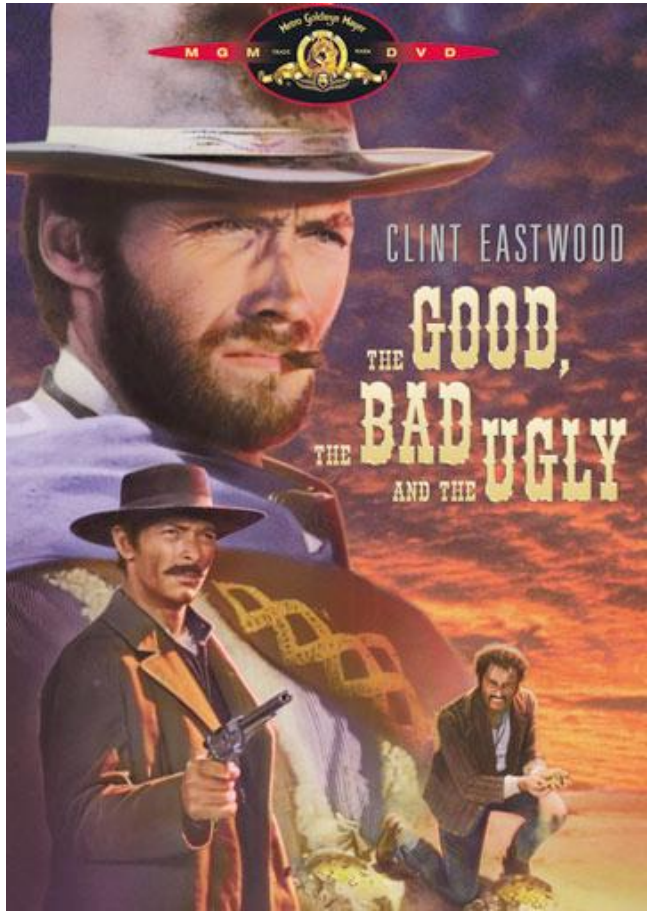
Security - the Grid View

The Good, the Bad and the Ugly



e-IRG Workshop
Zurich, April 24, 2008
Christoph Witzig
christoph.witzig@switch.ch

www.eu-egee.org

Information Society and Media

Content

- Introduction
- Technical Side
- Organizational Side
- The road ahead

Introduction (1/2)

- **Security: is the condition of being protected against danger or loss** (source: Wikipedia)

- **Counter measures:**
  - Good walls
  - Good soldiers

  (Technical and organizational measures)

- **Grids: Sharing of resources across administrative domains**

  --> easy and open access vs danger and loss

Introduction (2/2)

- *Google on* “Grid Security” *yields*
  - **GSI = Grid Security Infrastructure**
    - **Certificates**
    - **Mutual authentication**
    - **Confidential communication**
    - **Private keys**
    - **Delegation, single sign-on**
  - Technical view

- **No standards on Grid security organization!**
  - EGEE security coordination group

Content

- Introduction
- Technical Side
- Organizational Side
- The road ahead

Grid Security Model (GSI) (1/2)

Swiss Passport

VO

attributes

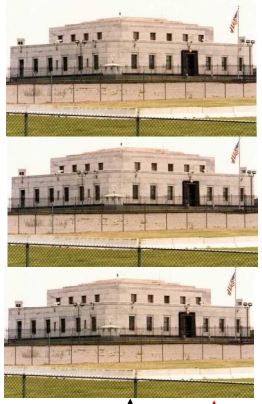
Swiss Passport X.509

Swiss Passport Proxy X.509 w/ VOMS AC

job sub-mission

Swiss Passport

Worker Nodes



Resource Broker

Swiss Passport

Computing Element (CE)

Swiss Passport

Grid Security Model (GSI) (2/2)

- **Issuance of long-lived certificates**
  - Revocation of certificates
- **Use of proxy certificates**
  - Needed for delegation !
  - Private key together with proxy certificate
  - Short lifetime
  - Need to be renewed
- **Grid services perform authentication and authorization of users**
  - Authorization policies not standardized, often inconsistently published

Summary Technical Side

- **Very successful --> basis on which existing Grid infrastructures have been built**
- **Based on certificates**
  - advantages and disadvantages
- **Use of proxies for delegation**

