BUILDING International Cooperation
for Trustworthy ICT

D4.5 BIC Workshop on success metrics and technical Working Groups (WGs)

Grant Agreement number: 25258655

Project acronym: ***BIC***

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

Funding Scheme: ICT-2009.1.4 [Trustworthy ICT]

Project co-ordinator name, title and organisation:

James Clarke, Programme Manager, Waterford Institute of Technology

Tel: +353 71 9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

Project website address: http://www.bic-trust.eu

Table of Contents

Executive Summary

At the 1st BIC Annual Forum[1] in November 2011, a key recommendation was made for enhanced coordination and information-sharing across the variety of bi-lateral International Cooperation (INCO) activities sponsored by the European Commission. As BIC spans multiple countries with a unique multi-lateral profile, BIC decided to further this recommendation by hosting a workshop that brings together the multiple projects and stakeholders that are already engaged in International cooperation

International Cooperation in the area of cyber-security is beginning to develop: the global approach is urgently needed because there is ultimately just one, single, global information communications and technologies 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, in addition to robust system defences, we have the ability to conduct comprehensive intelligence collection and evaluation on any developing cyber-threat, followed by near-simultaneous processing, exploiting and disseminating of the information to activate our response. This depends on multi-stakeholders engaged in collaboration, including data exchange and sharing (and also knowledge sharing) between countries.

One of the main objectives during the workshop was to discuss how to move from a more tactical based approach (bi-lateral) towards a more strategic approach (multi-lateral approach), although no clear procedure on how it can be done was identified, when for instance a particular research topic, e.g. cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach may not be suited for this type of longer term strategic activity. It was agreed that this needs to be addressed especially by the programme management and funding stakeholders.

A number of key elements are essential to be considered from the outset to establish the objectives and manage cooperation, duly taking into consideration the challenges. The UN Resolution 57/239 from 2003. *Creation of a global culture of cyber security*, (attached as Annexe 1) called for the sort of international cooperation and collaboration envisaged by the workshop.

A successful set-up of a framework for international cooperation calls for consideration of the inevitable complexities and multiple dimensions requires: an inclusive and pervasive approach, clear scope of work, appropriate management structure, focus, vision, mission and target, etc. and, of course, funding.

Different FP7 initiatives, and approaches to international cooperation foreseen in H2020 were addressed during the workshop, as well as the approaches of other funding agencies and initiatives connected to ICT trust and security in BIC related countries: Brazil (CNPq, CTIC, FUNTEL), South Africa (DST, CSIR, NRF, SPII) and India (the main one is DIT).

Interesting discussions on a variety of several hot issues including the identification of “success metrics” for international cooperation and collaboration were held in the workshops. The difficulty of this task was acknowledged by most participants, as countries have different ways and mechanisms for carrying out Research and Technological Development (RTD) management, funding, plans and implementations, and also the success metrics can refer to several levels (market results, new standards, technologies, policies, regional knowledge interchanges, amongst others).

[1] http://www.bic-trust.eu/events/1st-bic-annual-forum/

1. Aims and Objectives

The European Commission is advocating and supporting strong cooperation internationally, with the following objectives:

1. To jointly develop ICT solutions to international societal and economic challenges relating to the security and trustworthiness of the global ICT systems, services and infrastructures;
2. To jointly respond to major global technological and operational challenges by developing interoperable solutions and standards;
3. To improve scientific and technological cooperation for mutual benefit.

At the 1st BIC Annual Forum[2] in November 2011, a key recommendation was made for enhanced coordination and information-sharing across the variety of bi-lateral International Cooperation (INCO) activities sponsored by the European Commission. As BIC spans multiple countries with a unique multi-lateral profile, BIC aims to further this recommendation by hosting a workshop that brings together the multiple projects and stakeholders that are already engaged in International cooperation with the intent to:

- Explore the insights and common experiences across projects;
- Identifying, discussing and assessing (a) key challenges, issues and priorities; and (b) mechanisms for international cooperation that are already available;
- Explore possible synergistic approaches for mutual collaboration, cooperation and organising future joint INCO research activities and its supporting programmes.

The Workshop spanned two full days. It aimed to achieve the following concrete outcomes:

- From the experiences and insights of the participants, determine the ways to move forward on international cooperation, and future calls for collaborative research;
- Forming the current bi-lateral (and potentially overlapping) country to country cooperation into a comprehensive and coordinated global cooperation;
- Compiling a who's who directory of agency and research contacts across the countries;
- Identification of "success metrics" for international cooperation and collaboration:
  - rationale – motives and goals – engagement in international cooperation;
  - success criteria with regard to results;
  - analysis and assessment of INCO impact.
- First face to face meeting of the three Working Groups of BIC.

[2] http://www.bic-trust.eu/events/1st-bic-annual-forum/

2. Drivers for International Cooperation

2.1 The rationale for International cooperation

As strategic technology competition among nation states for national advantage intensifies, an ideological divide could emerge between the like-minded democracies and more authoritarian states, centred on values of Internet freedom, respect for intellectual property, privacy, data protection, and free and fair economic competition.

This conflict of views arises against the backdrop of a dramatic build out of vulnerable ICT products that has created easy opportunities for malicious action, and enabled largely unchecked cyber crime, extensive industrial espionage, and dangerous foundations for cyber conflict.

As digital societies become ever more reliant on ICT, careless outsourcing of protection of freedom, privacy and security is a recipe for strategic loss. In this environment, it is more important than ever for the democracies to retain technological leadership so that all can benefit from safer products that protect individual freedom, intellectual investments, and privacy. Like-minded countries need to develop universal norms for system engineering and for design certification. They need to produce high-integrity products reflecting these principles as they drive ICT standards that reduce opportunities for bad cyber behaviour, while enhancing international stability, and promoting orderly international interactions.

With this in mind, from the European perspective, cooperation with third countries and international organisations has been and will be promoted with the following objectives:

- strengthen EU's excellence and attractiveness in research and innovation
- strengthen EU's economic and industrial competitiveness
- support EU's external policies
- with international collaborators jointly address global societal challenges.

2.2 Strategic Approach for international cooperation

One of the main objectives during the workshop was to discuss how to move from a more tactical based approach (bi-lateral) towards a more strategic approach (multi-lateral approach) as seen in figures 1 and 2.

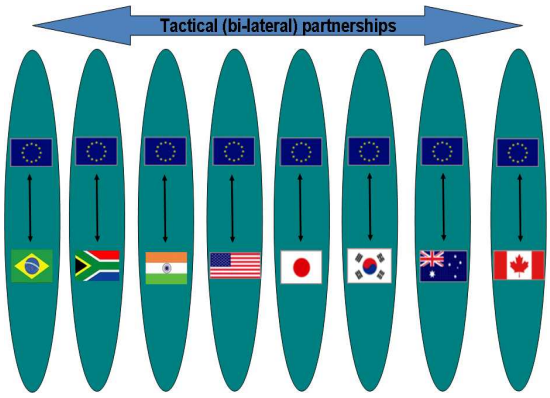


Figure 1. Tactical (bi-lateral) approach

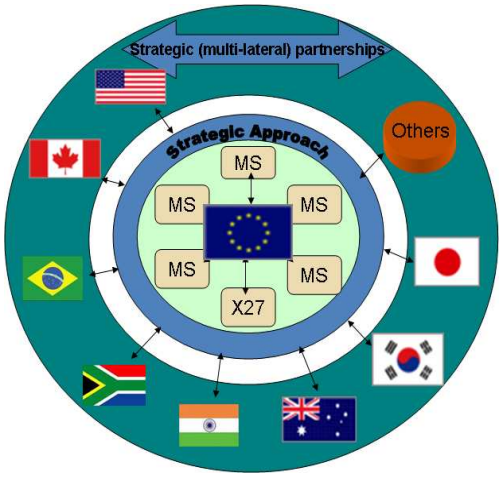


Figure 2. Strategic (multi-lateral) approach

In order to examine this challenge, the workshop brought together a majority of the projects engaged in international cooperation with long standing expertise in both bi-lateral and multi-lateral international cooperation (working with governments and/or specific agencies) to enable the following outcomes:

1. discuss their experiences and insights in order to brainstorm a strategy to move forward on international cooperation in future calls for collaborative research;
2. Forming the current bi-lateral (and potentially overlapping) country to country cooperation into a comprehensive and coordinated global cooperation.

In addition to BIC, a wealth of experiences was represented from the following international cooperation projects: IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU – India Spirit, Synchroniser, Euro-IndiaGrid2, OpenChina-ICT, FIRST, FORESTA, PAERIP, SEACOOP, EuroAfrica-P8, IST-EC2 (EU funded FP6 project to foster research in ICT between Europe & Canada), and AMERICAS.

These projects gave their insights on their experiences and suggestions for improvement and the main point was agreement that it is a very good idea to move towards a more multi-lateral strategic position. However, in the discussions, it wasn't very clear how this strategy shift could occur within the current mechanisms that focus bi-laterally on seven (7) distinct regions. While this regional approach may work for higher level themes, the main difficulty arises when a particular research topic, for example, cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach is not suited for this type of longer term strategic activity.

In order to address this, in the BIC project through the interactions with the International Advisory Group (IAG) and Working groups (WGs), they are trying to capture a more strategic approach and this was presented at the workshop and is summarized in the next sections.

2.3 Key elements for International Cooperation

The terms of reference of BIC Working Groups specify that WG3, (Programme/funding and focus/identify community,) will focus on a multi-disciplinary approach towards establishing international cooperation between all stakeholders.

Having recognized the importance and relevance of International Cooperation to addressing the critical issue of ICT Trust & Security, it is essential to appreciate that the organisation of this level of cooperation needs special treatment to identify and define objectives and manage their execution to achieve the intended results.

A number of key elements are essential to be considered from the outset to establish the objectives and manage cooperation, duly taking into consideration the challenges.

In this context, it is appropriate to note UN Resolution 57/239. *Creation of a global culture of cyber security*, attached as Annex 1 to this report.

The participants agreed that in order to reach the stage of mutually beneficial international collaborative research projects, the stakeholders must systematically go through a number of contributory phases:

1. setting the strategy and designing the framework processes;
2. establishing the framework – both the procedural and technical aspect. this requires close cooperation with the funding bodies;
3. setting up collaborations and projects within the framework;
4. carrying out the joint research and development work.

This process is not intended be overly rigid: it is recognised there must be overlaps and potential of activities out-of-sequence, e.g, BIC may be seen as preceding any agreed framework, and is thus part of phase (1). The necessary strategy for the successful set-up of a framework for international cooperation calls for consideration of the inevitable

complexities and multiple dimensions involved. The following (non-exclusive) key elements need to be addressed for projects[3] (including projects related to the development of strategies for international cooperation e.g. BIC, AMERICAS, IST Africa, …) that are going to contribute to international cooperation.

1. **Inclusive & All Pervasive approach** with a focus on excellence should be an essential theme for building up the right team(s) and the scope of project(s) and participants.
2. **Clear Scope of Work (SOW).** Defining the SOW with clarity is the next essential part for smooth progress of work and avoiding any ambiguity at a later date.
3. **Appropriate Management Structure** commensurate with the SOW and deliverables with unambiguously defined hierarchy of role and responsibilities is another key element to help ensuring effective management.
4. **Focus:** Projects of such diverse dimensions are prone to getting diverted from the original path / objective. Caution against such pitfalls and constant reviews are essential to stay focussed.
5. **Vision, Mission & Targets:** A management approach with well defined vision, mission & targets is essential. While the project objectives should have a vision beyond an estimated period of time say five years, there has to be mission oriented approach for achievements in medium length of time, say 3-5 years. At the same time, the progress of the project must also define short term action plans and targets that must be achieved within the time blocks of 3 months, 6 months and one year.
6. **Project Management:** The project would also need to follow established principles of project management with special emphasis on following aspects:
    a. Planning of resources, costs and time (time lines & mile stones) and a clear roll out plan.
    b. A suitable monitoring mechanism associated with regular review of processes, people and benchmarks.
    c. Provision for Course Corrections of the project activities may also be required at times after the reviews.
7. **Long Term Strategy:** The current and emerging threats to trust & security are an ongoing challenge, with constant possibilities of new types of threats coming up with time; the project needs to have long term strategy and provision for collaboration with future projects.
    a. **Metrics:** It would also be essential to measure the progress in concrete terms and; suitable metrics are essential to assess the state of the project at any point of time. More discussion on metrics, or indicators, for success is given in section 2.5 below.
    b. **Project roadmap:** The nature of international strategy development projects like BIC and others would not allow the classical approach to define the roadmap right in the beginning. A flexible approach with regular reviews at some defined milestones would be more appropriate to maintain a meaningful direction.
    c. **Successful outcome:** A good project needs to strive for a successful outcome in line with the defined deliverables. Metrics for goal setting & achievement for assessing proper implementation and provisions for carrying forward to a next stage, if applicable, providing for such continuity for a project to smoothly roll on to a subsequent stage are essential elements for the concluding phase. However, it was

[3] A ‘project’ can cover any funded group collaborative activity in any of the above four phases, not just the productive, phase (4) elements

noted at the workshop that the mechanisms available in the Framework Programmes don't always enable this to happen as there might be a shift in the priorities of the call text and resulting evaluation interpretations and focus leaving the project participants in a difficult situation to have any level of continuum.

8. **Funding:** YES – absolutely! – but, planning and building a strategy for long term international participation involves ongoing work by individuals and bodies from different countries, and organisations with diverse backgrounds. 'Voluntary' participation is often needed and relied upon, particularly in the early days and between phases; this is based mainly more on a personal basis than on the involvement of a particular project (probably non-existent anyway: projects come and go; the people and their know-how stick around). However, for this sort of arrangement to work, there needs to be some longer-term support-funding available to cover necessary associated costs – travel, coordination, central administration, secretariat, venues, etc. It is recommended that the IAG, in particular the programme management members, explore the options and possibilities for establishing such support; a sort of 'trust fund[4]', and/or, perhaps set of interconnected 'trust funds' to be used if and when required.

2.4 Stakeholders, Mechanisms & Frameworks

The BIC Project has two main stakeholders:

1. Researchers in both academic and industrial capacities: these are the specialists in the field, expected to explore various options, carry out necessary research and technological developments for the proposed solutions. The role of the industry will be to develop the products and solutions based on the designs provided by the researchers and take the developed products and solutions to the market, to the users.
2. Programme Management: These are the government bodies related to the area of research that are engaged in the facilitation of the mechanisms and frameworks for funding. They are involved in the examination and evaluation of the proposals, allocation of the funds, and formulating the process of regulating the required funds and disburse the same in accordance with the defined process.

2.4.1 Europe

Within Europe, the European Commission's Framework programme 7 (FP7) has supported international cooperation, including within areas related to trust and security research, in a number of different ways.

The first is a '**general opening**', where international partners are welcome to participate in all Challenges and Objectives with the following eligibility criteria:

- Minimum 3 different EU Member States or Associated Countries
- Beyond this minimum, all non-EU/non-AC countries can participate

The second is a '**targeted opening'**, where the participation of third countries is particularly encouraged. The targeted openings are explicitly mentioned in some of the Objectives (e.g. Australia, South Korea under WP2013).

The third is part of '**Horizontal Actions'** including bi-lateral coordinated calls. Some examples include the coordinated calls with Brazil and Japan (under WP2013) and international partnership building and support to dialogues (Objective 10.3 under WP2013).

A number of targeted openings in WP2013 were highlighted during the workshop including:

[4] a government fund administered separately from other funds and used for a specified purpose.

1. Objective ICT-2013.1.5 Trustworthy ICT: EU-Australia cooperation on building user trust in broadband delivered services
   - Demonstrate in a real-life environment the maturity and practicality of a digital authentication framework in broadband delivered services working across several jurisdictions (organisational, governmental) with high levels of assurance.
   - Funding: up to €3 million
2. Objective ICT-2013.1.7 Future Internet Research Experimentation (FIRE):
   - EU-South Africa cooperation on future internet experimental research and test-bed interconnection
   - EU-China cooperation on future internet experimental research and IPv6
   - EU-South Korea cooperation on future internet experimental research
3. Objective ICT-2013.2.2 Robotics Use Cases and Accompanying Measures:
   - Robotics networking - help identify new users and markets and new research areas through sector-based analysis; establish a strategy towards sustainable international cooperation in robotics, focussing initially on the United States.

A number of coordinated calls available in WP2013 were highlighted.

1. ICT-2013-10.1-EU-Japan Research and Development Cooperation. A number of important events have taken place between the European Commission and EU research communities with Japan (MIC/NICT) over the last few years in the “Future Internet” domain. This work has led to the organisation of an EU-Japan coordinated call that is part of the research Work Programme 2013.

   The topics for consideration include:

   a) Optical communications
   b) Wireless communications
   c) Cybersecurity for improved resilience against cyber threats
   d) Extending the cloud paradigm to the Internet of Things – Connected object and sensor clouds within the service perspective
   e) Federation of test-beds: control, tools and experiments
   f) Green and content centric networks

The funding scheme for the coordinated call with EU- Japan is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 9 million (a similar budget for the call is expected from the Japanese MIC and NICT). The timing for the call is 2 Oct – 29 Nov 2012.

The whole work programme is subject of an information day in Warsaw, Poland on 26 and 27 September 2012. See information at:
http://ec.europa.eu/information_society/events/ictproposersday/2012/index_en.htm.

In addition, concerning the EU-Japan R&D activity, a dedicated page has been opened where you can submit your ideas, partner search, and take this opportunity to be part of the EU-Japan networking session that takes place on 27 September 2012. You will find the relevant additional information at:

http://ec.europa.eu/information_society/events/cf/ictpd12/item-display.cfm?id=8435

2. ICT-2013.10.2 EU-Brazil Research and Development Cooperation. The topics for consideration include:

a) Cloud computing for Science

b) Sustainable technologies for a Smarter Society

c) Smart Services and applications for a Smarter Society

d) Hybrid broadcast-broadband TV applications and services

The funding scheme for the coordinated call with EU - Brazil is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 5 million (a similar budget for the call is expected from the Brazilian Ministry of Science, Technology and Innovation (MCTI). The timing for the call is 10 Jul – 24 Oct 2012.

The Horizontal International cooperation actions available in WP2013 include Objective ICT-2013.10.3 International Partnership Building and Support to Dialogues, where the goal is to support dialogues between the European Commission/the EU and strategic partner countries and regions, and to foster cooperation with strategic third country organisations in collaborative ICT RTD both within the EU's Framework Programmes (FP7, Horizon 2020) and under relevant third country programmes. The Targeted countries/regions include:

a) ACP countries (in particular Africa)

b) Asia (in particular China, India, South-East Asia)

c) Eastern Europe and Central Asia

d) High Income Countries: Subgroup 1: North America (Canada, USA)

e) High Income Countries: Subgroup 2: East Asia/Oceania (Australia, Japan, Korea, New Zealand, Singapore, Taiwan)

f) Latin America

g) Mediterranean Partner Countries

It is expected that each targeted area will be covered by at least one project, and that duplication of effort in an area is avoided. The Funding scheme/expected budget is Coordination and Support Action (CSA) (SA) with €8 million (maximum EU grant of EUR 800 K per proposal). The date of publication of Call 10 is 10/07/2012, call deadline: 15/01/2013.

