EGEE III Security Training and Dissemination

Mingchao Ma, STFC – RAL, UK

OSCT

www.eu-egee.org

Science & Technology
Facilities Council

Information Society
and Media

Barcelona 2009

Enabling Grids for E-sciencE

- **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)

Enabling Grids for E-sciencE

- **Service Reference Cards**
  - Security section
- **Security training events/workshops**
  - Security trainings at EGEE07, EGEE08 and EGEE09
  - Security trainings at ROCs
    - France ROC
    - AP ROC
    - UKI ROC
    - DECH ROC
- **Security and dissemination area on OSCT public website**
  - Ongoing work
- **Security RSS feed**

Enabling Grids for E-sciencE

- **Service Reference Cards**
  - to gather useful general information and to provide links to detailed information for each service
  - Specifically have a "security information" section
  - 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

Enabling Grids for E-sciencE

- **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 ROC
    - glite-DPM Disk Pool Manager
  - Oscar Koeroo
    - glExec

Enabling Grids for E-sciencE

- **Security training session at EGEE 07**
  - http://indico.cern.ch/conferenceTimeTable.py?confId=18714

- **Training topics:**
  - Introduction: Grid and security
  - Grid systems installation and configuration
  - Centralized logging
  - Protecting administrative credentials
  - Testing and monitoring Grid systems
  - Incident response (policies and procedures)

Enabling Grids for E-sciencE

- **Joint security training session at EGEE08**
  - http://indico.cern.ch/conferenceTimeTable.py?confId=32220

- **Training topics:**
  - Introduction: Grid and security
  - Middleware security overview and pattern matching
  - Security recommendations: lcg-CE
  - Security recommendations: CREAM CE
  - Security recommendations: WMS
  - Security recommendations: LB
  - Security recommendations: SE
  - Handling security incidents: procedures and recommendations

Enabling Grids for E-sciencE

- **Joint Security training session at EGEE09**
  - http://indico.cern.ch/conferenceDisplay.py?confId=55893

- **Training topics**
  - Managing grid security incidents
  - Security Monitoring, Pakiti and Nagio-based monitoring
  - Command line security tools: introduction and job-lookup-by-subject
  - Command line security tools: testing client connection
  - Authorization Service, Argus command line tools and Central banning
  - User traceability and log analysis

Enabling Grids for E-sciencE

- **France ROC**

- **AP ROC**

- **UKI ROC**

- **DECH ROC**

- **Duration: 2 days**
- **Participants:**
  - Site security contacts
    - From production sites and sites under certification
  - Organisational security contacts
    - Secretariat-General for National Defence (government institution)
    - Security officers from the institutions participating in the French JRU
    - Security contacts from the French NREN (RENATER)
    - Grid security contact from one industrial site
  - 26 people in total (plus the person responsible for the technical organisation)
- **Contributions came from:**
  - French OSCT members
  - Site security contacts
  - Institutional security contact
- **http://indico.in2p3.fr/conferenceDisplay.py?confId=1605**

Enabling Grids for E-sciencE

- **EuGridPMA**
- **Overview of security related bodies of EGEE and their roles**
- **More detailed: Role of OSCT and OSCT-DC**
- **Security Service Challenges how-to and results**
- **Sources of information about grid security**
  - Policies, which ones, where to find them, how to change them
  - Hints, where they are and where they come from
  - Handling a security incident on a CE (and how to crack a CE ;-))
  - Incident handling procedure in general and existing communication channels
- **Self audit**
- **Discussion about SLAs**
- **Security handling by example: three different organisations presented their ways**
- **Discussion on cooperation models in the future NGI**

- **Specific grid security training event or workshop not planned for the near future**
  - Nevertheless, a repetition would be necessary from time to time for the newcomers
- **Instead, integration of grid security topics into other events**
  - Example: French EGEE to NGI transition conference in October

