BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services

1st Annual Forum
29th November 2011
Brussels, Belgium

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

BIC is a Coordination Action Project within the European Commission, DG INFSO Unit F5, Trust and Security

Jan. 2011—Dec. 2013

http://www.bic-trust.eu

Table of Contents

EXECUTIVE SUMMARY

The EU FP7 BIC project[1] held its first Annual Forum on 29th November 2011 in Brussels. The main goal of the BIC Co-ordination Action project is to engender co-operation of EU researchers and program managers with their peers in emerging countries, namely Brazil, India and South Africa**.** The project is facilitating a technical and programme level catalyst for engagement, collaboration and networking activities internationally. In addition, the BIC project will provide continuity and bring together a truly global collaboration with the participation of the already established countries from the INCO-TRUST project, including the United States, Canada, Japan, Korea and Australia. One of the means in accomplishing this ambitious goal is the holding of a BIC Annual Forum on Trustworthy ICT.

The **mission** of the BIC annual forum is discussion and agreement on technological challenges/gaps of common interest amongst the countries, agree on what can and needs to be done internationally (who can contribute to what), and then work at an international level towards delivering on cooperation towards solving these joint technological challenges. The forum will enable the working towards the definition of tangible international activities, including success metrics and setting up global projects.

The **objectives** of the BIC Annual forum are:

- Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;
- Highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation;
- From the insights of the researchers and programme managers, to explore how best to organise future International cooperation (INCO) research activities and its supporting programmes, together with the key challenges, issues and priorities.

Significant **momentum** amongst the participants to build an international research community focussing on mutually beneficial research topics in trust, security and privacy was noted throughout the forum. There was a strong message from the participants to forge ahead with the necessary cooperation towards building the communities around the identified thematic areas of priority from their countries. Hence, an important outcome of the Annual Forum was the establishment of three working groups (WGs), two technical and one logistical, that would be facilitated by BIC. It would be the intention of the BIC project to additionally form longer term action groups based on the successful outcomes of these WGs to ensure implementation and take-up. The established WGs are entitled: WG1. Human oriented/citizen security; WG2. Network Information security / Cybersecurity; and WG3. Programme/funding focus/ identify community.

This shortened version of the BIC Annual forum report contains a high level summary of all of the results from the sessions. There is a longer version of the report with an annex II containing detailed summaries of the presentations. This long version can be found at http://www.bic-trust.eu/events/event/upcoming-event-bic-annual-forum/.

[1] http://www.bic-trust.eu/

INTRODUCTION

The EU FP7 BIC project[2] held its first Annual Forum on 29th November 2011 in Brussels. The main goal of the BIC Co-ordination Action project is to engender co-operation of EU researchers and program managers with their peers in emerging countries, namely Brazil, India and South Africa**.** The project is providing a technical and programme level catalyst for engagement, collaboration and networking activities internationally. In addition, the BIC project will provide continuity and bring together a truly global collaboration with the participation of the already established countries from the earlier INCO-TRUST project that included the United States, Canada, Japan, Korea and Australia. One of the means in accomplishing this ambitious goal is the holding of a BIC Annual Forum on Trustworthy ICT.

To prepare for the Annual forum, a BIC session[3] dedicated to the planning of the forum was held in Amsterdam on 6th July 2011 during the SysSec workshop[4] in which a number of topics were already identified for inclusion that were carried forward to the agenda. In addition, contributions were invited from the research communities of ICT trust and security to put forward position papers on topics requiring international cooperation.

MISSION AND OBJECTIVES OF THE ANNUAL FORUM

The overall mission and objectives of the BIC annual forum are to bring together the wider and global trust and security communities to explore how best to organise future International Cooperation (INCO) research activities and its supporting programmes, together with the identification of the key challenges, issues and priorities to tackle together. The agenda was formed to cover the core objectives of the Annual Forum.

Objective 1. *Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;* This objective was being covered by a presentation on identification of advantages for INCO and the trust and security technological challenges – BIC review of research topics already identified; and panel session 2: Human oriented approaches to security, privacy and trust and how international cooperation can benefit; and panel session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.

Objective 2. *Highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation;* This objective was being covered by the opening session on Setting the scene with DG INFSO views onINCO and Panel session 1: Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.

Objective 3. *From the insights of the researchers and programme managers, to explore how best to organise future International Cooperation (INCO) research activities and its supporting programmes, together with the key challenges, issues and priorities.* This objective was being covered by Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects; and panel session 2. Human oriented approaches to security, privacy and trust and howINCO can benefit; and panel session and 3. Digital ecosystems network and information security and howINCO can provide mutual benefits; and the closing session on planning and operations.

[2] http://www.bic-trust.eu/
[3] http://www.bic-trust.eu/events/event/bic-session-syssec-workshop/
[4] http://www.syssec-project.eu/events/1st-syssec-workshop-program/

AGENDA

9:00	**Welcome and Introduction** Jim Clarke, Waterford Institute of Technology, BIC Coordinator
9:10	**Setting the scene with DG INFSO views on International Cooperation.** Alvis Ancans, European Commission, DG INFSO, International Relations Unit Gustav Kalbe, European Commission, DG INFSO, Deputy Head of Unit F5, Trust and Security
10:00	**Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.** Projects (Panelists): EU – India Spirit (Tom Williamson), Synchroniser (Katja Legiša), EURASIAPAC (Fernando Kraus Sanchez), SECFUNET (Marcelo Pasin), BILAT/ACCESS4EU/SECAS (Rado Faletic).
10:30	**Identification of advantages for international cooperation and the trust and security technological challenges – BIC review of research topics already identified.** Michel Riguidel, Telecom Paris-Tech, ENST, France
11:00	**Coffee and networking break**
11:30	**Panel Session 2. Human oriented approaches to security, privacy and trust and how international cooperation can provide mutual benefits.** Chair: Priscila Solis Barreto, University of Brasilia, Brazil Panellists: Karima Boudaoud, France; Ioannis Krontiris, Germany; John Zic, Australia; Jan Eloff, South Africa; Fabio Martinelli, Italy.
13:00	**Lunch break**
14:00	**Panel Session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.** Chair: John C. Mallery, MIT, USA (for Karl Levitt, University of California, Davis, USA) Panellists: John C. Mallery, USA; Bart Preneel, Belgium; Abhishek Sharma, India; Hiroyuki Hishinuma, Japan; Razvan Gavrila, Greece.
16:00	**Coffee and networking break**
16:30	**Planning and operations session** Moderated by BIC partners
17:30	**BIC Annual Forum closing**

RESULTS OF THE ANNUAL FORUM

This section will summarise the high level results of each of the individual sessions. Please note that an extended version of the report with detailed summaries of the individual talks in an annex II can also be found at http://www.bic-trust.eu/events/event/upcoming-event-bic-annual-forum/.

