

TNC 2017 WISE Session Proposal: The Art of Creative Networking

Title: Mastering the Art of Collaboration for WISer Global Security

Session Chair: Hannah Short

Keywords: Security, Trust, Federation, Collaboration, Risk

Authors: Warren Anderson – LIGO Scientific Collaboration

Sven Gabriel – Nikhef, EGI

David Groep – Nikhef, EGI

Nicole Harris – GÉANT

Urpo Kaila – CSC, EUDAT

David Kelsey – Science and Technology Facilities Council (STFC), EGI

Jim Marsteller – Pittsburg Supercomputing Center (PSC)

Alf Moens – SURF

Ralph Niederberger – Research Center Jülich (JSC), Human Brain Project (HBP), PRACE and EUDAT

Hannah Short – CERN

Adam Slagell – National Center For Supercomputing Applications (NCSA) and XSEDE

Romain Wartel – CERN

For research and education to successfully defend ourselves against targeted online attacks, we're going to have to get creative... we're going to have to be WISE! The call for proposals for TNC17 asks us to consider the creativity required when building our networks; in security we witness attackers forming their own tight-knit communities to great effect – if we are to keep up we must master the art of collaboration and share best practices in Information Security.

As most are fully aware, cybersecurity attacks are an ever-growing problem as larger parts of our lives take place on-line. Distributed digital infrastructures are no exception and action must be taken to both reduce the security risk and to handle security incidents when they inevitably happen. These activities are carried out by the various e-Infrastructures, such as through the EGI CSIRT, and it has become very clear in recent years that collaboration with others both helps to improve the security and to work more efficiently.

There is no one way of preventing security incidents, but a range of security controls can help to reduce their likelihood. In some infrastructures, such as commercial clouds, the emphasis is on detecting incidents, handling them and charging the persons responsible for any damage they cause. In many research e-Infrastructures, the emphasis is more on a series of measures to help prevent incidents happening. There is more control over who can access an infrastructure, and who is allowed to do what.

The first line of defence is policy, which states what the various parties that interact with the infrastructure can and cannot do. Another is to ensure that sites that host the distributed infrastructure are managed and configured in a secure manner, and this is carried out by ensuring that sites fulfil certain conditions before they are able to join and by ongoing monitoring to ensure that they, for example, are not running software that is known to have serious security problems.

The choice of technology being used on an infrastructure is also important, to ensure that it does not have any obvious security problems, can be configured to comply with data security policies and is under security maintenance. It is important that any software vulnerabilities discovered are fixed by the software provider in a timely manner, and that the patches are deployed in the appropriate places. The rapidly changing and proliferation of technology makes all these activities more of a challenge. The fact that many different infrastructures deploy similar technologies and share user communities means that security incidents can rapidly spread between them.

The WISE (Wise Information Security for collaborating E-infrastructures) community was born as the result of a workshop in October 2015, which was jointly organised by the GÉANT group SIG-ISM (Special Interest Group on Information Security Management) and SCI, the 'Security for Collaboration among Infrastructures' group of staff from several large-scale distributed computing infrastructures. All agreed at the workshop that collaboration and trust is the key to successful information security in the world of federated digital infrastructures for research.

WISE provides a trusted global framework where security experts can share information on topics such as risk management, experiences about certification processes and threat intelligence. With participants from e-Infrastructures such as EGI, EUDAT, PRACE, XSEDE, NRENs and more, WISE focuses on standards, guidelines and practices, and promotes the protection of critical infrastructure. To date WISE has created five working groups, each tackling different aspects of collaborative security and trust.

The next WISE Workshop is planned for March 2017, where each working group will meet for focused activity on their deliverables and objectives. TNC 2017 is primarily placed to promote and share the published outputs with a wider audience of NRENs and User Communities, and gain feedback on the direction of WISE.

Session Overview:

We propose a full 90-minute session for TNC 2017. This session will start with an overview of the WISE Community and will be followed by a set of 10 minute presentations on the work being done both within our Working Groups and further afield. A selection of these talks is discussed here in further detail. The session will conclude with a moderated discussion (30 minutes) with audience participation. This open conversation will encourage feedback on the WISE activities and directions.

- In conjunction with Internet2, we will pool experiences of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for the Internet of Things (IoT) from both Europe and the US. The increasing number and variation of devices connecting to our networks introduces interesting new challenges for security experts. As IoT devices have evolved from printers, to wearable fashion, to home surveillance, there has been little regulation of security requirements despite the increase in associated risk.
- The STAA-WG (Security Training And Awareness Working Group) will present their overview of the supply and demand of security training, as well as a catalogue of recommended courses and resources for security teams. Training is wanted and needed for security professionals, system and network managers and engineers, users of the infrastructures and for decision makers, for a wide range of topics. Whereas security previously was mainly about hardening systems and incident response, it now involves a lot more topics such as risk management, compliance, data leak analysis and reporting. The STAA-WG is tasked with identifying such capabilities and the corresponding training offerings.
- We will hear from the SCIV2-WG (SCI version 2 Working Group), whose objective has been to update the 'Security for Collaboration among Infrastructures' (SCI) framework. The SCI group defined best practices, trust and policy standards for collaboration, with the aim of managing cross-infrastructure operational security risks. Version 2 of the SCI document will be finished early in 2017. It addresses a wider range of stakeholders, specifically the NRENs, and conflicts for new participants will have been addressed. An accompanying guidance document on interpretation of the standard will also be produced at the same time.
- The SBOD-WG (Security in Big and Open Data Working Group) will present their whitepaper on security issues in Big and Open Data. There are big datasets from scientific research that have to be accessible worldwide, replicable for security reasons

(damage) or with high-speed access (available at different sites to spread download capacity), but accessible by everyone or by distinct people or working groups only. Security issues in this context concentrate on confidentiality, integrity and availability.

The four talks above will be complemented by presentations from User Communities, highlighting the challenges they face in Information Security.

We propose to ask our colleagues in the WISE Steering Committee to be responsible for managing the final agenda (<https://wise-community.org/steering-committee/>). We are open to including other related TNC presentation submissions in this session.