# Grid Services Security Vulnerability and Risk Analysis

*Dr Linda Cornwall*

*RAL*

www.eu-egee.org

Information Society and Media

# Contents

- Why we setup the Grid Security Vulnerability Group
- Starting up the GSVG
- Initial strategy and disclosure policy
- Vulnerability Task in EGEE II
- Setup of the GSVG in EGEE II
- Disclosure policy in EGEE II
- Risk Assessments
- Other vulnerability related activities in EGEE II

# Why we set up the Grid Security Vulnerability Group (GSVG)

- **A lot done concerning Grid Security Functionality**
  - Authentication, Authorization
- **Not much being done to ask "Is the Grid Secure"**
- **We know the software isn't perfect**
  - Some vulnerabilities are in the process of being fixed
  - Some are probably waiting to be exploited
- **It will be really embarrassing if when the Large Hadron Collider comes on line at CERN we get a serious attack which prevents data being stored or processed**
- **Hackers Conference HOPE mentioned Grids**
  - Unfriendly people without credentials aware of us
  - Cannot rely on security through obscurity
- **Real Grids are being deployed**
  - No longer a research/proof of concept activity

# Starting up the Grid Security Vulnerability Group (GSVG)

- **Started up in 2005 with part of my time and a few “best efforts” volunteers**
- **Aim to inform developers and deployment people of vulnerabilities as they are identified and encourage them to produce fixes or to reduce their impact.**
  - Aim to keep grids deployed, avoid incidents, improve Grid Security with time
- **Joint effort between Large Hadron Collider Grid (LCG), UK particle Physics Grid (GridPP), and EGEE**
- **Some people were worried about the legality of not making info available to all**
- **Defined a policy and strategy for carrying out the work**
- **Got project management approval of our terms**

# Initial strategy and disclosure policy

- **Log issues, set a Target Date (TD) usually 45 days**
- **If issue is still open on TD, distribute information including risk assessment to LCG security contacts**
  - Vulnerability group does not make issues public
  - Security contacts considered internal
- **Includes both software and deployment issues**
- **Issues entered by anyone**
  - Developers enter issues they know about
  - Includes information from internal knowledge
  - Includes impact of missing functionality which will not be available in the short term

# Achievements and problems

- **Collected 84 potential issues**
  - 18 closed (8 fixed, 9 invalid/not a problem, 1 duplicate)
  - 6 fix rolling out/ awaiting the next release
  - 61 reports sent out to the LCG security contacts
- **Do not see enough issues closed by TD**
  - Not enough priority given to investigating or fixing issues
  - TD set to a default (problem prioritizing)
  - Looks worse than it is
    - Some issues are missing functionality
    - Many not directly exploitable
- **Some people who would have been very useful in the team didn't want to join**
  - Despite project approval

# The Vulnerability Task in EGEE II

- **In EGEE II there is funded manpower for the "Grid Services Security Vulnerability and Risk Assessment" Task ☺**
- **The aim is "to incrementally make the Grid more secure and thus provide better availability and sustainability of the deployed infrastructure"**
  - This is recognition that it cannot be made perfect immediately
- **The Grid Security Vulnerability Group (GSVG) is the largest activity in this task**
  - Which continues to deal with specific issues

# Setup of the GSVG in EGEE II

**The GSVG in EGEE II consists of**

- **Core Group Members**
  - Run the general process
- **Developers from the various development Clusters**
  - Can confirm/check information on issues and fix issues
- **Risk Assessment Team (RAT)**
  - Carry out Risk Assessments
- **RAT people are security experts, experienced system administrators, deployment experts and developers**

# Process of the GSVG in EGEE II

- **Issue logged in Database**
  - Anyone can submit an issue
  - Only GSVG members can read or modify
  - Issues can also be submitted by e-mail
- **Issue is allocated to Risk Assessment Team (RAT) member**
- **RAT member**
  - Checks information,
  - Carries out a Risk assessment
- **2 other RAT members also carry out Risk Assessment**
- **Target Date (TD) set according to Risk**
  - To improve prioritizing
- **The issue is then allocated to the appropriate developer**