Taking into consideration the mission, objectives and inputs received for the annual forum, the programme was designed in a way to include a good mix of presentations, panel sessions and discussions. In summary, the programme outcomes consisted of the following elements.

The opening session of the Forum was an opportunity for the European Commission, in particular, **Alvis Ancans,** DG INFSO, International Relations Unit and **Gustav Kalbe,** DG INFSO, Deputy Head of Unit F5, Trust and Security, to set the scene for the BIC annual forum and present perspectives on INCO between the EU and other countries in the context of the ICT theme of EU's 7th Framework and the importance of INCO within ICT Trust and Security research. As part of this session, there were details presented on past, current and future activities in the pipeline already identified that are directly or even indirectly related to trust and security. During these two talks, the following points were highlighted:

- The Commission recognises the strong need to cooperate internationally, with the following objectives:
    - To jointly develop ICT solutions to major global societal challenges;
    - To jointly respond to major global technological challenges by developing interoperable solutions and standards;
    - To improve scientific and technological cooperation for mutual benefit.
- There are a number of targeted EU – Japan calls open presently in calls 8 and 9
    - Objective ICT-2011.1.1 Future Networks (Call 8);
    - Objective ICT-2011.1.2 Cloud Computing, Internet of Services and Advanced Software Engineering (Call 8);
    - Objective ICT-2011.3.1 Very Advanced Nanoelectronic Components (Call 8);
    - Objective ICT-2011 9.6 FET Proactive: Unconventional Computation (UCOMP) (Call 8);
    - Objective ICT-2011.5.2 Virtual Physiological Human (Call 9).

It is expected that there will be further joint calls in Work Programme 2013 that is under construction, including Brazil, Russia (currently under discussion; topics: high-performance computing and semantic web) and the possibility of coordinated Calls with Australia, South Africa, Mexico and Japan are in the pipeline – more likely in 2013 or later.

Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.

A panel session was comprised of a number of INCO-related projects with direct or indirect linkages to ICT trust and security aspects. The session was supported by the following projects - panellists:

Euro-India SPIRIT[5] project - Tom Williamson, European Research Consortium for Informatics and Mathematics, European Economic Interest Grouping) ERCIM EEIG. He is the project co-Ordinator of Euro-India SPIRIT project.

SYNCRONISER[6] project - Katja Legiša, an Italian consultant with seven years of experience in international and EU project management, promotion and support of research and development activities. Her professional and educational background is in Project Management, Public Relations and Communication. Since 2006, she is coordinating EU-India projects. She is now the Project Coordinator of the SYNCRONISER project.

EURASIAPAC[7] project - Fernando Kraus Sanchez, Director of the Foreign Affairs Sector within the Research and Innovation division of AToS in Spain. Fernando has over fifteen years of experience in participating in the implementation of ICT projects including the EURASIAPAC project. He has wide experience in the field of exploitation and marketing activities as a senior consultant both in the private and public sectors of different countries (Argentina, Azerbaijan, Brazil, Cameroun, Dominican Republic, Egypt, ..).

SECFUNET Project - Marcelo Pasin, Assistant professor at the University of Lisbon. Previously, he was a researcher at INRIA (France, 2007-2008) and tenured associate professor at the Federal University of Santa Maria (Brazil, 1991-2007). He has worked for CoreGRID, EGEE and EC-GIN in FP6, and is now working for TClouds and SECFUNET in FP7. SECFUNET is a project from within the recent EU-Brazil joint call held during Call 7 of FP7.

FEED/AUS-ACCESS4EU/SECAS - Rado Faletic's involvement with the Forum for European-Australian Science and Technology cooperation (FEAST) stems from his interest in promoting, encouraging and highlighting science and new ideas, along with the personal satisfaction he receives from facilitating individual collaborations.

The purpose of this session was to broaden the perspectives and to gain insights from other projects related to both INCO and trust and security. The format of session was the panellists were asked interactively to address key questions by the moderator and any other questions from the audience.

The following tables contain a condensed summary of the responses to the questions raised to the panellists (full responses are detailed in Annex II):

[5] http://www.euroindia-ict.org/
[6] http://euroindiaresearch.org/synchroniser/
[7] http://eurasiapac-fp7.eu/

Question 1	**How does your project contribute to International cooperation and trust and security?**
EU-India Spirit	• EU – India collaboration with working groups in ICT Addressing Societal Challenges; AudioVisual Media & Internet; and Emerging Technologies & eInfrastructures. • Trust and security: strong topic in all three working groups and hence, one of the umbrella themes.
SYNCRONISER	• Boosts impact of the policy dialogue by identifying EU-India research priority areas and recommendations on how to improve the cooperation. • one of identified research priority areas is *Security, Privacy & Monitoring* (data management system, secure storage system, person identification and tracking systems; for healthcare, governance and education).
EURASIAPAC	• Eurasiapac focuses on ICT research cooperation between the EC and the Asia-Pacific region, mainly Korea, Japan, Australia and New Zealand. • Trust and Security has been identified as one of the priorities among the topic of interest in ICT research in the countries participating in the project.
SECFUNET	• SECFUNET is a STREP in FP7, with EU and Brazilian partners. • It proposes to create a new generation in the Internet security that is very simple to use.
FEED/ AUS-ACCESS4EU/ SECAS	• *SECAS: Strategies for European ICT RTD Collaboration for Australia and Singapore* identified ICT thematic capabilities and areas of potential synergy, performed policy analysis and has made strategic recommendations for improved cooperation policies. • Trust and security topics are clearly identified in the final report, which is now available online.

