Vulnerability handling, Risk management, and plans for transition to EGI

Linda Cornwall

STFC, The Rutherford Appleton Laboratory.

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

www.eu-egee.org

e-infrastructure

Contents of talk

- Brief reminder of strategy for handling Grid Security Vulnerabilities in EGEE-III
- Status update
- Plans for transition to EGI
- Questions on Vulnerability handling and transition to EGI

- Plans for an Overall Security Risk Assessment to be led by the Security Co-ordination Group (SCG)

The Grid Security Vulnerability Group (GSVG)

- Started in EGEE-II, continuing in EGEE-III
- “The Purpose of the Grid Security Vulnerability Group is to eliminate Grid Security Vulnerabilities from the software, and prevent new ones being introduced. The aim is to provide a high level of confidence in the security of the deployed infrastructure, thus reducing the risk of incidents.”
- Largest part of the work is the handling of specific Grid Security Vulnerability issues as they are found

People involved in GSVG issue handling

Linda Cornwall, Stephen Burke (RAL, UK)

Vincenzo Ciaschini (INFN, Italy)

Ákos Frohner, Maarten Litmaath, Romain Wartel, Gergely Debreczeni (CERN)

Oscar Koeroo (NIKHEF, Holland)

Daniel Kouril (CESNET, Czech Republic)

Kálmán Kővári (KFKI-RMKI, Hungary)

Eygene Ryabinkin (RRC-KI, Russia)

Åke Sandgren (HPC2N, Sweden)

GSVG Issue handling summary

- **This was established and approved in EGEE-II**
- **GSVG handles issues concerning the EGEE middleware, it's deployment, and more general concerns**
- **Anyone may report an issue**
  - By e-mailing to grid-vulnerability-report@cern.ch or
  - By entering in the GSVG savannah https://savannah.cern.ch/projects/grid-vul/
    - Note that bugs are private so cannot be read except by members of this savannah project
- **The Risk Assessment Team (RAT) investigates the issue , and for valid issues carries out a Risk Assessment**

Risk Assessments

- **Each valid issue is placed in 1 of 4 risk categories**
  - Extremely Critical
  - High
  - Moderate
  - Low
- **Target Date for resolution set according to risk**
  - Extremely Critical – 2 days
  - High – 3 weeks
  - Moderate – 3 months
  - Low – 6 months
- **This allows for the prioritization and timely resolution of vulnerabilities**

Disclosure

- **Information kept private – until advisory is released**
- **Advisory released on**
  - Target Date or
  - When a patch is issued
    - Advisory refers to the release
    - Release notes refer to the advisory
  - Whichever is the sooner
- **Advisories are released on the GSVG web page at http://www.gridpp.ac.uk/gsvg/advisories/**

  (earlier advisories were in the release notes)

What GSVG does not do

- **GSVG does not handle vulnerabilities in operating systems**
  - If information is reported to us we will pass it on
- **GSVG does not handle vulnerabilities in non-Grid specific 3rd party software**
  - Again we will pass it on
- **Fix vulnerabilities in software**
  - But some GSVG members are members of development teams so do fix vulnerabilities
  - not a GSVG task
- **GSVG does not handle incidents – i.e. where issue has been exploited**
  - Incident prevention
  - If incident is due to a vulnerability – GSVG will get involved

Some numbers (17th Sept 2009)

- **174 Issues submitted since started in 2005**
  - (28 submitted in last 12 months)
  - For those fully risk assessed (since current strategy started mid 2006) 1EC, 19 High, 21 Moderate, 39 Low
- **111 closed**
  - 64 closed as fixed, 16 invalid, 5 duplicates, 10 OSCT informed, 5 software no longer in use, 11 more general concerns adequately addressed
- **63 open**
  - 17 awaiting TD, 15 disclosed, most of the rest either very low risk or more general concerns rather than specific vulnerabilities
  - Situation with open issues not awaiting TD described in document at https://edms.cern.ch/document/1011173/1
    - Unlikely to contain any surprises

Experience of Issue handling

- **The majority of issues get investigated in a timely manner (i.e. within 2-4 working days)**
- **Earlier on there was possibly a tendency to put things in too high a risk category**
- **RAT members now usually agree on Risk categories – probably we get it about right now**
- **The majority of issues which remain open long term are more general concerns over security rather than vulnerability bugs**
  - These will be considered as part of the Overall Security Risk Assessment

