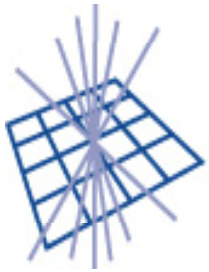

GridPP
UK Computing for Particle Physics

RAL 1957 2007
Celebrating 50 years of world class science

Security Concerns from GridPP and GSVG – feedback to MWSG

Dr Linda Cornwall, Rutherford Appleton Laboratory , Harwell Science and Innovation Campus, Didcot, OX11 OQX United Kingdom

EGEE'07, Budapest, 2rd October 2007

www.eu-egee.org

Information Society and Media

Contents

- Motivation
- GridPP concerns
- GSVG concerns
- Abbreviated checklist
- Discussion

Motivation

- **Discussions took place concerning security at the GridPP meeting in August**
  - Asked what are peoples biggest concerns
- **Certain types of concerns keep coming up in GSVG**
- **Feedback to MWSG so they can be discussed and dealt with**

GridPP concerns - glexec

- **Serious concerns about glexec**
  - Widespread concern
  - Quality of code
  - Really don't like setuid to root, possible side effects
  - Possible implications on traceability, accounting, non-repudiation
  - It is essential that you can trace who carried out an action
  - Noted that setuid is already present on the WN
- **Need to make sure that glexec**
  - model complies with security requirements, is not inherently flawed
  - does not contradict policy
  - is coded securely
  - does not expose vulnerabilities
  - sites are happy
- **(I know some testing is underway)**

GridPP concerns – RPMS and releases

- **Would like glite rpms to be signed**
  - 18 people agreed
- **Source RPMs should be made available**
  - Both for the purpose of being able to build on different platforms and so that it is easy to examine the code
  - Problems with large number of dependencies
- **Release notes are not always clear enough, in particular it is not clear which dependencies need updating**

GridPP Concerns – contd.

- **Don't like use of pool accounts**
  - 8 people agreed
  - Particularly concerned with the re-cycling of pool accounts
  - this may be due to concerns about traceability
- **VOMS rules should be consistent across the Grid**
- **VOs need to be able to manage their resources across the grid**
- **Tools should be available to enforce policy**
  - There was a debate as to whether the tools should or should not allow users to carry out actions that contradict policy, whether by signing the policy should simply mean users agree to comply with policy
  - Concern that general tools rather than grid tools may be available to users

GridPP general concerns

- **Lack of feedback from sites**
  - Possibly need to ensure that appropriate mechanisms are in place where sites can express opinion and know that they will be considered
- **Also someone stated ‘no-one thinks about security before something is released’**
  - Probably need to demonstrate that EGEE does!

GSVG concerns

- **Authorize all actions**
  - ensure Authorization cannot be bypassed
  - include file and information access
    - Confidentiality is a big concern for some applications
  - several issues due to lack of R-GMA authorization
    - both for read and write
    - in development
- **Ensure model/design is secure and complies with policy**
  - New EGEE security Architect

GSVG concerns (2)

- **Grid wide quota system is needed**
  - Per user, per VO
  - Processes, file space etc per WN, Per site..
    - Prevents DoS from overload
  - And globally
  - Related to the GridPP VOs need to be able to manage their own resources
- **Better logging is needed**
  - More efficient incident handling
    - Requirement to trace original DN
  - Useful for users too
  - Cannot be bypassed, e.g. using setuid
  - In work
    - https://twiki.cern.ch/twiki/pub/EGEE/EGEEgLite/logging.html

GSVG concerns - contd

- **VO code and Middleware code integrity**
  - Ensuring sites install ‘real’ code
  - Users/VOs being able to ensure that when they run a job it is using code as expected
  - Software signing – as strong GridPP request
- **Virtual Machines would make Grid more secure**
- **Restricting outbound access**
  - Prevention of Grid being used to attack other systems

Short developers checklist

- **Need to minimize the introduction of new vulnerabilities**
- **In 2005 produced a document including a checklist for developers**
  - http://www.gridpp.ac.uk/gsvg/docsguides/GridPPVulnerability.pdf
- **Tended not to be used, developers have too much to do, was probably too long**
- **Suggest a list of 10-20 top things to watch out for e.g.**
  - several vulnerabilities are simple file permissions
    - Both middleware developers and those producing yaim configuration files need to ensure file permissions are set correctly
  - checking input – avoiding SQL injection and XSS vulnerabilities
  - Still get buffer overflow vulnerabilities
- **Would such a simpler checklist be useful?**

Discussion

- **Over to you….**