Question 2	What are the benefits and expected impact to your project brought on by international cooperation?
EU-India Spirit	• The Indian partners have increased visibility and familiarity with Commission-funded projects, in particular, and EC processes in general as well as strong relationships with consortium members and related entities.
SYNCRONISER	• The project has provided a more practical, consultation approach to boost the impact of policy dialogues on Joint research priority areas. This will feed into the upcoming High level working group meeting in 2012. • Synchroniser uses a bottom up approach in which the project provides the EC with the evidence from the experts, on which they can make policy decisions.
EURASIAPAC	• The contacts and the fact that some main stakeholders in ICT research have been directly involved in the project has raised interest in launching joint calls with some of the countries. • Joint calls with Japan and Australia are under preparation and are being considered for the future.
SECFUNET	• SECFUNET's partners are very heterogeneous providing different yet complementary skills. Specifically from Brazil we get different perspectives, very different regulation frameworks and very different concerns and Brazilians also include a pioneer researcher in intrusion-tolerance and a national networking research laboratory. • SECFUNET also allows for leveraging previous cooperation, that would otherwise be impossible.
FEED/ AUS-ACCESS4EU/ SECAS	• Both FEED and AUS-ACCESS4EU have greatly contributed to the flow of information between Europe and Australia regarding overall funding modalities available for international collaboration, but more importantly have identified and developed strategies on how to most successfully use these mechanisms (including FP7, COST[8], ARC[9] and NHMRC[10]). SECAS has produced a concrete set of strategic recommendations, which are available in the final public report online.

[8] http://www.cost.eu/
[9] http://www.arc.gov.au/
[10] http://www.nhmrc.gov.au/

Question 3	**International cooperation is not an easy task and requires a lot of patience and time. What are the issues encountered and how did you address them?**
EU-India Spirit	• Difficulties in scheduling and organising face-to-face meetings are obviously magnified in international cooperation projects with such significant scale; • When involving external experts, need significant advance notice time for stakeholders.
SYNCRONISER	• The difference of viewing time and deadlines is different between the two countries, which brings to difficulties in carrying out joint activities. • The difference between Formal and Informal communications plays an important role in getting things done and especially when passing a message across.
EURASIAPAC	• Although the Eurasiapac project focuses on ICT cooperation between EC and the Asia-Pacific region, it's difficult to deal it as a homogeneous region because each participating AP country (Japan, Korea, Australia, New Zealand) has different characteristics, institutions and approach to ICT research. • In Europe, the EC FP7 creates a common approach to research, but it doesn't exist a similar common institutions in the Eurasiapac targeted countries. Each country needs to be dealt in a different way. • difficult working cooperation process due to time zone differences. • IPR is always an issue in international ICT research cooperation and needs to be dealt at a very early stage of the research process.
SECFUNET	• In time scales, although evaluated at the same time, the start times of projects were very different (by 6 months) and this caused significant start-up problems between the countries. • Cooperation projects in Brazil are not structurally the same as in EU. Brazilians operate in a more independent fashion and don't over-rely on meetings as we do in the EU. • The evaluation process is also very different between EU and Brazil. In Brazil, reporting is carried out mainly in the very end of the project, therefore, making it difficult to get things going in terms of a common progress reporting mechanism between the countries. Another example is Brazilians are not responsible for delivering to the EC. • These efforts need to be harmonised between the participants in the different countries.
FEED / AUS-ACCESS4EU/ SECAS	• One of the issues of most importance has been the persistent lack of understanding, particularly in Europe, regarding how to include third country partners on FP7 proposals. • FEED and AUS-ACCESS4EU have been working actively (through email alerts, but more affectively through targeted seminars and direct communication) to education both Australian and European researchers on *the facts* as well as *the realities* of including Australian partners on FP7 projects. This includes issues of funding support. • SECAS has identified issues ranging from abstract political ones (e.g. that policies need to be concrete, should also include technical content, and need follow-up actions) to practical ones at the researcher level (e.g. how to best work over long distances, the benefits of setting up joint labs, the challenges of researcher exchange, etc.).

Question 4	**In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy?**
EU-India Spirit	• The EU – India Spirit project is finishing at the end of December 2012 so it is difficult to plan a longer term strategy beyond this and it hasn't been built into the legacy planning. • In terms of BIC, it is highly recommended to continue the collaboration in the countries and it has been a highly mutual benefit to have a number of the BIC members involved in the working groups of EU – India Spirit from the very start.
SYNCRONISER	• Both the EU – India Spirit and Synchroniser projects have had long term planning problems due to the periodic postponements over the last 2 years of the main DIT/EU meeting. However, this same situation resulted in this very topic of long term planning to be included as a key recommendation being made by the project. • For liaising with other projects like BIC, this is also included in a recommendation that the follow up work can be directly or indirectly supported by other projects and/or other initiatives or channels. • Recommendations on improving the longer term cooperation between the countries via other means apart from the projects as projects have limited duration. Some examples in discussions include: Executive bodies, collaboration with EU based eTPs, forming India based eTPs, which would be discussed in more detail later. This approach came up as the project recognises that research priorities have a strong tendency to change from year to year and we need something more everlasting. This is what is missing now and needs to be addressed as a matter of urgency.
EURASIAPAC	• This is an issue that was highlighted and attempted by EURASIAPAC also but it was found to be incredibly difficult as even though the project's overall goal was to consider the cooperation between the EU and the entire ASIAPAC region as a whole, in actual fact, there are considerable differences between the countries involved and these always need to be factored into the discussions and cooperation models. • Therefore, a bi-lateral approach is absolutely necessary even if there are some common cooperation issues across the regions.
SECFUNET	• As a perspective for longer term exploitation, as it is a STREP project carrying out RTD that will have eventual exploitation value, SECFUNET have several industrial partners. We feel it is the combination of the companies that are going to do their development of their products within the projects in order for the project to have a longer term impact for both the partners and the project in general. • Examples: Twinteq wants to develop its products in near-field communication, EtherTrust and Implementa work with secure elements like SIM cards, and Infineon wants to boost its trusted components for the future networks. More generally, SECFUNET wants to establish a sound security infrastructure that could be used by anyone.
FEED / AUS-ACCESS4EU/ SECAS	• The issue of sustainability has been a very important one especially within the FEED/BILAT projects where they have started working already with what we call 'multipliers' to impart our knowledge and key ideas around Australia. For other projects, it is an issue. What can projects do during their lifetime so the work can continue? BIC can talk to the SECAS project to see if there is anything BIC can do to help create this value. • BILAT project, one of which just finished are putting together significant workshops on specific topics. BIC can help develop the content and identify the individuals who can contribute to this workshop. This can lead to more lasting co-operations.