# Disclosure Policy for EGEE II

- **We plan to move to a responsible public disclosure policy**
- **On Target Date, information on the issue is made public**
  - Regardless of whether a fix is available
- **This depends on management approval,**
  - We need to prove we can do good Risk Assessments
  - Agree formula for setting the TD according to Risk

# Main changes

- **A risk assessment is carried out straight after issue is entered**
- **Improved Risk Assessments**
- **Target Date is set according to Risk**
  - By TBD formula
- **Information to be made public on the Target Date**

- **Good Risk Assessments and setting of TD according to risk is key to making the improved process work**
  - Which effectively prioritizes issues

# Risk Assessments

- **Currently establishing the best way to carry out Risk Assessments**
  - Risk Assessment Team (RAT) is working on this
- **Common Vulnerability Scoring System (CVSS)**
- **Location of issue on "Who can Exploit" "Effect" matrix**
- **Any other method RAT members propose**
- **What RAT members actually think**

# CVSS

- **CVSS is the Common Vulnerability Scoring System**
  - http://www.first.org/cvss/cvss-guide.html
- **Takes account of various factors e.g.**
  - Can it be exploited remotely
  - Access complexity
    - (whether it can be exploited at will or only in certain circumstances)
  - Authenticated or not
- **Modifies this according to temporal factors**
  - Availability of exploit code
  - Availability of fix or workaround
- **Modifies according to the environment**
  - This could be considered the Grid environment
- **CVSS provides a score between 0 and 10**
  - Possibility of translating this to a Target Date

# CVSS limitations

- **It is designed for information systems, not Grids**
- **Does not take into account some factors important on the Grid**
  - In particular, “who can exploit” is restricted to authenticated or not
- **We cannot, for example, ignore that one Grid node can affect others**
  - E.g. one sysadmin should not be able to setup a system that disrupts the Grid

# Exploit/effect matrix

- **Site security officers most fear is an attack that gives access to the whole site**
  - Especially if it can be carried out anonymously
  - DOS tends to be considered no more than medium risk
- **A vulnerability that can be exploited by an authorized user is less serious than one that can be exploited without credentials**
- **We can't ignore the possibility that credentials may be stolen**
- **Nor can we ignore that we may have a rogue sysadmin**
  - 100s sites in 10s countries
  - Grid expanding globally

# Matrix

| | Root Access | Local Account | Authz | Authn | No Cred | Other |
|---|---|---|---|---|---|---|
| System info | | | | | | |
| Local grid service Disruption | | | | | | |
| Confidential Data | Restricts usage for certain applications | | | | | |
| Unauthz usage | | | | | | |
| Grid-wide Disrupt | | | | | | |
| Impersonate | | | | | | |
| Attack other systems | | | | | | |
| Site Access | | | | | | |
| Root Access | | | | | | |

# Risk Assessments - Contd

- **Meeting at CERN shortly to see if we can agree a strategy**
  + Formula for Target Dates resulting from Risk
- **In future, possibly we will look at combining the CVSS calculation with the position on the matrix**
  – Plus any other criteria we define

# Other Vulnerability work in EGEE II

**Other activities currently ramping up**

- **Providing best practise guidelines for developers**
- **Co-ordinating code walkthroughs/reviews**
  - Largely to be commissioned by the Integration, testing and Certification Task in SA3
- **The vulnerability task is involved in co-ordinating the specific (security) tests as part of the certification process**
- **The possibility of carrying out Ethical Hacking is being considered**

# Summary

- **The GSVG is attempting to prioritize specific issues identified through risk assessments and setting Target Dates**
- **Other activities for reducing vulnerabilities**
  - Testing
  - Code walkthroughs
  - Ethical hacking
- **This work is important, the Grid has been described as a "Beautiful Amplifier" of vulnerability issues**

# Questions/Discussion