BIC session on Building a long term INCO strategy in Trustworthy ICT

System Security and Cyber-Defence:
requirements for an international approach to technological challenges and open issues

6 July 2011

Location: During SysSec workshop at Vrije Universiteit, Amsterdam

http://www.cs.vu.nl/dimva2011/venue.shtml

Table of Contents

Executive Summary

This EU FP7 BIC project[1] is organising a session as a step in the development of plans and proposals for international collaboration in research towards a vision of cyber-space that supports fundamental freedoms, privacy and the free flow of information in a secure and reliable manner, while protecting the essential information infrastructures on which we depend. The session is being held on 6th July 2011, afternoon of the SysSec workshop Venue: Vrije Universiteit, Amsterdam– see http://www.cs.vu.nl/dimva2011/venue.shtml.

The session will:

- Address the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT
- Explore *Frameworks for Data Sharing*, as a specific enabler for collective defence and response to cyber-attack.

Session Goals

- Prepare the ground for the extended BIC workshop being planned for 2011, Q4;
- Clarify scope for international collaboration on cyber-security;
- Develop the Secure International Data Exchange Architecture for Cybersecurity, introduced at the May, 2010 workshop to explore the technical and organisational requirements and constraints.

International Data Exchange

The exchange and sharing between responsible states and organisations of information and intelligence on cyber-attacks is seen as an essential component of collective cyber-defence against malicious action (as well as accidents and flaws). It is central to the ability to anticipate and respond: longer-term in the preparation of strategic, collective defensive measures, and short-term in recognising, isolating, and recovering from, attack – threatened or actual.

Participation and Contributions requested

The time allocated for the session is 90 minutes. Therefore, brief presentations and written positions are being invited for the five moderated topic areas for discussion [2-3 slides maximum and position papers can be in supportive text]:

1. Motivation and vision
2. Threat models, actors and capabilities
3. Technologies to support the International Data Exchange Architecture
4. Legal, regulatory, political, social, economic, and environmental challenges
5. Next steps for planning

Submissions must reach the organisers by 30-June-2011 for inclusion in the discussions and the proceedings. Please email directly to jclarke@tssg.org.

Additional details on the structure, scope, motivation and approach of the session can be found on the following pages.

We look forward to your active participation. The organising committee:

Jim Clarke, Waterford Institute of Technology, Ireland
Evangelos Markatos, FORTH, Greece,
John C. Mallery, MIT, USA
Aljosa Pasic, ATOS Origin, Spain
Karl Levitt, The University of California, Davis, USA
Neeraj Suri, TUD, Germany
Michel Riguidel, Telecom Paris-Tech, France
Rebecca Wright, Rutgers University, USA

[1] FP7 Coordination and Support Action BIC: Building International Cooperation for Trustworthy ICT http://www.bic-trust.eu/

Structure of the session

The session will explore and elaborate the following topics as aspects of an International Data Exchange Architecture. A broader by-product will be scope and priorities for international R&D collaboration.

Topic 1. Motivation and Vision (20 minutes)

- What are we doing and why?
- What are the expected impacts?
- What kind of data should we share?
- What kind of collaborations do we need?
- What kind of analysis do we need?
- What are the incentives to participate?
- What are the risks?

Topic 2. Threat Actors (10 minutes)

- Who are the threat actors and what are their capabilities?
- What threat models follow from the actors' business models and capabilities?
- How are consequences of breach or disruption assessed and their criticality determined?

Topic 3. Technologies to support International Data exchange architecture (45')

- Review of the straw man architecture in more detail
- What are the enablers eg. Cryptography based obfuscation, sensors on the network, monitoring traffic capabilities
- Basics of how we share recognizable data, especially on critical infrastructures and across different countries. eg. share patterns for recognizing advanced persistent threats without losing efficacy if they are exposed. What obfuscation and security measures would make patterns easier to share?
- Architecting for leakage and resilience under compromise.