Content

- Introduction
- Technical Side
- **Organizational Side**
- The road ahead

Use Case 1

1. **A system administrator of the IT services discovers during regular check at his site that a Grid resource in a temporary test-bed has been compromised (e.g. sshd). The resource was installed and maintained by a user group in a department of the university.**
2. **Site security officer is informed**
    1. National CERT and OSCT are informed (over restricted mailing lists)
3. **OS reinstallation, host (and user) certificate revocation**
4. **All hosts maintained by this user group are checked:**
    1. Accounts have been compromised
    2. Weak passwords are found
    3. Incoming SSH connections are possible on pool accounts
    4. Firewall rules needed cleanup
5. **User group receives additional training by local CERT team**
6. **OSCT takes this incident as an example at their next training session at the EGEE forum**

Outcome: One weak spot in the Grid was fixed and lessons learnt.

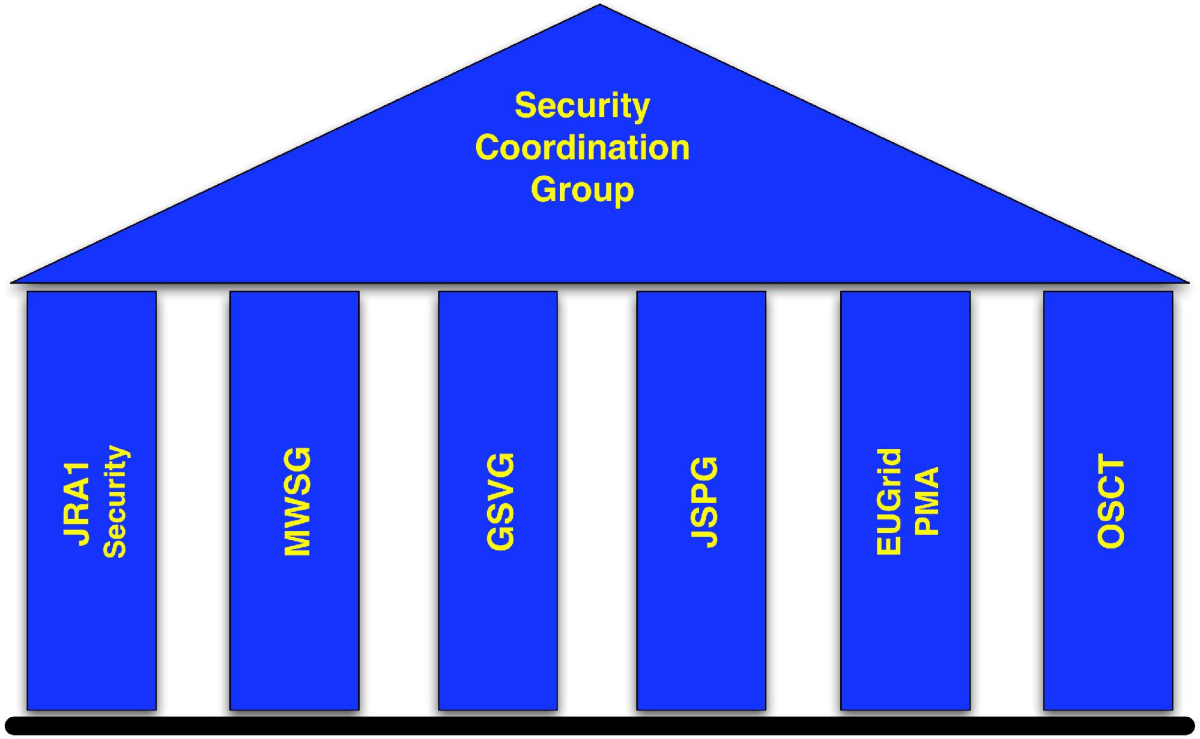
Use Case 2

1. Local site administrator discovers by pure chance a vulnerability in a script on a grid resource. He mentions it to a colleague, who mentions over coffee it to the local CERT.
2. The CERT member (not a Grid specialist himself) asks another colleague to post a mail on the MSWG mailing list.
3. A discussion starts whether this is a “bug or a feature”, i.e. poor scripting or a site security issue.
4. Key person is on vacation - nothing happens.
5. OSCT insists on a quick action: Warnings are given to grid site security personnel. Script is modified, tested, certified and released.
6. A bug in the script is discovered while it is being installed in the entire Grid --> back to step 5.

Outcome: Long, painful and inefficient resolution of a simple problem.

