EGI-InSPIRE

EGI Security Policy Update

EGI Technical Forum
Prague, 18 Sep 2012

David Kelsey, STFC/RAL

GridPP
UK Computing for Particle Physics

e-infrastructure

Outline

- Introduction
- Security policies adopted since TF2011
- SPG current work
- IGTF: Guidelines for Attribute Authority Service Provider Operations
- SCI: A Trust Framework for Security Collaboration among Infrastructures

EGI Security Policy Group

https://documents.egi.eu/document/64 *(ToR)*

SPG Purpose and Responsibilities

- Develop and maintain Security Policy
  - For use by EGI and NGIs
  - Define expected behaviour of NGIs, Resource Centres, Users and others
  - To facilitate the operation of a secure and trustworthy DCI
- May also provide policy advice on any security matter related to operations

Terms of Reference

SPG Membership

- Each (associate) participant of EGI.eu is entitled to nominate one voting member
  - But consensus wherever possible
- Also each external Resource Infrastructure Provider with signed MoU
- In addition, SPG should aim to include expertise in its deliberations from other stakeholders

SPG membership

- See https://wiki.egi.eu/wiki/SPG:Members
- 16 NGIs represented today
- Is your NGI there?
- Would be good to expand membership

Current EGI Policy

- Current EGI Security Policy is available at *https://wiki.egi.eu/wiki/SPG*
- As formally adopted by EGI.eu

Security policies

Top-level Grid Security Policy:

- Grid Security Policy

For all Users:

- Grid Acceptable Use Policy

For all Sites:

- Service Operations Security Policy
- Security Policy for the Endorsement and Operation of Virtual Machine Images

Security policies (2)

For all VOs:

- VO Operations Policy
- Virtual Organisation Registration Security Policy
- Virtual Organisation Membership Management Policy
- VO Portal Policy
- Service Operations Security Policy
- Security Policy for the Endorsement and Operation of Virtual Machine Images

Security policies (3)

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 security policy documents:

- Security Policy Glossary of Terms
- And the general EGI glossary

New in 2012

- Service Operations Security Policy
  - Generalise Site policy to include anyone running a service (real or virtual)
- Security Policy for the Endorsement and Operation of Virtual Machine Images
  - Security related issues for the generation, distribution and operation of virtual machine images as part of the trusted computing environment
- Both effective from 1st Feb 2012

SPG current work

- Revision of Top-level Security Policy
  - To bring up to date
- Generalise Policy on user-level job accounting (Data protection)
  - Phase 1: to include storage accounting and new retention periods
  - Phase 2: to generalise to all forms of logging
- Proxy certificate/Attribute certificate lifetimes
- Modify Service Operations Policy
  - Remove IPR statement & address central user banning

- Other related security policy activities
  - Involving the chair, deputy chair and other members of SPG

Attribute Authorities

- IGTF has lots of policies and guidelines regulating Authentication (X.509 PKI)
- EGI has a security policy on VO membership management
- 2011: nothing on how to operate an Attribute Authority (e.g. VOMS)
- EUGridPMA has now produced a first version document on this (during 2012)

AA Service Providers

- Guidelines document
- *http://www.eugridpma.org/guidelines/aaops/*

- Aimed at the institute that runs Attribute Authorities (the AA Service Provider)
- The document defines best practices and minimum standards for running an AA
- Next step is to compare some real VOMS instances with the guidelines

Security for Collaborating Infrastructures

- Work that started in 2011
  - 2 meetings held in 2012 jointly with EUGridPMA
- A trust framework to enable interoperation of collaborating infrastructures
  - To manage operational security risks
  - Building Trust and Developing Policy **standards** for collaboration
- WLCG, EGI, OSG, XSEDE, PRACE and others
- *http://indico.cern.ch/categoryDisplay.py?categId=68*

SCI: some example text

Each collaborating infrastructure must have the following:

- [IR1] Documented security contact information for all service providers, resource providers and communities together with expected response times for critical situations.
- [IR2] A formal Incident Response procedure. This document must address: roles and responsibilities, identification and assessment of an incident, minimizing damage, response & recovery strategies, approved communication tools and procedures.

SCI (2)

- [IR3] The capability to collaborate in the handling of a security incident with affected service and resource providers, communities, and infrastructures.
- [IR4] Assurance of compliance with information sharing restrictions on incident data obtained during collaborative investigations…
- Etc etc

SCI document

- Completed at a meeting last week
- *http://www.eugridpma.org/sci/SCI-20120911-v9.pdf*

- Next steps
  - – Each infrastructure will now self-assess their compliance with the document

Summary

- Progress on revision of two documents
- A few smaller tasks too
- Plenty of work to do for rest of year!
- Attribute Authority SP and SCI documents
  - Both finished during year
- Plenty of room for more active members of SPG
  - Please contact me!

Links

- EGI SPG https://wiki.egi.eu/wiki/SPG
- IGTF http://www.igtf.net/
- EUGridPMA http://www.eugridpma.org
- SCI http://www.eugridpma.org/sci/

Questions?