A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

[1]GÉANT Association, Amsterdam, The Netherlands; [2]Nikhef, Amsterdam, The Netherlands; [3]GEANT Ltd., Cambridge, United Kingdom; [4]SURFsara, Amsterdam, The Netherlands; [5]CSC, IT Center for Science Ltd., Espoo, Finland; [6] STFC Rutherford Appleton Laboratory, Didcot, United Kingdom; [7]SURFnet, Utrecht, The Netherlands; [8]Forschungszentrum Jülich GmbH (FZJ), Jülich, Germany; [9]Indiana University, Indianapolis, USA; [10]National Center for Supercomputing Applications, University of Illinois, Urbana Champaign, USA; [11]Institut du développement et des ressources en informatique scientifique (IDRIS-CNRS), Orsay, France; [12]Martel Innovate, Dübendorf, Switzerland; [13]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [14]Karlsruher Institut für Technologie (KIT), Eggenstein-Leopoldshafen, Germany

Abstract: The Security for Collaborating Infrastructures working group (SCIv2-WG) is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. SCIv2-WG members include information security officers from several large-scale distributed Research Infrastructures and e-Infrastructures. The aims of the trust framework defined in this document are to enable interoperation of collaborating Infrastructures and to manage cross-Infrastructure operational security risks. It also aims to build trust between Infrastructures by defining standards for collaboration, especially in cases where specific internal security policy documents cannot be shared.

Target audience: This document is intended for use by the personnel responsible for the management, operations and security of a Research Infrastructure or an e-Infrastructure.

Other Sources / Attribution / Acknowledgements: The “SCI version 2” document, “A Trust Framework for Security Collaboration among Infrastructures (SCI version 2)”, is a derivative of “A Trust Framework for Security Collaboration among Infrastructures” by D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz and J. Wolfrat, used under CC BY-NC-SA 4.0, from the proceedings of "International Symposium on Grids and Clouds – ISGC 2013" PoS(ISGC2013)011. https://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

1. Introduction

The Security for Collaborating Infrastructures working group (SCIv2-WG) is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. SCIv2-WG members include information security officers from several large-scale distributed Research Infrastructures and e-Infrastructures[1]. The aim of the trust framework defined in this document is to enable interoperation of collaborating Infrastructures for the purpose of managing cross-Infrastructure operational security risks. It also aims to build trust between Infrastructures by defining standards for collaboration, especially in cases where collaborating organisations' specific internal security policy documents cannot be shared, but more general security policies are allowed to be made public. The SCI group published version 1 of its trust framework in 2013 [1]. REFEDS published version 1 of the Sirtfi trust framework, a derivative of SCI version 1 in 2016 [2]. The WISE SCIv2-WG has now produced this document which defines version 2 of the SCI trust framework. In the future, SCIv3 will consider recombining the derivative documents.

Security in a distributed collaborative environment is governed by the same principles that apply to a site-managed cluster, but is complicated by the diversity of sites, both in terms of hardware and software systems and in terms of local policies and practices that apply. The lack of a centralised management hierarchy with the necessary authority to mandate that certain operations to be performed is also a significant factor.

The governing principles of security in such an environment are:

- Managing risk by both mitigating the most likely occurring and dangerous risks, and taking counter measures that are commensurate with the severity of the risks identified;

- Minimising the impact of a security incident while keeping services operational. 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, to control their access to resources. Mechanisms used to enforce this control must be sufficiently robust and commensurate to the value of the resources and the level of risk and must comply with the applicable regulatory environment.

[1] WISE SCIv2-WG currently includes security personnel from the following Infrastructures: Dutch National e-Infrastructure coordinated by SURF, EGI, EUDAT, GÉANT, GridPP, HBP, OSG, PRACE, WLCG and XSEDE.

In this document, we lay out a series of numbered requirements in five areas (operational security, incident response, traceability, participant responsibilities 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 of each function or feature according to the following levels:

- Level 0: Not implemented for critical services;
- Level 1: Implemented for all critical services, but not documented;
- Level 2: Implemented and documented for all critical services;
- Level 3: Implemented, documented, and reviewed by a collaborating Infrastructure or by an independent external body;
- "Justifiable exclusion": In the unlikely case that the function or feature is not relevant for the infrastructure.

In the interest of promoting trust, Infrastructures should make their maturity assessments available to collaborating Infrastructures. The documentation required for Levels 2 and 3 should either be publicly available or made available on request by a collaborating Infrastructure.

2. Glossary

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

Infrastructure	All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services.*
Service	An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.
Service Provider	An entity responsible for the management, deployment, operation and security of a *service.*
Participant	An entity providing, using, managing, operating, supporting or coordinating one or more *service(s).*
User	An individual or an organisation authorised to access and use *services.*
Collection of Users	A group of *users*, organised with a common purpose, and jointly granted access to the *infrastructure*. It may act as the interface between individual *users* and the *infrastructure*.