A brief overview of international cooperation in Horizon 2020 (H2020) was given:

- International cooperation will be a cross-cutting issue in H2020;
- The approach will be similar to the current practice and may include a general opening of the programme, targeted openings, horizontal actions on international cooperation and coordinated calls;
- Collaborative actions with specific third countries or their groups will be implemented on the basis of common interest and mutual benefit;
- Reciprocal access to third country programmes will be encouraged;
- Changes will be made to the ICPC list, or its concept as such potentially excluding certain middle-income countries (e.g. BRICs) from that list. This will be specified at the WP level;
- A Commission Communication is scheduled to be adopted in Sept 2012, which will provide further detail on how the principles outlined above will be applied across H2020.

In operational terms, the European Commission's Directorate General (DG) Information Society and Media (DG-INFSO), through its "Trust and Security" unit F5, through which the BIC project is funded, has been entrusted with supporting and coordinating research across

the continent and through international cooperation in the areas of trust and security. As of 1st July 2012, a few days after the BIC workshop, DG-INFSO is becoming DG CONNECT (Communications Networks, Content and Technology) and the impact on the Trust and Security unit was explained to the BIC workshop participants.

The trust and security unit leaves the former INFSO Directorate F "Emerging Technologies and Infrastructures" and becomes a part of CONNECT Directorate H "Sustainable and Secure Society". Directorate's H's main goals are to address selected ICT challenges for a sustainable, healthy and secure society, and to develop a full-cycle roadmap to get the output into the EU economy, through innovation tools such as pilot-lines, pre-commercial procurement, and standards. Directorate H is the leader for Horizon 2020/Societal Challenges.

The Trust & Security (H.4) priorities are the following:

- Elaborate a European strategy on Internet security and remove Cyber security related obstacles to the proper functioning of the Internal Market.
- We will manage implementation of the e-privacy Directive and follow-up of all issues related to the protection of privacy on-line.
- Manage the various financial programmes (FP7, CIP, H2020) supporting the Internet and ICT security.
- Promote a better coordinated and coherent approach on cyber incident management worldwide.

To find out more information about the transition to DG CONNECT, please visit http://ec.europa.eu/dgs/information_society/connect_en.htm

2.4.2 Brazil

The Brazil funding agencies for ICT, including trust and security related research were presented during the workshop. These include:

- CNPq (National Research Council) and FINEP (financiadora de estudos e projetos) have public calls for funding. These are national foundations linked to the Ministry of Science and Technology. More information at http://www.cnpq.br/english/cnpq/index.htm and http://www.finep.gov.br/english/FINEP_folder_ingles.pdf.
- CTIC is the Research and Development Centre for ICT of the Ministry of Science and Technology. They are an alternative to CNPQ but with focus in ICT. Currently they have several funding lines, one in DigitalTV, another in Cloud Computing, another in Smart Cities and another in Network Virtualization. Website can be found at http://www.ctic.rnp.br/.
- FUNTEL, which is a fund for technological development of Telecommunications. FUNTEL is linked to the Ministry of Communications of Brazil. http://www.funtel.com.br
- State Research Foundations - Each State has its own foundation with its own budget and they have freedom to establish their own calls, but it is not only specific to ICT.

As an example of a successful international targeted call involving a security element, the recent Brazil – EU call was highlighted. In September 2010, the CNPq of Brazil and DG INFSO of the European Commission launched a coordinated call for bi-national projects in ICT with the total amount of R$ 11million/ 5 million Euro, with up to R$ 3 million/1.5 million Euro per project. Five areas were included in the call (Edital CNPq No. 066/2010): Future Internet - Experimental Facilities, Future Internet – Security, Networked Systems and Control, e-Infrastructures and Microelectronics/Microsystems. But only one project per area were able to receive the budget.

As a result to this call, a range of research groups in Brazil and EU had the common objective to promote interaction and cooperation, but for many research groups in Brazil it

was the first experience of preparing a project proposal with FP7 requirements and format. Nevertheless, several consortiums were formed, but not so many achieved the coordinated project submission.

Lessons have been learned with the coordinated project submissions, mainly considering that the coordinated call is fundamental to have a formal means to promote cooperation between researchers from European and Brazilian communities. More specific calls to Future Internet and related topics would stimulate more projects, and encourage consortiums to improve the quality and experience of the partners.

As mentioned above, within WP2013, there is another ICT-2013.10.2 EU-Brazil Research and Development Cooperation. The topics for consideration include:

a) Cloud computing for Science

b) Sustainable technologies for a Smarter Society

c) Smart Services and applications for a Smarter Society

d) Hybrid broadcast-broadband TV applications and services.

2.4.3 South Africa

The key funding bodies/programmes in South Africa are the following:

1. Dept of Science and Technology (DST) – http://www.dst.gov.za engages in mostly institutional funding eg to science councils like the Council for Scientific and Industrial Research (CSIR) http://www.csir.co.za/, space agency, and large science initiatives like Square Kilometer Array.
2. DST - EU-South Africa Science and Technology Advancement Programme (ESASTAP) (http://www.esastap.org.za), which provides seed funding for proposals, National Contact Point funding, co-funding of FP7 projects and COST travel funding.)
3. DST - Technology Innovation Agency - http://www.tia.org.za provides funding for development and commercialisation.
4. NRF, National Research Foundation - http://www.nrf.ac.za provides funding for schools, university research, research chairs, furthering education, and international bilateral S&T programmes.
5. NRF - THRIP = Technology and Human Resources for Industry Programme in collaboration with Dept Trade & Industry, http://thrip.nrf.ac.za provides funding for industry based programmes.
6. SPII - support programme for industrial innovation (Dept of Trade & Industry) - www.spii.co.za
7. eSkills Institute as part of the Dept of Communications -http://www.doc.gov.za provides internal funding for eLearning and eSkills programmes.

2.4.4 India

The main funding agency responsible for funding Research and Technological Development (RTD) in India is the Department of Information Technology (DIT), which falls within the Ministry of Communications & Information Technology of the Government of India. The units in DIT dealing with all areas of ICT trust and security are described below.

The Cyber Laws & eSecurity Group, as shown in Figure 3**,** contains a number of different programmes:

- Cyber Security strategy [1] - A cyber security strategy has been outlined by DIT to address the strategic objectives for securing country's cyber space and is being implemented through the following major initiatives: Security Policy, Compliance and Assurance; Security Incident Early Warning & Response; Security training skills/competence development & user end awareness; Security RTD for Securing

the Infrastructure, meeting the domain specific needs and enabling technologies; and Security Promotion & Publicity.

- Cyber Laws strategy [2] - Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes.
- Cyber Security R&D strategy [3] – promotes research & development activities through grant-in-aid support to recognized autonomous R&D organizations and academic institutions proposing to undertake time-bound projects in the thrust areas identified.

The closest to Unit H.4 Trust and Security within DG-CONNECT of the European Commission [17] would be a combination between the Cyber Security strategy and Cyber Security R&D groups, probably more so towards the latter. The DIT mainly funds research and academic institutions. There are other programmes that may also touch upon some of the other topic areas covered in the EU including one dealing with judicial matters in relation to Cyber space, the Cyber Appellate Tribunal (CAT[4]); Indian Computer Emergency Response Team (ICERT[5]), the nation's referral agency of the Indian Community for responding to computer security incidents as and when they occur; and Controller Of Certifying Authorities (CCA[6]), provided for by the Information Technology Act, 2000 [7] as the governing authority which licenses and regulates the workings of Certifying Authorities [8], who issue digital signature certificates for electronic authentication of users.

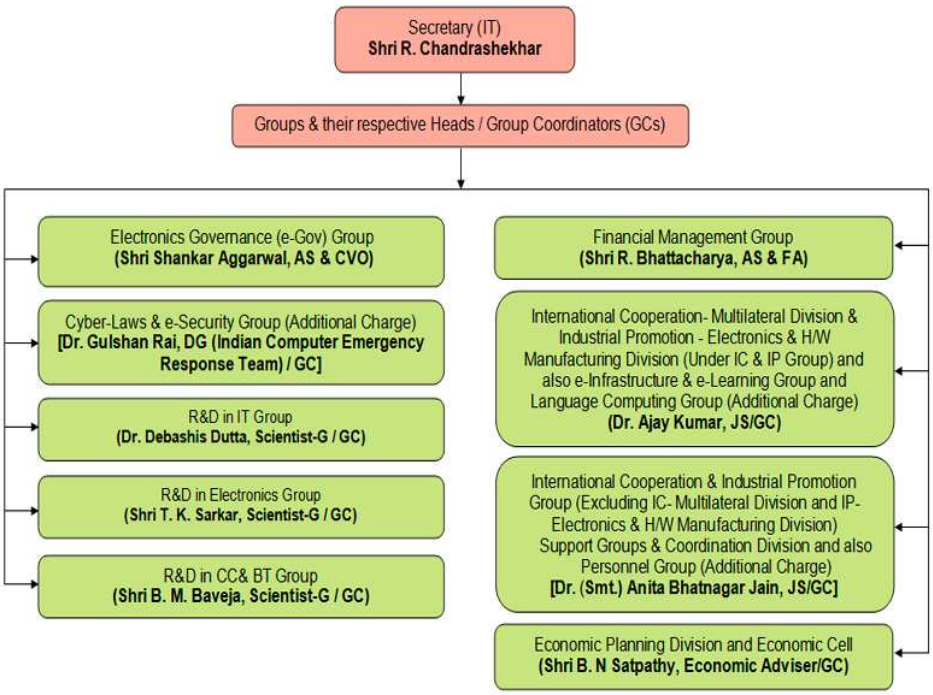


Figure 3. DIT Groups and their respective Heads/Group coordinators [4]

With regards to International cooperation and how it links to Trust and Security, there is an International cooperation Directorate that works very closely with the Directorate under which the Cyber Security and eSecurity group belong. There are a number of departments related to international cooperation and the most appropriate one for Trust and security research would be the Department of International Cooperation & Industrial Promotion, Bilateral Trade Division [9]. There are already a number of FP7 projects engaged in EU – India cooperation (e.g. ERNET India connectivity with European Research Network – GEANT) and these are detailed at [9].

How funding or R&D projects in Cyber Security Works

Department of Information Technology (DIT) invites R&D project proposals in Cyber Security area. Cyber Security R&D initiative of DIT in an open call fashion that is aimed at promotion of basic research, technology demonstration, proof-of-concept along with indigenous development of technology in the area of Cyber Security [10].

The Cyber Security Programme also includes establishment of test bed projects for enhancing indigenous skills and capabilities.

As detailed above, the thrust areas of research and development identified include (a) Cryptography and cryptanalysis, (b) Network and systems security, (c) Security architectures, (d) Vulnerability and assurance and (e) Monitoring, surveillance and forensics.

R&D proposals are invited from autonomous academic and R&D organizations in the following specific areas: (i) Mobile Security, (ii) Malware detection and analysis, (iii) Network and system security assurance, (iv) Cryptography and cryptanalysis, (v) Monitoring tools for network and system security, (vi) Enterprise forensics and (vii) Mobile forensics.

The proposals may be single or multi-institutional, with clearly defined milestones/timelines and role of individual institution. Project proposals duly endorsed by the institution (in 25 copies in prescribed format enclosed) may be sent to Member Secretary, Working Group, E-Security Division, Department of Information Technology, Electronics Niketan, 6 CGO Complex, Lodi Road, New Delhi -110003.

2.5 Success metrics / Impact evaluation

There were very interesting discussions on the identification of “success metrics” for international cooperation and collaboration and an agreed approach to come up with measures for success for this. Some noteworthy comments made during the presentations regarding success metrics were the following:

- It is difficult to predict the future; research on several topics is just a way to be prepared for the unknown future;
- ‘Things happen’ as a result of our activities but it isn’t always clearly identified as a direct result;
- Measures for success should include rationale – motives and goals – for active engagement in international cooperation;
- Although difficult, as a working group already engaged in these activities, we could try to draw up some success criteria regard to results and monitoring;
- It would be useful for us as a community to agree on ways to carry out analysis and assessment of INCO impact.

During the discussions, a number of points were discussed and agreed by the participants:

- Setting up multi-lateral international cooperation is not an easy endeavour as the countries all have different ways and mechanisms for carrying out Research and Technological Development (RTD) management, funding, plans and implementations, which are inherently difficult to set up (vision, interests, meetings, agendas). Furthermore, it takes a considerable amount of time, effort and patience to set up fruitful examples of INCO on a bi-lateral basis and even more complications on a multi-lateral basis. Therefore, the establishment of success metrics and measures will subsequently be as difficult with all of the factors involved. A clear example of this could be success could be garnered in one country but would then be classified as a failure if another country couldn’t stand up to their side of the agreement due to some unforeseen reason.

- There were a number of ways to cooperate on an international basis. There could be a focus on Research / Dissemination & Exploitation activities (Academic interest/ industry). This is made complicated because some countries only focus on academic and research institutes whereas others have a stronger focus on industry funding; local/regional topics vs global cooperation topics in which there are calls open for specific topics, sometimes cooperation is needed for other topics not in open EU calls, which makes it very frustrating for the research communities. There is a need for more cooperation at the government and policy levels and not only at the research levels.
- How to measure the impact of INCO? The success metrics should be broken down at the various levels, e.g.
    - Market: business done, what has been exploited/how, number of companies created, new research plans, etc.
    - Knowledge gained: specifications, new standards, new technologies;
    - Regulation, Policy: exp. new directives for Europe
- When thinking about metrics, would INCO for Security, Trust & Privacy RTD have special or different properties or considerations that make INCO
  (a) more important?
  (b) more difficult?
- We must think at a global level as there are key questions and there are notions related to security, trust and privacy have different meanings in the EU (South/North) as well as in third countries e.g. India/ Japan / China (with regard to cultural aspects). Scalability is also very important (e.g. China, India: >1 billion people for ID card) and cultural aspects e.g. the take up of biometrics where photography is involved.
- For topics like identity management, the research communities need to be talking at an international level: necessary to understand what identity means in Japan, China, India, etc… A similar argument has to be made for dealing with cyber attacks / hackers have different behaviours depending upon geography, legislation and culture. It must be taken account that some security topics cannot be shared easily e.g. geostrategic, exchange of data, and ways of incentivising this must be discussed.
- We need to determine how success can be measured in terms of contributions to multi-disciplinary research and technological development. What are the specific S&T issues and RTD challenges that must be addressed in a global context. A measure of success depends on a number of influential factors, including where the starting point is (whether a new collaboration or a more mature collaboration of long standing and the audience, whether they be the European Commission, the research communities, industry members, or other parties willing to engage in international cooperation.
- There is a tendency for people to only pay attention to the entities e.g. projects, initiatives, platforms, … that bring in the ‘big bucks’. However, there could be some unsung heroes involved in these awards who don’t get the recognition. Therefore, there is a need to have qualitative as well as quantitative evidence included in our measures of success.
- What should projects like ours measure? If you want to measure your results, outputs, deliverables, contacts made, … on a range from 1 to 10 grid, then you want to know about each of these items for the kinds of collaborations and influencing factors as mentioned above (maturity level and audience). How to characterise the things to measure is not altogether clear. It was suggested that a questionnaire could be sent to all the projects to try to identify the measurement items with weighting for each. It is difficult to measure the kinds of things being asked for as it is difficult to predict the future and ‘things happen’ as a result of our activities but it isn’t always clearly identified as a direct result. A number of cases were discussed during the

workshop where project participants learned of new projects spawned as a result of their projects many years afterwards.

- How do we measure non-scientific aspects (the ability to effectively network and eventually collaborate) along with more scientific aspects e.g. forming successful research proposals that pass the ever lowering barrier of success rates.
- How / when do you find the actual number of proposals / projects that were put together based on your earlier work. It is quite difficult to get all of the information on submitted proposals and even if you get these, how do you know they originated from your earlier work?
- We should clarify the purpose of these measurements, whether it be to develop the strategy for increased international cooperation or to justify the need for international cooperation projects (we believe it is the former mainly and that should be our focus).
- Is there a way to measure the change in number of non EU partners over time (numerator)?
- Measures of success should incorporate the rationale – motives and goals – for engagement in international cooperation, success criteria with regard to results and monitoring; and, finally, analysis and assessment of INCO impact.
- Would there be a way to calculate the amount of money that could be saved by engaging in international cooperation. For each topic area, are there any measures that could be realised e.g. it was suggested a good example could be international cyber security research, which could save the countries xyz euros if done together? Is it possible to put a number on how much is saved by involvement of international partners?
- Is there a way of distinguishing what makes sense of doing it alone in the EU and what makes sense carrying out on an international scale? Can we find out definitively which makes more sense? It depends on the research topic is and what resources are required for the research. Although we all believe it is important, due to many of the points raised above, it is difficult to quantify the benefit of international cooperation. We should work on this together to at least try and find this out in the future.
- Do we start by measuring the past? Or just start in the future? Do we start measuring new international cooperation beneficiaries. Also, should we measure the number of beneficiaries with whom you consult but then don't achieve success due to other factors outside your control? E.g. no interest in collaboration or funding isn't an issue in their own countries.
- Is it possible for us to measure Return on Investment (ROI)? In order to do this, we would need to measure utilization with some degree of precision. Although it is important to monitor where the money is being spent, you really want to measure increased productivity and effectiveness, but let's set that as an aspirational goal. During the workshop, we tried to capture a number of stories anecdotally about how consortia where formed (examples in EU-Africa, EU-India, EU-Australia, EU-United States).
- How would we go about calculating ROI from international community involvement (e.g., in FP7 and H2020)? Can we each contribute to how we could agree to quantify the benefit of international community involvement. A suggestion was made to create a success metrics survey to ask some of these questions.
- Perhaps measure the amount of collaboration with academic and industry in a region and try to quantify the role this has in sparking innovation and as serving as a catalyst within private industry, including the potential for a number of start-ups.

- We spoke about extended working groups and outreach to other interested parties. Is there a way to measure the success of these undertakings (no. of meetings held, topics/themes generated, visitations made, awareness, training and teaching courses held, consortia being formed, …?). However, we should not be placed in a position to measure items that will deliberately make our cooperation(s) look bad. In other words, it's a useful measure if you're trying to improve the community building mechanisms and not to destroy them.
- Is there a way to measure retention rate–how many of the community remain over a particular period as opposed to transient members who get involved once or twice. However, we must be careful that we don't categorise transient participants who use the resources for a short time in a way to count them as failures. There could be mitigating circumstances where their research was carried out successfully and there was no further need to collaborate. This should, therefore, be classed as a success.
- Is there a way to measure excellence in an impartial way? In other words, how can actions that are supposed to be impartial separate excellence from mediocrity if encountered in the process?
- A participant (from India) suggested a tool could be customised for indicating metrics for success of international cooperation. This would be taken up following the workshop as the first step would be to get the participants to highlight the measures for success and give them appropriate weights. The tool could then be designed according to these.
- We should examine why some countries seem to have more of a success rate e.g. Australia and New Zealand. Could it be true that it was because they did/didn't need the resources.
- Reference to the ongoing tools, based on technology platforms should be included, as they are mechanisms to foster the networking and cooperation between high level researchers and international partners are invited to join. The success case of the technology platforms as built for some Latin American countries represent a valid reference for other actions with other regions.