Conclusion: Efficient organization is key for success

EGEE Security Organization



JRA1 / Security

Grid Security Vulnerability Group

EUGridPMA

Middleware Security Group

Joint Security Policy Group

Operational Security Coordination Team

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

Security in EGEE-III: 440 PM

Middleware Security Group

- **Meeting place for security architects and security related groups**
- **Co-chaired by EGEE and OSG**
- **Longer-term middleware issues as well as short-term important issues**
- **Challenges:**
  - Transition from ideas into implementations
  - Stronger interaction between middleware and site security specialists
    - Emphasis for EGEE-III

Grid Security Vulnerability Group

- **Purpose:**
  - find and eliminate any Grid Security Vulnerabilities in the Grid middleware and its deployment, and prevent any new Grid Security Vulnerabilities from being introduced
- **Eliminating Vulnerabilities by handling specific issues**
  - Most of the work done so far is in this area
  - Grid security Vulnerability issues may be reported by anyone
  - Or may come as a result of code walkthroughs or security testing and reviews
  - Since start of activity 133 issues submitted, currently 55 open issues
  - Detailed process described at http://www.gridpp.ac.uk/gsvg/
  - Advisories at: http://www.gridpp.ac.uk/gsvg/advisories/
- **Prevention of the introduction of new vulnerabilities**
  - Education – developer guidelines and checklist
  - Plan to further develop this area in EGEE-III.

Joint Security Policy Group

- **Prepare and maintain security policies for EGEE and WLCG**
  - And advise on any security matter
- **Aim for simple, general and interoperable policies of use to many Grids**
  - To allow VOs to easily use resources in multiple Grids
- **Joint effort by EGEE and WLCG**
  - With strong participation by OSG, NDGF and others
- **Policy documents on**
  - General Grid Security
  - Acceptable Use
  - Site Operations
  - VO Operations
  - User, Site and VO registration
  - Traceability and Logging
  - Security Incidents response
- **Aim for EGEE-III: involve more NGIs**
- **http://proj-lcg-security.web.cern.ch/proj-lcg-security/default.html**

EUGridPMA

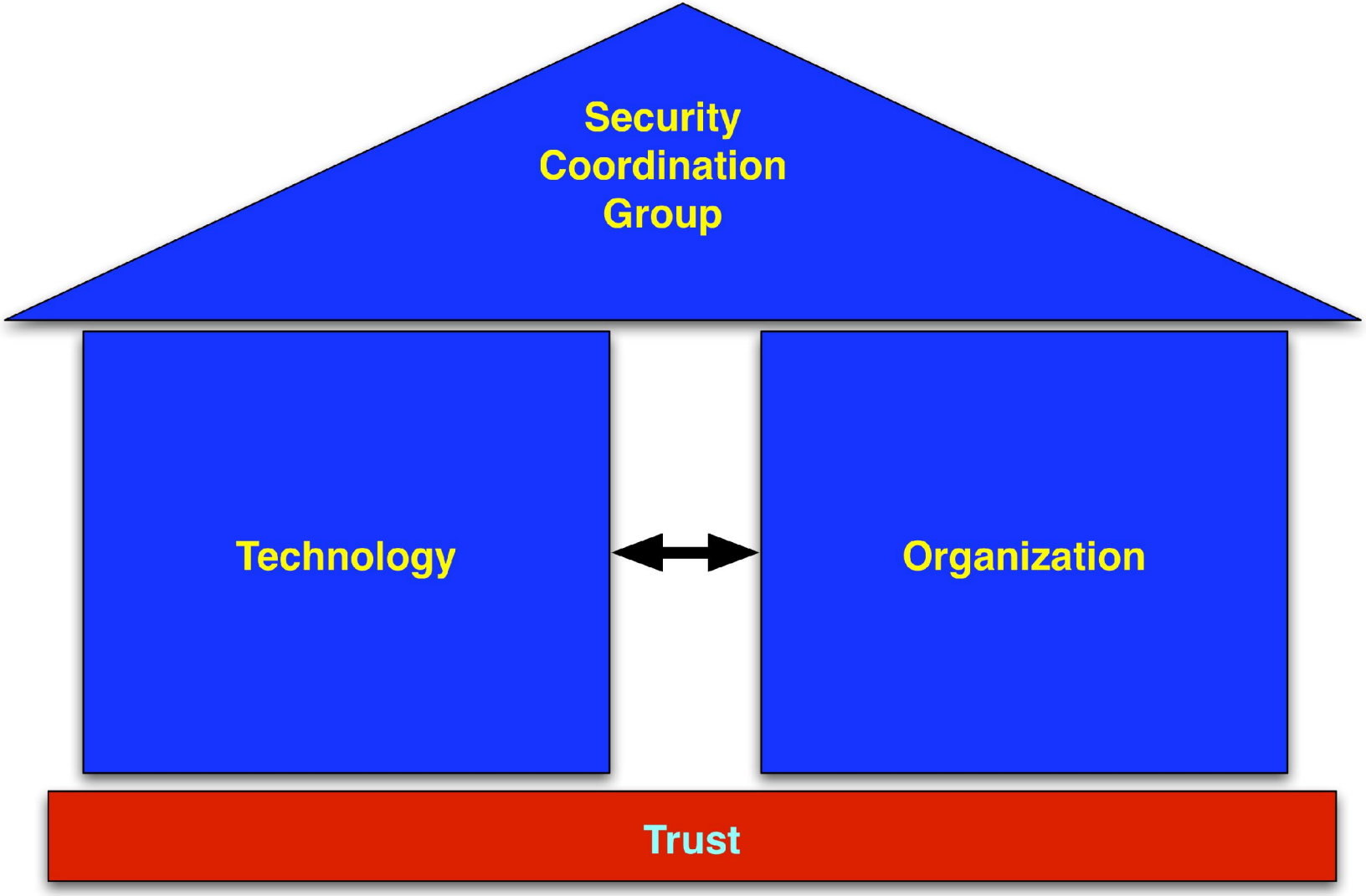
- Coordination of the (PKI-based) trust fabric for e-Science Grid authentication in Europe
- Collaboration with peer organizations in America and Asia (IGTF)
- Basis for the guidelines on the accreditation procedure and profiles for CAs
- Distribution of CA root certificates

