EGEE III Security Training and Dissemination

Mingchao Ma, STFC – RAL, UK

OSCT Amsterdam, 22 March 2010

Overview

- **Training and dissemination:**
  - Estimated efforts: 35 PM
- **Activity coordination**
  - UK (3 PM)
- **Training and dissemination contributions**
  - APROC (4 PM)
  - ITALY (4 PM)
  - SWE (4 PM)
  - SEE (4 PM)
  - DECH (10 PM)
  - FRANCE (2 PM)
- **Website, communication and outreach**
  - RUSSIA (3 PM)

Activities

Service Reference Cards

- **Service Reference Cards**
  - https://twiki.cern.ch/twiki/bin/view/EGEE/ServiceReferenceCards
  - SEE ROC
    - glite-PX MyProxy server
    - glite-VOMS Virtual Organisation Membership System
    - glite-MON Monitoring System Collector Server
  - DECH ROC
    - glite-VOBOX Virtual Organisation Node
    - glite-FTS File Transfer Service
    - glite-LFC LCG File Catalog
    - lcg-CE LCG Computing Elements

Service Reference Cards

- **Service Reference Cards**
  - FR ROC
    - gLite-AMGA ARDA Metadata Catalog
    - gLite-UI User Interface
  - SWE ROC
    - gLite-WMS Workload Management Service
    - gLite-LB Logging and Bookkeeping service
    - glite-BDII Berkeley Database Information Index
  - IT ROC
    - glite-WN Worker Node
    - glite-CREAM_CE gLite CREAM Computing Element
  - CERN
    - glite-DPM Disk Pool Manager

Security Training

- **Targeted Audience**
  - System Administrators and Site Managers
- **Topics including**
  - Middleware security
  - Incident handling
  - Security policy
  - Security monitoring
  - Log management
  - Patch management
  - … …

Security Training

- **EGEE '07**
  - http://indicoprev.cern.ch/conferenceTimeTable.py?confId=18714
  - Introduction: Grid and security
    - Remi MOLLON (CERN)
  - Grid systems installation and configuration
    - Louis PONCET (CERN)
  - Centralised logging, Eddie ARONOVICH
    - (Tel-Aviv University)
  - Protecting administrative credentials
    - Mingchao MA (STFC - RAL)
  - Testing and monitoring Grid systems
    - Michal PROCHAZKA (CESNET)
  - Incident response (policies and procedures)
    - Carlos FUENTES BERMEJO

Security Training

- **EGEE ’08**
  - Joined MWSG and OSCT security training
  - http://indicoprev.cern.ch/conferenceTimeTable.py?confId=32220
  - Introduction: Grid and security
    - Mingchao Ma, STFC – RAL
  - Middleware security overview and pattern matching
    - Christoph WITZIG , SWITCH
  - Security recommendations: lcg-CE
    - Maarten Litmaath, CERN
  - Security recommendations: CREAM CE
    - Massimo Sgaravatto , INFN Padova
  - Security recommendations: WMS
    - Francesco Giacomini
  - Security recommendations: LB
    - Ákos Frohner, CERN
  - Security recommendations: SE
    - Daniel Kouril, CESNET
  - Handling security incidents: procedures and recommendations
    - Carlos Fuentes, IRIS-CERT, RedIRIS

Security Training

- **EGEE '09**
  - http://indicoprev.cern.ch/conferenceTimeTable.py?confId=55893
  - Managing grid security incidents
    - Romain WARTEL, CERN
  - Security Monitoring, Pakiti and Nagio-based monitoring
    - Daniel KOURIL, CESNET
  - Command line security tools: introduction and job-lookup-by-subject
    - Christoph WITZIG, SWITCH
  - Command line security tools: client connect
    - Tunde BALINT, NIKHEF
  - Authorization Service, Argus command line tools and Central banning
    - Christoph WITZIG, SWITCH
  - User traceability and log analysis
    - Giuseppe MISURELLI, INFN

Other Trainings

- Organized by ROC security officers
- Attended by system admins/site managers withion the ROC
- https://twiki.cern.ch/twiki/bin/view/LCG/OSCT-EGEEIII-tasks

AP ROC Security Workshop'09

- Incorporated into The International Symposium on Grid Computing (ISGC) 2009, Taipei,Taiwan
- Half day security training workshop on 19th April
- http://www2.twgrid.org/APTeam/index.php/2009_ISGC_EUAsiaGrid/EGEE_Tutorial