2.6 The Way Forward

A significant amount of work and research studies in the areas of ICT "Trust & Security" are already going on across different parts of the world. Many individuals and organizations – research institutes and industry – within projects are busy doing work independently. Unfortunately, most of the work is happening in isolation, in a disjointed manner with no systematic coordination and cooperation amongst each other. They are only accessing each other through open access methods of published papers, journals etc. Therefore, there is strong need to create a platform and associated mechanisms such as that offered by BIC, which can bring all such work together in such a fashion that there is systematic and regular information exchange and mutual support. This cooperation platform would facilitates the work to become better-coordinated and consolidated such that combined and consolidated work is very comprehensive and becomes a formidable defence against the regular emerging threats to our digital lives across the globe and also ensures that duplication of work is minimized.

Structured Multi-Lateral Approach

At present, the International Advisory Group (IAG) formed under BIC, is there to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC WG Terms of Reference [11], have been formed comprising specialists from different countries and different specializations. Indeed, these WGs form the backbone of the Project; however, they alone

would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and Sub-Groups in a structured manner, at the management and functional level with defined focus area, roles and responsibilities.

Since the nature of the project requires interactions amongst all participant countries to share the information, resources etc, the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. EU-India, EU- Brazil, EU- SA, … to multi-lateral approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course, the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

A possible multi-lateral structure is outlined below, with an extended proposed structure in Annex 2.

a. Core Working Group (CWG); based on the current BIC IAG and supporting WGs as shown in Figure 4.
b. Extended Working Groups (EWGs) – specific for each participating country as shown in Figure 5.
c. Special Function Groups – operating under EWGs as specialists at functional level.

Note: This is only an initial proposed structure and will be discussed in more details as part of the Working Group 3 and the International Advisory Group.

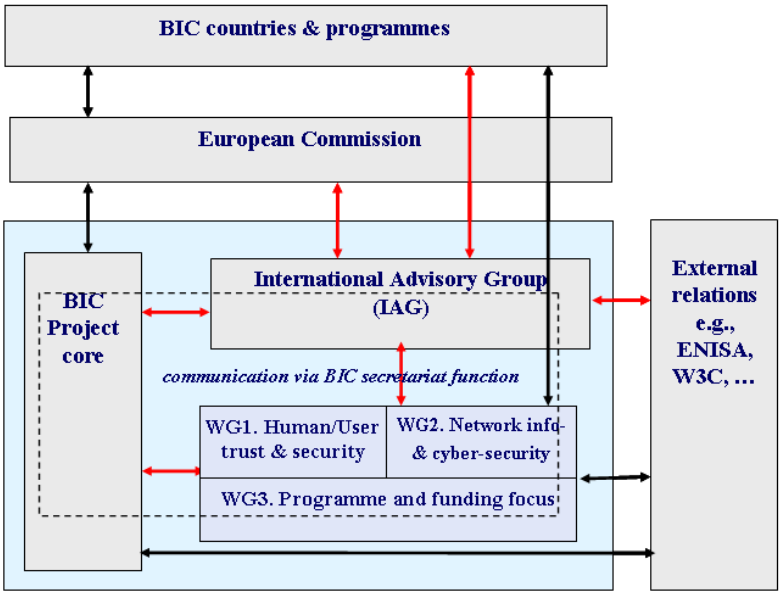


Figure 4. Overall structure of BIC project and external bodies

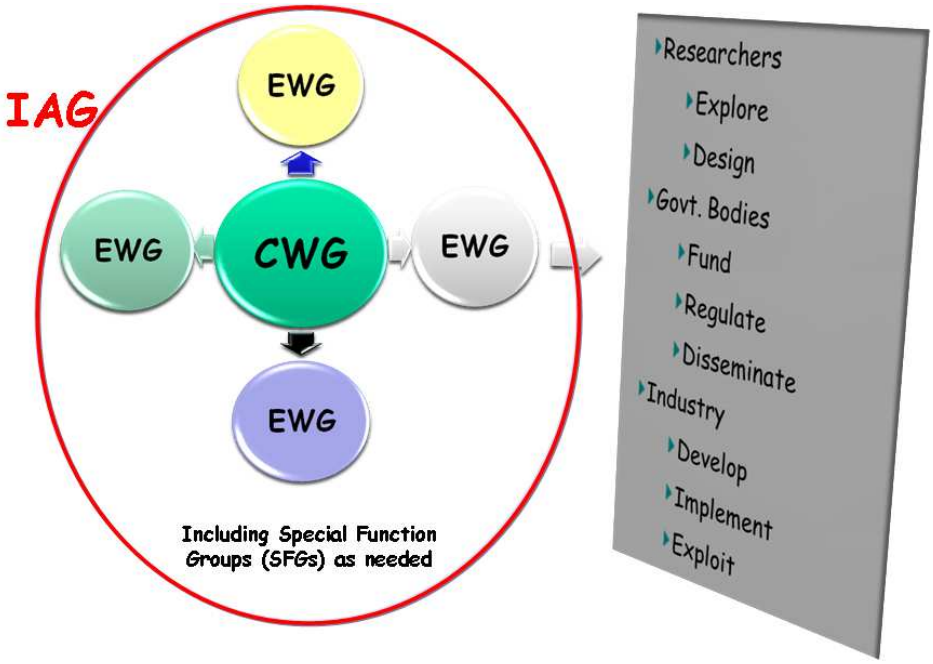


Figure 5. Basic structure of IAG including Core Working Groups and External Working Groups and SFGs

3. Break out session Work Group reports

3.1 WG1. Human oriented/citizen approaches for trust, privacy and security

3.1.1 Chair/Rapporteur Introduction

Authors: Fernando Kraus Sanchez, Henning Arendt, Mounib Mekhilef and contributions from animators.

After welcoming all participants, a brief introduction highlighting the multiple dimensions of trust, privacy and security and the difficulties to grasp all their implications far beyond from pure technological standpoint, opened straight into the presentations, which are summarised below.

3.1.2 User centricity

Animator(s): Karima Boudaoud, I3S Laboratory - University of Nice Sophia Antipolis/CNRS, France and Mounib Mekhilef, Ability Europe Ltd., France

User centricity for trust, privacy and security (TPS) means designing security solutions that are oriented towards the users. Nowadays, we cannot ignore the fact that in order to improve the use of security and strengthen it, we need to involve the point of view of the end-users to take into account the real needs of the citizens and stop designing security solutions from the point of view of security experts only. Consequently, designing user centric TPS solutions implies considering the: different kinds of users, different generations of users, different cultures and different societal values. Taking into account the Human aspect is not enough we need also to design TPS solutions that are compliant with the law of the country where the TPS solutions will be deployed (for example in Europe, solutions will have to be compliant with the EU Data protection regulation).

To move towards a user-centric approach, we need:

- Strong collaboration between different actors and experts from different disciplines (psychologists, sociologists, economists, legal, government, education, ICT and

security) to take into account the cultural heritage/history, societal & individual values, psychological characteristics, technology, laws and regulations, etc.

- Creation of Living labs for trust, privacy and security to drive the design and development of security solutions.
- Education of the existing users and preparation of the next generation of users to raise awareness regarding trust, privacy and security. Education of users requires an education program strategy based on shared values: building roadmaps for stakeholders in education and curriculum for primary and high schools.

From an international point of view, different actions are required:

- Collaboration with:
  - International security experts having a user-centric approach regarding trust, privacy and security (Brazil, India, South Africa, Canada, USA, France, etc.)
  - International experts from different disciplines to take into account the differences in terms of culture, laws, etc.
- Collaboration with international standardization organisations such as W3C, ETSI, IETF, etc.

These collaborations can start through:

- Creation of multidisciplinary working groups in each targeted country (right experts from each discipline).
- Organization of international multidisciplinary workshops in targeted countries (involving wider public).

In conclusion, the Human-oriented/citizen approaches for trust, privacy and security WG must allow actions to finally start changing the way in designing security solutions in order to move towards a more effective user centric approach for Trust, Privacy and Security.

3.1.3 Privacy and Data protection

Animator(s): Alan Hartman, IBM, Israel and Claudia Diaz, COSIC, KU Leuven

The notion of privacy is changing, and there are active campaigns to promote the thesis that “Privacy is dead – get used to it” as stated by several leading American academics and business people. The rise of social networking online means that people no longer have an expectation of privacy, according to Facebook founder Mark Zuckerberg. (guardian.co.uk)

An experiment conducted by Steve Rambam reveals the extent of data available on the internet concerning most US citizens. The situation in Europe is relatively better, since privacy laws are stricter and more strictly enforced. The „Privacy is dead“ thesis is actively being promoted by the marketing industry and social networking sites, since the sale of data, which in Europe is private, is an increasingly profitable industry (see the recent New York Times article on the Acxiom corporation).

The questions that need to be discussed in order to stop the erosion of privacy are:

- Who is responsible for the preservation of an individual’s privacy? Is it the government? The corporations? Or the responsibility of the individual?
- How can we as a research community empower the individual to take control of his or her own private data?
- What new powers are needed by the governments to restrain the „privacy violation industries“?
- How can corporations be convinced of the added value provided by privacy preserving services (see the ENISA report on the Monetization of Privacy)?

International cooperation projects are necessary to tackle these questions for several reasons. The foremost of these challenges to address being the trans-national nature of most information available on the internet, the different legal frameworks in a variety of countries, and the social variability between individuals in different regions of the world. (See the BIC presentation by Marijke Coetzee of University of Johannesburg on the different social norms in emerging markets – section 3.1.7).

The types of international based socio-technical projects necessary are the following:

- For the individual: A comprehensive, easy to use, privacy enhancing technology, that takes into account the "do not track", "do not link", and "minimize data exposure" principles. Some of these technologies already exist, but none are widely available in a single package, that can be tuned to individual preferences, and used unobtrusively whenever the individual engages in online activity.
- For corporations: A set of tools and an extensible framework for the conduct of privacy audits. Currently privacy audits are conducted manually using highly skilled personnel – and are prohibitively expensive for small enterprises. It should be possible to create tools to analyze web-sites, data-stores, and other corporate activities using a framework with plugins for the different legal frameworks under which the audit is being conducted.
- For governments: A privacy policing toolbox for the detection of privacy law breaches, and the gathering of evidence for privacy violation prosecution. This could also be a by-product of the previous bullet.

In conclusion, further international projects in the area of privacy education should also be promoted, including instruction on the use of privacy enhancing technologies, and on the protection of children and other vulnerable groups.

Important note: The Annual Privacy Forum 2012 (APF'2012) is being held on the 10th and 11th of October 2012 in Cyprus. The forum is being organised by ENISA in collaboration with DG CONNECT, University of Cyprus and Cyprus Presidency of the Council of the EU. The provisional programme is available on the website http://privacyforum.eu/programme and registration is available at http://privacyforum.eu/programme/registration. Registration is required by the end of September 2012. Additional details can be found in section 5.3.

3.1.4 Trust management in secure software

Animator(s): Fabio Martinelli, National Research Council of Italy, Italy

The scale of the emerging global infrastructure, combined with the need for fully autonomous operation, surpass the usefulness of existing security infrastructures such as authorization services, certificate issuance and validation services. Having a certified identity (maybe granted using sloppy/undocumented procedures) in a dynamic and open environment does not a priori guarantee an acceptable behaviour and performance of software and services.

In particular, it is not enough for informed decisions on access restrictions and control, the selection among potential candidates for interaction. Entities need to be distinguished not only based on their static (certified) identities but also based on their (un)expected, dynamically varying qualities that are relevant to the specific interaction context. Decisions are often based on directly verifiable evidence, but in a highly open system could be also based on indirect evidence reported by other entities. In these cases, the notion of trust becomes central.

Indeed, trust is a very general concept, with different meanings in different communities. Usually, trust is declined in several dimensions: We can trust a system for correctly functioning (system trust), we can trust a persona to act in our behalf (delegation trust), etc. In general, we trust something/someone for a purpose in a given context, and such interpretation is often used in computer science where several trust management models

have been developed (initially for modeling access control issues, and more recently to model relationships in social computing). Indeed, in modern pervasive ICT systems, trust is a first-class object that need to be evaluated, analyzed, used, negotiated.

As mentioned, trust may be based on several features:

- verifiable evidence: E.g. proof methods, rigorous design & analysis techniques, …
- direct experience: E.g., previous interaction history (monitoring the target entity behaviour is a main tool …)
- indirect experience: E.g. third party recommendation (then you need to trust someone to recommend others and so on …)

These must be represented, combined, monitored and negotiated in several ways. Some computational models of trusts based have been proposed on social networks, probability theory, formal semantics and logic, game theory, etc.

Trust is also used when we certify software. Basically, we trust a third party to assess properties of software installations produced by another party. In addition, trust management aspects are necessary in usual Service Level Agreements (SLA) in service oriented architectures/infrastructures and in particular for secure service composition. Indeed, several stakeholders with different trust levels are involved in a typical service composition and a variety of potentially harmful content/service sources. This is attractive in terms of degrees of freedom in the creation of service offerings and businesses. Yet this also creates more vulnerabilities and risks as the number of trust domains in an application gets multiplied, the size of attack surfaces grows and so does the number of threats. Furthermore, the Future Internet will be an intrinsically dynamic and evolving paradigm where, for instance, end users are more and more empowered and therefore decide (often on the spot) on how content and services are shared and composed. This adds an extra level of complexity, as both risks and assumptions are hard to anticipate.

There are several technical areas that need further development in the trustworthy ICT research community (in no specific order):

- Models for trust formation, evolution, delegation, dissolution
- Social models of trust
- Trust models for secure software/service composition
- Certification models for software (producers, vendors, testers, etc.)
- Integrated assurance/trust techniques
- Security level prediction of software based on recommendations
- Trust models for application market
- Usability of trust and security information/metrics
- Empirical studies relating trust perception and trustworthiness
- User perception of software trustworthiness
- Role of trusted computing for secure software
- Btw, trusted by whom?

From an international cooperation perspective, we can highlight:

- Commonly agreed trust models for service interaction;
- The standardization of the software and service certification process, including the necessary interoperability and automation information;
- The standardization of Service Level Agreeement (SLA) among services;

- From a policy based perspective, there is clearly the need to define certification standards to whom high level assurance services need to adhere in several scenarios.

3.1.5 Accountability in Cloud computing

Animator(s): Nick Papanikolaou – HP Labs Europe, with contributions from Siani Pearson and Nick Wainwright of HP Labs Europe

Introduction

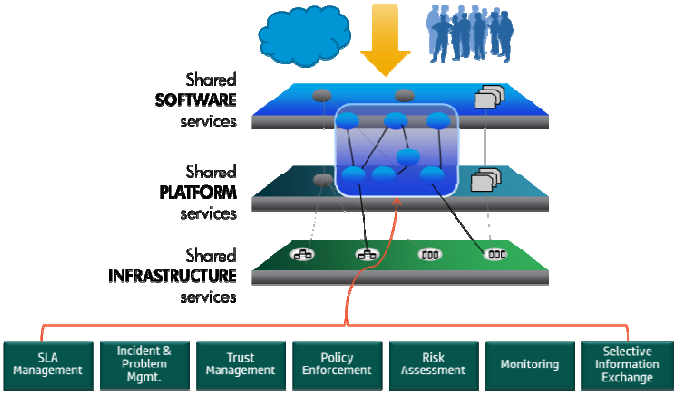
Cloud computing, which has been enthusiastically received in many of the areas where Information Technology (IT) is a dominant factor in day to day life, is the most recent manifestation of a long term shift towards the provision of information technologies by specialist IT service providers. Whereas previously consumers bought Personal Computers (PCs), and businesses had IT departments which owned servers and ran business software, future IT needs will be met by infrastructure, platforms and software provided as services from the cloud. The cloud, a complex and globally distributed ecosystem of networked online services, runs on huge data centres, which store and process vast quantities of data gathered from many sources including from the people and business they serve, the transactions they process, the environment and many other sources.

As more aspects of business and personal lives shift into this cyber world of online services, concerns have arisen over how we can have confidence that they will protect it and handle it responsibly. Data protection regulation aims to address consumer trust and the imbalance of power between the individual consumers and these new IT services. Businesses using cloud services engage in service level agreements (SLAs) with providers which aim to cover (amongst other things) how business data should be handled and what it may be used for; however, there are difficulties in ensuring that these address the complexities of operating in the complex ecosystem of cloud services. For the cloud service provider (CSP), the complexities of compliance with data protection and business regulations is a barrier to offering cloud services, and the risks and consequence of non-compliance are a serious concern.

Accountability can help us tackle these challenges in trust and complexity. It is especially helpful for protecting sensitive or confidential information, enhancing consumer trust, clarifying the legal situation in cloud computing, and facilitating cross-border data transfers. Accountability provides a way forward in dealing with data-protection issues arising from handling personal data in the cloud but these issues transcend personal data handling and generalize to other types of data, beyond privacy concerns.

Accountability is enshrined in regulatory frameworks for data protection across the globe, notably the Organization for Economic Cooperation and Development (OECD) privacy guidelines (1980), Canada’s Personal Information Protection and Electronic Documents Act (2000) and Asia Pacific Economic Cooperation (APEC)’s Privacy Framework (2005). Accountability is used here in the sense that the data controller should be accountable for complying with that particular data protection legislation. Similarly, EU Directive 95/46/EC (1995) contains rudimentary accountability provisions, such as pre-processing regulatory notification, information provision requirements and data subject access, but these are ad-hoc mechanisms, not part of an overarching accountability regime. The resulting 'accountability gap' is one of the causes of what is conceived as regulatory failure: lack of faith in the regulatory framework amongst the general public; the low priority data protection compliance receives amongst data controllers including innovation of higher levels of privacy protection in new ICTs; and lack of attention for data privacy breaches.

While all of these regulatory frameworks provide a foundation for data protection, none is specifically designed with the cloud computing in mind. What makes data processing in the cloud challenging is the scale and complexity of networked cloud services, the pervasive role they will play in the future business and personal life, and the ability of advanced data



mining techniques to draw inferences about data subjects from the large data sets under their control. The "data-centric" nature of cloud computing creates a tension between service suppliers who perceive that the business data they hold could be a strategic business resource and their customers who are increasingly aware of risks posed by the lack of control over data in the cloud.

Providing Accountability in the Cloud: Approaches and Solutions

Accountable organisations ensure that obligations to protect data are observed by all who store and process the data, irrespective of where that processing occurs. To achieve this for the cloud a "chain of accountability" needs to be established that mirrors service user-provider relationships. Furthermore, it encompasses the complete ecosystem of individual and business users, the whole service provider value chain and all aspects of the regulatory process, including business governance and audit.

