

The EGI Security Groups – Keeping the Infrastructure Secure

Linda Cornwall (RAL), David Groep (NIKHEF), David Kelsey (RAL), Mingchao Ma (RAL), John White (CERN)

The purpose of security is to allow people to enjoy the benefits to which they are entitled. We lock the doors to our homes to prevent our belongings from being taken, thus ensuring we can enjoy the benefits of the belongings we have. Computer security should allow users to enjoy the benefits of the system, which includes convenient access to the resources they authorised to use, surety that their data is not modified, and privacy of data. If someone carries out an unauthorised action, this may prevent others from being able to carry out their work.

The EGI Security Policy Group (SPG)

The EGI Security Policy Group can be likened to the law or rule makers. By using or providing services, users and sites agree to abide by certain rules and policies. Just because a user can find a way to circumvent a rule or policy, does not mean that the user is allowed to any more than it is lawful to steal because a homeowner has left their door ajar. The EGI Security Policy Group is charged with developing and maintaining security policy for use by EGI and the NGIs.

This EGI Security Policy defines the expected behaviour of NGIs, Sites, Users and other participants required to facilitate the operation of a secure and trustworthy distributed computer infrastructure.

Various policy documents are produced by this group, including a top level Security Policy, a Site Operations Policy, a Traceability and logging Policy, an Incident Response policy, and various policies concerning the operations of Virtual Organisations (VOs). Users should be familiar with the Grid Acceptable Use Policy as they have to sign it when they join a VO. Further information is available from the EGI SPG Wiki at <https://wiki.egi.eu/wiki/SPG>

The EUGridPMA

The EUGridPMA is the international organisation to coordinate the trust fabric for e-Science grid authentication in Europe. The various Certificate Authorities in Europe have to demonstrate that their policies and procedures are satisfactory to the EUGridPMA, in order that the certificates that they issue meet the requirements of the International Grid Trust Federation and are therefore trusted for use in EGI. More information is available at <http://www.eugridpma.org/>

The EGI Software Vulnerability Group (SVG)

This can be seen as making sure that the locks which are broadly installed work correctly and cannot be bypassed. The purpose is

To eliminate existing vulnerabilities from the deployed middleware, prevent the introduction of new ones and prevent security incidents.

This is done in 3 main ways:

- Handling potential vulnerabilities reported
- Checking code for vulnerabilities (Vulnerability Assessment)
- Educating Developers to write secure code

What if you find a vulnerability?

DO NOT discuss on a mailing list - especially one with an open subscription policy or public archive

DO NOT post information on a web page

DO NOT publicise in any way, e.g. to the media

IMMEDIATELY report it to report-vulnerability@egi.eu

Further information is available from the EGI SVG Wiki at <https://wiki.egi.eu/wiki/SVG>

EGI Unified Middleware Distribution (UMD)

EUROPEAN MIDDLEWARE INITIATIVE EMI			Initiative for Globus in Europe IGE
gLite	ARC	Unicore	Globus

The software (middleware) to make the Grid work is to be distributed by EGI as the Unified Middleware Distribution (UMD). This Middleware is provided by various projects and technology providers external to EGI. It includes software to allow Authentication and Authorization of actions, which effectively makes the middleware providers the lock and key makers. EGI works closely with the Middleware providers to ensure that the requirements are met, the software is secure, and suitable for the users.

The EGI Computer Security Incident Response Team (CSIRT)

This can be likened to the group who makes sure the locks are fitted correctly (including training the lock fitters) and investigates when a break-in occurs. The most important function is

To handle day to day operational security issues and co-ordinate Computer Security Incident Response across the EGI infrastructure.

What if you think an incident has occurred at your site?

DO NOT re-boot or power off the host

IF feasible, try and contain the incident.

E.g. If you are sufficiently familiar with the host/service and your local policy allows unplug the network connection.

Note any actions you take with a timestamp

IMMEDIATELY inform your local security team and report it to abuse@egi.eu

Look at the steps on https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting for more information.

Further information on CSIRT activities is available from the EGI CSIRT Wiki at <https://wiki.egi.eu/wiki/CSIRT>

The EGI Security Coordination Group (SCG)

The EGI Security Coordination Group brings together representatives of the various security functions in EGI to ensure that there is coordination between operational security, security policy governing use of the production infrastructure and the technology providers whose software is used. It is also helps to ensure that the procedures carried out by CSIRT and SVG implement policy. This provides a co-ordinated response and planning on EGI security issues.