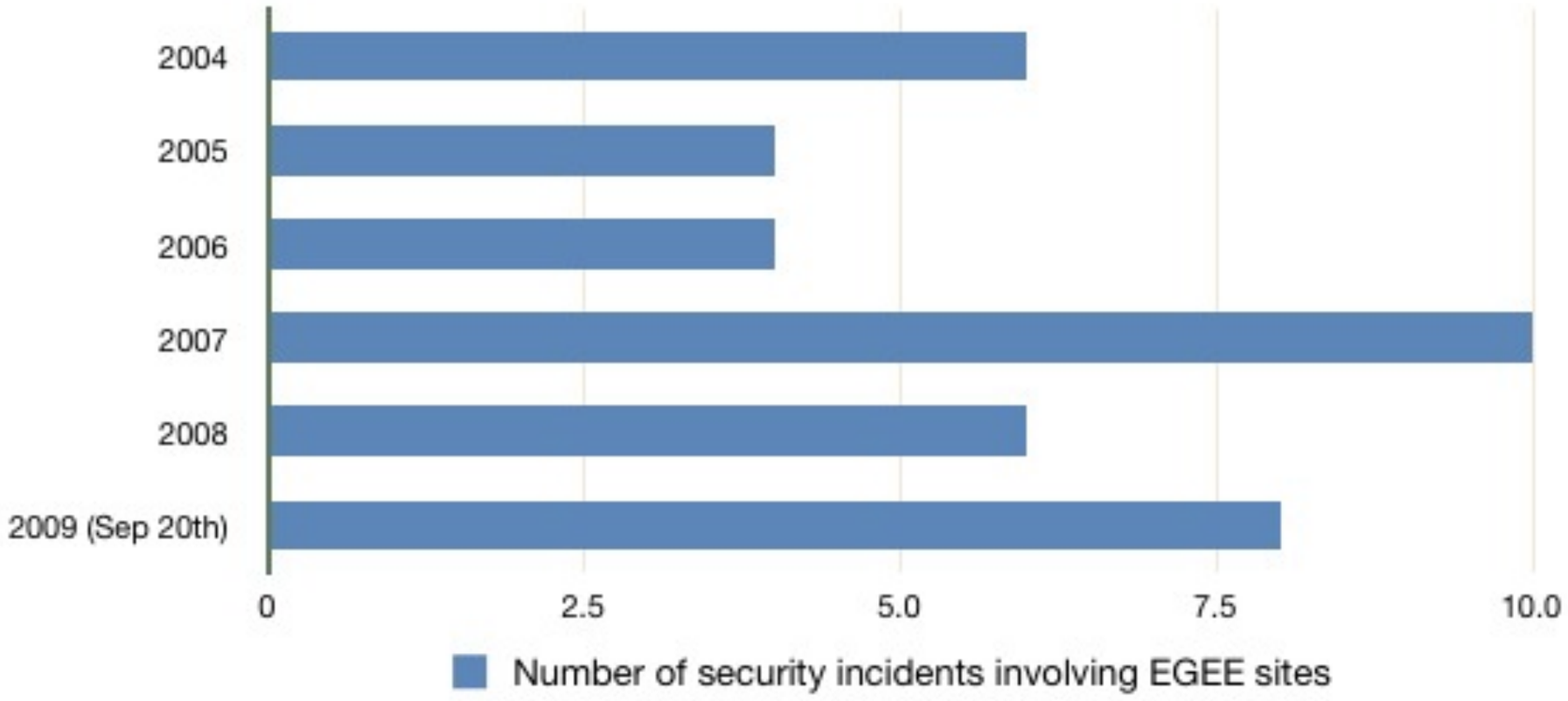
Typical incident

1. **Gain local access**
   - Stolen account
   - Web application vulnerability
   - Design errors (incorrect AFS ACL, password on CVS, etc.)
   - etc.
2. **Attempt to obtain root privileges**
   - Use a (or wait for a new) “local root exploit vulnerability”
   - Exploit the system, gain root access
   - Game over.
3. **Maintain access with a rootkit, harvest credentials**
4. **Use new harvested credentials against further hosts**
5. **Go to step 1**



Statistics

- **EGEE statistics on security incidents**



- **Several incidents avoidable if sites were up-to-date with security patches**

Soon or later...

- **Each site has been or will be affected by a security incident**
  - Either by exploiting a local vulnerability
  - Or through a user account from a partner site

- **Part of normal operations, just need to ensure**
  - It is "cheap" to deal with
  - The overall infrastructure is not affected

- **It is essential to prepare for this event to reduce its:**
  - Impact (appropriate and timely response, precautionary measure, etc.)
  - Likelihood (prevention, service hardening, etc.)

- **The EGEE incident response procedure is documented:**

https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf

http://cern.ch/osct/incident-reporting.html

incident response procedure

- **Inform your security team/ROC Security Contact**
- **If you are familiar with the service, contain the incident**
- **Announce the incident (project-egee-security-csirts@in2p3.fr) (4 h)**
- **If needed, report downtime**
  - "Security operations in progress"
- **Perform appropriate forensics and take necessary corrective actions**
  - Identify and kill suspicious process(es) ... but aim at preserving info
  - Suspend the relevant accounts
  - Check the VO has been contacted (if the credentials have been abused)
  - Check the CA has been contacted (if the credentials are compromised)
- **Send additional reports if needed, and a final report (30 d)**
  - Templates are available
- **Restore service and re-activate suspended account(s)**
- **Contact project-egee-security-support@cern.ch for any help!**