The individual service user should be able to hold the organisation that is providing them with a service accountable for how data is used and handled; this is their primary service provider (PSP). The PSP must be able to hold the CSPs that it uses accountable for their handling of data as it moves through the supply chain, establishing a chain of accountability throughout the supply network. Regulators and the business governance functions of organisations using the cloud service must be able to monitor and verify that all parties in the supply chain or supply network are operating as accountable organisations. Where data includes personal information, the PSP will be the data controller for the purposes of data protection and will be accountable to data protection regulators.

Trusted third parties (TTPs) supported by trusted tools and services can provide stakeholders with appropriate views of data and how it is used and protected.

Through contractual agreements, all organizations involved in the cloud provision would be accountable. While the PSP, as the first corporate entity in the cloud provision, would be held legally accountable, it would then hold the initial service provider accountable through contractual agreements, requiring in turn that that SP hold its SPs accountable contractually as well.

To increase trust we must address the needs of all stakeholders – users, providers and regulators. Users need a way to understand and make choices about how data may be used in the cloud and the consequences and risks associated with those choices. They also need to be confident that service providers are treating data appropriately and that they can retain control over how it is used, as well as that the legal frameworks are effective and that they have ways to hold providers accountable for what happens to that data. Service providers need a way to meet customer expectations for greater transparency and control, and therefore accountability, over what they do with data – this means technical

and legal mechanisms that work together. Further, they need to have confidence that providers further down that chain will meet their obligations and responsibilities. Finally regulators need to be able to monitor and check compliance and to attribute responsibility for any failure.

Our solution is to address these objectives through an orchestrated set of mechanisms: preventive (mitigating risk), detective (monitoring and identifying policy violation) and corrective (managing incidents and providing redress), using interdisciplinary co-design to ensure that legal and business processes and technical mechanisms work in support of each other. The grid in the figure above is populated with examples of such mechanisms (although it does not show a complete set). For example, decision support tools may be used to assess risk and privacy harms based on context before transferring personal information in the cloud, to advise on obligations to be passed to a CSP (within the contract, and associated with data) or to assess the suitability of a CSP before using it.

In conclusion, the basic accountability framework was presented with a number of mechanisms across legal, regulatory and technological areas required. Some technological pieces are quite mature and others are less so. Further work is necessary on various fronts including provision of integrable techniques for attribution and redress.

3.1.6 Data Provenance

Animator: Priscila Solis Barreto, University of Brasilia, Brazil

Introduction

When we see data on the Web, currently, we do not know where it came from and how it got there. This information and its source (provenance) is typically lost in the process of copying/ transcribing/transforming databases. Provenance is essential to data integrity, currency and reliability.

Research in data provenance

For provenance and its applications, we can focus on different motivating domains:

1. Scientific Domains: - Scientists deal with greater heterogeneity in data and metadata- Trust, quality, and copyright of data are significant when using third-party data- E-Science - Business Domains
2. Virtual organizations: workflows, warehouse environments, where lineage information is used to trace the data in the warehouse view back to the source from which it was generated.
3. Governamental Domains: In Brazil, within the social inclusion policies this is a very important issue. Ex Voting system, taxing system
4. Data Quality: use of lineage to estimate data quality and data reliability based on the source data and transformations
5. Audit Trail: trace the audit trail of data, determine resource usage and errors in data generation. - Replication Recipes: allow repetition of data derivation, help maintain its currency and re-do replication
6. Attribution: the pedigree can establish the copyright and ownership of data, help to determine liability in case of erroneous data.
7. Informational: use of lineage to query metadata for data discovery.

Some examples of the applications in the different domains are such as collecting and modelling provenance from heterogeneous applications and data sources, integrating distributed and incomplete provenance information to compose complete provenance models and the effective management and querying of distributed, semantic provenance repositories for different applications.

There are a number of recommended actions within the scope of research cooperation projects are standardization of provenance models, services, and representations, provenance management architectures and techniques, analytic provenance and the relationship between provenance and visualization, provenance and the semantic web, human interpretation of provenance security and privacy implications of provenance, provenance and social media and provenance implications for trust.

Within the BIC workshop, there was a suggestion is to foster concrete cooperation around a specific application domain such as Scientific, Business, Government and multidisciplinary approaches to include the concept of trust, privacy and security in future coordinated calls.

3.1.7 Social computing in emerging countries

Animator: Marijke Coetzee, University of Johannesburg, South Africa

Introduction

Social Computing enables user-centric, collaborative knowledge sharing to build communities of people using the Internet. When Social Computing emerged around 2003, it was not thought that a few years later millions of users across the world would be using Social Computing applications such as online social networks, blogs, collaborative filtering of content, and many more. Social computing supports social behavior with computational systems by recreating social conventions and contexts using technology. At a more technical level, Social Computing is supported by technologies such as collaborative filtering, online auctions, and reputation systems and social network analysis. There is great value in Social Computing systems as they are empowering users and driving the creation of new digital divides. Social Computing is a driver for growth and employment, is disrupting many industries and has the potential to reshape work, health and learning.

Social Computing in emerging countries

In Africa, Internet access is not affordable. In addition, low availability of international bandwidth, poorly structured markets, lack of existing infrastructure and low population densities all ensure that mobile is a strong entry point for networks in Africa. In many developing nations, the majority of mobile web users are mobile-only. For example, Egypt has 70% percent, India has 59 % and South Africa has 57% mobile-only users who tend to be under 25.

Given the popularity of mobile-only Internet usage, it come as no surprise that the largest social network in Africa is Mxit (www.Mxit.com), a mobile social network. Mxit is a Java mobile application that connects users with a mobile phone to the Internet. It is estimated that Mxit has around 50-million users in 120 countries, supporting the sending of 23-billion very low-cost messages a month. The key to Mxit's success lies in its simplicity. As the interface is not graphical and games are text-based, it works on nearly any mobile phone. This makes it ideal for emerging markets where smart phones are still out of reach for most people. This African success story indicates that there is real potential in this market.

In developing countries such as those found in Africa, mobile phones can be used as a tool to intervene and act as a competitive force in the social, economical and political development. For example, Egyptians changed history when they used social networks to bring down their president. There is an opportunity to develop mobile social networking as a business in Africa, to growth the very small enterprises in these countries. This can ensure that communities can develop into positive, productive and outstanding environments by combining modern technology with the natural predisposition of people to culturally support each other. This is because African entrepreneurs run profit ecosystems rather than business units. These ecosystems interact with other ecosystems in a culturally involved manner to ensure that the ecosystem will survive in the face of adversity. Social capital and social ties support these ecosystems and communities in large parts of Africa where members of communities pool resources together in an attempt to meet economic and social needs for both individual members and the general community. An identified need is the development of social computing technologies to support the growth and development of these ecosystems and communities to allow them to flourish.

Social Computing challenges to address are Security and Privacy, as Social Computing applications have weak user identification management systems and Trust as it is a main driver for collaboration and innovation.

A research topic identified for international cooperation is the development of trust models, mechanisms and architectures to support Social Computing systems to support business ecosystems in rural Africa. For these systems, it is important that trust management takes into account concepts relevant to the target context. An important identified focus of the research is the study of culture on trust. For Individualistic cultures, for which most trust management systems have been developed, consumer trust is facilitated through trust mechanisms such as institutional guarantees, laws and policies, information security mechanisms, and social controls. In contrast, Collectivist cultures, found in Africa, Asia, India and South America have different needs as they interact in different ways. For example, in collectivist cultures people emphasize interpersonal relationships where loyalty is obtained by protecting the group members for life. Individuals see themselves as subordinate to a social collective such as a state, a nation, a race, or a social class. They prefer group harmony and consensus to individual achievement.

In conclusion, this research topic is thus of interest not only to the African context, but to any environment where different types of cultures exist, and where an understanding of the influence of culture on trust is limited. It is therefore a topic that is ideal for collaboration between parties found in different countries in Europe, Africa, India and Brazil.

3.1.8 Global perspectives of personalized Identity Management Ecosystem (GINI-SA vision)

Animator: Lefteris Leontaridis, NetSmart S.A., Greece

Introduction

GINI-SA is a Support Action for the European Commission, which aims to analyse how a Personalized Identity Management (PIM) ecosystem in which individuals can manage their digital identities and control the exchange of their identity information. Under the GINI vision, individuals would manage their identities by means of an Individual Digital Identity (INDI), a self-generated and self-managed digital identity, which is verifiable against one or more authoritative data sources. Once created, users would have the ability to link their INDI with authoritative identity data maintained by both public- and private-sector entities. This data (or links thereto) could then be presented by the user towards relying parties.

Personalized IDM Ecosystem

GINI foresees that INDI-type online identities will emerge and personalized services based on INDI requirements and features will be available to citizens and consumers in the following years, with a market appearing and maturing between 2015 - 2020. The emergence of such services will be underpinned by business models which drive, and are driven by, the emergence of an ecosystem linking three types of actors: Individual users, Relying Parties and Data ources

The INDI allows individuals to act in various roles, for instance as citizens, employees, or customers. GINI assumes an operator model, i.e. the actor's "User", "Data Source", and "Relying Party" are served by intermediary entities called INDI Operators. It may be possible for different roles to be managed through a single INDI operator, or to utilize multiple ones for different interactions, allowing for disintermediation and enhanced privacy. The user chooses which roles to act in and what information to reveal under the different roles. As one, or several, INDI operators may be used for different kinds of context, the user is able to manage a set of partial identities in a manner similar to the physical world, by providing the information that is relevant for each situation, including those cases where anonymity, pseudonymity, and limited attribute provision are desired and acceptable.

As INDI is a new infrastructure, with no INDI market or operators existing as of today, there is a need of determining what prerequisites must be put in place, in order to enable private organizations to assume the tasks of INDI Operators. A variety of business models for INDI

Operators will emerge once the technical aspects of the INDI ecosystem's infrastructure are implementable and a set of governance procedures are in place.

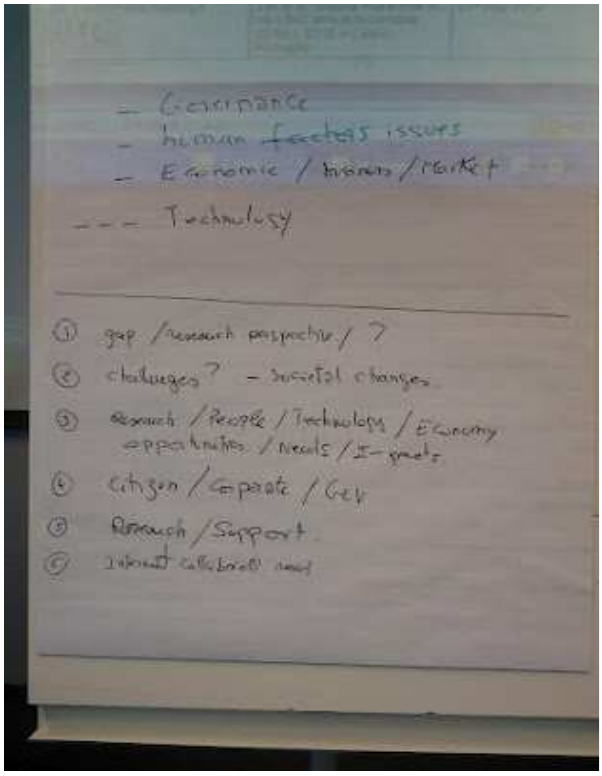
The INDI ecosystem could be built upon a one-sided market, where the service provider and customer interact directly with one another, or a two-sided market, where different business models and pricing schemes are involved in a unified set of business transactions. Creating a two-sided market is much more complex and often transfer fees and other similar pricing models need to be applied.

GINI Recommendations for Government, Industry and Researchers

GINI is putting forward a set of recommendations towards three types of stakeholder: Industry, government and researchers. All these stakeholder communities are global and therefore strong international cooperation is needed to achieve the vision of an INDI-like ecosystem of global dimensions. Therefore, the following recommendations are indeed directed to the global stakeholders:

1. Concerted action and international cooperation between global ICT market actors and particularly service providers such as Cloud operators and various identity intermediates is necessary to build consensus on where common understanding must be the basis for broad industry-wide agreements a issues such as user-centricity requirements and user control to identity and attribute provision, as well as privacy-enhancement principles and rights of individuals including, but not limited to, the requirements of the upcoming privacy-related regulation in the EU.
2. Industry-wide standardization initiatives should be undertaken at a global scale with a strong international cooperation dimension, supported by major technology and service providers, in order to define various dimensions of inter-operator interfaces, concerning interoperability and data handling processes ensuring privacy for users and confidentiality for relying parties, portability specifications aiming for compliance with upcoming EU regulation, protocols, APIs, auditing and security for cross-operator relaying of claims and assertions.
3. Data handling principles and decisions by governments will be pivotal for the emergence of an INDI-like ecosystem. Privacy-respecting legislation should be harmonized globally in order not to create silos and market fragmentation. All world regions and major markets should cooperate towards a shared, commonly accepted governance and regulatory framework.
4. The role of governments should be examined to determine whether (and to what extent) further regulation is needed or whether (and to what extent) industry self-governance would suffice. This needs to happen at a global scale so international cooperation is essential as no single world region can contain identity provision services.
5. Further RTD work is needed on trust meta-models through interdisciplinary research involving more than technology but also social sciences, with a strong dimension for international cooperation. Further RTD work is needed on the process of technology-linked innovation, particularly as driven by behavioral motivation, e.g. by privacy. Strong international cooperation is needed in these research areas to account for cultural differences across world regions.

3.1.9 Photos from the session



WG1 breakout session

3.2 WG2. Network Information Security / cyber security

3.2.1 Chair/Rapporteur Introduction

Authors: Jim Clarke, Waterford Institute of Technology, Ireland; Michel Riguidel, Telecom ParisTech, France, and contributions from the animators.

The research areas related to network and information security / cyber security are now receiving high priority for international collaboration. Some recent examples are highlighted here:

- EU–US INCO-Trust workshop of May 2010 [12],
- Munich Security Conference, 4-6th February, 2011 [13]
- US-UK Cyber Communiqué of 25th May 2011[14],
- Recent accession to the Budapest Convention on Cybercrime [15],
- 28th Annual International Workshop on Global Security on June 16, 2011 [16],
- Vienna Security conference, 1st July 2011 [17],
- London Cybersecurity Conference (1-2nd November 2011) [18], and
- BIC Annual Forum (29th November 2011) [19].

A key message throughout all of these events is the acknowledgement that international cooperation 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 multi-stakeholders engaged in collaboration, including data exchange and sharing (and also knowledge sharing) between countries. This WG will focus on the key elements within these important areas and inter-related technical areas.

As a starting point, it was agreed that WG2 would focus on the following topics:

- International data exchange architecture for cybersecurity;
- policies relating to how the collected cyber-intelligence is to be handled, exchanged, shared and utilised;
- Open source trustworthy host platform for collaborative research and education;
- International cooperation in Cryptology;
- Mobile security of software services;
- The planning and improvement of joint exercises related to cyber security across borders.

While the majority of these were covered during the workshop, we were also delighted to receive additional contributions / position papers / requests for topics from the following research fields for international cooperation during the planning phase of the workshop: Emerging threats and actors, Digital forensics, security and virtualization, international approaches for critical infrastructure protection, and implications arising from identity and privacy related issues on a global scale.

The presentations were of a very high quality and the content and discussions are summarized here.

The key points are:

1. The emergence of new threats and new vulnerabilities with new architectures (e.g. clouds), new usages (e.g. social networks), and massive mobility applications (mobile applications within smartphones) and huge multimedia exchanges (generalisation of music and video flows);
2. The obligation of a n international cooperation to exchange cyber security data and intelligence to fight against borderless attacks;
3. The reinforcement of coordination in cryptography application at the european level to develop robust algorithms for the new usage (enhanced privacy, massive exchange in core networks, mobile e-commerce).;
4. The massive emergence of smarrtphone applications with new vulnerabilities and future attacks;
5. The requirement of a better resilience for critical infrastructures and the enhancement of specification and dissemination for crisis management procedures and tools.
6. The new situation of computer science application in computing, storing and communication with the virtualization phenomenon which erases the notion of space and boundaries, making more difficult indeed impossible the legislation enforcement at the country level;
7. The reinforcement of digital identity at the global scale, requiring more efforts to protect privacy of individuals and enterprises.

3.2.2 Emerging threats and actors

Animator: Sotiris Ioannidis, FORTH, Greece

Introduction

The recent Stuxnet incident has been an eye-opener regarding the possible impact of advanced, targeted attacks that can be performed by sophisticated actors with significant resources at their disposal. The attack clearly showed how our current defence tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific target instead of blindly targeting the entire community.

Malicious hardware can also be used as a very subtle vector to perform extremely hard to detect attacks against critical infrastructures, large corporations, and government organizations. However, targeted attacks do not necessarily need to be extremely sophisticated and, even in their simplest forms, can pose a very serious threat against normal users. Targeted SPAM, for example, is extremely effective in phishing users credentials. We envision ad-hoc banking trojans could be developed in the near future to avoid detection by targeting only a restricted group of individuals.

In addition, we believe there is a serious risk that attackers will soon start developing automated techniques to customize attacks based on private user information and aggregated data collected from multiple online sources.

Security of New and Emerging Technologies:

Analyzing and securing emerging technologies has always been a core objective in the area of system security. Unfortunately, it is often the case that new services and new devices are released before the research community has had a chance of studying their security implications.

In the near future, we can identify four topics, in the area of international cooperation and new and emerging technologies, which need to be studied from a security point of view:

1. Cloud Computing - The Cloud is quickly changing the way companies run their business. Servers can be quickly launched and shut down via application programming interfaces, offering the user a greater flexibility compared to traditional server rooms. From a system security perspective, there are a number of aspects that are specific to cloud computing. For instance, the impact of “insider threats”, the issues related to privacy and “data management”, and the attacks against the “virtualization” infrastructure.
2. Online Social Networks - As these online communities, such as Facebook, MySpace, Orkut, Twitter, LinkedIn, and others, have been adopted by millions of Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc. Monitoring and securing social networks is therefore very important to protect the users from a large spectrum of attacks.
3. Smart Meters - This new class of devices is a clear example of a new technology that has been rapidly deployed without the required security protection mechanisms. Studying and fixing these devices in particular, but also extending previous work done in more general sensor networks should therefore be one of the goals of system security researchers.
4. SCADA Networks - Even though SCADA is not exactly a new technology, these devices were initially designed to be isolated and thus built with certain underlying security assumptions. Since many industrial process control systems became reachable from the outside (even when, as shown by Stuxnet, the attacker has to cross an “airgap”), the security of these networks has become an important priority.

3.2.3 International Data exchange architecture for cooperation on cyber security and intelligence

Animator: John C. Mallery, CSAIL, Massachusetts Institute of Technology. USA

International collaboration and coordination can rapidly reduce defensive gaps across the individual countries and build capacities for crisis response. Without systematic and expeditious international coordination, attackers can replay attacks across different countries. This structural advantage for attackers can only be offset by collective defences incorporating rapid international learning to identify, disrupt and defend against innovative attacks across their lifecycles from reconnaissance and testing to deployment.

