Keynote: Identification of advantages for international cooperation and the trust and security technological challenges – BIC review of research topics already identified – Michel Riguidel

Speaker: Michel Riguidel is Professor Emeritus, previously the Head of the Department of Computer Science and Networks, at Telecom ParisTech (École Nationale Supérieure des Télécommunications, www.telecom-paristech.fr) in Paris, where he lectures in security and advanced networks. His research is oriented towards security of large Information Systems and Networks and architecture of communication systems (Security of the Future Internet, Trust, Privacy and Advanced Networks). In the European Projects, he is contributing to the Coordinated Action in international security research of the FP7 BIC (2011-2013) and caretaker for security and trust of the FIA (Future Internet Assembly). He has several patents in security (firewall, watermarking and protecting CD ROM, illicit content downloading).

In starting out his talk, Michel Riguidel explained in some detail the shifts in paradigms that we are encountering where it is increasingly difficult to attain a trusted and secure global digital communication and information handling system via a dependable international ICT infrastructure. This will continue to be based on an evolving Internet, together with the many services that rely on it to deliver their benefits. Many of these services are now integral parts of our daily lives and the fabric of our societies, and are increasingly part of our cultures. However, the whole edifice – Internet and Services – is currently quite frail and vulnerable to both attack and failure. The remedies include repair, shoring up and reinforcement, and eventual replacement over time by more modern robust or resilient designs and components.

A general recommendation made by Professor Riguidel is that it is essential to continue current initiatives and the ongoing consensus towards our goal of increasing the trustworthiness, dependability, and security of interoperable global ICT. Through the BiC project – Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services and previously INCO-Trust as explained in the opening talks, work is already in progress that will maintain, and indeed extend, the dialogue between Europe and international partners in pursuance of our goal. Through these projects, we are engaged in identifying topics and themes recommended for further elaboration leading to international collaboration and cooperation leading towards a stronger, more trustworthy global communications – where this inevitably involves the Future Internet.

Within the INCO-Trust project, a number of recommendations were made within their final deliverable D3.1 INCO-Trust Final recommendations **report**[1]. Two groups of recommendations are Strategic and Tactical and these were presented in brief by Prof. Riguidel. It was pointed out that the ordering of the recommendations is not meant to imply any over-riding chronological order, but that the Strategic group are meant to be the pre-requisite enablers for international cooperation, setting out the frameworks, common understandings and motivations, and overall landscape to ensure the possibility and effectiveness of the more concrete Tactical group recommendations.

[1] http://www.inco-trust.eu/media/D3_1_report.pdf

The recommendations made here are split into two groups:

- Strategic: setting out the frameworks, common understandings, and overall procedural and governance landscape that takes into account the diversity of social, economic, and cultural norms and requirements worldwide;
- Tactical: research towards the technical building blocks and their relationships that will enable a trustworthy, secure ICT ecosystem.

(a) Strategic Recommendations

SR1 **International alignment**: preparation of policy frameworks to enable global collaboration and interoperability

SR2 **Variety**: cooperation on topics related to security and diversity.

SR3 **Scalability**: cooperation on topics related to security and complexity

SR4 **Reciprocity**: cooperation on topics related to security and interoperability

SR5 **Secrecy**: cooperation on the issues of digital sovereignty and dignity

SR6 **Negotiation**: cooperation on the theme of security and trust

SR7 **Security expertise**: cooperation on topics related to security and technological challenges of security

SR8 **Protection:** cooperation on topics related to security and cyber-defence

(b) Tactical Recommendations

The international ICT trust and security community should collaborate on research to:

TR1 Support strengthening infrastructure resilience and control crisis management.

TR2 Support securing the current and future Internet related to diversity, complexity and interoperability.

TR3 Support securing cloud computing for enterprises.

TR4 Support designing identity and accountability management frameworks.

TR5 Support new privacy infrastructure, reconsidering privacy spaces, storage function areas.

TR6 Support repositioning trust infrastructure at the same level as security infrastructure.

TR7 Support metrics and standardization issues.

TR8 Initiate green security.

TR9 Support cooperation in cyber-defence against the asymmetric challenge

TR10 Enable the engineering of secure and trustworthy software and systems.