Question 5	What are your recommendations for improving effectiveness?
EU-India Spirit	• Greater emphasis should be placed on widening the net of participating international partners, so as to ensure that consortia are to the greatest extent possible comprised of partners with the most appropriate competencies and not the limited pool of potential partners who are already familiar with the FP7 structure and have previously participated in projects. • In this regard, projects promoting international cooperation such as BIC, India-Gate and its equivalents for the other BRIC countries are crucially important.
SYNCRONISER	• Recommendations include setting up collaboration with ETPs and xETP Initiatives in order to launch the Indian Technology Platform Channel. • Recommendation to involve Indian experts in the ISTAG related activities: Search on the mechanism which would allow Indian experts to get involved in the relevant bodies shaping priorities and strategic directions of the FP7/Horizon 2020. • Another recommendation is to establish a JWG Action Group for executing JWG outcome: Proposal to establish a JWG Action Group that could execute the JWG outcome. The form could be flexible (nomination of officers by EU and India, Support Project, Tenders, ...). The Action Group would be a sort of executive office to undertake the decisions adopted by the JWG. • Another recommendation is a proposition of a Co-funding Model for DIT: *Analyse Energy and Biotechnology co-funding programmes (between EC & DST).*
EURASIAPAC	• Recommendation to create more agile processes to define, launch and approve ICT cooperation initiatives. Many of the Asia-Pacific institutions involved in the projects, mentioned that the period of time to create, prepare and launch a cooperation initiative should be shorter as the view is that EC processes take too long. • Understanding legal and administrative EC funding processes are not always easy for non EC institutions; simplified methods may enhance international participation.
SECFUNET	• As recommendations for improving effectiveness, better agreements with non-European authorities, with, for instance, better definitions in the commitments, and better synchronisation. It could include previous negotiation for project management standards, as, for example, how to deal with deliverables, project review and evaluation. • The European Commission should help the targeted applicants to have knowledge of its rules and evaluation standards, using, for example, concertation meetings in the targeted countries.
FEED / AUS-ACCESS4EU/ SECAS	• Recommendation for better coordination and information-sharing between the variety of INCO activities across FP7. Consideration should be given to this issue in future INCO calls. • Recommendation that activities be developed to facilitate the integration of activities amongst all INCO projects, particularly so that findings can be directly implemented into ongoing projects (rather than waiting for final reports, which in any case are rarely read by other INCO actors).

Keynote Presentation: Identification of advantages for international cooperation – BIC review of research topics already identified.

In this keynote presentation, Professor Michel Riguidel presented the key technological challenges and themes already identified from within BIC thus far and previously within the INCO-Trust project[11]. These findings would be used as a benchmark later on during the discussions. During the presentation, a number of points were highlighted including:

- The need for the international ICT trust and security community to collaborate on identifying both strategic and tactical recommendations and priorities[12];
- Four main themes have been highlighted for INCO in trust and security:

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

+ INCO in trust and security. The full table can be found on the next page.

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

Summary of interactions between INCO countries to date, showing the programme/funding agency contacts, research level contacts and priority research themes.

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.

Panel Session 2. Human oriented approaches to security, privacy and trust and how international cooperation can benefit.

The panel session was supported by the following researchers/presentations engaged in the panel session topic areas.

- Karima Boudaoud, University of Nice, France: "Human oriented and usable security management"
- Ioannis Krontiris, Goethe University Frankfurt, Germany: "Privacy-respecting Authentication"
- John Zic, Commonwealth Scientific and Industrial Research Organisation (CSIRO) ICT Centre, Australia: "Human-oriented approaches to trust, security and privacy and the role of international cooperation"
- Jan Eloff, SAP Meraka UTD / SAP Research Pretoria, South Africa: "Collaboration with Africa / BRICS [13] for human oriented approaches to security, privacy and trust"
- Fabio Martinelli, Istituto di Informatica e Telematica - IIT; National Research Council - C.N.R., Italy: "Network of Excellence on Engineering Secure Future Internet Software Services and Systems"

Based on these presentations and discussions at the end of the session, a number of research items for Human oriented approaches to security and INCO were elaborated by the participants.

Multi-disciplinary International cooperation amongst all stakeholders

Security management should be more accessible to all kind of users and especially non-security experts evolving towards a more human oriented security management vision. To address today's security issues, we need to: 1) move from the traditional technology-only oriented design of security solutions towards user-centric security management and 2) bring together experts from psychology, social science, economics, legal, technologists and security experts to address security and privacy from a user point of view and put her/him at the heart of problem. From an international point of view, we need:

- Collaboration between security experts and experts from other disciplines (psychology, social science, etc.) and from different countries, in addition to collaboration with international government institutions.
- Organisation of **multidisciplinary** and **international workshops** targeting wide public.
- Set up of **multidisciplinary** and **international working groups** in targeted countries.
- Collaboration with international standardization organisations.