Collective cyber defence against threats from cybercriminals, hacktivists, terrorists and nation-states in peace or in war requires an effective architecture for scalable real-time data sharing, collaborative analysis, and rapid threat mitigation. Development of such real-world defensive capabilities poses challenges that can drive both applied and fundamental research.

An international program of research will broaden awareness, understanding and capacity across participating countries, and deepen technical knowledge around data sharing and analysis tasks. The integration of national expertise and experience can facilitate faster learning and transfer new and effective concepts into operational practice to fight crime, close defensive gaps, protect intellectual property and coordinate defences against malicious state actors. Objectives include creation of shared data collection, analysis and protection methodologies. International aggregation of cyber data on crime and law enforcement, black markets, economics, state interactions, long-term cyber-fuelled transformations will enable tracking trends as they emerge and counteracting malicious techniques, tools and procedures before they diffuse widely. These transnational datasets on breaches, attack patterns, best practices, and defensive coordination will enhance common situational awareness and will enable retrodictive metrics of efficacy for countermeasures.

Legal and regulatory barriers to cyber data sharing remain a significant challenge to defensive coordination. Thus, international cooperation can also drive legal harmonization to support shared collection, fusion, analysis, and response capabilities. Legal and policy incentives, in combination with actionable results, will also need to motivate private and public actors to coordinate at the sectoral and national levels.

International dimension and its challenges

The first step in an international initiative is to engineer a cyber data strategy that recommends what to collect in each domain prioritized by its purpose, and how to harmonize processing and analysis. The strategy needs to identify clear procedures for sharing various data according to sensitivity, for sanitization based on concerns about privacy or sources and methods, and for defining exchange formats and delivery times. They should include context, specific sharing purpose, and ultimately lifespan of the sharing. Importantly, the strategy needs to identify synergies arising from integrating data across national boundaries and its impact on the participating countries.

Numerous precedents can inform the strategy across a range of sectors and issue areas. The European Network & Information Security Agency [5] (ENISA) collects, analyzes, disseminates data on InfoSec in a pan European context. DHS Predict [6] (US) has developed a legal framework for sharing cyber data within the United States, which has

5 European Network & Information Security Agency, http://www.enisa.europa.eu/

6 DHS Predict, https://www.predict.org/

been extended to Canada and soon to the European Union. The European Commission funded Wombat Project[7] has fielded collaborative sensors for Internet malware and attack data. The European Public-private Partnership For Resilience[8] has focused on critical information infrastructure protection. The Financial Services Information Sharing and Analysis Center[9] (FS-ISAC) brings together US financial sector entities and aggregates data collected from its members after anonymizing it. The non-profit National Cyber Forensics and Training Alliance[10] (US) integrates information and analysis for the financial services sector across private, public and academic communities. The Confickr Working Group is a well-known example of informal but effective cooperation as are the Anti-Phishing Working Group and Digital Phishnet. Lessons can be drawn from these and other collaborations to architect effective international cyber data collection and analysis.

The critical ingredient for success is incentivizing participation of national governments and private actors by demonstrating the advantages of multinational scale, the synergies of international cooperation and the direct benefits to participants. International scale can help drive increased quality and integrity of data. Guidelines for managing data collection and sharing that respect local law and cultural sensitivities can reduce impediments to participation. Finally, clear identification and mitigation of the risks of sharing can assuage concerns of governments and private actors. Furthermore, security solutions[11] for acquisition, storage, processing and transfer of data can be deployed to reduce risks while enabling benefits.

Some of the research and development areas necessary to support this effort include:

- Architectures for collection, analysis, policy enforcement
- Representation and structure of data
- Policy representation and understanding
- Implementation of data sharing, including data formats, standards, tools, usability
- Security, including secure host with strong isolation, access control management, policy enforcement, data integrity, provenance tracing
- Cryptographic techniques, including data splitting, differential privacy, cypher text arithmetic
- Development of a trustworthy platform for data sharing and analysis
- Creation of a test bed for concept demonstration.

As shown in Figure 6, a strawman architecture was generated and this was described in more detail at the workshop. Due to the duration of the session, it wasn't possible to get

7 European Commission FP7 Wombat Project, http://www.wombat-project.eu/

8 European Public-private Partnership For Resilience,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

9 Financial Services Information Sharing and Analysis Center (FS-ISAC),

http://www.fsisac.com/

10 National Cyber Forensics and Training Alliance, http://www.ncfta.net/

11 Security solutions will include operating system security, cryptographic techniques, harmonized vetting procedures and access control mechanisms, and data protection techniques like slicing, aggregation or incremental revelation.

into very technical discussions but there was instead a focus on advancing this work to the next level and commitment to formulate a strategy for research and development coordination, which will enhance the outcomes through tactical planning, leveraging and combining task-relevant national expertise.

Malicious actors in cyberspace actively exploit the shortcomings in the ability of defenders to coordinate their activities. They can rerun the same attacks against different countries, sectors and organizations so long as cyber data and countermeasures are not being shared effectively.

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.

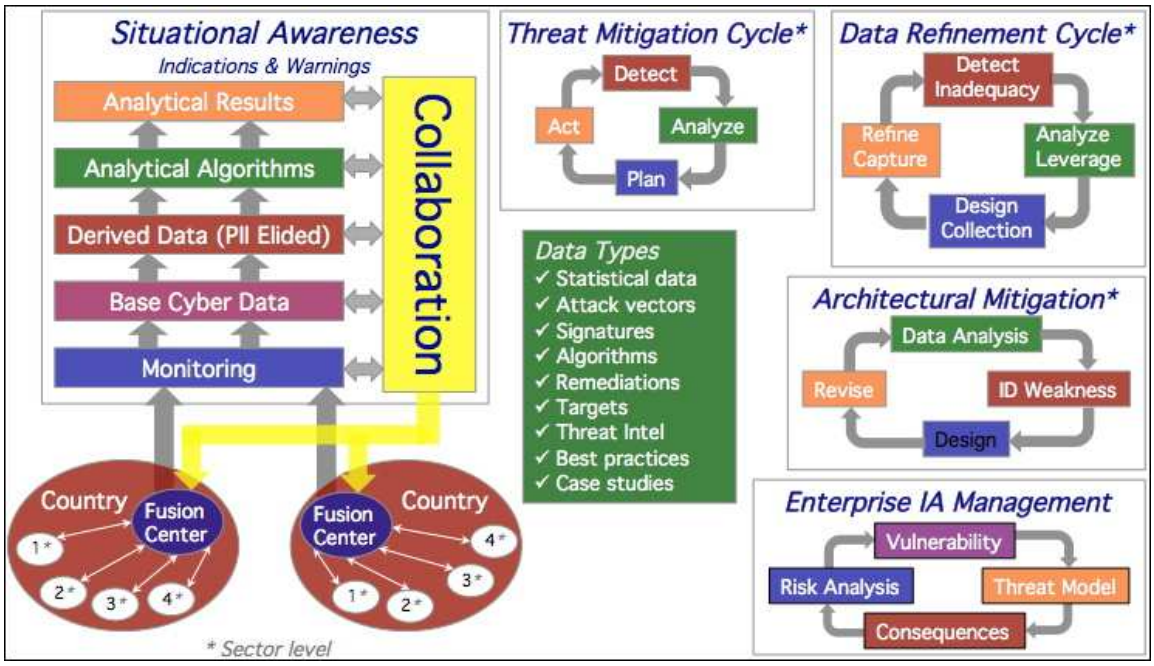


Figure 6. *A Strawman International Cyber Data Sharing Architecture*

Figure 6 illustrates an international cyber data sharing architecture that integrates data from multiple countries and sectors and returns collaboratively produced analyses and threat mitigation techniques. Country fusion centers integrate country information and expertise internationally. Within each country and across its sectors, shared monitoring infrastructures capture base cyber data at sources. This data is processed to remove personally identifiable information (PII) before being analyzed using shared algorithms to produce results fed back into shared situational awareness. The architecture supports sector-based threat mitigation cycles as well as enterprise information assurance management of value at risk. The architecture supports learning modalities like data refinement to improve data capture, analysis and utility in threat mitigation. Based on knowledge gained about vulnerabilities and attacker vectors, the architecture helps drive improvement of enterprise and infrastructure architectures to improve defensibility.

This kind of sharing scenario can drive research along many trajectories. The type of data collected needs to be effective and offer leverage for cyber defense. Large-scale analytics over the data need to reveal important patterns in real time and lead to timely threat mitigation. Given an effective sharing architecture, major malicious actors will endeavor to corrupt the data and subvert its operation, and so resilient and trustworthy engineering will

be needed for all components from sensors to hosts, monitoring, analysis and mitigation actions. At the same time, PII and enterprise information must be protected to respect important societal values and incentivizing sharing. Difficult technical, legal and administrative challenges in international authentication, authorization, encryption and remote policy enforcement must be overcome to reach higher levels of trust and sharing necessary for weaponizable data like critical infrastructure attacks and mitigations.

We need to look at optimising the integration of both technical and economic perspectives to favour defensive interventions that disrupt malicious business models. Figure 7 illustrates the limited scope of conventional technical approaches to cyber defence. By integrating understanding of the attack business model, defenders gain additional opportunities to disrupt the attacker anywhere on his value cycle using passive or active means. Additionally, the resources, capabilities and motivations of the attacker provide constraints on the range of technical defences necessary for effective defence.

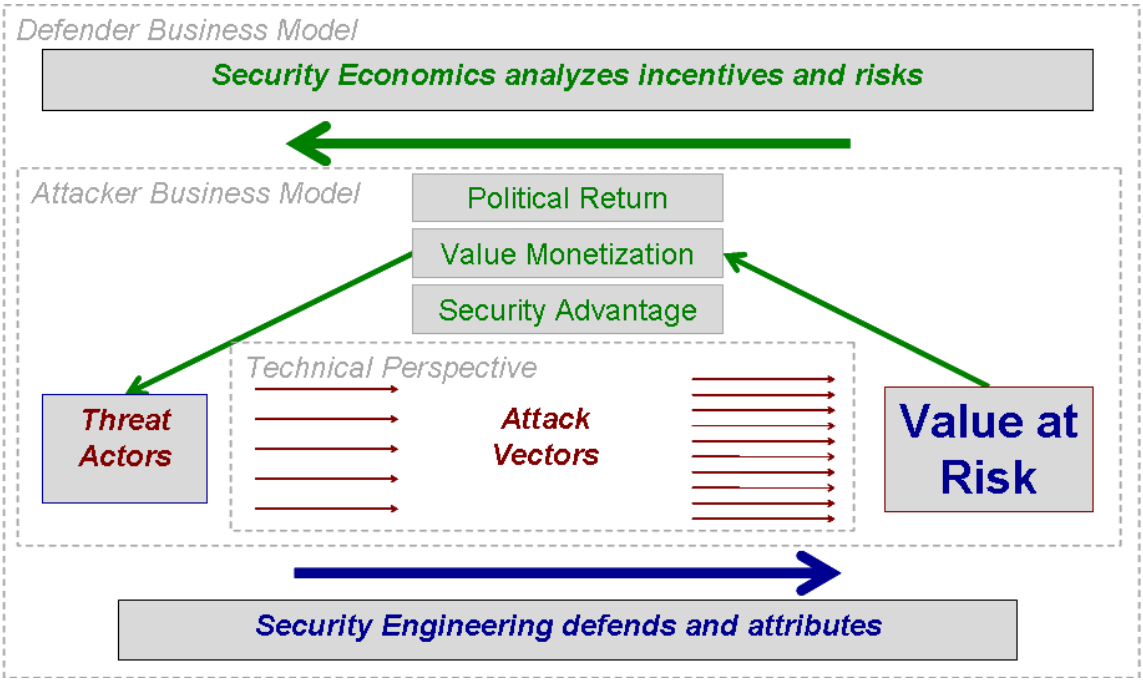


Fig. 7 Optimising integration of technical and economic perspectives for cybersecurity.

At the workshop, there was strong agreement to identify the stakeholders in the architecture diagram (Figure 6) and to assemble a team to begin developing an international project consortium together, perhaps starting with a smaller number of countries and advancing to more later.

3.2.4 International Approaches to cryptography

Animator: Bart Preneel, COSIC, KU Leuven

The key developments in ICT are the trend towards cloud computing and towards the Internet of things; both complex environments will have to interact in a secure way. These developments impact the future research agenda in cryptology, as explained below.

In the area of cryptographic algorithms, the main challenge is to push the limits for high speed performance in the cloud and to optimize the energy and footprint for the Internet of things. An important challenge is the creation of highly efficient and robust algorithms for authenticated encryption. For a limited number of applications long term security is required; in order to push the lifetime of current public key systems beyond 30 years, a sustained research effort is needed on novel algorithms (post-quantum cryptography). The most appropriate way to achieve these goals is through open international competitions that stretch over multiple years. Such competitions also require the development of common tools for the evaluation of the security and performance of cryptographic algorithms.

Advanced cryptographic protocols are needed to support privacy and user control in the cloud and in the Internet of things; as these two worlds need to interoperate, key goals are the development of functional encryption, the distribution of secrets to avoid single points of failure, the optimization of dedicated multiparty protocols and the development of novel protocols based on tamper resistance. Cryptography has a key role to play in the developments of privacy-by-design, and this in applications such as metering, subscriptions, information sharing and data retrieval. A particularly challenging and high-impact application is e-voting.

Creating cryptographic implementations that are secure and efficient is extremely challenging. In this area there is a need for foundational research combined with the development of advanced tools. Novel technologies such as Physical Unclonable Functions (PUFs), whitebox cryptography should be further explored, as they have a high potential for particular contexts.

Global context

The worldwide cryptographic community consists of several thousand researchers. Typically, around 1,600 are members of the IACR, the International Association for Cryptology Research; this not-for-profit association sponsors the seven top conferences and workshops in the field; and an additional 7-10 events are organized each year in cooperation with the IACR. The IACR also publishes the prestigious Journal of Cryptology, the leading journal in its field.

European researchers play a central role in this organization and it is fair to state that European researchers take a very strong position internationally; the ECRYPT and ECRYPTII networks of excellence have played a central role in strengthening this position. In several fields, such as symmetric cryptology, novel public key algorithms, lightweight cryptography, cryptanalysis, cryptographic hardware, cryptographic software for embedded systems, and secure implementations, European researchers are internationally leading. However, cryptographic standardization is mostly driven by US, as the key bodies are NIST and IETF. In addition, one can observe that in both the US and Asia (China, India, Japan, Korea, Singapore) there is a substantial increase of funding in this strategic area; these developments will make it harder for European researchers to remain competitive. The emergence of cloud computing has also strengthened the impact of US industry on the global processing and protection of data.

The fast developments in the area of cryptology require a long term research effort to maintain and strengthen the leading position of the European academic and industrial world. Cryptology plays a strategic role in the security of our society, as cryptology defines

who controls and accesses information and devices; this is essential for protecting the privacy of the European citizens and the transparency and efficiency of markets.

As the developments of cloud computing and the Internet of things are global developments, there is also a strong need for international collaboration on a strategic research agenda in cryptology.

3.2.5 Mobile Security

Animator: Abhishek Sharma, Beyond Evolution TechSolutions Pvt. Ltd., Gurgaon, India

Introduction

The extent and dimensions of the usage of mobile devices flooded with numerous applications has extended to practically all spheres of human life. These devices are now used for communication by voice, entertainment, social media, utility, information gathering - news, sports etc are assuming unimaginable proportions. With organizations increasingly looking toward mobile devices (e.g., iPhones, iPads, and Android smart devices) to deliver content and functionality to both their employees and their customer base and the people started utilizing power of mobile applications more and more, the mobile devices are becoming the fastest growing consumer technology. However, most find it difficult to understand and evaluate the security concerns that surround mobile platforms. Since mobile computing is a relatively new concept in the enterprise, many organizations have not yet updated their information security policy to cater for it. With about 600 million smart phones in 2010, they are poised to crossing approximately the 1.9 billion mark by the year 2013. Moving along with this, the growth and availability of mobile applications are multiplying the threat factors exponentially. Hence, Smart Phones, mobile apps, remote data, consumerization of IT and the rise of malware and criminal intent presents a lethal cocktail of security threats to the consumer, corporation and the mobile networks.

Mobile Security Scenario

In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. The enormously growing popularity of mobile applications has attracted enough hackers to make the potential for serious security threats a reality. More than 55,000 new pieces of malware are seen on a daily basis as per the report. Research shows that the number of mobile malware more than doubled in 2011 from 2010.

Ten years ago, CTOs wanted company phones locked down, camera phones and iPods banned from the office. Now they are being forced to contemplate bring-your-own-device (BYOD), whether that's a smart phone or a tablet, which is probably a CTO's worst nightmare. Meanwhile, consumers and business people alike are adopting a laissez-faire attitude to downloading mobile apps – powerful computer programs that could potentially contain malicious code – from unknown authors, something few people would do on their PC. Yet, a staggering 96 percent of Smart Phones and tablets do not have third-party security software installed. On the other hand, 2,500 different types of mobile malware were discovered in 2011.

What is under Threat?

Mobile devices increasingly face various types of threats, from mere annoyance to invasion of privacy, propagation, malicious tools or stealing money. Some of the most threatened mobile applications are money transfers or mobile commerce; Stored data on phone devices – this is growing in volume with growing storage capacity of the devices; Remote Data Storage OTA-with applications allowing data storage on cloud the three elements - Transmission, Storage and Access - have become vulnerable; Mobile Health Care, a very potential and fast growing area for mobile applications; OS Platform- they make the mobile

itself useless; many other utility applications such as Maps, Location Based Services; Games, other entertainment applications – here the hackers take advantage of people's weakness to get glued to games and thereby ignore warnings.

Threats to mobile money transactions could be one of the most dangerous and painful security threat. The value of mobile payment transactions is projected to reach almost $630 billion by 2014. Mobile money transactions are an attractive target for attackers as they allow direct monetization of attacks.

App Vulnerability: Like desktop / laptop computers, mobile apps too suffer from a myriad of security vulnerabilities. Many of these vulnerabilities are unintentional, caused by poor programming practices. Vulnerabilities can also be intentional and malicious, hidden within a seemingly safe and legitimate app. Some security vulnerabilities occur when sensitive data is transmitted to and from remote servers over unencrypted channels. Perhaps the most severe app vulnerabilities are those that exploit lax security of stored data.

How does the Threat work?

Besides analyzing the vulnerability, it is important to analyze the sources of such threats and how they manage to cause damage. The damage from a threat is a combination of source and channel to carry out the threat. While few of the main sources causing security threat are malicious applications, spyware and phishing besides many more, of which the commonly used channels are social networking, Bluetooth, Wi–Fi Hotspot and Botnets.