Vulnerabilities and EGI

- **It is recognised that Grid Security Vulnerability issue handling will be needed as the Grid moves to EGI**
- **The main purpose should continue to be the elimination of vulnerabilities from the deployed infrastructure and prevent the introduction of new ones**
  - This should be part of EGI (not the software process) to ensure that the focus is on ensuring the deployed infrastructure is as secure as possible.
  - The issue handling process also needs some independence from the Software development process, so that information on issues can be disclosed in a timely manner
- **Close co-operation will be needed with the EGI software distribution**
  - such as the Unified Middleware Distribution (UMD) and software development teams

Software Vulnerabilities Group (SVG) in EGI

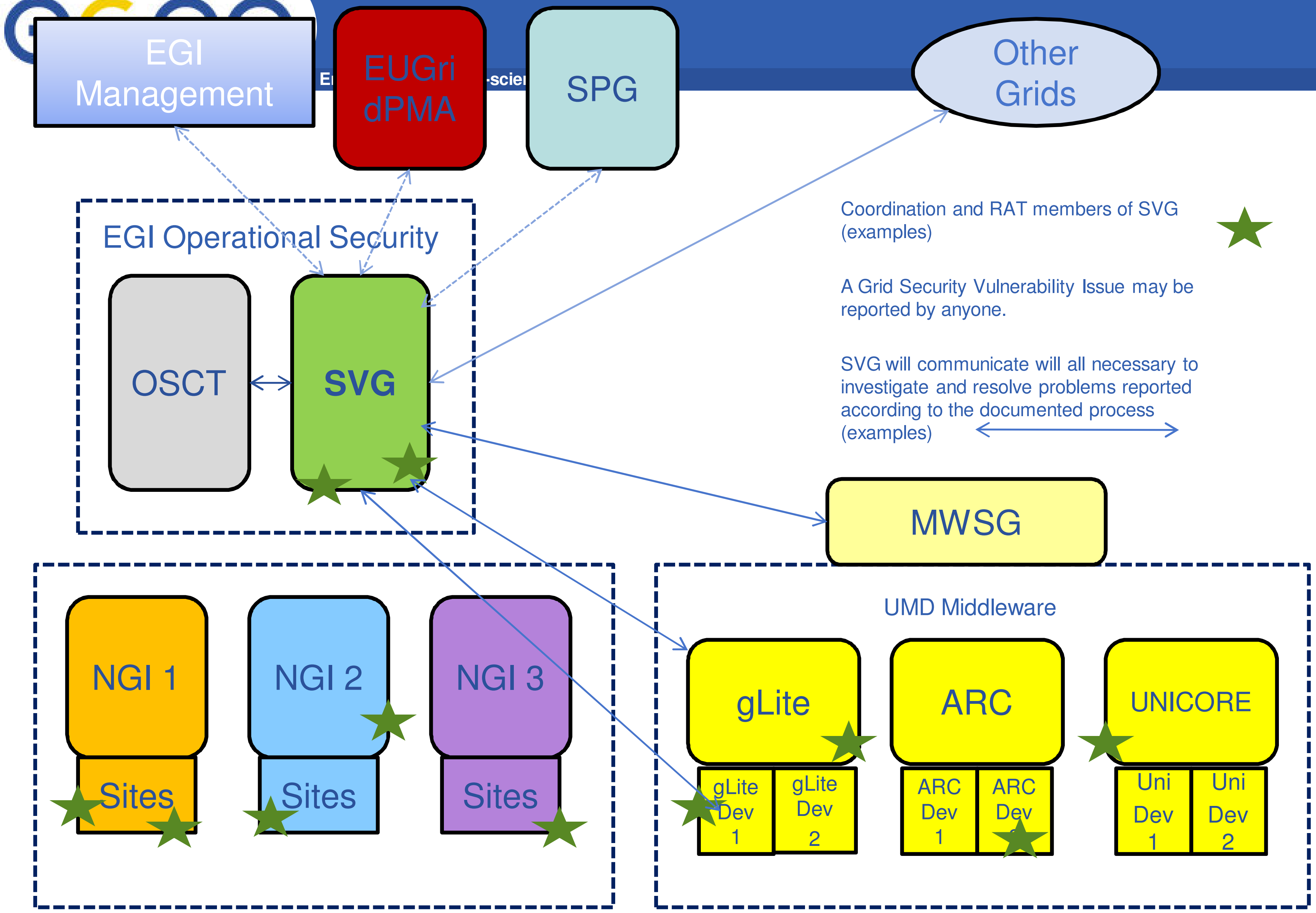
- **The Software Vulnerabilities Group will be part of Security Operations**
- **SVG chair along with 2-3 deputies will co-ordinate the activity**
- **Risk Assessment Team (RAT) members will continue to be needed**
  - Better to have a reasonable size group of people spending a small % of their time on this activity, for max range of expertise
- **Members will be drawn from NGI site administrators and other deployment teams, software development teams and other security experts**
  - Influence on exactly how things are done is established by providing effort
  - This gives incentive to provide effort

