M-grid Security Policy

Introduction

What is M-grid?

M-grid, the Finnish Material Sciences National Grid Infrastructure, is a collaboration between seven universities, Helsinki Institute of Physics (HIP) and the Finnish IT center for science, CSC. The partners are University of Helsinki, Helsinki University of Technology, HIP, University of Jyväskylä, Lappeenranta University of Technology, Tampere University of Technology, University of Turku, University of Oulu and CSC.

At the time of writing, M-grid is based on nine PC clusters located at eight sites running Linux and NorduGrid ARC grid middleware. Each cluster consists of a frontend server, an administrative server and computing nodes. M-grid provides dependable, consistent, pervasive and inexpensive access to high-end computational resources.

For more information about M-grid, see: http://www.csc.fi/proj/mgrid/

Objectives and scope of the security policy

This M-grid Security Policy sets out the rules and regulations for the activities of M-grid participants regarding the confidentiality, integrity and availability of grid facilities and resources. The policy gives authority for actions and places responsibilities on individuals as defined by the roles and responsibilities later in this document. Management has approved, supports and will enforce this policy.

This Security Policy is based on

- Risk identification and assessment of M-grid
- Appropriate choice of security controls
- General information on good security practices

This policy has been reviewed by the M-grid consortium and Funet CERT.

Additional security documents supplementing this policy are

- Risk Analysis for M-grid.
- M-grid Administrator Security Guide.
- M-grid User Security Guide.
- M-grid Acceptable Use Policy.

Participants, roles and responsibilities

The participants of M-grid can be defined as the users (those who use the system for computation) and the administration (those who manage the system for the users and the upper level management who supervise administrators.)

- The upper level management is responsible for ensuring that sufficient staff and funding are provided to ensure high availability of the system, for delegating responsibilities to administrators, and for supervising that administrators have adequate resources and perform their duties.
- Administrators are responsible for implementing, managing and complying with security policies. This includes, but is not limited to, ensuring users are provided with and informed about security policies, and limiting access based on the policies. Administrators must respond to security breaches in a timely manner.
- Users must be aware of, understand and comply with the Acceptable Use Policy. The users are also responsible for ensuring that their use of the system falls under the terms of acceptable use. Administration can clarify policies for users.

The role of individual sites is to ensure policies are followed. Each individual site should have good relations with their hosting organisation's IT department and they should co-operate on security issues when possible.

The role of CSC is to co-ordinate, provide centralised services and participate in system administration as defined later in this document. Further, CSC co-ordinates regular meetings for site administrators, which administrators should attend when possible. Authorative decisions about the security and operations of M-grid can be made at these meetings.

CSC does not provide administration for University of Oulu. All administration responsibilites of CSC mentioned in this document will be taken care of by University of Oulu for their part in an equivalent way.

Physical security

Information security is based on adequate physical security arrangements.

- Physical access to the machines and peripheral hardware must be restricted.
- Active console sessions must not be left unattended.
- Local administrators should be aware of how physical access to the servers is restricted. The group with access should be kept as small as possible.
- It is recommended that service personnel and contractors are supervised when they work in the server room.

User accounts and access control

Local accounts

Sites create local user accounts and are responsible for them.

- Accounts are personal and must not be shared with other people.
- Users are required to read and accept the M-grid Acceptable Use Policy before getting an account.
- Users with administrative privileges are required to read and accept the M-grid Security Policy and read the M-grid Administrator Security Guide.
- CSC administrators have administrative privileges in all M-grid resources.
- Sites are allowed to create time-limited accounts for persons working in documented collaboration projects outside the site's organization.
- Unaffiliated external users are not permitted.
- Sites are responsible for having up to date contact info of each user.
- Accounts of users who are not affiliated with the site any more should be removed or disabled within two weeks.
- Accounts must be protected by a good password or other method providing equivalent security.

Grid accounts

Each user who has a local account in one of the clusters can be provided with a grid account. Grid identities are tied to personal user certificates.

- The private key of the certificate must be stored securely and protected by a good pass phrase.
- Users are allowed to run both preinstalled software and their own software in the grid.
- Grid identities must be mapped to local accounts so that an audit trail is maintained.

Virtual Organization management

User authorization is managed as groups, called Virtual Organizations (VO).

- Sites can manage VOs consisting of their own users.
- CSC can manage VOs consisting of users of several sites.
- Authorizing external VOs must be approved by the M-grid administration.

Certificate Authorities

Certificate Authorities (CA) are trusted for signing user and host certificates.

- CSC maintains a list of trusted CAs at http://www.csc.fi/english/research/Computing_services/mgrid/data_security_and_privacy/index_html
  - No other CAs should be trusted
- When requesting a certificate, users must follow the policies of the CA.
- The Certificate Revocation List (CRL) of each CA must be kept up to date.