- Security Policy
  - David KELSEY, STF-RAL, UK
- Grid Security and Incident Handling
  - Mingchao MA, STF-RAL, UK
- SSC3 at AP ROC
  - Jinny CHIEN, ASGC, TW
- Middleware Security
  - David GROEP, NIKHEF, Netherlands

AP ROC Security Workshop'10

- **Incorporated into The International Symposium on Grid Computing (ISGC) 2010**
- **One day security workshop on 7th March 2010**
- **Update on Security Policy**
  - David Kelsey, STFC - RAL, UK
- **Manage Security and Handle Security Incident**
  - Mingchao Ma, STFC - RAL, UK
- **Understanding and preventing common attacks**
  - Romain Wartel, CERN, Switzerland
- **Middleware Security**
  - David Groep, Nikhef, The Netherlands
- **Introduction to SAML-based federations**
  - Milan Sova, CESNET, the Czech Republic
- **Security Service Challenge and Security Monitoring**
  - Jinny Chien, Academia Sinica, Taiwan

Other Regional Security Workshops

- **France Security Workshop**
  - http://indico.in2p3.fr/conferenceDisplay.py?confId=1605
  - 2nd April 2009
  - Workshop in French ☹
- **UK Security Training Workshop**
  - Incorporation with HEPSYSMAN workshop;
  - One day security workshop on 1st July 2009
  - Also invited UK JANET CSIRT and Oxford University CSIRT to give a talk
- **DECH ROC Security Training Workshop**
  - Half day Security training incorporate into GridKa School
  - http://gks09.fzk.de/Agenda.html
  - 4th September 2009

OSCT website

Enabling Grids for E-sciencE

EGEE Operational Security Coordination Team

Mission | Incident reporting | Dissemination | Alerts | Operational notices | Monitoring | Security challenges | Policies | Meetings | Contacts

EGEE Operational Security Coordination Team

Hot news

Flyer for the TF-CSIRT and OSCT collaboration. Please, read on and disseminate in your region.

OSCT mission

The EGEE Operational Security Coordination Team (OSCT) provides an operational response to security threats against the EGEE infrastructure. It mainly focuses on computer security incidents handling, by providing reporting channels, pan-regional coordination and support. It also deals with security monitoring on the Grid and provides best practice and advice to Grid system administrators.

The OSCT is lead by the EGEE/LCG Security Officer and includes Security Contacts from each EGEE region. They are providing support for daily security operations as part of an on-duty rota.

One can contact OSCT via project-egee-security-support@cern.ch.

Other EGEE Security groups

There are six other major security groups in EGEE.

- EGEE Security Coordination Group (SCG) — coordinates the overall security work.
- Middleware Security Group (MWSG) — security architecture.
- Joint Security Policy Group (JSPG) — security policies.
- EGEE Security Middleware Development (EGEE/JRA1/Security) — gLite security development.
- Grid Security Vulnerability Group (GSVG) — finding and eliminating Grid security vulnerabilities.
- EUGridPMA — coordinating Grid authentication in e-Science.

More details are available at http://egee2.eu-egee.org/security/.

EGEE Operational Security Coordination Team

Looking Forward

- **Continue both project-wide and regional security workshops if possible**
  - EGI Technical Forum in September 2010
  - Security workshops organized by NGIs are strongly encouraged
  - A good opportunity to build contact with NERN CSIRT team
- **OSCT website => EGI CSIRT website**
- **Considering other training materials (next slide)**

Other Training Materials

- **TERENA TRANSIT Training Material**
  - Designed for CSIRT team members
  - TF-CSIRT also organizes training, twice/year
  - Not cheap
  - http://www.terena.org/activities/csirt-training/events.html

- **ENISA CERT exercise material and the accompanying Live DVDs**
  - https://www.enisa.europa.eu/act/cert/support/exercise
  - Documents on how to setup and run a CERT/CSIRT team
  - Clearinghouse for Incident Handling Tools
    - https://www.enisa.europa.eu/act/cert/support/chiht

Links

- **Service Reference Cards**
  - https://twiki.cern.ch/twiki/bin/view/EGEE/ServiceReferenceCards
- **Security workshops**
  - https://twiki.cern.ch/twiki/bin/view/LCG/OSCT-EGEEIII-tasks
- **Other training materials**
  - Security policies
    - http://www.jspg.org
  - Incident response procedure
    - https://edms.cern.ch/document/428035/
  - OSCT website (security monitoring, Security challenges etc.)
    - http://osct.web.cern.ch/osct/
  - TERENA TRANSIT Training
    - http://www.terena.org/activities/csirt-training/
  - ENISA CERT exercise material and accompanying Live DVDs
    - https://www.enisa.europa.eu/act/cert/support/exercise