

Human-oriented approaches to trust, security and privacy and the role of international cooperation – John Zic

John Zic is a research team leader in the Commonwealth Scientific and Industrial Research Organisation (CSIRO) ICT Centre, specialising in the area of privacy, security and trust. He is a co-inventor of the patented Trust Extension Device, which was the world's first portable USB trusted computing platform to incorporate a TPM cryptographic microcontroller. He holds Honorary Senior Research Fellow positions at the Department of Computing, Macquarie University and with the School of Computer Science and Engineering, UNSW. John has recently given invited presentations and keynotes at the EU FP7 INCO-TRUST workshop in New York in 2010, MIT Kerberos Consortium Conference in 2010 and 2011, and the Vanguard/TTI CyberINsecurity Conference in 2010 and participated in the 11th Joint EU and Australian Science and Technology Cooperation Committee in 2010. John was a member of the Australian Academy of Technological Sciences and Engineering Working Group on Cloud Computing from 2009-2010 advising on privacy, security and trust.

Fundamentally, the basis for human oriented approaches to trust, security and privacy relies on having a real (recognized) need for people to work together on a work package that cannot be addressed by a single entity. By grounding and focusing the work within a collaborative setting, a solid, practical understanding of the requirements for trust, security and privacy may be developed.

Further, partner organisations (commercial, government, and academic) will understand how best to contribute their own respective capabilities within the collaboration. To emphasise that there is a continuum of requirements for trust, security and privacy, two case studies were presented: one dealing with a specialist committee to respond to Australian biosecurity issues, and the other dealing with smart infrastructure and the relationships between residential customers and service providers. These two cases were used to demonstrate the diversity of collaboration types.

It is important to note that underpinning any successful collaboration requires not only that the partners understand their respective roles and contributions, but can also properly commit their respective resources and fund the work.

Establishing international co-operation is important in two respects. First, it offers collaborating partners increased access to potential receptors for ideas and cross-fertilisation of markets. Second, by definition, it builds a larger research community, and this in turn can enable future, potentially larger/more complex collaborative projects in trust, security and privacy. However, alignment and commitment is required at multiple levels, from the individual researchers to their respective organisations and to the participating governments. This complexity should be in the first instance address in a methodical manner.

First, identifying partners who are like minded and interested in addressing similar, relatively small scale but concrete problems with real needs (such as addressing the information management and process requirements of the biosecurity community). These can be regarded as pathfinder projects, which stand a good chance of being identified, proposed and finally supported by the broader community. Of course, any such project requires funding and commitment from each partner, and in the case of international co-operation, agreements need to be in place between the respective governments to allow the collaboration to proceed. This is particularly significant, as success requires the respective governments' policies and budgets to agree to participate in the international collaboration.

Actions that can be taken to build international co-operation include the development and building of local expertise and a community of users through such path-finder

projects. The success of these is then used to promote further development of international collaborations to the broader community. Path-finder projects may also be used to build up international linkages on an incremental level, with the community of users developing internal and external trust in each other to be able to successfully work together. As part of the community building, the development and engagement of partners in formal forums (such as the Internet of Things Forum, for example) is very important, with regular face-to-face meetings (both formal and informal) occurring during these fora. Once again, as a part of the community building exercise, it is important that each potential partner is able to support the work through assuring some funding and resourcing is set aside specifically for this activity. Good will is necessary, but not sufficient, for ensuring a successful collaboration or community building exercise.