Operational Security Coordination Team

- **Operational response to security threads against EGEE infrastructure**
  - Focus on computer security incident handling
  - Providing reporting channels (OSCT -> ROC -> site)
  - Pan-regional coordination and support
  - Security monitoring
  - SSC: Security Service Challenge
  - Best practice and advice for Grid system administrators
    - Training http://osct.web.cern.ch/osct/dissemination.html

- **Much needed feedback for middleware developers**

EGEE Framework

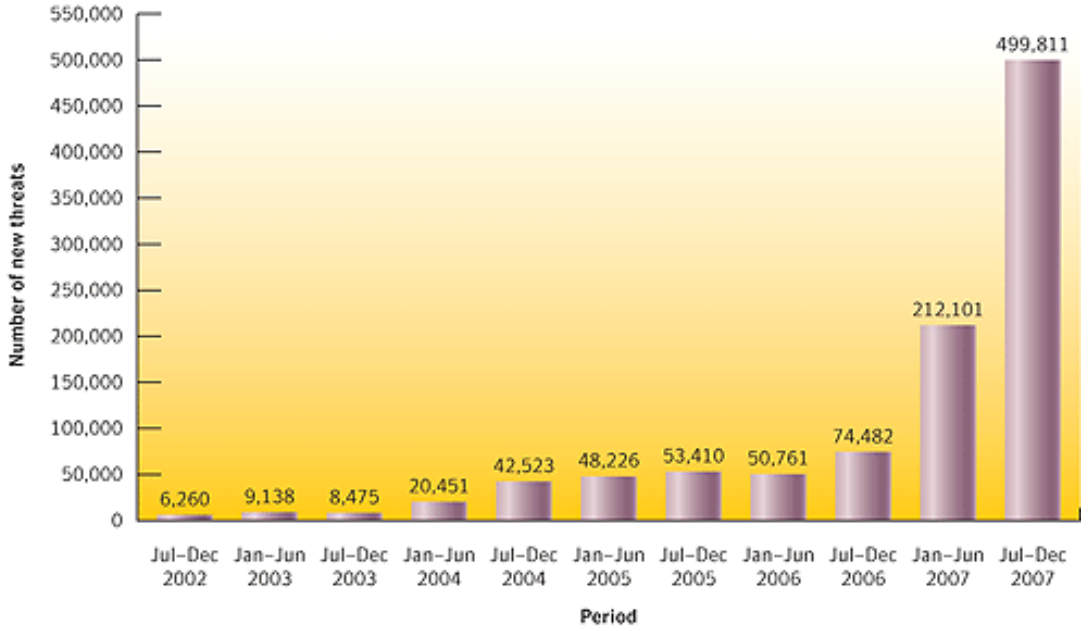


Content

- Introduction
- Technical Side
- Organizational Side
- **The road ahead** (personal view)

The Road Ahead … (1/3)

1. **Security threats will only increase**
   - It's all about money !