Effort for EGI SVG

- Current members will, of course, be invited to continue
- Further effort will be invited
- As people either join, or continue from GSVG details of the EGI strategy will be defined

Issue Handling in EGI

- **Issue handling should follow similar principles to within EGEE-II and EGEE-III but with the major difference that software will effectively be 3rd party**
- **If vulnerabilities are reported to SVG, then they will be handled in a similar way to the EGEE-II/EGEE-III GSVG issue handling strategy**
  - Risk Assessments carried out
  - Advisories disclosed on or before Target Date
- **If vulnerabilities are found and fixed by the software provider, it is necessary to ensure that the patches are incorporated in the EGI/UMD software in a timely manner**



Coordination and RAT members of SVG (examples) ★

A Grid Security Vulnerability Issue may be reported by anyone.

SVG will communicate will all necessary to investigate and resolve problems reported according to the documented process (examples) ⟷

Transition to EGI

- **A description of the principle of Grid Security Vulnerability issue handling and responsible disclosure will be produced early**
  - Ask for formal approval from EGI project
- **When a software provider ‘signs up’ to be part of the UMD/EGI software distribution they agree to**
  - The principle of the SVG including the responsible disclosure strategy
  - Provide contact details for developers when the SVG is investigating an issue
  - A response time, and to co-operate in the investigation of issues
  - Co-ordinate distribution of software with EGI if they find a vulnerability themselves
  - And decide whether they wish to supply effort to the process

When does transition occur?

- **Once middleware is distributed by EGI/UMD any vulnerabilities in that middleware will be handled using the EGI strategy**
  - The transition to EGI for vulnerability handling will happen as the transition to distribution from EGI happens.
  - The speed of transition from the EGEE GSVG issue handling to the EGI SVG handling will largely depend on when software becomes distributed by EGI rather than by the current methods
- **A lot of the process details will be established at this time**
  - Established by the EGI SVG team which provides both acceptance of the process and incentive to supply effort

Before move on

- Any questions on vulnerability handling and transition to EGI?

Overall Security Risk Assessment

- **Here we consider security threats and risks to and resulting from the Grid deployment**
  - This is a risk assessment for high level threats, not specific vulnerabilities
- **This work will be carried out by the EGEE Security Co-ordination Group (SCG), and members of GSVG, OSCT, JSPG and others.**
- **This is partly an update of the LCG Risk analysis carried out in 2003**
  - 44 high level risks were identified
  - Committee decided on risks

http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html

LCG Risk Analysis

ID	Description	Risk Analysis				
		Likelyhood		Impact		Computed
		Avg	Stdev	Avg	Stdev	Risk
Security Issues - Intentional or malicious attacks						
Misuse of LCG resources - CPU, storage, network etc						
M1	Resources used to launch online attacks on other sites via DOS, Virus, Worms, SPAM etc	3.0	0.0	3.0	0.0	9.0
M2	Resources used for offline attacks on other sites, e.g. to crack passwords or pass phrases	2.0	0.0	2.0	0.0	4.0
M3	Resources used to distribute or share non-LCG data, e.g. copyrighted, illegal, or inappropriate material	3.0	0.0	3.0	0.0	9.0
M4	Resources misused by inappropriate setting of access control or priority	3.0	0.0	1.0	0.0	3.0
M5	Use of LCG resources by unauthorized parties	3.0	0.0	1.0	0.0	3.0
M6	Use of LCG resources for unauthorized purposes, e.g. financial gain	2.0	0.0	2.8	0.5	5.5
Confidentiality and Data integrity issues						
C1	Theft of credentials, e.g. private keys	3.0	0.0	2.0	0.0	6.0
C2	Data or passwords/pass phrases exposed, e.g. in unprotected files or on the network	3.0	0.0	2.0	0.0	6.0
C3	Falsification of scientific data, analysis and/or results	1.8	0.5	3.0	0.0	5.3
C4	Unauthorized monitoring of network communications	2.0	0.0	2.0	0.0	4.0
C5	Unauthorized access to data	3.0	0.0	1.0	0.0	3.0
C6	Unauthorized distribution or exposure of data	2.8	0.5	2.0	0.0	5.5
C8	Identity or usage information is harvested by unauthorized persons	2.0	0.0	1.0	0.0	2.0
Disruption of LCG infrastructure for political or other reasons						
D1	Disruption via exploitation of security holes	3.0	0.0	3.0	0.0	9.0
D2	Corruption of or damage to data	1.0	0.0	2.8	0.5	2.8
D3	DOS attacks towards LCG to prevent normal working of network or services	1.8	0.5	3.0	0.0	5.3