Briefly describing a few major ones – a Botnet is a collection of compromised devices connected to the Internet. The malware gives hackers remote control of the compromised devices, which can then be instructed to perform harmful acts. The easiest way for an attacker to benefit from a mobile Botnet is to send an SMS or multimedia message service (MMS) communications to a premium phone account that charges victims fees per message. Malicious applications are usually free and get on a phone because users voluntarily install them. Once on a handset, the programs steal personal information such as account passwords and logins and send it back to the hacker. Social Networking has seen growth in enormous proportion with the similar growth in the use of smart phone. As fallout, mobile malicious links on social networks are effectively spreading malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites. Spyware available online are used to hijack a phone by hackers, allowing them to hear calls, see text messages and e-mails, and even track a user's location through GPS updates. Bluetooth enables direct communication between mobile devices. Such Wireless devices broadcast their presence and allow unsolicited connections. In the case of Wi-Fi, hackers intercept communications between smart phones and Wi-Fi hotspots. In such a scenario, with no encryption to protect transmitted data, the hacker gets in between the user and the hotspot provider and hijacks the session via a man-in-the-middle attack. Phishing poses the same risk on Smart Phones as it does on desktop platforms. Mobile phishing is particularly tempting because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and MMS. Social media phishing is becoming a major issue as social networking sites contain an increasing amount of personal information. So to sum it up, the way the threat works may be classified as follows:

- Intentional & Malicious Vulnerabilities: These are
  - Malware hidden within seemingly safe Apps – they attack OS and make the devices unusable.
  - Rogue Apps – they lead to some undesirable performances or even some intentional misdirected actions such as stealing personal data or money transfers
  - Attacking stored Data-once the access to the data is achieved, almost any misuse of someone's data is possible.

- Unintentional Vulnerabilities: these are mainly attributable to mistakes committed by users themselves such as not using password protection or weak password, download Apps without verification of source, unprotected use of mobile internet etc.
- Programming Practices & Languages: App developers at times fail to validate input from the Web, allowing adversaries to access protected files, or they might hardcode passwords, allowing unauthorized access to user files and the app's source code. Some vulnerabilities arise from the programming languages with which apps are implemented. For example, languages such as JavaScript open the possibility of attacks via those who exploit Web browser vulnerabilities. Older programming languages such as C are prone to a host of well-known security vulnerabilities, such as buffer overflows, heap overflows, format string attacks, etc. Using third-party libraries, regardless of the implementation language, can also open up the potential for vulnerabilities.

How to address the Threat?

At the core of addressing such security threat in the mobile environment are two basic concepts - Wireless Intrusion Detection System (WIDS) & Wireless Intrusion Prevention System (WIPS). Keeping these basics as the building blocks, it is required to focus at few specific approaches

- Vetting the Apps by Purchasing organizations or a third-party labs before buying them is another approach. Currently, app stores don't incorporate a vet ting process that thoroughly examines potential security vulnerabilities in apps. This is partly attributable to the cost and time associated with vetting an app, as well as the complex and contentious interactions needed with developers, given the growing potential for dangerous and widespread vulnerabilities, it's becoming increasingly critical to vet apps for such vulnerabilities.
- Creating Strong Mobile platform with robust OS and associated with traditional safety approaches such as preventive measures like firewall and usage of anti-virus software.
- Increased usage Encryption software and encouraging more and more researchers and industry elements such as companies to work on this area. At present there are not many such apps as there development is complicated and challenging and the market is limited.
- Incorporating some regulatory aspects ensure and manage the usage of encryption software which takes into account some other associated aspects related to laws of the land, other security concerns of the government such as lawful interceptions to address crime and terrorism.
- Inclusion of certain E-Services that are specifically designed and developed to Protect Privacy such as vetting the mobile apps before they are allowed to be used, defining limits for accessibility to stored data etc. it's also necessary to vet the app store. However, the vetting process poses several challenges, such as specifying security and analysis requirements; identifying appropriate tools, mechanism, and approaches for analyzing security vulnerabilities and finding appropriate personnel to manually vet the apps.. and an infrastructure for testing the apps for security.
- Enhancing the scope of App certification process to pay special emphasis on the Trust & Security aspect of the App to be certified is another way to ensure threat avoidance from third party apps. Today the app certification approach and extent varies with platform – Java, Symbian etc.
- Education is key: It all comes down to education. Users have to be made aware of the threat and ways to protect their devices and Apps. But also it is important to build devices that protect the user without them having to make informed decisions – but

as we have seen with PCs this isn't easy. Awareness about Mobile Access confidentiality is a simple and effective way which although already provided by the OEMs, the lack of awareness and the indifferent attitude of users pose a major challenge to the success of this approach.

Way Forward - Key suggestions

- Collaborative efforts: Lots of work is going on across the globe to address threat to the mobile security and associated entities. Unfortunately, a majority of all that are happening in isolation, in pockets. Major collaborative efforts are required, in highly organized manner to achieve the maximum out of all those efforts and to derive the best possible results optimally.. The coordination and collaboration is required to Create a Centralized Body (like ITU) who shall Formulate Regulatory Policies, define Standards, Tools & Test Beds, organize Coordination amongst different scattered research bodies and entities involved in developing mobile security measures and apps, organize consolidation and compilation of available and ongoing work and organizing their development and dissemination through industry sources. The International Advisory Group (IAG) within BIC can make major contributions in this direction through its supporting Core Working Group (CWG) and Extended Working Groups (EWG).
- Structured Management: In order to achieve the organized coordination, structured management approach is essential. Apex body at the core supported by bodies and groups formed function wise and region wise with similar dissemination further on to micro level ensuring the numbers of layers kept at bare minimum are essential to manage such huge, complex and critical objective.
- Focused Objectives: The research work has inherent weakness of growing out of proportion and at times also loosing focus. It is imperative at the part of the all coordinating and managing bodies to start the work with well defined objectives and stay focused on the same.
- Introducing specific Regulatory mechanism through ITU: In addition to the above, one of the most important and possibly most effective measure would be to create a mandatory regulated mechanism controlling security aspects right at the device OEM level. The greater possibility of these attacks will place an increasing importance on mobile device makers to include security features and configuration options in place. The central Telecom regulatory body ITU need to setup an empowered body within itself to impress upon the OEMs and ensure that suitable security measures are incorporated within the devices such that only certified applications be made available to users either for Free usage or paid ones. This aspect will of course impose certain restrictions on the genuine App developers but by way of keeping the costs of such certifications low (e.g. just few dollars) but at the same time making the tests procedures thorough and comprehensive particularly against any security threats, would go a long way in ensuring the safety of the mobile, mobile apps and mobile users.

Why is international cooperation important in this particular topic?

Today, the information and communication technologies, be it voice or data, has made the geographical boundaries irrelevant. Along with this today and more so in future, significant amounts of confidential operation like banking transaction, mail/ data exchanging will take place from mobile only. In addition, critical utility services management of power, water and other infrastructure services too besides services like health care and education would have mobile phones and apps playing major role. However, despite the world getting connected, the regional elements on the demands, requirements, behavior and need of the people still vary to a great extent. At the same time the provisioning of the mobile systems - devices and applications are happening across the globe cutting across the regional

boundaries. Devices and applications developed in one corner of the globe are equally utilized across the globe. The same is the case with the creation and proliferation of malware, rogue applications and such security risks. Accordingly, since the smartphone / mobile penetration is increasing globally, it makes a lot of sense that all regions of the world - Europe, Asia/ India/China, Americas, Africa collaborate closely for the Research & Industrial Developments. It is therefore not just natural but essential that the research and development work to address the threats and risks to mobile security is pursued with help of intense International cooperation and managed with globally collaborative mechanism.

The Final Word

As the spread and utilization of mobile devices grow, they will face risks of growing attacks in number and variety. It is critical to understand what is there to lose before a mobile security breach occurs. The ultimate goal is not about aiming to achieve something unrealistic -complete elimination mobile security risks. Such ultimate safety and risk prevention may not be possible. However it is rather essential to have systems in place to minimize the impact when breaches occur. Towards this goal, there is need for regular and sustained work across all stakeholders - Device OEMs, App developers, VAS providers, Network Service Providers/ TELCOs and, last but not the least, the mobile users themselves to first, take the threat seriously and then, constantly participate in the lookout for threats and search for their solutions.

3.2.6 International approaches to critical infrastructure protection

Animator: Manmohan Chaturvedi, IIT Delhi, India

Introduction

Critical infrastructures (CI) have become the central nervous system of the economy in all countries and a key national security concern. Their interdependencies compound the challenge in securing them from various threats. From the available statistics we can safely conclude that threats to Critical Infrastructures from state and non-state actors, driven by diverse underlying motivations, have grown in number and intensity. The challenge to a nation state is to initiate comprehensive steps to mitigate their ill effects. We need to identify a comprehensive yet parsimonious set of steps that can be initiated at national level to address these emerging threats.

Need for a suitable metric

We cannot improve anything unless we can measure it. While it is easy to measure physical parameters like temperature and pressure, complex constructs like security level of a nation or a critical sector are difficult to articulate in social science.

International Challenge

Critical Infrastructure protection is an international concern. Multi-dimensional approach is necessary to achieve success in this venture. Following key questions need to be addressed:

a) How to identify and prioritize the dimensions of an Index to measure the CI protection initiative?

b) How to identify and prioritize important indicators under each dimension?

c) How to measure progress on each dimension?

d) Is it possible to provide a composite index of a CI's security status at regular interval?

e) Is it possible to identify areas in need of urgent action?

Recommended Methodology for CI protection

Amongst the various CIs of our modern society all appear important when viewed individually. Delphi methodology may help identification of "critical few" from a comprehensive list. Delphi Method, first introduced by Norman Dalkey and Olaf Helmer during their association with the Rand Corporation in the 1950s is uniquely suited to studying topics with little historical evidence, related to rapidly changing events and of great complexity. In Delphi approach we are interested in collecting the judgments of experts on a particular topic to document and assess those judgments.

Interpretive Structural Modeling (ISM) (Warfield, 1974) can articulate the hierarchical relationships among them in terms of driving power and dependency. This permits short listing CIs that are at root of the hierarchical model for further prioritized action. Matrice d'Impacts Croises Multiplication Appliquee a un Classment (MICMAC) analysis (Duperin and Godet, 1973) can be used to unveil hidden indirect influences among these CIs.

AHP is one of the Multi-Criteria Decision-Making (MCDM) methods and the underlying principle of MCDM is that these decisions have to be made by means of sets of criteria. By applying this principle; Saaty (1980) developed AHP which models a hierarchical decision problem framework that consists of multiple levels of criteria having unidirectional relationships. AHP works with such hierarchy that can combine both subjective (intangible) and objective (tangible) criteria.

Illustrative research approach to derive index of a critical sector

At IIT Delhi, we have attempted in an ongoing research to define a construct of National Information Security Index (NISI) in Indian context using combination of Delphi and AHP. The interim findings of the research and illustrative use of NISI to measure a nation's security index provide us a template for design and computation of a sector specific security index.

Recommendations

- The illustrative use of the NISI for tracking India's progress to secure her Cyber Space can be replicated to design Security Index for the prioritized CIs/sectors
- The index can be used to track progress in securing these prioritized CIs/sectors
- Suitability of this approach to EU and other national context could be considered

Relevance of International Cooperation in CI protections

The threats to the ICT systems of all CIs can emanate across national boundaries and therefore, all nations can benefit from cooperation. For the Horizon 2020, the security of the evolving Next Generation Networks (NGN) could be considered for the international cooperation. The NGN would amplify the threat vectors with their IP protocol based approach to communication and ubiquitous use of smart phones as the preferred mode of online transactions.

3.2.7 Security and virtualisation

Animator: Syed Naqvi, Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC), Belgium

Introduction

Virtualization infrastructures present promising features to address the ever-increasing demands of information society. The concept of virtualization is not new in the field of ICT. It dated back to the inception of programming language compilers that virtualize the object code [20]. However, the concept of virtualization infrastructures, where physical resources are dynamically mapped to address the spontaneous business needs, is relatively new. Moreover, the scale and scope of this novel concept brings several challenges for its

deployment including a lot of uncertainty as to how and where to implement security [21]. Classical security solutions and practices are getting obsolete in the face of the peculiar security requirements of virtualization infrastructures. Therefore, security and dependability issues of virtualization infrastructures are emerging as gauging factor for measuring the success of this Endeavour.

The inherent nature of virtualization requires totally different security provisioning approach than the classical one developed decades ago. Classical IT security solutions and practices require precise information of the underlying infrastructure for their deployment and functional validation. They cannot be applied to these virtual infrastructures due to the intrinsic characteristic of virtualisation that provides abstraction to the underlying resources and infrastructures. This section examines two major security challenges of virtualization infrastructures – security audit and digital investigations. Finally, a quick glance of a federated Cloud security experiment funded by the European Commission is given before drawing some perspectives of international cooperation in the area of virtualisation security.

Security Audit of Virtualisation Infrastructures

Security audit assess the security of a networked system's physical configuration and environment, software, information handling processes, and user practices. Various security audit standards such as Payment Card Industry Data Security Standard (PCI-DSS) require audit of the physical controls [22]. The virtualisation infrastructures provide an abstraction layer to the underlying lower-level details. This situation raises several security concerns such as multi-tenancy; lack of security tools [23]; and disparity with the classical IT security audit practices. Another important issue in this regard is the data export control that requires operators and providers to ensure that particular kind of data should only be stored and processed in some specific location. Audit inspectors need to certify compliance to these regulations for the issuance of the operating licenses to infrastructure and service providers. Check-pointing mechanisms including monitoring tools are indispensable for auditors (both internal and external) to verify that operators and providers are respecting the corresponding regulations.

There exist a number of generic monitoring tools such as hardware monitoring (e.g. HP Insight Manager, Dell Open Manage, VMWare Virtual Center, etc.), performance monitoring (e.g. VizionCore, Veeam Monitor, Vmtree, Nagios, etc.), machine state monitoring (e.g. Virtualshield, Logcheck, etc.), and security monitoring (e.g. intrusion detection, honeypots, etc.). However, these tools may not be suitable for security audit controls of virtualization infrastructures as physical controls can be distributed that will require onsite checks by the local controllers. There is a strong need of a new set of matrices for measuring security strength. With more reliable matrices, new check-pointing models need to be developed. Besides these technical requirements for carrying out security audit of the virtualisation infrastructures, there is also a need of new regulations/legislations for the cross-border deployment of resources used in virtualisation infrastructures.

Digital Investigations of Virtualisation Infrastructures

While virtualization infrastructures are poised to drive cybercrimes in the near future [24], these virtualisation infrastructures (such as Clouds) have no 'forensic friendly' design characteristics. Therefore, classical investigation techniques (such as confiscation of computing resource, copying and analysing digital contents) is not feasible as unplugging of a Cloud is not the option its stakeholder are willing to choose! Moreover, a Cloud is required to copy the contents of the Cloud under investigation. Furthermore, another Cloud is required to have computational capacity to analyse the contents of the Cloud being analysed. The current practice of carrying out digital investigations of Clouds involves analysis of individual computers connected to a Cloud. These investigations include recovery of connection details, logins, and data exchange to establish the sequence of actions carried out on the Clouds and to eventually demarcate the responsibilities. The Cloud operations are therefore not affected by these investigations of individual PCs.

However, this paradigm is not sustainable in the advent of shrinking features on the client side of Clouds. Complete externalisation of software artefacts (from the operating systems to the applications) will not provide any meaningful information to the investigators. This paradigm is already realised in 'Cloud PCs' (e.g. Wyse technology's X00m Cloud PC [25]). Dell's takeover of Wyse technology to expand their enterprise business heralds a widespread use of Cloud PCs in the very near future. Cloud PC X00m has only 2GB RAM with no storage or optical device connected to it. Digital forensics analysis could not be performed on these Cloud PCs without including Cloud infrastructure in the investigations. This paradigm will give birth to a number of serious security challenges including operational challenges (such business continuity assurances for the customers) as well as legal challenges (notably acceptability of the proofs originating from a 'virtual' world).

BonFIRE Security Experiment

European Future Internet experimental facility and experimentally driven research project BonFIRE [26] is executing a security monitoring experiment that aims to examine the implications of security on the virtualisation infrastructures – i.e. federated Cloud infrastructures. This experiment – ExSec: Experimenting Scalability of Continuous Security Monitoring – aims to develop a mean of quantifying the impact on security functions under various operating conditions and parameters of federated Cloud deployments. The results of this experimental study will help businesses to identify the best security architecture that will fit their Cloud architectures and performance requirements.

The main objectives of the ExSec experiment is to study and quantify the impact on the quality of protection of Future Internet based virtualisation infrastructures that will be highly scalable in nature and use heterogeneous underlying technologies. These experimental evaluations will be useful to determine the stretching limit of Cloud security functions; and eventually, workout some remedial solutions especially to explore the possibility of making use of abundance of Cloud resources to compensate the performance degradation.

Perspectives of International Cooperation

Virtualization infrastructures envision a number of promising benefits for global businesses such as resource management, service provisioning and cost effectiveness. However, the scope of these infrastructures requires them to be dependable and secure, as markets will depend on them, as much as governments, to function properly. Globalisation of computing and storage resources require security solutions at the global scale, otherwise it will be impossible to achieve concrete security assurances for these infrastructures. International collaboration is crucial for ensuring security of the emerging networked society's core architecture whether it is security audit framework for virtual infrastructures or their digital investigations.

Recent economic meltdown has shown the degree of dependence at the global scale in general and among the emerging and developed economies in particular. This situation obliges us to take some international dimension for virtualisation security. It is understood that bringing different societies and cultures to a common understanding of security requirements is not trivial. Even member states of politico-economic blocs such as European Union maintain conflicting views of IT security [27]. Still, we need to involve all the stakeholders in a constructive cooperation to workout a common vision for securing virtual infrastructures. Significant breakthrough could be made if some business dimensions are added by bringing commercial stakeholders on-board. For example, best practices proposed by payment card industries (such as VISA & MASTER) are adopted and followed by all the players irrespective of their political and societal affiliations. Without some effective international cooperation, there will be a number of Achilles' heels that malicious entities will use to attack the critical information infrastructures from their safe havens with complete impunity.

Acknowledgements

This work is partially funded by the European Union's seventh framework programme (FP7 2007-2013) Project BonFIRE under grant agreement number 257386.

3.2.8 Implications arising from identity and privacy related issues on a global scale

Animator: Alberto Crespo, Atos Spain S.A.

The powerful technological, social, economic and political drivers of globalisation are shaping the evolution of electronic services towards greater integration through management of complex relationships spanning across borders and world regional areas. The complex ecosystem of greater cross-border information flows opens opportunities for creation of wealth in modern knowledge societies, but also risks to individual fundamental rights and freedoms, especially privacy. The goal then must be to ensure public networks are more natively trustworthy, providing privacy-protecting, secure and identity-based online interactions which prevent misuse of personal data.

The trust in the emerging eServices in the areas of cloud computing, mobility, Internet of Things, Future Internet, etc. essentially depends on the realisation of a highly interoperable techno-legal layer that enables privacy-respecting and trustworthy electronic identity services. This should be manageable dynamically as a service with proper auditability and accountability and should be bi-directional allowing to establish reliable identification of all parties involved in potentially composable transactions where legal certainty as to applicable jurisdiction needs to match the emerging nature of new ICT paradigms. International cooperation is key to achieve the mentioned goal of enhancing trustworthiness of ICT systems operating on a global scale, allowing a more effective prevention and combating of multiple forms of cybercrime and large-scale threats to security and privacy, e.g. identity-related crimes of fraud and theft.

