A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]

STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines

Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep

Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila

CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

Christos Kanellopoulos

GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller

Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

---

[1] Speaker

Ralph Niederberger

Forschungszentrum Jülich GmbH
Wilhelm-Johnen-Strasse, 52425 Jülich, Germany
E-mail: `r.niederberger@fz-juelich.de`

Vincent Ribaillier

IDRIS
Campus universitaire d'Orsay, rue John Von Neumann, Boîte postale 167, F-91403 Orsay cedex, France
E-mail: `Vincent.Ribaillier@idris.fr`

Romain Wartel

CERN
385 Route de Meyrin, 1217 Meyrin, Switzerland
E-mail: `Romain.Wartel@cern.ch`

Willy Weisz

University of Vienna
Computational Science Center, Nordbergstrasse 15, 1090 Wien, Austria
E-mail: `willy.weisz@univie.ac.at`

Jules Wolfrat

SURFsara
Science Park 140, 1098 XG Amsterdam, The Netherlands
E-mail: `jules.wolfrat@surfsara.nl`

The Security for Collaborating Infrastructures (SCI) group is a collaborative activity of information security officers from several large-scale distributed computing infrastructures, including EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE. SCI is developing a framework to enable interoperation of collaborating Grids with the aim of managing cross-Grid operational security risks and to build trust and develop policy standards for collaboration especially in cases where we cannot just share identical security policy documents.

The International Symposium on Grids and Clouds (ISGC) 2013
March 17-22, 2013
Academia Sinica, Taipei, Taiwan

1. Background

The Security for Collaborating Infrastructures (SCI) group is a collaborative activity of information security officers from several large-scale distributed IT infrastructures (DIIs), including EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE. SCI is developing a trust framework to enable interoperation of collaborating DIIs with the aim of managing cross-infrastructure operational security risks. We also aim to build trust between the DIIs by developing policy standards for collaboration especially in cases where we cannot just share identical security policy documents.

SCI was created to help address several issues. Firstly, the WLCG infrastructure which uses resources from several DIIs, including EGI, OSG and NDGF, found itself in the position where agreeing security policy documents was becoming more difficult. Different DIIs had similar policies addressing similar issues but agreement on the exact wording was in many cases not possible. What was needed was a higher-level agreement on the types of security policies required and the issues they should address rather than the detailed policy words. Secondly, the various operational security teams were finding that they needed to work more and more often together on shared security incidents. This collaboration was often found to be successful, but all agreed that having a common security policy framework would help enable a more formal trust environment. Finally, it was recognised that the adoption of a common security policy framework would also help facilitate interoperation between the DIIs in the sense of shared communities of users.

There are several series of national or international standards defining best practice in the management of Information Security, including ISO 27000 [1] and NIST 800-53 [2]. These standards provide extremely useful guidance for handling security within a single management domain but are not really of much use when dealing with the management of security across multiple DIIs where each DII already consists of resources from many different sites each having their own management. We are not aware of any other activity to define standards and a trust framework as presented here.

The detailed requirements for security differ between our DIIs, but nevertheless, in this SCI activity we are concentrating on those issues which are common to all infrastructures. The characteristics may differ and some issues may be more or less important, but all of them should be considered by every DII.

Many of the requirements expressed in this current document are left deliberately vague, e.g. by not setting minimum requirements for the content of policy documents, nor defining detailed procedures, e.g. the time limit for security patching. Experience has shown that these are often the areas where DIIs differ and that it works better to allow infrastructures the freedom to define the detailed procedures according to their own environment and needs. Future versions

of the SCI document, which may always be found on our web site [3], may well define some of these issues more tightly.

The SCI deliberations have been conducted by face to face meetings, by telephone or video conference and by email. Most of our face to face meetings have been co-located with meetings of the International Grid Trust Federation (IGTF) [4] as it involves many of the same individuals. IGTF has also agreed to host our web-site. This is very appropriate in that this is a neutral, DII-independent, location and IGTF is after all in the business of building global trust.

The document presented here is written by our group but is not yet approved by the management of our infrastructures. SCI does not have the authority to force new policy standards on our parent infrastructures, nor can we commit effort to performing self-assessments. The next stage of the work will involve wider consultation with our DIIs to gather feedback on and wherever possible will also include seeking endorsement of the SCI document. We aim to perform self-assessments of the extent to which our DIIs meet the documented requirements according to the maturity scale presented here. Based on the feedback received and the results of our self-assessments it is likely that we will need to further refine the SCI document.

