Security for Collaborating Infrastructures (SCI)

Draft text - V7 - 5 May 2012

Operational Security

Operational security in a distributed collaborative environment is governed by the same principles that apply to a local centrally managed system, but complicated by the diversity of sites (both in terms of hardware and software systems and in terms of local policies and practices that apply), and by the lack of a centralized management hierarchy that can "order" certain operations to be performed in specific ways.

Governing principles include:

- The management of risk; both to mitigate the most likely occurring and dangerous risks, and to take counter measures that are commensurate with the scale of the involved risks
- Containing the impact of a security incident while keeping services operational, but in certain cases this may require identifying and fixing a security vulnerability before re-enabling user access
- Identifying the cause of incidents and understanding what measures must be taken to prevent them from re-occurring

A collaborating infrastructure for operational security in a distributed environment must address the following issues:

- *Risk mitigation*: A process that ensures that security patches in operating system and application software are applied in a timely manner, and that patch application is recorded and communicated to all members of the collaboration.
- *Risk mitigation:* A documented process to manage vulnerabilities (including reporting and disclosure) in any software distributed within the infrastructure. This document must be publicly available or made available upon request and must be sufficiently dynamic to respond to changing threat environments.
- *Incident prevention*: The capability to detect possible intrusions and protect the infrastructure against significant and immediate threats on the infrastructure.
- *Incident prevention:* A documented capability to regulate the access of authenticated users.

- *Collaborative cooperation*: The capability to identify and contact authenticated users, service providers and resource providers.
- *Collaborative cooperation:* The capability to enforce the regulation of security policies, including an escalation procedure and the powers to require actions as deemed necessary to protect resources from or contain the spread of an incident.

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. This document must be publicly available or made available upon request and address: roles and responsibilities, identification and assessment of an incident, minimizing damage, response & recovery strategies, approved communication tools and procedures.
- 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 with affected service and resource providers, communities, and infrastructures.
- Assurance of compliance with information sharing restrictions on incident data obtained during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with site-specific security teams on a need to know basis, and will not be redistributed further without prior approval.

Traceability

The management of risk is fundamental to the operation of any Infrastructure. Identifying the cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.

The minimum level of traceability for the Infrastructure is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, etc) and the individual who initiated them. In addition, sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational. It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.

The aim is to be able to answer the basic questions "who, what, where, when and how" concerning any incident. This requires retaining all relevant information, including accurate timestamps and the digital identity of the user, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect.

A collaborating infrastructure must provide the following:

- Traceability of service usage, by the production and retention of appropriate logging data, to identify the source of all actions as defined above.
- A specification of the data retention period, consistent with local, national and international regulations and policies

Participant Responsibilities

All participants in a group of collaborating infrastructures need to rely on proper behavior by various actors in both their own and other infrastructures. We separate these responsibilities into behavior expected of:

- individual grid users (including AUPs)
- collections of users (VOs or VRCs), especially with respect to registering and training individual users
- individual sites providing resources

Scope

- similar software environments, shared threats, shared incidents
- But also there can be cases where we share user communities
    - When Infrastructure A wants to extend access to participants registered inside the scope of Infrastructure B
- Who are the participants within an Infrastructure?
    - Resource Providers, Service Operators, Individual Users, Collections of Users[1]
- Infrastructure B must have a Conditions of Use Policy to be accepted by all Users

Individual Grid Users

The Infrastructure B must have a process in place to ensure that users understand and agree to abide by expected standards of behaviour, including:

- Users must be aware that their work may utilise shared resources and may therefore affect the work of others. They must show responsibility, consideration and respect towards other users in the demands they place on the Infrastructure.
- Users must have a suitable authentication credential issued as approved by the Infrastructure. They must ensure that others cannot use their credentials to masquerade as them or usurp their access rights.Users may be held responsible for all actions taken using their credentials, whether carried out personally or not. No intentional sharing of credentials is permitted.
- Users must be aware that their jobs will often use resources owned by others. They must observe any restrictions on access to resources and information that they encounter and must not attempt to circumvent such restrictions.

[1] An entity which acts as the interface between the individual users and the Infrastructure. Examples include but are not limited to: Virtual Organisations, Virtual Research Communities, Projects, Science Gateways, Geographically organised communities, Application/Research/Academic Communities.