Technological research can also greatly benefit from international cooperation when it comes to taking into consideration the human factors in designing technologies. The following questions should be examined:

- How people perceive technological solutions and how that affects the adoptability of the corresponding technologies?

[13] BRICS group of countries: Brazil, Russia, India, China, and South Africa

- How to best explain to people the potentials and features of the existing solutions?
- How to best design user-interfaces to encourage usability and adoptability?

The answers to these questions will vary for different cultures and by opening up research beyond the European borders. It would give us a great insight in these aspects and eventually help us design better technology.

To address the above challenges, collaboration opportunities should allow EU-project consortia to open up and include various kinds of actors in the international setting: user communities, governmental organizations, regulatory authorities, and research institutes. A framework for enabling such collaboration should encourage joint working groups, organization of public events with experts from both sides and collaboration in standardization activities.

Privacy concerns in an international setting

Currently, European RTD projects engaged in privacy research e.g. ABC4Trust are building architectures based on privacy requirements collected within the European setting (e.g. Greece and Sweden). However, privacy concerns differ in the international setting. These differences can be attributed to differences in cultural values and perception of privacy, differences in the familiarity with Web privacy practices, or even differences in regulations. In that respect, international cooperation could greatly help exchanging views with other cultures, collect different application scenarios and requirements from other cultures and effectively broadening the perspective of privacy-ABC architecture.

Privacy and information utility are conflicting requirements. As the level of privacy increases, the level of information utility decreases. This is because as we hide more information to preserve privacy, the usefulness of the released information decreases. Local context and culture also influence what information should be regarded as private, and what information is considered as useful. It is, therefore, an open research question to be discussed how privacy relevant processing with and in countries like Brazil, India or South Africa can be handled within the European context.

- How are concepts like proportionality, unlinkability, minimal disclosure etc. being perceived in other countries?
- How other legal systems outside Europe can be affected by and have effects on Privacy-ABCs?
- How to ensure an optimum balance between privacy and utility, taking into account local contextual needs and preferences?

The establishment of "Path-finder" projects

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 (addressing the information management and process requirements of the bio-security communities in the EU and Australia was used as an example). These can be regarded as "Path-finder 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.

Secure software-services development

Security concerns must be addressed from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process. In light of the unique security requirements the Future Internet will expose, new results will be achieved by means of an integrated research, as to improve the necessary assurance level and to address risk and cost during the software development cycle in order to prioritize and manage investments. To address this, the NESSoS project research covers several main areas: A first set of activities represents the traditional early stages of (secure) software-services development: from secure requirements over architecture and design to the composition and/or programming of working solutions. These three activities interact to ensure the integration between the methods and techniques that are proposed and evaluated. In addition, NESSoS research programme adds two horizontal activities that span the service creation process: Both the security assurance programme and the programme on risk and cost aware SDLC will interact with each of the initial three activities, drive the requirements of these activities and leverage upon, even integrate their outcome; finally, notice that all 5 research activities mentioned above will be inspired and evaluated by their application in specific FI application scenarios.

NESSoS has set up a Networking and Liaison Board (NaLAB) for international cooperation mainly aimed at representatives of Technical WGs in the topics of the NoE. The creation of the NaLAB is in progress right now and it is explicitly meant to collect researchers from outside Europe. Several NESSoS components would benefit the international cooperation: the NESSoS Common Body of Knowledge; the engineering tool workbench; open competition, research activities. NESSoS plans to identify the main stakeholders in the NESSoS topics world-wide and create connections among researchers/WGs especially using the NESSoS internal mobility programme. Some possible cooperation topics include comparison of tools and techniques; usage control of disseminated data; and focus on SLA with protection of information, possibly in cooperation with other projects as ASSERT4SOA and ANIKETOS.

Research and technology outputs

International collaboration should be based on context awareness. Traditional user-centred approaches for technology development do not consider cultural and contextual needs. This results in deriving user requirements that do not give a correct view of the real needs, leading to technology shortcomings. Examples of contextual factors that should be considered include:

- Cultural norms and tradition
- Appropriate tactics for community entry and engagement
- Appropriate research techniques that involve the users and communities
- Appropriate needs assessment practices
- Infrastructure capacity of the targeted community
- Solution maintenance and life-cycle costs

The technology developed should be advantageous from the viewpoint of the local users. Therefore, technology development should be based on an understanding of the real requirements as well as an understanding how existing technology can be adapted to meet contextual requirements. Lastly, solutions developed should be relevant to local users, their needs and the available infrastructure.

Enhanced Collaboration methodology

European funding opportunities (e.g. Framework Programmes) should encourage collaboration with partners in Africa / BRICS. European Project consortia should be more open to accept African / BRICS partners, which should not just provide use cases, but should also develop and adapt technology for their local needs.

We also recommend the following three areas of research topics for international cooperation with regards to security, privacy and trust.

International approaches to usable security

In Africa / BRICS, mobile phones are the most common ICT device used. Typical users of such devices may not fully understand the security vulnerabilities the use of these devices pose. Security configuration of such devices for most users will therefore be a challenge. Therefore, the research challenge to address with regards to facilitating usable security is: How to quantitatively analyze and design appropriate user interfaces for mobile devices to enable a typical user to make informed decisions about different security settings?

International approaches to Trust

In African communities, trust is influenced by social network position. Social position governs activities within rural communities. For example, the chief of a village can influence business collaborations. Rural communities, therefore, require a different approach to business due to unique social structures, social norms, and traditions. Therefore, the research challenge to address with regards to trust is: How to ensure that trust management takes into account concepts relevant to the target context?

In conclusion, by facilitating international cooperation to provide human oriented approaches to security, privacy and trust, we believe that both European and African / BRICS partners will benefit. The great potential of the Africa / BRICS market can be exploited, while at the same time, these markets will be provided with solutions that are appropriate, affordable and contextually-relevant.

