WISE SCIV2-WG

David Kelsey
STFC-RAL

3rd WISE workshop, DI4R, Krakow

27 September 2016

Overview

- A short history of the SCI group
  - The Version 1 document
- WISE SCIV2-WG
  - Aims
  - Workplan
  - Next steps

A Trust Framework for Security Collaboration among Infrastructures (SCI Version 1)

David Kelsey (STFC-RAL, UK)

Science & Technology Facilities Council

Authors of the 1st SCI paper

- K. Chadwick (FNAL)
- I. Gaines (FNAL)
- D. Groep (Nikhef)
- U. Kaila (CSC)
- C. Kanellopoulos (GRNET)
- D. Kelsey (STFC)
- J. Marsteller (PSC)
- R. Niederberger (FZ-Juelich)
- V. Ribaillier (IDRIS)
- R. Wartel (CERN)
- W. Weisz (University of Vienna)
- J. Wolfrat (SURFsara)

Early days of Grid Security Policy

- Joint (WLCG/EGEE) Security Policy Group (JSPG)
- In 2005
  - EGEE, OSG, WLCG agreed a common version of the *Grid Acceptable Use Policy*
    - Accepted by all users during registration with a VO
  - And used by many other (Grid) Infrastructures
- EGI and WLCG in general continue to use the same Security Policies
- *Often not easy to agree on identical policy words*

Build a new Trust Framework

- Several large-scale production e-Infrastructures
  - Grids, Clouds, HPC, HTC, …
- Each has their own resources, users, policies and procedures
- BUT subject to many common security threats
  - Common technologies
  - Common users (spreading infections)
- Security incidents can spread rapidly
- Need to share information and work together on security operations

Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, HBP…
- Developed a *Trust framework*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

SCI Document – V1

- Proceedings of the ISGC 2013 conference

http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

- The document defines a series of numbered requirements in 6 areas

PROCEEDINGS OF SCIENCE

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

http://pos.sissa.it

PoS(ISGC 2013)011

SCI: areas addressed

- Operational Security
- Incident Response
- Traceability
- Participant Responsibilities
  - Individual users
  - Collections of users
  - Resource providers, service operators
- Legal issues and Management procedures
- Protection and processing of Personal Data/Personally Identifiable Information

SCI Assessment

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: … and comprehensively documented
  - Level 3: … and reviewed by independent external body

Further info

- Security for Collaborating Infrastructures

http://www.eugridpma.org/sci/

- SCI meetings

https://indico.cern.ch/categoryDisplay.py?categId=68

- Sirtfi – Started from SCI V1

https://wiki.refeds.org/display/GROUPS/SIRTFI

Now to the WISE SCIV2-WG

SCIV2-WG Aims

- Work towards a Version 2 document
- Involve wider range of stakeholders
  - GEANT, NRENS, Identity federations, …
- Address conflicts in version 1 for new stakeholders
- Add new topics/areas if needed
  - security audit/peer review, security risk assessments and software security review
- Give guidance on the assessment of infrastructures against the SCI requirements
- *We are not an operational security/trust group*
  - *Not compete with other op sec trust activities*
  - *But will seek feedback from such groups on our work*

SCIV2-WG Workplan

- Self-assessments against Sections 4 (Operational Security) and 5 (Incident Response) in SCI version 1
  - To decide what guidance is needed and what words need to be changed. (completed)
- Produce draft guidelines for sections 4 and 5.
  - all topics considered and questions discussed (see wiki)
- Tune words of sections 4 and 5.
  - And write the guidance for those sections
- Move on to other sections.
- Aim for version 2 of the SCI document by the 12-month anniversary of the group (May 2017)
- After version 2 produced consider re-merging text with Sirtfi and Snctfi work (AARC and REFEDS)

Meetings & Next steps

- To date we have held 4 one-hour meetings
  - All by video conference
  - Work also can be done via the group mail list
- Next meeting October? (tbd)
- Work will concentrate on tuning the words of sections 4 and 5. And to write the guidance for those sections
- Drafts of both of these before end of 2016

Final words

- We have plenty of room for more people in the working group
- Please volunteer
- Contact one of the two chairs (David Kelsey, Adam Slagell)
- Join the WG mail list
  - *https://lists.wise-community.org/sympa/subscribe/sciv2-wg*

Questions?