SCI is an open group. Other DIIs interested in contributing to the group's activities or using our documents and assessments are very welcome to join our deliberations.

The SCI document itself follows after the Glossary starting with the section: "Introduction".

2. Glossary

The following terms are defined for use in the SCI document:

Infrastructure	All of the IT hardware, software, networks, data, facilities, processes etc. that are required to develop, test, deliver, monitor, control or support *services*.
Distributed IT Infrastructure (DII)	An *Infrastructure* together with its management, *Resource Providers* and *Service Operators*. It provides, manages and operates (directly or indirectly) all the *services* required by the *Resource Providers* and their collections of *users*.
Resource	The equipment (CPU, disk, tape, network), software, middleware and data required to run a *service*.

PoS(ISGC 2013)011

Service	Any computing, storage, preservation, or software system which provides access to, information about or controls *resources*.
Resource Provider	The smallest *resource* administration domain in a DII. It can be either localised or geographically distributed.
Service Operator	An entity responsible for the management, deployment and operation of a *service*.
Participant	Any entity providing, using, managing, operating, supporting or coordinating one or more *service(s)*.
User	An individual or an organisation who has been given authority to access and use *resources*.

3. The SCI document - Introduction

In recent years we have seen the implementation of a variety of infrastructures supporting distributed computing environments and sharing of resources. Each such infrastructure consists of distributed computing and data resources, users (who may be organised into separate user communities), and a set of policies and procedures. Examples of such infrastructures include computing grids and/or clouds, as well as cooperating computing facilities managed by different organisations.

Even when such an infrastructure considers itself to be decoupled from other infrastructures, it is in fact subject to many of the same threats and vulnerabilities as other infrastructures because of the use of common software and technologies. Moreover, there may be users who take part in more than one infrastructure and are thus potential vectors that can spread infection from one infrastructure to another. Finally, one infrastructure may want to extend rights to use its resources to users who are enrolled in a different infrastructure. In each of these situations, the infrastructures can benefit from working together and sharing information on security issues.

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
- Identifying users, hosts and services, and controlling their access to resources, all of which must be sufficiently robust and commensurate to the value of the resources and the level of risk and must comply with the regulatory environment

In this document we lay out a series of numbered requirements in six areas (operational security, incident response, traceability, participant responsibilities, legalities, and data protection) that each infrastructure should address as part of promoting trust between infrastructures.

To evaluate the extent to which the requirements described in this document are met, we recommend that each infrastructure assess the maturity of its implementation according to the following levels:

Level 0: Function or feature not implemented

Level 1: Function or feature exists, is operationally implemented but not documented

Level 2: Function or feature is comprehensively documented and operationally implemented

Level 3: Function or feature implemented, documented, and reviewed by an independent external body

We encourage openness and transparency in the documentation and for Levels 2 and 3 we recommend that wherever possible such documents should be made available to collaborating infrastructures as a way of promoting trust.

4. Operational Security [OS]

Retaining operational availability and integrity is the most urgent and visible aspect of security. Each of the collaborating infrastructures must therefore have the following:

- [OS1] A security model addressing issues such as authentication, authorisation, access control, confidentiality, integrity and availability, together with compliance mechanisms ensuring its implementation
- [OS2] 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 the appropriate contacts

- [OS3] A process to manage vulnerabilities (including reporting and disclosure) in any software distributed within the infrastructure. This process must be sufficiently dynamic to respond to changing threat environments
- [OS4] The capability to detect possible intrusions and protect the infrastructure against significant and immediate threats on the infrastructure
- [OS5] The capability to regulate the access of authenticated users
- [OS6] The capability to identify and contact authenticated users, service providers and resource providers
- [OS7] The capability to enforce the implementation of the 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

5. Incident Response [IR]

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.

It is imperative that every infrastructure has an organized approach to addressing and managing events that threaten the security of resources, data and overall project integrity.

Each infrastructure must have the following:

- [IR1] 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 must address: roles and responsibilities, identification and assessment of an incident, minimizing damage, response & recovery strategies, communication tools and procedures
- [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. 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

6. Traceability [TR]

The minimum level of traceability for the Infrastructure is to be able to identify the source of all actions (executables, file transfer, etc.) together with the individual[2] initiating the actions.