Panel Session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.

The panel session was supported by the following researchers/presentations engaged in the panel session topic areas.

- John C. Mallery, Massachusetts Institute of Technology, USA, “International Data Exchange and A Trustworthy Host: Focal Areas For International Collaboration In Research And Education”
- Bart Preneel, Katholieke Universiteit Leuven, Belgium. “International Cooperation in Cryptology”
- Abhishek Sharma, NetEdge Tele-Solutions (P) Ltd., India, “Trust and Security for Mobile Communications Services”
- Raznan Gavrila, European Network and Information Security Agency (ENISA), Greece, “EU-US joint CIIP Exercise, Cyber Atlantic 2011”

Based on these presentations and discussions at the end of the session, a number of research items for Digital ecosystems network and information security and international cooperation were elaborated by the participants.

International Data Exchange architecture for Cybersecurity needed

A key message is the acknowledgement that international cooperation in Cybersecurity is nascent and a more global approach is urgently needed because there is ultimately just one, single, global information environment, consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between countries. We need comprehensive research towards international *intelligence*, *surveillance*, and *reconnaissance* (ISR) in the cyberspace domain.

The challenges can be characterized as follows:

- **Problem:** Attackers can replay attacks across different countries without rapid international learning to defend against attacker innovations
- **Benefits:** International collaboration and coordination can rapidly reduce defensive gaps across the OECD and build crisis-response capacities
- **Leverage:** Bias work factors in favour of defence and against cyber attack
- **Approach:** Exchange data related to cyber crime, attack patterns and best defence practices
- **Research:** Motivate technical research via needs of realistic data sharing scenarios

An architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than countries, sectors or organizations might otherwise achieve individually. A strawman architecture for an

international data exchange framework was presented that would enable the international cybersecurity community to securely carry out cyber data sharing and collaborative analysis as follows:

- Build shared awareness and understanding of cyber phenomena across countries
  - Employ shared data collection methodologies
  - Integrate measurements of phenomena across borders
  - Focus early on cyber crime and economic incentives
- Create comparable transnational data sets
  - Capture cyber breaches, attack patterns, best practices, defensive coordination
  - Include aggregate data on crime, black markets, economics, state-state interactions, long-term transformations
- Field a cyber data sharing framework that helps countries to:
  - Collect cyber data for compatible sharing
  - Fuse data to create common situational awareness
  - Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
  - Exchange derived data in real time
  - Provide mechanisms for controlled drill down needed for law enforcement, advanced persistent threats (APT) or cyber emergencies
- Build shared collection, fusion, analysis, and response capabilities.

Open source trustworthy host platform for collaborative research and education

An open-source trustworthy host platform for collaborative research and education is required to address the following challenges:

- Problem: Attackers are subverting legacy architectures, which are inadequate for current threats
- Benefits: Development and evolution of a clean-slate trustworthy host will:
  - Create reference host architecture for computing, routers, cloud, embedded, wireless
  - Integrate best information assurance (IA) engineering from the open literature
  - Provide a reference paradigm for cumulative research and education
  - Drive higher assurance for open source and commercial software
- Leverage: Raise work factors required to compromise commodity hosts
  - Eliminate remote access penetration vectors
  - Prevent privilege escalation
  - Manage information leakage
  - Verify tool chain and resulting software
  - Rapidly detect and remediate flaws or breaches
- Approach: Pool research efforts across OECD countries to create and evolve a shared host platform reflecting best IA engineering practices
- Research: Motivate technical research via needs of an existing and readily-accessible free implementation.

International Cooperation in Cryptology

With respect to cryptology research on an international level, there is a need for integrated research and policy levels between the EU and counterparts around the world, and collaborative research is required across academia, industry and government

agencies. To build an international strategy for INCO in cryptology, there is a need for collaboration on cryptographic algorithms with the establishment of open competitions with shared governance; effective standardization and continual updates of a key lengths and parameters document register (management of standards). Collaboration also should take place on cryptographic protocols motivated by distribution of trust and privacy (key component in privacy by design) and joint research also need to occur in these areas. We can be more effective by avoiding duplication and increasing impact on both the technology and policy levels. During the discussions, it was also pointed out that for the International open source trustworthy host platform presented, a common cryptographic software stack is a requirement agreed by everyone.

Mobile Security of Software Services

In future, significant confidential operations such as banking transactions and mail exchanging will take place largely from mobile devices. In these cases, it is vital to protect the customer data and applications from attack. Since the Smartphone/Mobile penetration is increasing globally, it makes a lot of sense that large regions, particularly regions like Europe and India/ Asia collaborate closely for the Research & Industrial Developments. Many companies are already putting effort in developing their goals and strategies for securing mobile data and applications.

Furthermore, it is critical to understand what there is to lose – the global vulnerability – before a major mobile security breach occurs. The ultimate goal is not about completely eliminating mobile security risks but rather having the proper systems in place to minimize the impact when breaches occur. Well thought out international controls involving the proper security technologies combined with the proper documentation and business processes are essential.

Mobile Security coverage of international technological research areas should include access, transmission, switching/ distribution, and storage. The international research communities should also focus on other related areas including policy, standards, tools, regulatory controls & test beds. There is already an Indo-Australia project covering international cooperation on mobile / wireless threats. It was suggested that this project should be examined and whether it could also include an EU element to it.

It was also suggested that the level of Industry participation may be increased from where it is and a higher mix of SMEs and large corporate with research bodies would be ideal. Towards this, BIC can be a key player in ensuring this critical coordination.

Joint exercises for Cybersecurity planning and improvement across borders

A presentation was made about the joint EU-US Joint CIIP exercise, called Cyber Atlantic 2011, co-organised by the European Union's cyber security agency, ENISA[14] and the Department of Homeland Security (DHS) in the USA. The first joint exercise was held on 3rd November 2011 and was set up as a centralised table-top exercise in which over 20 countries were involved (17 countries played).