Such international cooperation requires articulation at several levels: political, organisational, technical, semantic, cultural, social, etc. Each of these layers requires involving several stakeholders in a trans-border dialogue which addresses specific problems and goals: from decision-makers and public sector agencies, to industry (ICT companies, electronic components manufacturers, service providers, security solutions integrators, etc.), NGO's (e.g. consumer associations or other advocacy groups), commerce institutions, international standardisation bodies, etc. The mutual cooperation can yield significant progress in the following fields:

- Effective engineering and technical solutions (e.g. PETs) to embed privacy by default and into the design of ICT systems.
- Interoperable electronic and Internet-based identity schemes allowing federation and cross-border, cross-domain, cross-sector interactions.
- Privacy respecting identity management involving private and government third parties: identity/attribute providers, service composition… In particular, this requires international agreement on consistent metrics and assurance levels as well as basic understanding and acceptance of common fundamental principles[12]13 underlying different data protection legislations which may be universally appliccable as a general framework (while recognising local specificities).

[12] Principles of proportionality, purpose specification, lawfulness/fairness and rights of access, rectification, deletion, objection as stated in 2009 Madrid Declaration of Data Protection and Privacy Commissioners.

[13] Principles of proportionality, purpose specification, lawfulness/fairness and rights of access, rectification, deletion, objection as stated in 2009 Madrid Declaration of Data Protection and Privacy Commissioners.

- More dependable ICT infrastructure articulated over mechanisms for accountability, liability, audit, compliance monitoring, enforcement… even across hetereogeneous legal and trust domains.

Still, such efforts may fail if they don't place at the center of their approaches the citizens and consumers in a user-centric manner, which effectively empowers people using technology (whose life is changing rapidly by it too). User's trust in e-Relations depends on their effective participation with choices to decide which personal data is to be released under specific conditions which gives the feeling of being in control (digital sovereignty and informational self-determination). The new draft of EU Data Protection Regulation constitutes a good basis in this direction and constitutes a good framework for discussion with other important countries seeking complementarity at policy level: Australia, Canada, the US, Brazil, APEC countries, etc.

International cooperation on fields like identity management assurance and e-Signature can yield valuable results allowing for the secure transmission of information with increased trust in its provenance (e.g. personal data attributes certified by reliable sources) or the effective establishment of architectures based on privacy-enhancing credentials where applicable (e.g. anonymous credentials, use of claims-based assertions). Furthermore, cooperation on usability of ICT can make systems easier to use for all citizens, with greater focus accessibility, multilingual interfaces and common approaches to informed online consent (e.g. allowing precise descriptions of destination of personal data and purpose of its collection and processing).

The existing visions on identity management ecosystems and interoperable eID infrastructures (e.g. OATH and NSTIC in the US, STORK in the EU, Kantara initiative, etc.) have potential to effectively build 'bridges' on a global scale, using existing solutions as 'building blocks' which are respectful of already working schemes at national levels. The EU can provide lessons learned from its experience in this area when it comes to making national systems (be it for health, justice, public procurement, public services for business or eID) interoperable in the context of larger pan-European frameworks which are respectful of existing technical, legal and organisational frameworks at national levels. It is thus possible to build solutions that work at a large-scale, connecting smaller-scale solutions by means of open standards and technologies (e.g. for effective translation of attributes names and values across heterogeneous domains), bringing unprecedented growth to our economies while satisfying the expectations from end-users in terms of personal data protection and trustworthy operation of ICT systems. At the level of eID management, STORK project has proven the feasibility of de-centralized approach to enable around 30 electronic services portals from 15 different European countries to authenticate securely foreign users presenting their national eIDs (more than 110 different eIDs are supported). Besides authentication of citizens, it is important to build semantically-rich solutions, like STORK 2.0 will do, which allow to represent and manage across borders roles, mandates and powers of representation to act on behalf of legal persons.

Solutions for adequate and explicit management of trust will be key in building globalized frameworks. This requires not only establishing trust chains that rely on technical mechanisms (authenticity and integrity of exchanged messages in commonly agreed formats) but also agreements to establish mutually recognised organisational measures (e.g. security audits, compliance with security standards, etc.) to determine with sufficient formality that involved subsystems and nodes are secure (e.g. sets of common minimum standards of data security rules and policies can be agreed and certified by mutually recognised third parties or Memorandums of Understanding signed). Pragmatic approaches should be sought as well in the area of Service Level Agreements and liabilities of involved parties.

In the area of data protection, international-level exchanges of personal data must intensify upon the basis of application domains and corresponding risks and benefits and focusing

on eliciting common understandings on concepts and principles which may be very differently understood in different areas of the world, e.g. “proportionality”, “data minimisation”, “anonymous data”, “sensitive data”, “legitimacy of processing”, “informed consent”, “data controller or custodian”, “data processor”, etc. Similarly, bases should be laid down for allowing international flows of personal data with sufficient guarantees to the respect of fundamental rights of data subjects in the originating countries (focus of cooperation in this field should examine the available options, e.g. bilateral agreements like EU-US Safe Harbor, grounds for ‘adequacy decisions’, binding corporate rules, contractual clauses, safeguards supporting privacy and standard clauses for data protection that privacy commissioners / DPAs may determine…). While addressing the complexity of national privacy laws (established in over 60 countries) may be too ambitious, discussion may take place on the basis of regional approaches (e.g. EU DPD/Regulation, APEC Privacy Framework). This kind of analysis can address underlying differences in approach: human-rights vs commerce-based, geography vs organisation focus, denial of flows of personal data unless legal basis present vs allow data flows with powers to limit them in some circumstances…

Finally, there is room for substantial progress in the following areas:

- Fostering good privacy practices as business differentiating factor: at same price people choose privacy-friendly vendors (privacy should “stand-out” for users)
- Consumers need a ‘choice menu’: choosing between personalised services that require identification and other services that minimise collection of personal data. Privacy notices should be available with clear language so user can compare with other providers. Consent should not be abusively used to process personal data.
- Support of data portability (e.g. profile portability between providers) subject to consent.
- Removal of excessive bureaucratic restrictions (e.g. approvals/regulatory filings) which create inefficiency.
- Encouraging organisationally-based transfer mechanisms (i.e. BCR, codes of practice, targeted audits, privacy seals…).
- Enforcement should focus more on the transfers that have greatest risk.
- Ways for implementing transparency and better rules for jurisdiction application (avoiding frictions between laws).

3.2.9 Internet of Things

Animator(s): Carmen Fernandez Gago, Gerardo Fernandez Navarrete, NICS Lab - University of Malaga, Spain. With additional contributions from Rodrigo Roman Castro, Institute for Infocomm Research, Singapore and Javier Lopez, NICS Lab - University of Malaga, Spain.

There has been considerable research work undertaken in Europe on the Internet of Things and roadmapping activities looking at the future research needs for the concept known as the “Internet of Things”. There are a number of widely used definitions for Internet of Things, including the following:

“Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Interconnected objects having an active role in what might be called the Future Internet.” source: *Internet of Things in 2020 - Roadmap for the Future. May 2008 [28]*

“Objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment and/or use actuators to interact with it”. source: *Internet of Things – An action plan for Europe. June 2009 [29]*

“A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols - Physical and virtual “things” have

identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network." source: *Internet of Things – Strategic Research Roadmap. September 2009 [30]*

All IoT definitions revolve around the same central concept: "a **world-wide** network of interconnected objects" with the following attributes: existence, sense of 'self', connectivity, interactivity, dynamicity, and sense of environmental awareness.

Therefore, a global approach must be taken to address the trust and security aspects of the Internet of Things and WG2 of BIC is a very useful place for addressing these.

As shown in Figure 8, there are a number of top level security research challenges. In summary, the challenges are the following:

Protocol and network security to deal with the large number of objects with significant heterogeneity. This would involve improved cryptography to make them operate in smaller environments requiring faster operation while keeping same levels of security so far. A Key management infrastructure is needed for the open configuration of IoT, in which the new systems need to be able to manage the keys in objects of small size where the current certificate based systems wouldn't work. The current Internet protocols are not usable in these environments.

Data and Privacy as carrying multitudes of objects can bring up a lot of privacy issues as they are not operating in an isolated way. This area can be addressed by using Privacy by Design (user should be able to decide which of his/her information and how it is being used); Privacy by Default (right to be forgotten); transparency (he should know when it is being used), and improved data and information management.

Identity management, which must be taken from a different perspective in IoT in which objects will have a core identity and yet a temporary identity must be possible. ID management systems should encompass Identification (how to define the identity of a "Thing"); Authentication (infrastructure that allows mutual authentication based on Centralized, Distributed, Local, Global, Attributes); and Authorization based on delegation (e.g. stethoscope) and granularity (e.g. classroom provides class schedule to everyone, syllabus only provided to students).

Trust and governance is required in order to obtain trust between the different objects (and from the user perspective). For the IoT, a trust management system is especially required inside in order to gain trust management from the user perspective. From the system perspective, governance is very important where policies should be contained and where the policies vs. control is dealt with;

Fault tolerance as the perimeters of the networks do not exist any more in IoT. Therefore, attackers will be all around and there is a need to provide solutions with the following attributes - Secure by default (Patch Tuesday?), Internal State and the ability to provide self - defence recovery.

Also shown in figure 8, there are two special "foundational challenges", including those related that are **Properties / Application-specific**. These are basic properties that all challenges must consider (e.g. Interoperability, Scalability, Resilience) and to the high-level, application-specific security mechanisms that make use of all the challenges above (e.g. Secure discovery of services); and **Architecture.** Within a system, it is necessary to provide some architectural support to integrate the different security services.

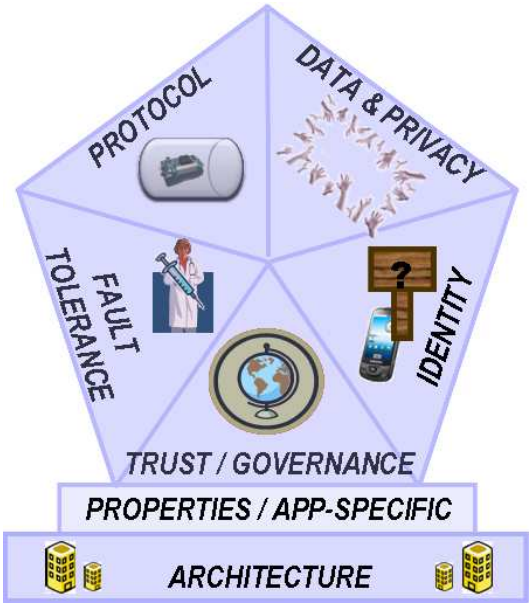


Figure 8. Trust and Security research challenges in IoT

3.2.9 Photos from the session

WG2. breakout session

4. Conclusions

The BIC project has organised a major workshop held over two full days in Brussels on 21-22 June 2012 with the participation of over 40 experts in different domains of international cooperation and trustworthy ICT, coming from 15 different countries (from Australia, United States, India, Brazil, and from Norway to South Africa).

Day 1 of the workshop (21st June 2012) focused on cross domain activities of international cooperation and Day 2 (22nd June 2012), focussed on technical themes in trustworthy ICT and international cooperation. The experts participating in the first day targeted strategic and tactical perspectives of INCO activities dealing with advantages and disadvantages of multilateral and bilateral approaches, what the current mechanisms are, barriers and obstacles, regional differences and they provided valuable comments on the best way to move forward.

Day 2 of the workshop (22nd June 2012) was structured in two parallel full-day sessions; the first working group focused on a multidisciplinary approach to trustworthy ICT human oriented, citizen centric; the second working group focused on the need for international cooperation for enabling the protection of networks and systems.

The multidisciplinary approach adopted by the BIC consortium for inviting and selecting the experts attending the sessions resulted in a fruitful and beneficial sessions with high level of knowledge transfer, sharing all type of experiences and coming to interesting conclusions that can provide useful hints for defining future programs in international cooperation.

A multi-lateral approach international cooperation approach in RTD initiatives complementing the predominant bi-lateral initiatives is suggested by the BIC International Advisory Group (IAG) and a high level basic structure is proposed and detailed for discussions. The IAG is there to suggest and formulate policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups have been formed as defined in the BIC IAG Terms of Reference and this workshop was their launch face to face meetings.

The multi-dimensional approach necessary for trust, privacy and security, and the difficulties in addressing all the cross-implications, go far beyond pure technological issues. The following are some of the key points raised by the experts during the workshop. The recurrent theme is the need for international cooperation and collaboration to address what is inherently a global – international – challenge.

- take full cognisance of the point of view of the end-users; take into account the real needs of the citizens; stop designing security solutions from the point of view of security experts only.
- The notion that - *Privacy is dead – get used to it* – as asserted by some quarters needs to be examined; the rise of social networking online may mean that (some, in cases many) people no longer have expectations of privacy; therefore, internationally-based socio-technical initiatives are necessary to support and develop such concepts as privacy as essential components of modern society.
- trust management in secure software: the scale of the emerging global infrastructures, combined with the need for fully autonomous operation, surpass the capability of existing security infrastructures such as authorization services, certificate issuance and validation services; having a certified identity (maybe granted using sloppy/undocumented procedures) in a dynamic and open environment does not give *a priori* guarantee of acceptable behaviour and performance of software and services; in particular, it is not enough for informed decisions on access restrictions and control,

the selection among potential candidates for interaction; trust is a first-class object that needs to be evaluated, analyzed, used, negotiated.

- as more aspects of business and personal lives shift into this cyber world of online services, concerns have arisen over how we can have confidence that they will protect and handle data and information responsibly; accountability can help us tackle these challenges in trust and complexity; accountability is enshrined in regulatory frameworks for data protection across the globe; to increase trust we must address the needs of all stakeholders – users, providers and regulators; an orchestrated set of mechanisms: preventive (mitigating risk), detective (monitoring and identifying policy violation) and corrective (managing incidents and providing redress), using interdisciplinary co-design to ensure that legal and business processes and technical mechanisms work in support of each other should be addressed.
- when we see data on the web, currently, we do not know where it comes from and how it got there; this information and its source (provenance) is typically lost in the process of copying/ transcribing/transforming databases; assurance of provenance is essential to data integrity, currency and reliability.
- social computing is enabling user-centric, collaborative knowledge sharing to build communities of people using the Internet in South Africa and also in Africa generally, eg, Mxit (www.Mxit.com); the key to whose success lies in its simplicity; the interface is text-based not graphical; it can work on nearly any mobile phone; in developing countries such as in Africa; mobile phones can be used as a tool to intervene and act as a competitive force in the social, economical and political development.
- A Personalized Identity Management (PIM) ecosystem is needed in which individuals can manage digital identities and control the exchange of identity information; under GINI-SA, which is a Support Action for the European Commission aimed to analyse this vision, individuals would manage their identities by means of an Individual Digital Identity (INDI), a self-generated and self-managed digital identity, which is verifiable against one or more authoritative data sources.
- attackers will soon start developing automated techniques to customize attack s based on private user information and aggregated data collected from multiple online sources; Cloud computing, online social networks, smart meters, SCADA Networks are potential targets for international cooperation; new and emerging technologies need to be studied from a security point of view.
- the trends towards cloud computing and towards the Internet of things are already on the future research agenda in cryptology; in the area of cryptographic algorithms, the main challenge is to push the limits for high speed performance in the cloud and to optimize the energy and footprint for the Internet of things; as the developments of cloud computing and the Internet of things are global developments, there is a corresponding need for strong international collaboration on a strategic research agenda in cryptology.
- smart phones, mobile apps, remote data, consumerization of IT and the rise of malware and criminal intent present a lethal cocktail of security threats to the consumer, business and commerce, the communications – particularly mobile – networks, and the whole societal infrastructure; at the core of addressing such security threat to the digital environment are two basic concepts - intrusion detection system, and intrusion prevention system; coordination and collaboration are required to create a centralized body (like ITU) the can formulate regulatory policies, define standards, tools and test beds, organize coordination amongst scattered research bodies and entities, and organize consolidation and compilation of available and

ongoing work, organizing their development; The International Advisory Group (IAG) within BIC can make a major contribution in developing the groundwork for this.

- the protection of the Critical Infrastructure(s) is an international concern that must be urgently addressed with a multi-dimensional; research is ongoing to define a construct of National Information Security Index (NISI) in Indian context using combination of Delphi and AHP; interim findings of the research and illustrative use of NISI to measure a nation's security index provide a template for design and computation of a sector-specific security index.
- virtualization infrastructures offer a number of promising benefits for global businesses such as resource management, service provisioning and cost effectiveness; however, the scope of these infrastructures requires them to be dependable and secure, as markets will depend on them, as much as governments, to function properly; globalisation of computing and storage resources require security solutions at the global scale, otherwise it will be impossible to achieve concrete security assurances for these infrastructures; international collaboration is crucial for ensuring security of the emerging core architecture of the networked society: whether it is security audit framework for virtual infrastructures or digital investigation and corrective action.
- trust in the emerging eServices in the areas of cloud computing, mobility, Internet of Things, Future Internet, etc. essentially depends on the realisation of a highly interoperable techno-legal *layer* that enables privacy-respecting and trustworthy electronic identity services; international cooperation is key to achieving the goal of enhancing the trustworthiness of ICT systems operating on a global scale, allowing a more effective prevention and combating of multiple forms of cybercrime and large-scale threats to security and privacy, e.g. identity-related crimes of fraud and theft.

A change in approach from the existing bi-lateral, e.g., EU-India, EU- Brazil, EU- SA, to multi-lateral is suggested as well as a possible multi-lateral structure, with a *Core Working Group* (CWG); based on a structure of the BIC IAG, *Extended Working Groups* (EWGs) specific for each participating country and *Special Function Groups*, operating under EWGs as specialists at functional level. With this in mind, a proposal for coordination and multi-lateral approach is presented taking into account the discussions at the workshop is included in Annex 2.

It is important to note that the building of international cooperation is even difficult when using a bi-lateral approach as it takes significant time for each of the parties to come together on a bi-lateral basis to try to align their activities and priorities. Therefore, it is exponentially more difficult for a multi-lateral approach when building a longer term strategy as proposed within the workshop. The BIC project has proposed a strategy and will follow up in the near future with interested countries as exemplars.