In 2007, Symantec detected 711,912 new threats compared to 125,243 in 2006—an increase of 468 percent; this brings the total number of malicious code threats detected by Symantec to 1,122,311 as of the end of 2007

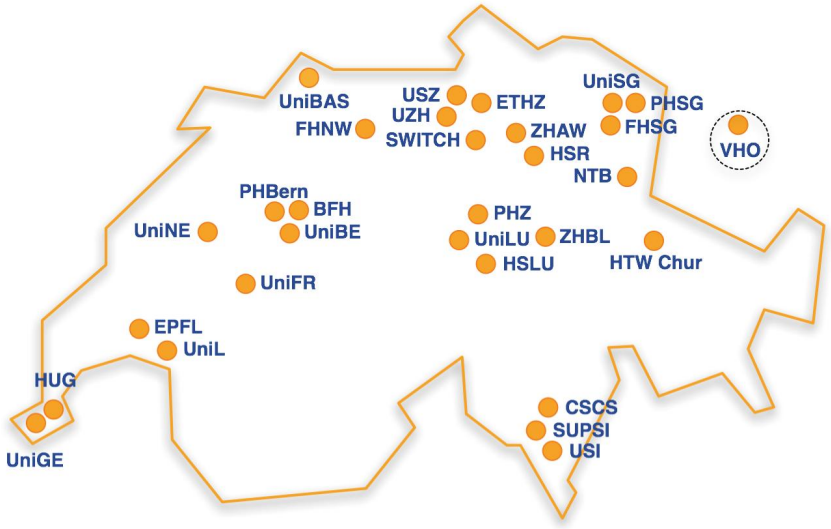
Source: symantec

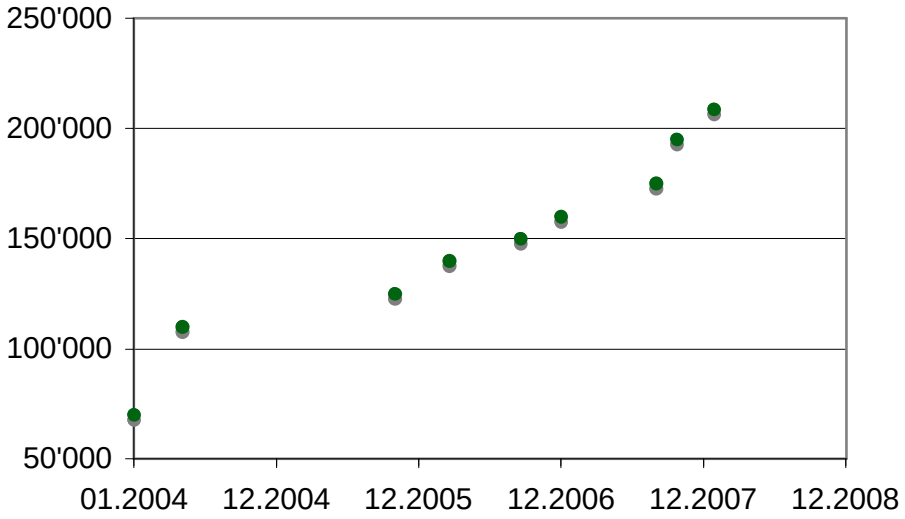
e-Science must not assume that it will not be a target

The Road Ahead … (2/3)

2. National Authentication and Authorization Infrastructures (AAI)

- Based on Federated Identity





- In CH: 80% coverage in higher education (220’000 accounts)
- Opportunity for Grids to grow significantly beyond existing user base

The Road Ahead … (3/3)

3. **Increased collaboration in security between Grid community and CERT / NRENs**
   - At institutional level
   - At national level
   - At international level

Conclusion

1. **Technical and organizational measures must be combined to increase security**

2. **EGEE Security Organization as a model for security in Grid infrastructure**

3. **(Personal) Outlook:**
   1. Federated identity offers perspective of large user community
   2. Increased collaboration between stakeholders in e-Science (Grid - CERT - NREN)
   3. Security challenges will only get bigger

Finale “the good, the bad and the ugly”

“there are two kind of men:
those with loaded guns and those who dig”

Q & A