Network security

The availability, integrity and confidentiality of M-grid services rely on how network security is implemented.

Network access and services

- Network access to the grid services should be allowed from all M-grid partners. It may be allowed from the whole world.
- Network access to other default services on the cluster frontend should only be allowed from local and CSC networks.
- Network access to the administration server is restricted to specific local and CSC networks.
- CSC controls the centralized software distribution server and is responsible for adequate security measures for it.

Additional services

- Sites may offer additional services related to M-grid use to a restricted user-base without approval of the M-grid administration.
- Sites may offer additional services which are open to a large user base, but these must be approved by the M-grid administration.
- Sites must not offer any additional services running on the administration server without approval of the M-grid administration.

Firewalls

- All the M-grid resources are protected by local firewalls. There may be additional university firewalls.
- Only necessary ports for each service and resource should be opened.
- The local firewall settings are controlled jointly by CSC and the local administrators.

Operational security

Operational security is based on measures to protect data from accidental or unauthorized access, modification or destruction.

- The M-grid system as a whole should be available at all times even if individual sites might experience some down time.
- High availability of the sites is desirable, and local policy should determine the response time for a system failure. This is covered further under the heading of Incident Response.
- A daily incremental backup should be made on each site. If such a facility is not readily available, a backup of critical system configuration data should be made on a regular basis.

Patches

The systems should be kept up to date and used software components should be actively maintained.

- Daily security updates should be made automatically.
- CSC is responsible for maintaining the core operating system and the grid middleware.
- Local site administrators are responsible for any additional software that they install.

Monitoring

Local site administrators are responsible for the monitoring the security of their site. Additionally, CSC provides tools to check system integrity and local administrators should perform checks routinely.

Confidentiality and privacy

The M-grid partners respect user confidentiality and privacy and reasonable efforts will be made to protect them.

Grid users

- As the M-grid is a developing research tool which is used voluntarily by researchers, in some cases information about grid users or their jobs may be available publicly via the Internet.
- Users and administrators will be advised what information is made available.

Local users and administrators

- Site administrators must have contact information for user account holders and grid users.
- Contact information will be kept confidential in accordance with Finnish law.
- User contact information and usage data can be shared between M-grid partners for administrative purposes.
- In their duties site administrators must respect the privacy and confidentiality of users' files and data.
- Users must respect privacy and confidentiality of other users' files and data.

Incident response

An information security incident is, for example, an unauthorized access or a break in. Incident response refers to the practice of detecting the incident and analysing it, and minimising the damage. The incident should then be documented.

- Local administrators should routinely perform integrity checks (at least twice a week) and should detect possible security incidents.
- If a security incident is suspected, the local administrator should immediately contact CSC and co-operate with them to find out the severity of the incident.
- If a security incident is detected, the local administrator must
  - follow the instructions in the Security guide
  - contact CSC and the M-grid administrators
  - inform the local security personnel
- The administrator, in consultation with CSC should also inform Funet CERT (cert@certNO-SPAMMING.funet.fi,

tel. +358-9-4572038) if the incident affects other M-grid sites.
- After the situation is resolved the proper authorities should be informed.

Compliance

This Security Policy has been created and reviewed to comply with the Finnish legislation related to privacy and information security.

The most essential related laws in Finland are:

- The Constitution of Finland (731/1999); 10 §.
- Act on the Openness on Government Activities (621/1999).
- Personal Data Act (523/1999).
- The Act on the Protection of Privacy on Electronic Communications (516/2004).
- Act on the Protection of Privacy in Working Life (759/2004).

This Security Policy and the administration of the M-grid should also comply with security policies and guidelines of the hosting university or organization.

Virtual organisations from other countries must accept and follow this policy when using M-grid services.

Exceptions

- If there is a conflict between legislation and this security policy or other security guidelines, the laws should be followed.
- If there is a conflict between this policy and security policies of local hosting organisations, the situation should be discussed.
- If some goals of this policy cannot be achieved due to lack of resources or technical limitations, a plan and a schedule should be created to correct the situation.

Approval and review

This security policy has been reviewed by IT managers and IT security managers of the local hosting universities and institutions, and by Funet CERT. The M-grid administration has approved this policy.

If and when there is a need to amend this document a new review should be performed.

Technical update

A technical update clarifying some of the sentences in this policy was performed on 18.1.2007 by the M-grid Security Working Group.

An update of a URL was performed on 22.3.2007 by the M-grid Security Working Group.

This topic: Extranet/MGrid/SecurityWG > Extranet/MGrid > MgridSecurityPolicy
History: r10 - 19 Sep 2008 - 11:39:31 - KalleHapponen