---

[2] For software agents initiating actions there must be a human individual responsible for all actions of the agent

In addition, sufficiently fine-grained controls, such as blocking the originating user, system or service 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 initiator, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorise (including identity changes) and disconnect.

Each infrastructure must provide the following:
- [TR1] Traceability of service usage, by the production and retention of appropriate logging data, to identify the source of all actions as defined above
- [TR2] A specification of the data retention period, consistent with local, national and international regulations and policies
- [TR3] A specification of the controls that the resource provider implements to achieve the goals of [TR1]

7. Participant Responsibilities [PR]

All participants in a group of collaborating infrastructures need to rely on appropriate behavior by various actors in both their own and other infrastructures. We separate these responsibilities into behavior expected of:
- Individual users
- Collections of users
- Resource providers and service operators

Each infrastructure must ensure that the various participants are aware that they have these responsibilities.

7.1 Individual Users

Each infrastructure must provide:

- [PRU1] An Acceptable Use Policy (AUP). The AUP must at least address the following areas: defined acceptable use, non-acceptable use, user registration, protection and use of credentials, data protection and privacy, Intellectual Property Rights (IPR), disclaimers, liability and sanctions
- [PRU2] A process to ensure that all users are aware of, and accept the requirement to abide by, the AUP
- [PRU3] Communication to their users of any additional restrictions or requirements on acceptable use that arise out of new collaborative partnerships

7.2 Collections of Users

A Collection of users is a group of individuals organised around a common purpose jointly granted access to the Infrastructure. It may serve as an entity which acts as the interface between the individual users and each Infrastructure. In general the members of the Collection will not need to separately negotiate with Resource Providers or Infrastructures.

Examples of Collections of users include: User groups, Virtual Organisations, Research Communities, Virtual Research Communities, Projects, Science gateways, and geographically organised communities.

Each infrastructure must have:

- [PRC1] A process to ensure that all Collections of users using their infrastructure are aware of, and accept the need to abide by, various policy requirements
- [PRC2] Policies and procedures regulating the individual user registration and membership management (registration, renewal, suspensions, removal, and banning). At a minimum these must address the accuracy of contact information both for initial collection and periodic renewal

Collections of users must:

- [PRC3] be aware that they will be held responsible for actions by an individual member of the collection which in turn may reflect on the ability of other members to utilise the infrastructure
- [PRC4] ensure a way of identifying the individual user responsible for an action
- [PRC5] keep appropriate logs of membership management actions[3] sufficient to participate in security incident response
- [PRC6] 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

7.3 Resource Providers and Service Operators

The Infrastructure must have policies and procedures in place to ensure that Resource Providers and Service Operators understand and agree to abide by expected standards of behaviour, including:
- [PRR1] vulnerability patching
- [PRR2] incident reporting
- [PRR3] physical and network security

---

[3] 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

- [PRR4] confidentiality and integrity of data
- [PRR5] retention of appropriate logs

8. Legal Issues and Management procedures [LI]

Infrastructures, resource providers, service providers and collections of users must have policies and procedures, appropriately communicated to all participants, that address legal issues including but not limited to the following:

- [LI1] Intellectual Property Rights clarifying the rights and obligations of the participants
- [LI2] Liability responsibilities and disclaimers to make the participants aware of their obligations
- [LI3] Software licensing clarifying the rights and obligations of the participants
- [LI4] Dispute handling and escalation procedures
- [LI5] Data Protection responsibilities (also see the next section)
- [LI6] Any additional regulations such as export controls, ethical use, externally imposed data protection and/or access control requirements

9. Protection and processing of Personal Data/Personally Identifiable Information [DP]

Infrastructures, resource providers, service providers and collections of users must have policies and procedures addressing the protection of individuals with regard to the processing of their personal data (PII) collected as a result of their participation in the infrastructure, including but not limited to:

- [DP1] Accounting Data
- [DP2] User Registration Data
- [DP3] Monitoring Data
- [DP4] Logging Data
- [DP5] Data owned by or produced by Users or Collections of Users

10. Acknowledgements

11. References

[1] ISO 27000 series of information security standards.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891
[2] NIST 800-53 series of standards.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[3] http://www.eugridpma.org/sci/
[4] http://www.igtf.net