Topic 4. Legal, Regulatory, political environment challenges (15')

- What challenges arise when dealing across multiple sectors and countries.
- How are these best addressed at a transnational level
- How are legal and regulatory issues including privacy, corporate responsibility best managed in order to improve coordinated defence?

Topic 5. Next steps for planning (25')

- What are the concrete next steps until the next event (expected Q4 2011)?
- How can we motivate countries to contribute and support the effort?
- See more details in agenda (next section)

Final Agenda of BIC session

Time	Description	Speakers
13:30 – 13:35	Overview / Purpose of Session	Jim Clarke, Waterford Institute of Technology -TSSG
13:35 – 13:55	Part 1. Motivation and Vision: Opening remarks US perspective EU perspective	 Samuel Weber, National Science Foundation, USA Karl Levitt, Univ. of California Davis Barbara Daskala, ENISA
13:55 – 14:05	Part 2. Threats and Actors	Sotiris Ioannidis, FORTH
14:05 – 14:50	Part 3. Technologies To Support International Data Exchange And Collaborative Analysis: Straw man architecture Data exchange architecture used in a financial application in South Africa. Identity related issues for data handling and aggregation	 John C. Mallery, Massachusetts Institute of Technology; Barend Taute, The Council for Scientific and Industrial Research (CSIR), South Africa; Glenn Gran, IKED. GINI SA project
14:50 – 15:05	Part 4. Legal, Regulatory, Privacy, and Political Challenges	Jody Westby, Global Cyber Risk LLC, Carnegie Mellon CYLAB
15:05 – 15:30	Part 5. Next steps for planning of workshop in Q4 2011 • Determining a comprehensive coverage of topics required; any gaps? • Identifying key topics for a workshop to be held in the Fall '11 (see next pages for initial draft terms of reference); • Identify Organising and Program committee; • Identifying the necessary participants; • Identify how to best collaborate between now and then (eg. establishment of working groups, electronic, ….)	BIC partners, interactive

BIC Fall Workshop Draft Terms of Reference *(Initial draft)*

Mission: Develop an international architecture for cyber data sharing and collaborative analysis that reduce threats to participants effectively. Catalogue the research and development requirements for medium- and long-term architectures.

Objectives: the workshop aims to achieve the following outcomes:

- Characterize architectures for cyber data sharing and collaborative analysis that enhance situational awareness and are effective for reducing operational threats
- Identify needed R&D necessary to enable and support sharing and collaboration, including secure computing, communications and storage
- Identify legal, regulatory, treaty or policy moves necessary to enable effective sharing and collaboration
- Help create supporting partnerships;
- Identify organizations that will fund, develop and implement the architectures
- Produce a statement of the benefits of such an activity for policy makers.

Proposed Dates: October 27-28, or November 3-4, 2011

Location: London or Brussels under consideration

Topics for consideration

1. Secure hosts
2. Secure and resilient storage
3. Remote policy enforcement
4. High leverage data for collection
5. PII anonymization techniques
6. High integrity monitoring and communications
7. Analytical techniques for threat identification
8. Visualization techniques for understanding threats
9. Techniques for rapid sharing of threat data and remediation techniques
10. Legal harmonization, including privacy protection
11. Economics of cybersecurity
12. How to best leverage international research communities
13. Incremental revelation techniques
14. Authorization systems, including authentication and crypto support
15. Cryptographic techniques for aggregating information while protecting source anonymity
16. Review of industry sharing best cases
17. Review of national sharing best cases
18. Review of international sharing best cases.

Scope and Objectives

The vision is for a cyber-space that supports fundamental freedoms, privacy and the free flow of information in a secure and reliable manner, while protecting the essential information infrastructures on which we depend.

This session is a stage in the development of plans and proposals for international research collaboration towards this vision. It will:

- Address the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT
- Explore basis of an Architecture for Data Exchange and Sharing, as a specific enabler for collective defence and response to cyber-attack.