5. Further information

5.1 References

[1] DIT, Cyber laws strategy, http://www.mit.gov.in/content/cyber-laws

[2] DIT, Cyber Security R&D strategy, http://www.mit.gov.in/content/cyber-security-r-d

[3] DIT, Organisation chart 2/5, http://www.mit.gov.in/content/organization-chart

[4] DIT, Cyber Appellate Tribunal (CAT), http://www.mit.gov.in/content/crat-dpl-other

[5] DIT, Indian Computer Emergency Response Team (ICERT), http://www.mit.gov.in/content/icert-dpl-other

[6] DIT, Controller Of Certifying Authorities (CCA), http://www.mit.gov.in/content/cca-dpl-other

[7] Information Technology Act, 2000, http://cca.gov.in/rw/pages/informationtechnologyact2000.en.do

[8] Certifying Authorities, http://cca.gov.in/rw/pages/becoming_ca.en.do

[9] Department of International Cooperation & Industrial Promotion, Bilateral Trade Division, http://www.mit.gov.in/content/europe

[10] DIT, Cyber Security R & D Call for proposals http://www.mit.gov.in/sites/upload_files/dit/files/CyberSecurity.pdf

[11] BIC Deliverable D2.3 - Interim report of the Working groups activities (restricted).

[12] http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST

[13] http://www.securityconference.de/Home.4.0.html?&L=1

[14] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommuniqu e-Final.pdf

[15] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=EN G

[16] Remarks at the 28th Annual International Workshop on Global Security, Paris, France 16th June 2011 http://www.defense.gov/speeches/speech.aspx?speechid=1586

[17] International cooperation "at nascent stage" - U.S. Secretary of Homeland Security Janet Napolitano, Vienna, 1st July 2011. http://www.reuters.com/article/2011/07/01/us-cybercrime-idUKLDE75T1CC20110701

[18] London conference on Cybersecurity, 1-2nd November 2011, http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/

[19] 1st BIC Annual Forum, 29th November 2011, http://www.bic-trust.eu/events/1st-bic-annual-forum/

[20] Jason Bloomberg, Building Security into a Service-Oriented Architecture, ZapThink Whitepaper, ZapThink LLC Publisher, May 2003

[21] Richard Adhikari, The Virtualization Challenge, Part 5: Virtualization and Security, TechNewsWorld, March 2008

[22] Payment Card Industry Data Security Standard (PCI-DSS) https://www.pcisecuritystandards.org/

[23] Edward L. Haletky, Virtualization Security - Security and Compliance within the Virtual Environment, DABCC online article 08 April 2009 http://www.dabcc.com/channel.aspx?id=279

[24] Trend Micro Report: The Future of threats and Threat Technologies – How the Landscape is Changing, December 2009 –

http://affinitypartner.trendmicro.com/media/34716/trend_micro_2010_future_threat_report_final.pdf

[25] DELL Wyse Cloud PCs – http://www.wyse.com/products/cloud-clients/cloud-pcs

[26] European 7th Framework project BonFIRE: Building Service Testbeds on FIRE (Future Internet Research Experimentation) – http://www.bonfire-project.eu

[27] F. Calderoni, The European legal framework on cybercrime: striving for an effective implementation, Crime, Law and Social Change 2010, Vol. 54, 339-357

[28] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[29] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[30] http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

5.2 Link to the Workshop Webpage, where all slides can be found.

http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

5.3 Reminder list of upcoming events

Date	Venue	Event	Description
26-27th Sept 2012	Warsaw, Poland	Information Day and networking session on EU – Japan cooperation.	Information day on whole work programme in Warsaw, Poland on 26 and 27 September 2012. http://ec.europa.eu/information_society/events/ictproposersday/2012/index_en.htm In addition, concerning the EU-Japan R&D activity, a dedicated page has been opened where you can submit your ideas, partner search, and take this opportunity to be part of the EU-Japan networking session that takes place on 27 September 2012. You will find the relevant additional information at: http://ec.europa.eu/information_society/events/cf/ictpd12/item-display.cfm?id=8435
10-11th Oct. 2012	Limassol, Cyprus	Annual Privacy Forum http://privacyforum.eu/	The Annual Privacy Forum 2012 (APF'2012) is being held on the 10th and 11th of October 2012 in Cyprus. The forum is being organised by ENISA in collaboration with DG CONNECT, University of Cyprus and Cyprus Presidency of the Council of the EU. The provisional programme is available on the website http://privacyforum.eu/programme and registration is available at http://privacyforum.eu/programme/registration. Note: registration is required by the end of September 2012.
27th Nov. 2012	Lisbon, Portugal	BIC International Advisory Group meeting and Workshop	As Lisbon is a good gateway for the BIC countries, the BIC forum would be 27th Nov. 2012 and would consist of the International Advisory Group (IAG) meeting (by invitation only) in the morning and an open forum workshop in the afternoon. This would raise impact for both BIC and the 2012 Africa-EU Cooperation Forum, which starts on 28th Nov.

Date	Venue	Event	Description
			2012
28-29th Nov. 2012	Lisbon, Portugal	2012 Africa-EU Cooperation Forum on ICT'	Now in its 5th edition, 2012 Africa-EU Cooperation Forum on ICT will be held in Lisbon (Portugal) on Nov. 28-29, 2012.

5.4 Registered Attendees

Name	Organisation	Country
Alvis Ancans	European Commission	Belgium
Henning Arendt	@bc	Germany
Vlad Arsene	Mira Telecom	Romania
Behzad Bordbar	University of Birmingham	United Kingdom
Karima Boudaoud	I3S Laboratory - University of Nice Sophia Antipolis/CNRS	France
Manmohan Chaturvedi	IIT Delhi	India
James Clarke	Waterford Institute of Technology - TSSG	Ireland
Marijke Coetzee	University of Johannesburg	South Africa
Alberto Crespo	Atos Spain S.A.	Spain
Paul Cunningham	IIMC International Information Management	Ireland
Claudia Diaz	COSIC	KU Leuven
Rado Faletic	Forum for European-Australian Science & Technology cooperation	Australia
Carmen Fernandez Gago	University of Malaga	Spain
Gerardo Fernandez Navarrete	NICS Lab - University of Malaga	Spain
Kraus Fernando	Atos Spain	Spain
Katrin Franke	Norwegian Information Security Laboratory	Norway
Alan Hartman	IBM	Israel
Sotiris Ioannidis	FORTH	Greece
Vishal Jain	451 Research	United Kingdom
Ashok Kar	Infra Technologies	France
Katja Legisa	TESEO	Belgium
Lefteris Leondaridis	NetSmart S.A. Greece	

Name	Organisation	Country
John C.Mallery	CSAIL	Massachusetts Institute of Technology
Fabio Martinelli	National Research Council of Italy	Italy
Alberto Masoni	INFN - National Institute of Nuclear Physics	Italy
Kay Matzner	Fraunhofer Institute for Factory Operation und Automation	Germany
Mounib Mekhilef	Ability Europe Ltd.	France
Martin Muehleck	European Commission	DG INFSO
Syed Naqvi	CETIC	Belgium
Nick Papanikolaou	HP Labs	United Kingdom
Bart Preneel	COSIC	KU Leuven
Michel Riguidel	Telecom ParisTech	France
Julián Seseña	ROSE VISION	Spain
Abhishek Sharma	Beyond Evolution Tech Solution Pvt. Ltd.	India
Parminder Jeet Singh	IT for Change	India
Priscila Solis Barreto	University of Brasilia	Brazil
Neeraj Suri	TU Darmstadt	Germany
Barend Taute	Council for Scientific and Industrial Research Meraka Institute	South Africa
Camille Torrenti	Sigma Orionis	France
Yolanda Ursa	INMARK	Spain

Annexe 1. UN Resolution – Creation of a global culture of cybersecurity

United Nations
General Assembly

A/RES/57/239
Distr.: General
31 January 2003

Fifty-seventh session
Agenda item 84 (*c*)

Resolution adopted by the General Assembly

[*on the report of the Second Committee (A/57/529/Add.3)*]

57/239. Creation of a global culture of cybersecurity

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the information society,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Aware also that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society,

Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity through the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all, *Noting also* the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies,

1. *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;

2. *Invites* all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;

3. *Invites* Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005;

5. *Stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity.

78th plenary meeting
20 December 2002

Annexe

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ("participants") must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(*a*) *Awareness.* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(*b*) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(*c*) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(d) Ethics. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(*e*) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(*f*) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(*g*) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(*h*) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(*i*) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

Annexe 2. Proposal for Coordination and Multi-Lateral Approach in International Cooperation

As presented by BIC International Advisory Group (IAG) member, Abhishek Sharma, beTS, of Gurgaon, India during the workshop.

As shown in Figure 9 of this report, the BIC International Advisory Group (IAG), is positioned to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC IAG TOR, have been formed comprising specialists from different countries and different specializations. Indeed, these WGs form the backbone of the Project; however, they alone would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and Sub-Groups in a structured manner, at the management and functional level with defined focus area, role and responsibilities.

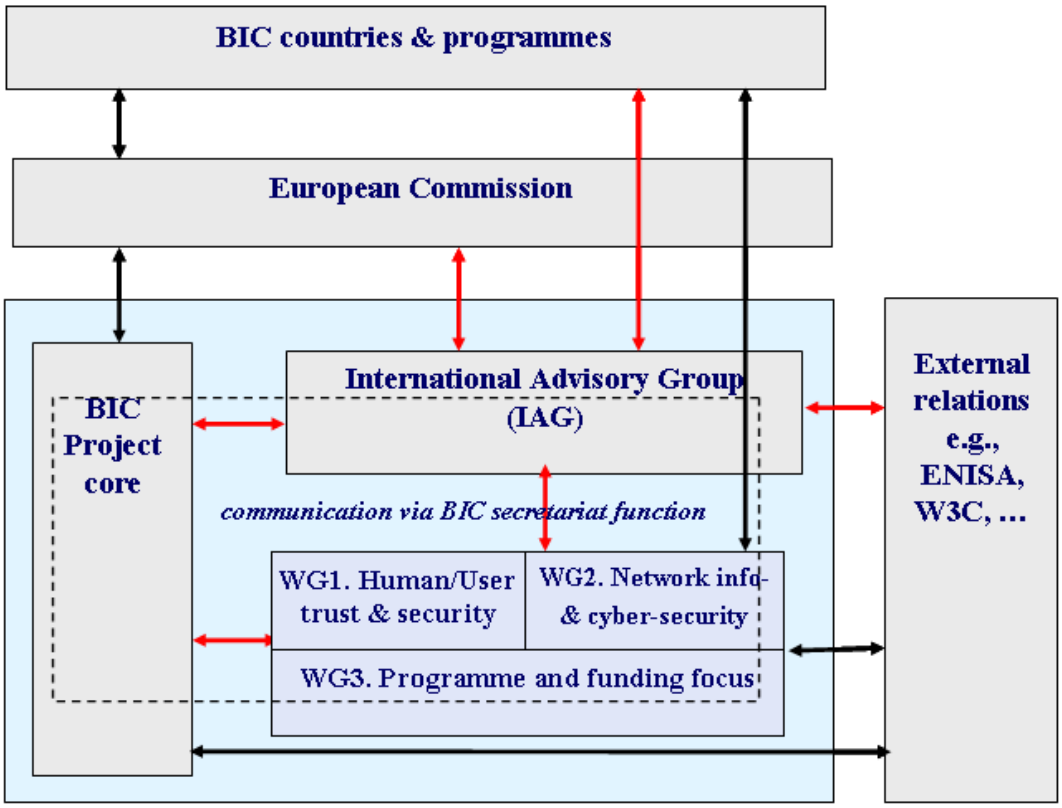


Figure 9. Overall structure of BIC project and external bodies

Since the nature of the project requires interactions amongst all participant countries to share the information, resources etc, the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. EU-India, EU- Brazil, EU- SA etc to multi-lateral approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

The following structure is thus proposed.

1. Coordination Group Structure

A multi-lateral supervisory structure under the auspices of the International advisory Group (IAG) with three main layers is proposed:

1. A Core Working Group (CWG);
2. Extended Working Groups (EWGs) – specific for each participating country
3. Special Function Groups (SFGs) – operating under EWGs as specialists at functional level.

2. The suggested role and function of this structure is as follows:

The CWG is at present constituted with three working groups WG1, WG2 and WG3 with representation from all participant countries and people chosen from different specialization. The composition of the CWG, with the three WGs at present, may be reviewed from time to time to assess if these WGs are adequate to cover all aspects of the projects or if any new aspects have emerged or any gaps are being observed for which additional WGs would be needed.

The role of the CWG is to address Strategy formulation, define high level objectives of the project and create a high level management structure and work flow processes to guide the project in the desired direction duly providing required support and assuming the overall leadership cum ownership position.

The CWG should be supported by Extended Working Groups (EWGs) which needs to be formed at each member country (see figure 10). The CWG should define the eligibility criteria for EWG members. The country representatives within the CWG should then take up the responsibility of forming the EWG of the respective countries selecting out of the eligible individuals, Research Institutes and the companies, mainly SMEs. Voluntary participation should be one of the main criteria to join the EWG. The EWG members would be the key functional entities whose primary role would be to steer the project within the country.

EWG would undertake the ownership of the following responsibilities:

I. Identify local functionaries: Researchers, Govt., Industry

II. Form a country specific consortium of functional entities with defined objectives, functions and deliverables. This consortium of functional entities may be labelled as Special Function Group (SFG)

III. Explain & Promote CWG Objectives & specific requirements to SFG by various means e.g. organizing regular workshops, seminars, events, interacting personally with other researchers and Govt. bodies thereby help forming a wider community.

IV. Prepare the project plan, in accordance with Project Objective and with emphasis on Project Cost, Resource Requirements and time frame/ time lines with the major involvement and support of the SFG.

V. Function as operational link between the CWG and SFG.

VI. Monitor & Manage In-Country progress through regular meetings/ Conferences.

VII. Gather Inputs & Process them: Analyze, Filter & Forward.

VIII. Become a functional element for Multi-Lateral Cooperation, in that:

- Interact closely with CWG and also EWGs of other countries

- Establish effective cooperation with other EWGs to share the work and resources mutually, in sync with the CWG.
- Encourage and Support SFGs for multi-lateral cooperation.

IX. Help prepare & consolidate Budgetary Estimates. If required, they will also help initiating the Proposals duly coordinating with CWG.

X. Act as Committed Process Owners.

CWG would undertake the ownership of the following responsibilities:

I. Identifying, coordinating and consolidating the Research and Technology Development (RTD) work of EWGs

II. Monitoring the progress of EWGs and ensuring sustained focus.

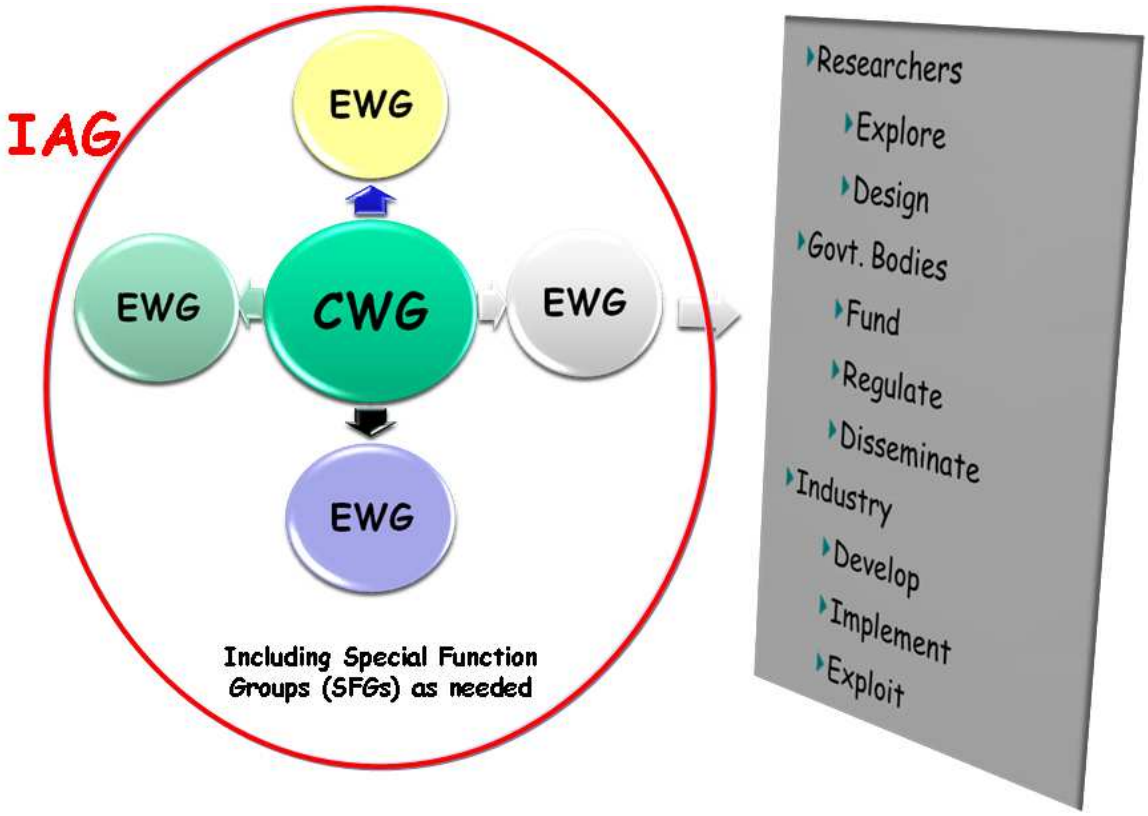


Figure 10. Basic structure of Core Working Groups and External Working Groups

3. Priority Areas for Research & Development (PARD):

Having formed the EWGs, CWG creates a high level list of Priority Areas for Research & Development (PARD) work and provides this list to EWGs for their respective assessment and opting for topics for the projects.

EWG interacts with SFGs, analyses the list of research area provided and reverts to CWG with their Proposed List of the Projects of Interest (PLPI).

CWG analyzes the PLPI, selects the priority projects and consolidates all such project lists to prepare the List of Selected Projects.

4. Project Assignment & Planning :

On finalization of the Selected Project, assignment of the same to EWGs is done by CWG where the commitment of EWGs is obtained. Having assigned the projects, the next steps are the following:

I. Prepare High Level Action Plan (HLAP)

II. Develop Macro Project Plan (MPP): Services of experienced Project Management professionals are obtained who are inducted at the CWG and EWG level at this stage. The MPP is prepared based on the micro level project plan obtained from EWGs.

III. Consolidate and finalize the MPP for each EWG.

IV. Analyze & Approve Project Resources as duly analyzed and proposed by EWGs.

V. Budgetary Estimates are consolidated. Process for Allocation & Release of Funds and Disbursement Mechanism are also finalized along with the criteria and plan for disbursement. This may be done in sync with EC standards and processes.

Monitoring & Review Process: Define the process specifying Schedule, Milestones & Benchmarks

Prepare Long Term Strategy: This should incorporate the following:

I. Provision for New Challenges & Threats,

II. Policy Review & Course Correction,

III. New Projects and

IV. Backup provisions for Management Team.

5. Conclusions

Strategy plays the most crucial role for the success of any project. When the size and complexities of the project assumes international dimensions, it is incumbent upon the main body to work out a proper strategy and define structures and processes. However, while on one hand it is essential to observe strict discipline to execute the projects as per plan, despite taking all care and precautions, possibility of unexpected future developments and new projects/ prospects cannot be ruled out. It would, therefore, be wise to incorporate provisions for flexibility and future changes in case of such wide and complex projects.