- **Security Training Workshop**
  - Half day security training workshop on 19th April;
  - The International Symposium on Grid Computing (ISGC) 2009, Taipei,Taiwan
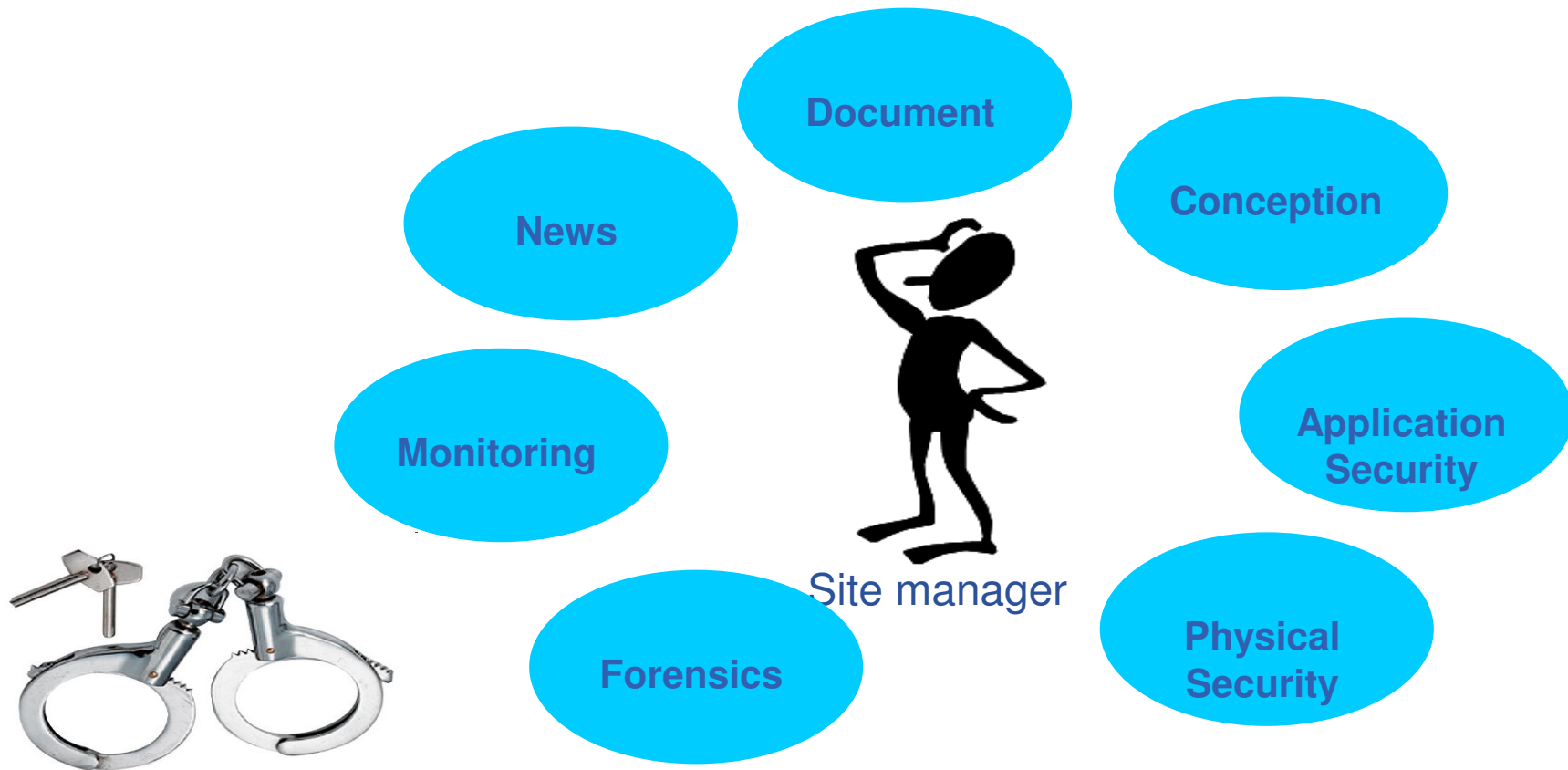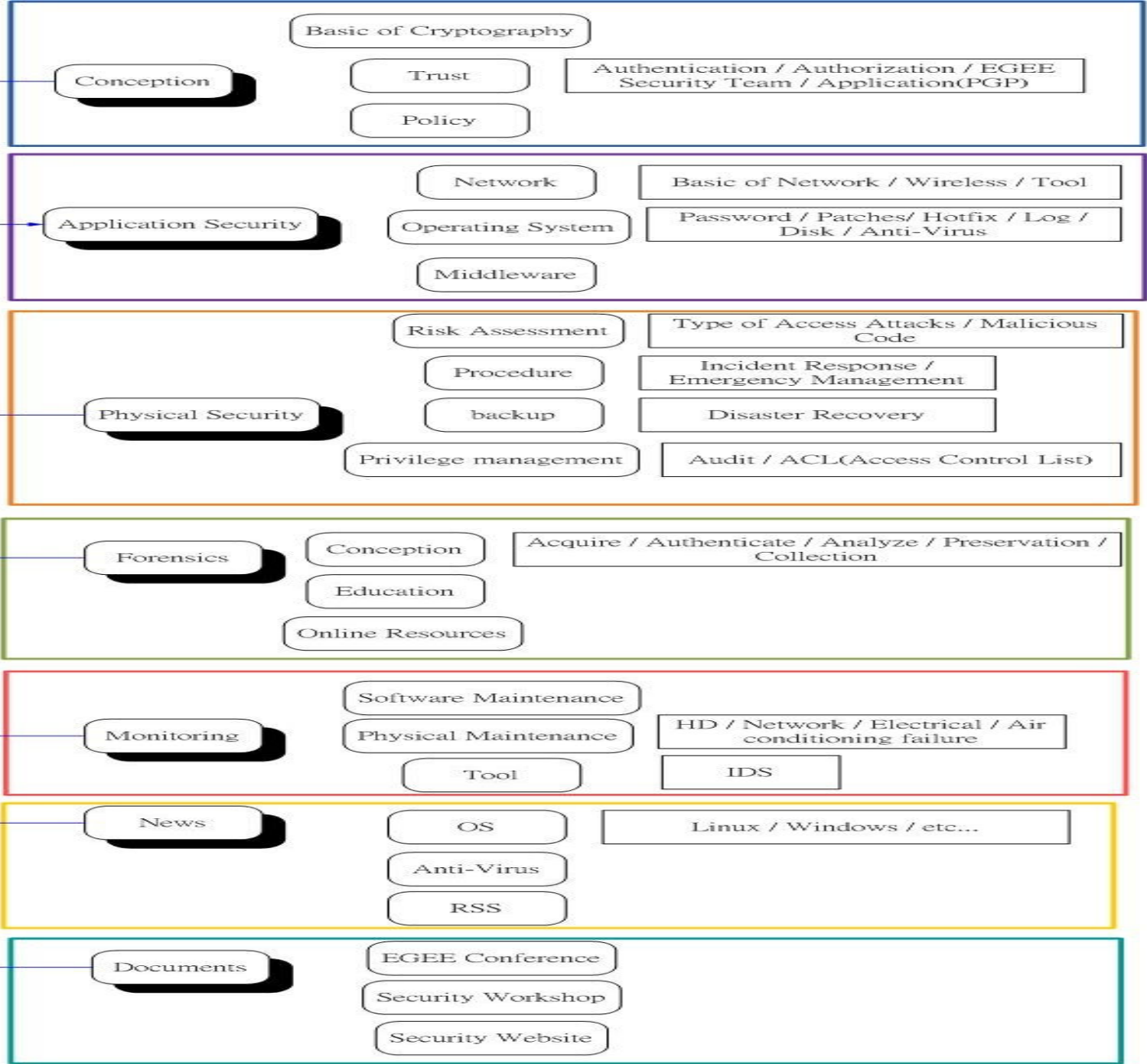 - http://www2.twgrid.org/APTeam/index.php/2009_ISGC_EUAsia Grid/EGEE_Tutorial

