Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

Security Policy Update

David Kelsey

UK HEP Sysman, RAL

1 Jul 2011

Outline

- Update since Ops-PMB at GridPP26 March 2011 in Brighton
- Current security policies
- EGI SPG work plans for 2011
- Service Operations Security Policy
- Endorsement and Operations of Virtual Machine Images
- Security for Collaborating Infrastructures
- Attribute Authority Operations

EGI Security Policy Group

- EGI SPG now firmly established – Terms of Ref, procedures etc.
- https://wiki.egi.eu/wiki/SPG
- Old JSPG (WLCG/EGEE) policy documents
  - Converted to EGI era
  - Approved by EGI EB in Sep 2010 (valid from 1st May 2010)
  - Apply to GridPP
- Where are they?
- https://wiki.egi.eu/wiki/SPG:Documents
- http://www.gridpp.ac.uk/security/policies/index.html

Current Security Policy

Top-level Grid Security Policy:

- Grid Security Policy

For all Users:

- Grid Acceptable Use Policy

For all Sites:

- Grid Site Operations Policy
- Site Registration Security Policy

For all VOs:

- VO Operations Policy
- Virtual Organisation Registration Security Policy
- Virtual Organisation Membership Management Policy
- VO Portal Policy

Other policies for all Grid participants:

- Traceability and Logging Policy
- Security Incident Response Policy
- Approval of Certificate Authorities
- Policy on Grid Pilot Jobs
- Grid Policy on the Handling of User-Level Job Accounting Data

Glossary of terms used in SPG policy documents:

- Security Policy Glossary of Terms

EGI SPG 2011

SPG work in 2011 includes:

- Revise Grid Site Operations policy
- Extend the HEPiX Virtualisation Working Group policy
- Revise top-level Security Policy (to EGI era)
- New Data Privacy policy: Extend to storage accounting and cover more general issues
- Evolving Glossary (as part of EGI Glossary)

Service Operations Security Policy

- Revision of the old Grid Site Operations Policy
- Extend to Services in general
  - Whoever runs them (Site, VO or other third party)
  - Virtual machines as well as services on real hardware
- Remove operational policy statements
  - Just keep the security issues
  - But for now we have to keep in some general issues
    - IPR, Liability, Dispute handling

Service Ops Sec Pol (2)

- https://wiki.egi.eu/wiki/SPG:Drafts:Operations_Policy
- *By running a Service on the Infrastructure, by providing a service that is part of the Infrastructure, or retaining state that is related to the Infrastructure, either provided as an independent service or hosted in a Resource Centre, You agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.*
- Internal SPG draft now completed (30th June 2011)
- External Draft about to be distributed for wider comment

Virtual Machine Images

- HEPiX Virtualisation Working Group policy
  - https://edms.cern.ch/document/1080777
  - *The aim is to enable Grid Sites to trust and instantiate endorsed VM images that have been generated elsewhere.*
- SPG is now extending this to additional use cases
- Policy on the Endorsement and Operation of Virtual Machine Images
  - https://wiki.egi.eu/wiki/SPG:Drafts:Virtualisation_Policy
- Aim to complete the internal draft during July and then go for external comment

Virtual Machines (2)

- VM image roles: *producer* -> *endorser* -> *operator*
- The *operator* is anyone who has root access to the instantiated image - held responsible for its security
- Use cases
  1. Endorser: Site, VM operator: Site (the trivial case)
  2. Endorser: Third party, VM operator: Site (HEPiX use case)
  3. Endorser: Third party, VM operator: Third Party (new)
- In case 3, The Site has no direct trust relationship with the Endorser and may decide to apply specific restrictions to control the access of the VM to other resources, including network services

Security for Collaborating Infrastructures

- SCI: An activity started this year
  - Building Trust and Developing Policy **standards** for collaboration
  - In cases where we cannot just share policy documents
- WLCG, EGI, OSG, TeraGrid, DEISA/PRACE and others
- *http://indico.cern.ch/categoryDisplay.py?categId=68*

SCI: some example text

Security Incident Response

- It is imperative that every collaborative entity has an organized approach to addressing and managing events that threaten the security of resources, data and overall project integrity. At a minimum a collaborating infrastructure must have the following:
- A formal Incident Response procedure...
- Documented contact information for site security teams and expected response times for critical situations...
- The capability to collaborate in the handling of a security incident ...
- Assurance of compliance with information sharing restrictions ...

IGTF policies for Attribute Authority Operations

- AuthZ is as (more?) important than AuthN
- IGTF has well established profile for AuthN
- We need minimum requirements for running trustworthy VOMS servers!
- Aim is to document currently accepted best practice
  - And improve where necessary
- See https://grid.ie/eugridpma/wiki/AA_Profile
  - Tackle all Attributes, not just those used for AuthZ
  - No longer limit to VOMS
    - Aim to be technology independent

Questions?