- Application software written or selected by users for execution on resources must be directed exclusively to the legitimate purposes of their User Community. Such software must respect the autonomy and privacy of the host sites on whose resources it may run.
- The Infrastructure B must communicate any additional restrictions or requirements on allowable use that arise out of new collaborative partnerships to their users
- AUP informs users that PII will be used for certain purposes

Collections of Users

A Collection of Users is a group of individuals organised around a common purpose jointly granted access to the Infrastructure. The existence of this Collection means that each individual user does not need to separately negotiate with Resource Providers or Infrastructures.

- The Collection of Users will be held responsible for certain actions by an individual member of the collection which in turn may reflect on the ability of other members to utilise the infrastructure
- The Collection typically registers individual users as members and may also have mechanisms for allocating resources to and monitoring usage by their members
- Some Collections, such as application communities are more loosely coupled, i.e. they do not formally register individual users, but they must still have a way of identifying the individual user responsible for an action
- Infrastructures must have policies and procedures regulating the individual user registration and membership management (registration, renewal, suspensions, removal, banning, ...)
    - At a minimum these must address the accuracy of contact information both for initial collection and periodic renewal
- Collections of Users must keep appropriate logs of membership management actions[2] sufficient to participate in security incident response
- The Collection must define their common aims and purposes and make this available to the Infrastructure and/or Resource Providers to allow them to make decisions on resource allocation

Resource Providers and Service Operators

The Infrastructure must have a policies and procedures in place to ensure that Sites understand and agree to abide by expected standards of behaviour, including:

[2] Examples include but are not limited to: Registration or renewal in a membership system, dynamic authorisation such as acquisition of VOMS attributes, authentication to a Science Gateway or portal, job submission or file transfer initiated by the Collection on behalf of an individual user

- vulnerability patching
- incident reporting
- physical and network security
- confidentiality and integrity of data
- retention of appropriate logs

Legal Issues

Infrastructures must have policies and procedures addressing legal issues including but not limited to the following:

- Intellectual Property Rights. It is recommended that Infrastructures include the following clause "Your provisioning of Services shall not in itself create any intellectual property rights in software, information and data provided to your Service or in data generated by your Service"
- Liability - It is recommended that Infrastructures include the following clause "Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided on an as-is basis only, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure, Resource Providers, Service Operators and Collections of users are not liable for any loss or damage in connection with your participation in the Infrastructure.

(or change to reference to document link as a suggested wording?)

- software licensing
- dispute handling and escalation

- Resource Providers and Service Operators do not acquire any additional IPR on data or results
- Infrastructures, Sites and Collections of Users are not liable
- Users are liable for their actions
- Should have an escalation procedure to handle disputes

Infrastructures must make available any additional restrictions to the Users such as export controls, licensing, externally imposed data protection and access control requirements

Data Protection

Infrastructures must have policies and procedures addressing data protection and privacy issues including but not limited to the following:

- Accounting Data
- User Registration Data
- Monitoring Data
- Logging Data

Lacking statements to the contrary it is assumed that protection of data contained within or produced by a job is the primary responsibility of the user or the Collection of Users and not the Resource Provider or Infrastructure.

Building Trust: Levels of Assurance

Many of the sections above require a collaborating infrastructure to have certain types of documents: policies, procedures, logs, lists of members, etc. In some cases there is no problem in making these documents available publically on the web. However, in other cases, privacy or security considerations may cause the infrastructure to want to restrict distribution of such documents, while at the same time assuring other infrastructures that the documents do exist and fulfill the requirements described above.

To accommodate these needs, we consider three levels of assurance an infrastructure can meet:

- Level 1: the infrastructure asserts the existence of all required documents but makes no comprehensive effort to prove the existence of the documents. Some documents may be published on the web.
- Level 2: the infrastructure makes their document set available in a protected and secured manner to some designated body that verifies the level 1 assertion that the documents exist. The "SCI" group could evolve into a more formal committee that performs such verifications, as regional PMAs do on behalf of the IGTF.
- Level 3: the infrastructure makes their document set available in a protected and secured manner to an independent body that not only verifies their existence but also performs an "operational review" that demonstrates the documents are accurate, up to date, and serve their intended purposes. Checklists for each type of document can be prepared to guide these operational reviews, which can again be performed by the "SCI" successor group.

Charts will be maintained showing what level of assurance different infrastructures have met, which will allow other infrastructures to make informed decisions about which partners are deserving of their trust.