3. Operational Security [OS]

Each of the collaborating *infrastructures* has the following:

- [OS1] A person or team mandated to represent the interests of security for the *infrastructure*.
- [OS2] A process to identify and manage security risks on a regular basis.
- [OS3] A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation.
- [OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.
- [OS5] A process to manage vulnerabilities (including reporting and disclosure) in any software recommended for use within the *infrastructure*. This process must be sufficiently dynamic to respond to changing threat environments.
- [OS6] Tools and techniques to detect intrusions and protect against significant and immediate threats to the *infrastructure*.
- [OS7] The capability to regulate the access of authenticated *users*, including emergency suspension during the handling of security incidents.
- [OS8] The capability to identify and contact authorised *users* and *service providers*.
- [OS9] The capability to enforce the implementation of applicable security policies, including an escalation procedure, and the authority to require actions necessary to protect assets from, or contain the spread of, security incidents.
- [OS10] Processes that include security considerations in the design and deployment of *services* or software, reviewed by the responsible individual or team identified in [OS1] above, or their representative.

4. Incident Response [IR]

Each *infrastructure* has the following:

- [IR1] A process to maintain security contact information for all *service providers* and communities.

- [IR2] A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the *infrastructure*, response and recovery strategies to restore *services*, communication and tracking tools and procedures, and a post-mortem review to capture lessons learned.

- [IR3] The capability to collaborate in the handling of security incidents with affected *service providers*, communities, and *infrastructures*, together with processes to ensure the regular testing of this capability.

- [IR4] Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with other security teams on a need to know basis, and will not be redistributed further without prior approval.

5. Traceability [TR]

Each *infrastructure* has the following:

- [TR1] Traceability of *service* usage, by the production and retention of appropriate logging data, sufficient to be able to answer the basic questions – who? what? where? when? and how? concerning any security incident.

- [TR2] A specification of the data retention period, consistent with local, national and international regulations and policies.

- [TR3] A specification of the controls that a *service provider* implements to achieve the goals of [TR1].

6. Participant Responsibilities [PR]

a. Individual users

Each *infrastructure* has the following:

- [PRU1] An Acceptable Use Policy (AUP) addressing at least the following areas: defined acceptable and non-acceptable use, *user* registration, protection and use of authentication and authorisation credentials, data protection and privacy, 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] A process to communicate changes to the AUP to their *users* that, for example, might arise out of new collaborative partnerships.

b. Collections of users

Each *infrastructure* has the following:

- [PRC1] A process to ensure that all *collections of users* of their *infrastructure* are aware of, and agree to abide by, *infrastructure* policy requirements, including the capability to collaborate in the handling of security incidents.

- [PRC2] Policies and procedures regulating the management of the membership of individual *users*, including registration, periodic renewal, suspension and removal, including forced removal due to policy violation. These must address the validation of the accuracy of contact information both at initial collection and on periodic renewal.

- [PRC3] A process to inform *collections of users* that they will be held responsible for the actions of each individual member of the *collection*, which may affect the ability of all members to utilise the *infrastructure*.

A *collection of users* has the following:

- [PRC4] A process to identify the individual *user* responsible for an action.

- [PRC5] Appropriate logs of membership management actions sufficient to participate in security incident response.

- [PRC6] Defined their common aims and purposes and made this available to the *infrastructure* and/or *service providers* to allow them to make decisions on resource allocation.

c. Service providers

Each *infrastructure* has the following:

- [PRS1] Policies and procedures to ensure that *service providers* understand and agree to abide by all applicable requirements in this document, including the capability to collaborate in the handling of security incidents.

7. Data Protection [DP]

Each *infrastructure* has the following:

- [DP1] Defined and enforced policies or a policy framework, together with associated procedures to protect the privacy of individuals according to legal requirements. These controls relate to the processing of their personal data (personally identifiable information) collected as a result of their participation in the *infrastructure*. Such data includes but is not limited to that used for accounting, *user* registration, monitoring and logging.

- [DP2] A process to make all *participants* aware, where applicable, that they must provide, in an easily accessible and visible way, a Privacy Policy covering the *participant's* processing of personal data for purposes necessary for the safe and reliable operation of their *service*, compliant with the *infrastructure* policy, or policy framework. This Privacy Policy should, where appropriate, describe the nature and scope of an individual's consent to processing, including rights for correction or erasure, and protections against unauthorised disclosure.

8. Acknowledgements

The authors acknowledge the support and collaboration of many colleagues in their respective *infrastructures* and the funding received by these *infrastructures* from many different sources. These include but are not limited to the following:

EGI acknowledges the funding and support received from the EGI Council Participants, and from the European Commission with the H2020 project EGI-Engage under Grant number 654142.

The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of more than 170 computing centres in 42 countries, linking up national and international Grid Infrastructures. Funding is acknowledged from many national funding bodies and we acknowledge the support of several operational Infrastructures including EGI, OSG and NDGF/NeIC.

The Extreme Science and Engineering Discovery Environment (XSEDE) is supported by the National Science Foundation.

9. References

[1] https://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

[2] https://refeds.org/sirtfi