Main similarities

- A team decides which threats to consider
- Identified threats are risk assessed based on people’s judgement of impact and likelihood
- The two are multiplied together to give a risk value

Main differences

- The current situation should be clarified for each threat/risk
- The risk assessment is based on the current situation
- The results are presented to management including the Technical Management Board (TMB) to encourage mitigation of the highest risks
- Suggestions may be made for what needs to continue to keep risks down, and what further may be done to reduce risk

1st step: establish a team

- Anyone interested in carrying out this assessment can join
- JSPG, SCG, GSVG, OSCT have been e-mailed about this

2nd step: Review the strategy

- **I have drafted a strategy in a brief document – the team should review it and modify if necessary**
- **Basically it is to**
  - Select threats/risks
  - Assign a team member responsible for each threat/risk
    - Probably all team members will have to be responsible for some threats
  - For each threat/risk the team member responsible establishes the current situation
  - Compute the risk
    - Review method of computation of risk
  - Present our findings – including comments and suggestions

3rd step: selection of threats

- **I have produced a draft selection of threats in a spreadsheet**
  - This includes all from the LCG Risk Analysis
  - Plus a few from OSG's list
  - Plus a few that have been reported to GSVG which are general concerns rather than software bugs
  - Plus others I have thought of
- **The team should decide which threats are assessed**
  - If a team member wishes to include a threat – it should be included rather than excluded
  - The team may consult others
- **Threats should be general rather than software specific**
  - However the software currently used may define the current situation and hence the likelihood aspect of the risk

Step 4: establishment of current situation

- **For each threat a ‘responsible’ is assigned**
  - Team members volunteer for threats they know most about
  - This does not mean they are responsible if the threat is carried out, or for the existence of the threat, they are just responsible for finding information
- **The responsible then checks the current situation for the threats he/she is assigned**
  - In some cases this may be trivial, in others may require some work
  - Other experts may be consulted
- **This is important, so that the risk can be computed according to the current situation, not some hypothetical situation**
- **The more safeguards in place – the lower the risk**

Step 5 Computation of Risk

Most actuarial computation (e.g. insurance) of risk is based on statistics, based on likelihood and cost.

We attempt to produce a numerical value for risk without appropriate statistics – based on judgement

Each team member gives their opinion on the

- Impact between 1 and 5
  - 1 low, 5 high
- Likelihood between 1 and 5
- Then discuss to see if we can find an agreement
- Multiply together to produce a numerical value of risk

This computation method is my first suggestion – the team should agree the method of computation of risk

Step 6: Present to management

- **Results of the Risk Assessment should be presented to management**
- **Suggestions and comments may be made on how to either mitigate threats, or ensure current mitigating action stays in place**
- **For the higher risks, it is hoped that action will be taken**
- **This is primarily the responsibility of management and the TMB**
  - The Overall Security Risk Assessment task ends with presenting findings to management
  - This does not mean team members will not help to mitigate risks

Docs and contact

- A brief document describing the Overall Security Risk Assessment plan, and a spreadsheet containing the first draft of the threats is available at:

https://edms.cern.ch/document/1020617/1

- If you are interested in participating, please e-mail me: Linda.Cornwall .at. STFC.ac.uk

TBDs concerning overall RA

- Does the strategy make sense?
- Should the process be carried out by e-mail, or does the team need to get together and work round a table?
- ???