Cyber Atlantic 2011 was an exploratory exercise with the following objectives:

- Explore and identify issues in order to improve the way in which EU Member States would engage with the US during cyber crisis management activities;

[14] http://www.enisa.europa.eu/

- Explore and identify issues in order to improve the way in which the US would engage with the EU Member States during their cyber crisis management activities, using the appropriate US procedures;
- Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

There was a two part scenario used for the scenario:

1. Advanced Persistent Threat (APT) scenario with a hacker group, “Infamous”, *exfiltrated* sensitive documents from EU and US – ‘Euroleaks’ web site and
2. Supervisory Control and Data Acquisition (SCADA) scenario highlighting vulnerabilities leading to backdoors (and failures) on Programmable Logic Controllers of power generation equipment.

The initial lessons learned (results ongoing) from Cyber Atlantic 2011 were:

- Mechanisms/structures for cross-border cooperation do exist; however, each country needs awareness of all communications options ;
- There is a further need to exchange Standard Operating Procedures (SOPs), training, exercises;
- Exercises need increased participation from all three areas: Technological, Law Enforcement, Policy/Political;
- Single Point of Contact in EU for US would help but is not compulsory;
- More exercises/workshops are needed!

CONCLUSIONS AND NEXT STEPS

A final dedicated session on the future planning and operations was designed to set out where the BIC project and the community will go in the next period, and to discuss what the trust and security research community would need in terms of support for these activities.

The chairs from the technical sessions started the session with a short summary of the recommendations made within their panel sessions.

Session 1: Opening session and panel of INCO projects.

James Clarke presented the recommendations from session 1:

- **Implement technical platforms or longer term initiatives apart from projects alone** (something lasting and that can help cooperation between multi-countries
- **BIC should talk to SECAS** partners about their **experiences** (see if their methodologies and approaches would be of use to BIC)
- **BIC** may help to develop **content** for upcoming **BILAT** workshops.
- **Efforts should be made to dramatically increase** visibility of RTD programmes.
- In addition to Working groups, look at possibility of setting up permanent **Action Groups** to improve collaborations (currently recommendations are highlighted but nothing is implemented, which leads to frustration amongst the key stakeholders)
- It is good to **take stock** of current INCO projects, to provide greater clarity on what important topics we want to focus on.
- **Bi-lateral** approach and initiatives are still very important and necessary, even when trying to establish a parallel **truly global community**.
- **Collaborations** between various countries will be at **different levels**, and over time could improve taking **ideas or building on experiences** from other countries established collaborations. **Patience is required**.
- **There is a need to co-ordinate** activities of INCO across **all areas (as an umbrella)**, to get a bigger picture of what's going on.

Session 2: Human Oriented Approaches to Security.

Priscila Solis Barretto presented the recommendations from session 2:

- It is important to consider that we are in a globally connected world with **different generations** of users.
- We need **the adaptation of experts** to what users need, not the contrary (**user centricity**).
- **Multidisciplinary workshops and building international working groups** is necessary, e.g. multi-disciplinary experts on human oriented security.
- Build **local expertise** and then establish key **international linkages**: local expertise based on local demands and then participate together in coordinated calls for formal cooperation.

- Development of solutions that take into account the **different social structures** (BRICs, developing countries, etc.).
- **Availability of Funding mechanisms:** good will is important but there must be a political work between agencies in the different countries to be successful.
- **Cooperation activities** to compare tools and techniques, avoid duplication, validation of case studies and shared testbeds **in different environments** and **cultures**.

Session 3: Digital ecosystem and network information security.

John C. Mallery presented the recommendations from session 3:

- As a community, we should pick the highest priority topics in network security and develop an **overall international R&D plan for policy makers.**
- Focus on **mutually beneficial topics** for **international cooperation:**
  - International data exchange architecture for cybersecurity;
  - Open source trustworthy host platform for collaborative research and education;
  - Cryptology;
  - Mobile Security of Software Services;
  - Joint exercises related to cybersecurity
- **Identify** R&D expertise in the relevant fields.
- Form a **planning group to get maximum impact.**
- Cryptography - Like to have **world scale competition**
- **Ecrypt II roadmap for next 10 years –** crypto for cloud computing/Internet of Things
- In the US, NIST drives crypto policies, in Asia, crypto policy is by country, **Europe joint research policy by country.**
- **We Need to bridge gap between research interaction with policy/**
- Algorithms – **More open competitions** with shared governance
- In order to foster Joint research – we need to **go beyond meetings.**
- Mobile applications – e.g. mobile health care, data storage – **threats lead to wider implications.**
- **Focus on** policy framework, build prototypes for DDOS, secure new services, mobile security.
- **Lessons** taken from the **EU – US Cyber exercise** should be taken on board and more of these kinds of exercises should be organised.
- In Japan, there is a large scale **International Project on Cybersecurity**. It should be checked as to the feasibility of forming co-operations around this.

BIC Working / Action Groups

Michel Riguidel presented a summary of the work items in which working groups would be established and supported by BIC. It would be the intention of the project to additionally form longer term action groups based on the successful outcomes of these working groups.

WG1. Human oriented /citizen security focus, which as a starting point would focus on the following topics:

- End to end trust assurance for users;
- Usability / user interface designs;
- Addressing prediction, validation and enforcement mechanisms needs and requirements;
- Putting users in control of their data and information;
- Taking into account cultural aspects.

WG2. Network Information security / Cybersecurity, which would focus on:

- International data exchange architecture for cybersecurity;
- Open source trustworthy host platform for collaborative research and education;
- Cryptology;
- Mobile Security of Software Services;
- Joint exercises related to cybersecurity.

WG3. Programme /funding focus/ identify community, which would focus on:

  - Identifying stakeholders (contacts in programme management and research communities);
  - R&D Planning/R&D experts of excellence;
  - Raising programme visibility.