- **Topics:**
    - Security Policy;
    - Grid Security and Incident Handling;
    - Middleware Security;
    - Security Service Challenge 3 at AP ROC;

eGee
Enabling Grids for E-sciencE

- **One day UK Security Training Workshop (one day)**
  - Incorporated into HEPSYSMAN workshop;
  - http://hepwww.rl.ac.uk/SYSMAN/June2009/agenda.html
- **Topics**
  - SSC3 case study
  - TCD security monitoring tool
  - OxCERT
  - Update on Security Policy
  - Security on storage element
  - Update on Security activities in EGEE, GridPP and NGS
  - JANET CSIRT
- **Invited UK JANET CSIRT and Oxford University CSIRT;**
- **Discussion on incident handling and cooperation among Grid CSIRT, NREN's CSIRT and University CSIRT**

- **Half day security training workshop**
  - GridKa-School 2009, organized by members of GridKa/OSCT
  - http://gks09.fzk.de/Agenda.html#Friday
- **Topics**
  - Grid Security Workshop for Administrators and Developers
  - Security Services Challenge @ Uni Bonn
  - Security Services Challenge @ TU Dortmund
  - Grid-CERT (DFN-CERT)
- **Future planned activity:**
  - Presentation about EGEE Incident Response Procedures and Security Service Challenges with anonymized results from ROC DECH at D-Grid security workshop,14./15. Oct 2009

Enabling Grids for E-sciencE

- **A security area on OSCT website**
- **Still working in process**

Document

News

Conception

Monitoring

Application Security

Site manager

Forensics

Physical Security

Conception
- Basic of Cryptography
- Trust
- Policy
- Authentication / Authorization / EGEE Security Team / Application(PGP)

Application Security
- Network — Basic of Network / Wireless / Tool
- Operating System — Password / Patches/ Hotfix / Log / Disk / Anti-Virus
- Middleware

Physical Security
- Risk Assessment — Type of Access Attacks / Malicious Code
- Procedure — Incident Response / Emergency Management
- backup — Disaster Recovery
- Privilege management — Audit / ACL(Access Control List)

Forensics
- Conception — Acquire / Authenticate / Analyze / Preservation / Collection
- Education
- Online Resources

Monitoring
- Software Maintenance
- Physical Maintenance — HD / Network / Electrical / Air conditioning failure
- Tool — IDS

News
- OS — Linux / Windows / etc...
- Anti-Virus
- RSS

Documents
- EGEE Conference
- Security Workshop
- Security Website

Enabling Grids for E-sciencE

Enabling Grids for E-sciencE

- **RSS feed for the security-related guidelines and best practices.**
  - http://rss-grid-security.cern.ch/rss.php

- **See security RSS feed guide to learn about the feed and how to integrate it into your own site**
  - http://rss-grid-security.cern.ch/