Professor Riguidel summarised the four main themes that have been highlighted in the project's bi-lateral cooperation events to date. These include:

Theme 1: Digital ecosystem security (Network & Information security) oriented to the System. This theme involves protection and trustworthiness with the strengthening of infrastructure resilience and control crisis management, crisis management (CIP), Security and cyber-defence (incl. against the asymmetric challenge). It also includes securing the current and Future Internet, network/system security, securing cloud computing for enterprises, Mobile security, security for mobile connectivity. In addition, it deals with policy properties such as variety, scalability, reciprocity, diversity, complexity and interoperability.

Theme 2: Trust & Privacy (including personal data protection) oriented to the Humans, Users. It incorporates topics related to responsibility (Identity versus Anonymity), designing identity and accountability management frameworks, international Privacy friendly authentication and reputation assurance. It includes measurement and negotiation, repositioning trust infrastructure at the same level as security infrastructure and trust management. Other areas under this theme include secrecy, dignity, sovereignty designing digital sovereignty and dignity, and new privacy infrastructures, reconsidering privacy spaces, storage function areas; and, last but not least, usability creating a Human oriented and usable security for citizens.

Theme 3: Global Framework & International alignment oriented to principles & governance. This includes properties such as interoperability, openness, transparency and secrecy; the preparation of policy frameworks to enable global collaboration and interoperability; Knowledge and International Data exchange architectures for cybersecurity; and socio-economic aspects including data policy, governance and secure, trustworthy and viable ecosystems.

Theme 4: Methodology, tools and technical challenges oriented to the tools. Under this theme is expertise sharing in science, technology & engineering; methods to support metrics and standardization issues; software security to enable the engineering of secure and trustworthy software and systems; protection of data and information with cryptology (digital signature, etc.) and other upstream topics including the initiation of green security.

In conclusion, Professor Riguidel presented a table showing a summary of all of the countries interactions to date, showing the programme /funding agency contacts, research level contacts and a sampling of the priority research themes for international cooperation in trust and security. The full table can be found on the next page.

Table 1. Summary of all of the countries interactions to date

Country	Program Level	Research level	Priority research themes for INCO
USA	National Science Foundation Department of Homeland Security	Massachusetts Institute of Technology, Rutgers University, University of California, San Diego, University of California, Davis, University of Illinois , Others	CyberSecurity/Privacy: Technology and Usage Issues Trustworthy International information exchange including data transfer and sharing, Security models for the Future Internet.
Canada	National Science & Eng. Res. Council	Univ. of New Brunswick, Ecole Polytechnique Montreal	Industry driven projects on trust, security and privacy.
Korea	Ministry of Knowledge Economy, KEIT	SoonChunHyang University, Seoul National Univ. Others	Internationalisation of data (identity management, privacy, end to end trust metrics, ...); Countermeasures against Massive DDoS; Security of Cloud computing e.g. Security of Smart Grid; Security compliance management and information security assurance; Security for VoIP and Mobile communications; Future Internet.
Japan	Japan Science and Technology Agency, CREST programme, MIC	NICT, University of Tokyo, Tokyo Inst. of Tech, JAIST, Others	Dependability, Security, Privacy and Trust of embedded systems
Australia	Australian Research Council (ARC)	CSIRO, NICTA, Macquarie University, Univ. of Sydney, IIS Partners, many others	Communications Security, Trust and Privacy in the Future Internet; Formal approaches for trust and security.; Sensor networks.
Brazil	CNPq (National Research council), FUNTEL, State Research foundations ITI (Instituto Nacional de Tecnologia da Informação)	Universidad de Brasilia, Univ. of Sao Paulo, CPqD Serasa Experian, Others TBD	Future Internet, Wireless Technologies: Security, Privacy, Trust over ad-hoc networks, Quantum crypto, ID management.
South Africa	SA Dept. of Science and Technology SA Technological Innovation Agency	Council for Scientific and Industrial Research (CSIR) – The Meraka Institute, SAP, University of Pretoria, University of Johannesburg, University of South Africa, others	Wireless Technologies: Security E-infrastructures security and trust
India	Dept. of Information Technology (DIT), ERNET, EuroSpirit India Support action (FP7)	India Institutes of Technology (IITs), India Institute of Science (IISc), Universities - Hyderabad, Pune, Anna amongst others).	Data Center Security, Data Privacy, ID card, ID management.