If interested to participate to these working groups, please contact **michel.riguidel@telecom-paristech.fr** and **jclarke@tssg.org**

Finally, in order to increase the networking potential of the international trust and security community, an international research network portal is being set up by the BIC project to enable a one stop shop for trust and security researchers from all countries. The information will be accessible and searchable by country, research topics, projects, and other criteria. The portal will also provide access to researchers other well established sites – LinkedIn, personal web sites, blogs, ..A number of people from the International research community have already volunteered to participate in the BIC portal in the first draft. Additional volunteers are welcomed to **jclarke@tssg.org.** An example screen shot is shown in Figure 1:

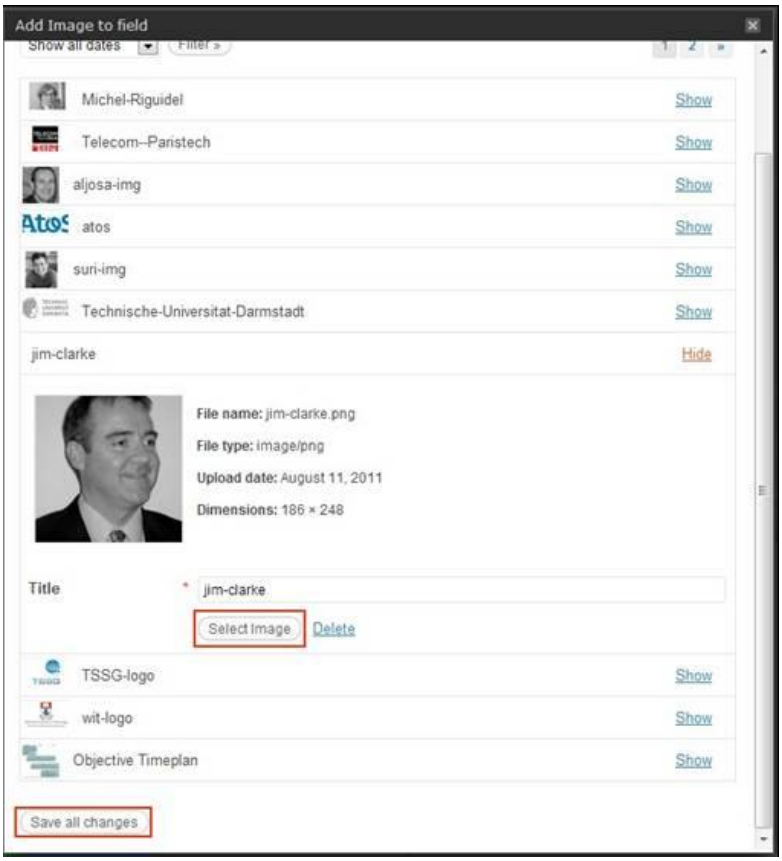

Figure 1. BIC Research network portal – data entry page

Acknowledgments

The BIC project is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research[15].

[15] http://cordis.europa.eu/fp7/ict/security/

Annex I. List of registered attendees

		BIC Annual Forum Registrants as of 28th November 2011	
Last Name	**First Name**	**Organisation**	**Country**
Aguilar	Virginia	Nato	Belgium
Ancans	Alvis	European Commission	Belgium
Arsene	Vlad	Vector Business Consulting (RO)	Romania
Barreto	Priscila Solis	University of Brasilia	Brazil
Boudaoud	Karima	University of Nice	France
Bus	Jacques	DigiTrust.EU	Netherlands
Clarke	James	Waterford Institute of Technology	Ireland
Cleary	Frances	Waterford Institute of Technology	Ireland
D'Antonio	Salvatore	University of Naples Parthenope	Italy
Eloff	Jan	SAP Meraka UTD & University of Pretoria	South Africa
Faletic	Rado	Forum for European-Australian Science and Technology cooperation	Australia
Gavrila	Razvan	European Network and information Security Agency (ENISA)	Greece
Hishinuma	Hiroyuki	National Institute of Information and Communications Technology (NICT)	France
Hoepman	Jaap-Henk	TNO, Groningen & Radboud University Nijmegen	Netherlands
Howker	Keith	Waterford Institute of Technology	Ireland
Ishigami	Megumi	Fraunhofer IFF	Japan
Kalbe	Gustav	European Commission	Belgium
Kar	Ashok	Infra Technologies	France
Kechadi	Tahar	University College Dublin, Ireland	Ireland
Krontiris	Ioannis	Goethe University Frankfurt	Germany
Legiša	Katja	TESEO Sprl	Belgium
Levitt	Karl	University of California, Davis	United States
Mallery	John C.	Massachusetts Institute of Technology	United States
Malone	Paul	Waterford Institute of Technology	Ireland
Martinelli	Fabio	National Research Council - C.N.R.	Italy
Massonet	Philippe	CETIC	Belgium
McManus	Gary	Waterford Institute of Technology	Ireland
Menevidis	Aki Zaharya	Fraunhofer IPK	Japan
Morales	Stephanie	Sigma Orionis	France
Morgan	Gary	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia
NIVOLIANITOU	Zoe	NCSR 'DEMOKRITOS'	Greece
OLIMID	Cristian	European Commission	Belgium
Pasic	Aljosa	AToS	Spain
Pasin	Marcelo	University of Lisbon - FCUL	Portugal
Preneel	Bart	Katholieke Universiteit Leuven - COSIC	Belgium
Riguidel	Michel	Telecom-ParisTech, ENST	France
Sanchez	Fernando Kraus Sanchez	AToS	Spain
Sekiguchi	Satoshi	AIST	Japan
Sharma	Abhishek	NetEdge TeleSolutions Pvt. Ltd.	India
Skellern	David	Macquarie University	Australia
Sora	Adrian	Vector Business Consulting (RO)	Romania
Torrenti	Camille	Sigma Orionis	France
Tsagalidis	Ross W.	FMKE	Sweden
Williamson	Tom	ERCIM EEIG	France
Yuncken	Elizabeth	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia
Zic	John	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia