EGI Security Threat Risk Assessment

Dr Linda Cornwall

Rutherford Appleton Laboratory /STFC

Contents

- D4.4 – Security Risk Assessment of the EGI Infrastructure
- EGI Security Threat Risk Assessment – Description
- EGI Security Threat Risk Assessment – Results
- Still to do/EGI Review 2012

D4.4

- Security Risk Assessment of the EGI Infrastructure
- D4.4 is a public document at:

https://documents.egi.eu/secure/ShowDocument?docid=863

- Completed at the end of January 2012

D4.4 What we considered

- Possibly the reviewers last year were not fully aware of the security activities taking place in EGI
- D4.4 aimed to be a comprehensive document describing the groups and activities
- As well as a plan for a Security Threat Risk Assessment.

Scope and aims of EGI security

- Where we give our answer to the question “what does it mean to be secure in the Grid”
- The EGI Ecosystem
  - Service and RPs, funding bodies, SW providers, User community.
- EGI’s Assets
- Aims and Role of EGI.eu

Scope and aims (cont.)

- Users and EGI Security
  - Including assurances they can expect/not expect and obligations
- Resource providers
  - Again assurances they can expect and obligations
- Data and information security
  - Including what types of data EGI infrastructure is/is not suitable for

EGI D4.4 other contents

- Security Groups and activities in EGI
- Practices and standards
  - This includes standards for information management e.g. ISO series and how some procedures are already partially compliant
  - Possible further future usage of standards and conclusions
- Operational Security during EGI
- Plans for the Security Threat Risk Assessment

EGI Security Threat Risk Assessment

- Threats are seen as threats to EGI's assets, whether they be technical threats or social threats
- Assets are listed
- Defined Steps for carrying out the Security Threat Risk Assessment
- Starting with establishing a team to carry out the work

The team

“The EGI Security Assessment group”

Riccardo Brunetti
Linda Cornwall
Carlos Fuentes Bermejo
Sven Gabriel
David Groep
Elisa Heymann
David Kelsey
Maarten Litmaath
Mingchao Ma
Giuseppe Misurelli
Leif Nixon
David O’Callaghan
Eygene Ryabinkin
Adam Smutnicki
Virginia Martin Rubio Pascual
Peter Solagna

Observers/for info:

Romain Wartel
Tiziana Ferrari

THANKS TO ALL OF THESE PEOPLE!!

For work on D4.4 and the Security threat risk assessment

How the team worked

- E-mail
- Series of EVO meetings
- Discussed and came to a consensus on methods we used
- Most of the work carried out in a spreadsheet

Assessment not public

- Not all the information should be public
- The assessment inevitably includes a list of weaknesses within the existing infrastructure and planned mitigations; if it were public it would be a valuable source of information to potential attackers

Threat categories

- Defined 20 threat categories, examples
  - Threats due to software vulnerabilities
  - Physical Security Threats to the infrastructure
  - Scientific and User data reliability
  - Illegal and general misuse
  - Threats to external parties
  - Security Threats from installation of new software and technologies

Selection of Threats

- Each team member given 1 or 2 categories, and asked to identify threats
  - and establish the current situation/mitigation in place
- Total of 75 threats identified
- Mostly high level threats, not technology dependent

Threat Category example

- Threats due to software vulnerabilities
  - Incident due to exploit of vulnerability in grid middleware
  - Incident due to exploit of vulnerability in commonly deployed software other than middleware widely used in the EGI infrastructure (e.g. Linux)
  - Incident due to vulnerabilities in other software installed on the infrastructure (e.g. VO software)

Computation of Risk

- Risk is usually the product of the likelihood and impact/cost
- Actuarial computation of risk
  - This is the typical method used by insurance companies based on statistics (e.g. death rates at a given age)
  - We have no suitable statistics
- So we looked for a way of providing a numerical value based on judgment

Method chosen for computation of Risk

- We decided to ask all members to rate the ‘likelihood’ and ‘impact’ of each risk between 1 and 5.
- Risk = ‘Likelihood’ x ‘Impact’
- That gives a max risk value of 25.
- Ratings based on current situation and mitigation in place
- We recognize that people’s ratings are always a bit subjective, so we tried to add some objectivity

‘Likelihood’ guidelines

1. Unlikely to happen
2. May happen 2-3 times every 5 years
3. Expected to happen once a year or so
4. Happens every few months
5. Happens once a month or more

Impact guidelines based on WLCG

- Impact guidelines based on WLCG Computer Security Risks Assessment
- http://rwartel.web.cern.ch/rwartel/security_teg/WLCG%20Risk%20Assessment.pdf

- Shortened description….

‘Impact’ guidelines

1. Minimal impact on EGI’s ability to deliver its services to users or on any asset
2. Minor impact, such as some operational or financial costs, local disruption
3. Serious localized disruption to some services for some users, for a week or more
4. Serious Multi-national disruption
5. Very serious disruption, damage to reputation and/or 3rd parties

Team members ratings

- We received 9 sets of ratings on likelihood and impact.
  - 2 were from 2 people jointly
  - Therefore 11 members effectively provided responses.
- In some cases blanks or question marks were present for some threats
  - These were not counted in the computation

Risk Computation

- Risk in each case computed by taking the product of likelihood and impact for each response
- Average risk computed – weighting those sets of results returned by 2 people twice
- Average impact also computed
- All is in a spreadsheet

Discussion on divergent ratings

- Then each member was asked to compare the result to their own ratings
- Members invited to highlight any threat they wished to discuss
- No numbers actually changed – but highlight some threats with higher risk or higher impact as a result of the discussions

Threats reported

- We reported threats having a risk value of 8 or more (out of max. of 25) - 18 found
- We reported threats having an impact value of 4 or more (max 5) - 3 found
  - Plus one other highlighted as a result of discussion
- This is out of 75 threats identified

Threats of highest risk value

- New software or technology may be installed which leads to security problems
  - History has shown that new technology or software comes with new set of problems
  - Risk = 11.3
- Incident due to exploit of vulnerability in software other than Grid middleware
  - E.g. linux
  - Risk = 11.0

Threats of highest risk value (2)

- Security problems arising from the move to IPv6
  - Risk = 10.9
- Insufficient staff may be available to carry out security activities
  - Risk = 10.6
- Incident spreads across the Grid
  - Risk = 10.5

Threats of highest risk value (3)

- The move to more use of Cloud technologies may lead to security problems
  - Risk = 10.1
- Un-patched software and host operating systems not updated
  - Risk = 9.9

Threats of highest impact value

- Authentication and Authorization Infrastructure compromised
  - Impact = 4.2
- Resources used for on-line attacks to external parties
  - Impact = 4.1
- Reputation damage due to security incidents
  - Impact = 4.0

Another threat highlighted

- After discussion
- Trusted staff, employees or ex-employees act in inappropriate manner
- We have tended to assume all trusted staff are trustworthy (site admins, CA admins etc.)
- Agree a lot of damage could be done if one wasn't

Still to do –

- Tidy the spreadsheet and make more suitable for management/wider project distribution
- Consider distribution of final report
  - Possibly to wider project audience
- Possibly distribute summary spreadsheet more widely
- More on mitigation of the highest risk and highest impact threats

EGI Review 2012

- D4.4 approved
  - Recommended that this document is kept under review and refined as circumstances change
- Security threat risk assessment
  - Good first step
  - Should be private
- We had thought we'd do another 18 months later
  - This plan supported by the reviewers

Questions?

- ??