Information needed

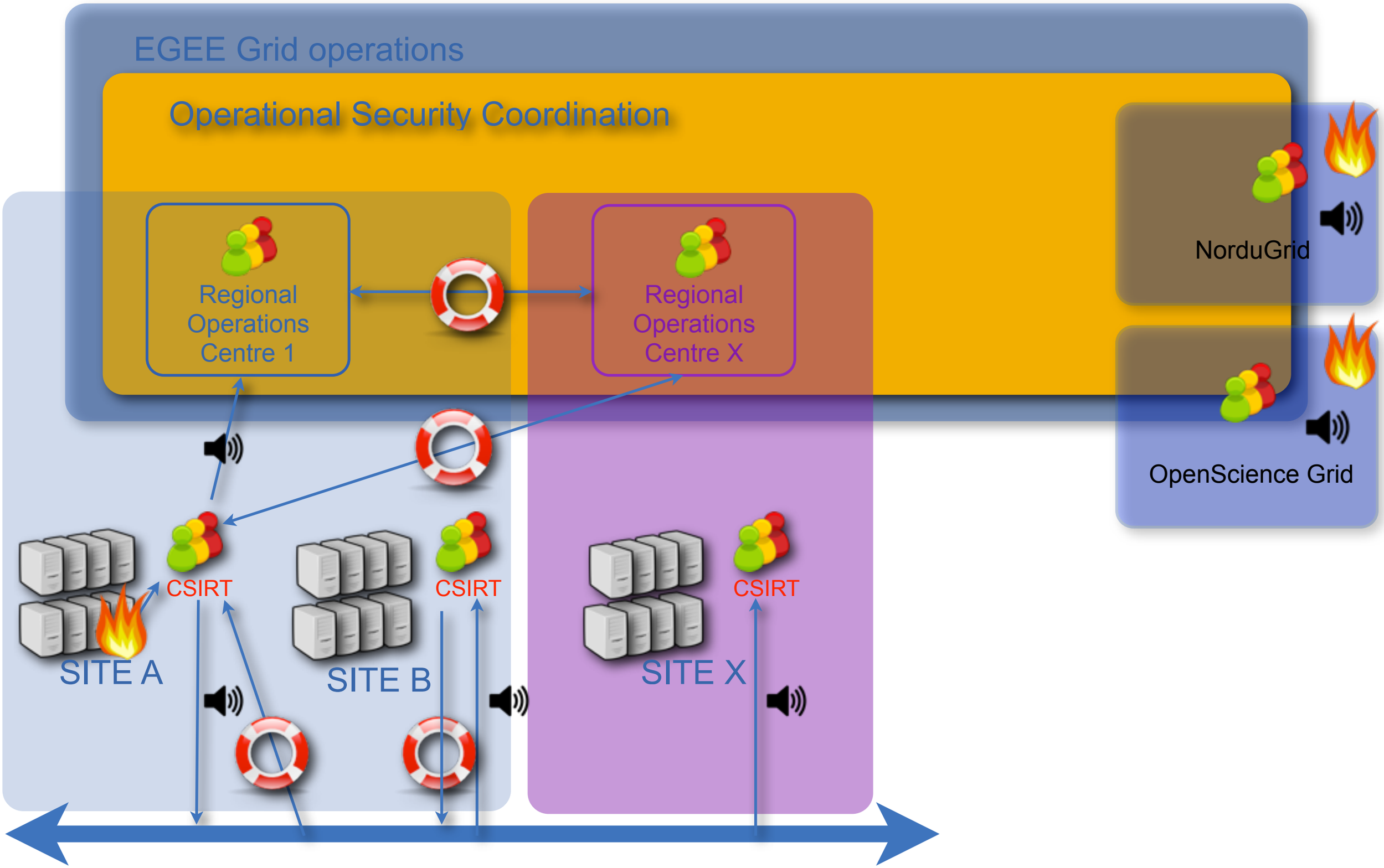
- **Essential to identify the source, to prevent re-occurrence**
- **Usually involves**
  - Logging information (IP addresses, timestamps, identities) from services
  - 6 months prior to the discovery of the incident for successful SSH logins
  - 3 months prior to the discovery of the incident for all other grid services
- **Sites are expected to produce the following information**
  - Host(s) affected (compromised hosts, hosts running suspicious code)
  - Host(s) used as a local entry point to the site (ex: UI or WMS IP address)
  - Remote IP address(es) of the attacker
  - Evidence of the compromise (suspicious files or log entry)
  - What was lost, details of the attack (compromised credentials/hosts)
  - If available and relevant, the list of other sites possibly affected
  - If available and relevant, possible vulnerabilities exploited by the attacker
  - The actions taken to resolve the incident

When contacted

- **When alerted about a security incident**

- **This is not “for your information only”: action is needed!**
- **Please check your logs with the information provided**
- **If you need assistance (or don’t know what to do):**
  - Please ask for help! (http://cern.ch/osct, your ROC security contact, ...)

Security incidents management



Infrastructure coordination

- **For each incident, a coordinator is appointed**
  - Actively stimulate and probe the affected participants
  - Aim at understanding the exact cause of the incident
    - Compromised assets(credentials, etc.)
    - How to resolve the incident
  - Help involved sites to resolve the incident
  - When needed send updated detailed reports to the affected sites
    - Interesting findings or possible leads that could be used to resolve the incident
  - When necessary, send updated summary reports to all the CSIRTs
  - Inform the sites that access from these accounts or identities can be restored

- **Coordinator ensures a timely and collaborative resolution**
- **Collaboration from all sites essential**

Conclusion

- **Prevention and preparation are essential**
- **Understand the incident resolution procedure**
- **Important to check technical information needed**
  - is available (central logging, etc.)
  - and usable (processing the logs, etc.)
- **Know in advance where to find information**
  - Support, procedures, policies, mailing-lists, contact points, support etc.
  - Not only in EGEE, but also both at your site and in your ROC/EGI
- **Process must be defined and clear (and customised?)**