The focus of this session is scoping, planning and prioritising what needs to be done and by whom in developing an international data exchange architecture as a key enabler for global cybersecurity. In this session, we will identify the relevant stakeholders and determine what the community needs to accomplish together in follow up work follow up work (via electronic means) until the next step, which would be a larger workshop, expected in the fourth quarter of 2011.

Your invited contribution before and during the session

Before the session, participants are welcomed to submit presentations and supporting position papers. Presentations should consist of maximum three slides for each of the topics above you would like to contribute to during the session (note: you can contribute to more than one if there is enough time to schedule them all).

Slide 1 is intended to provide an overview snapshot on the points you would like to make and/or issues or challenges you have identified on the topic(s) and

Slide 2 is intended to provide more details on the topic(s).

Slide 3 contains name(s) of contributor(s), organization(s) and relevant references.

Please fill in a separate set of slides for each topic if you are presenting in more than one topic.

In addition, it would be very advantageous for participants that would like to present to submit a short position paper on the topics and the following sections here can be used as a starting point or as background information as a guide for your position paper and slides contributions.

Note: The organizers must have the contributions by 30th June 2011 due to the short timing of the session and the need to plan the talks for each panel in the correct ordering.

Please email them to jclarke@tssg.org so they can be reviewed and pre-loaded on the machine.

Background

Motivations

The quantity and seriousness of cyber attacks have been growing over the past six years and have surged over the last three months. Although there have been real improvements of aspects of cyber defences, threats and attacks have been outpacing them. Recent attacks have taken various forms from spear phishing email accounts as a foothold into other organizations, infiltration of international economic bodies (possibly with insider advantage), and other neo-mercantilist industrial espionage. Added to these, there is also growing ideological hacktivism and an embrionic threat of cyber-terrorism against critical services and infrastructures as it has not yet emerged as an attack source even if they use ICT to recruit and coordinate.

Cybersecurity is now receiving high priority on a joint bi-lateral collaboration bases. Some recent examples are highlighted here:

- *EU–US INCO-Trust workshop* of May 2010 [1],
- *US-UK Cyber Communiqué* of 25th May 2011[2],
- recent accession to the *Budapest Convention on Cybercrime* [3],
- 28th Annual International Workshop on Global Security on June 16, 2011 [4], and
- Vienna Security conference, 1st July 2011 [5].

A key message from all of these is an acknowledgement that international cooperation is at a nascent stage and a more global approach urgently needs to be taken as there is ultimately just one, single global domain within the information environment, consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between all countries. We need comprehensive research towards international intelligence, surveillance, and reconnaissance (ISR) in the cyberspace domain. The anticipated benefits of an international data exchange system include:

- **Data exchange and sharing capabilities** for monitoring of trends with availability of retrodictive cyber statistics across the OECD; enhanced anti-crime counter-measures better identifying cyber crime targets, vectors, methods, and counter-measures; closing defensive gaps with better defensive coordination and best practices; and enhancement of IP protection with the detection and prevention of industrial espionage.

- **Expertise integration** to focus collective expertise on important cyber data and analysis tasks.

- **Collaboration and coordination** reducing defensive gaps across the OECD and better crisis response.

- **Research and development coordination** to leverage and combine national expertise.

Our approach

The report of the May 2010 joint workshop [1] states that the EU and US Programme Management "*… are committed to furthering international collaboration, especially in the areas of international data exchange, security, trust, and privacy. Moreover, the active participation within the workshop of the and research communities of Korea, Japan, Canada, Australia, South Africa, and Brazil, is a clear indication that these countries are also interested in furthering collaboration on these important subjects*."

Therefore, the aim of this session is to continue the work that was started during the earlier workshop, specifically the topic of a Secure International Data Exchange Architecture for Cybersecurity outlined by the *Technical Challenges for Transnational Repositories* session [6]. Such a capability would reduce defensive gaps across the contributing states, and build crisis-response capacity and an international system for data exchange related to cyber crime. This would include attack patterns and '*signatures*', best defence practices, and response and recovery – individual and collective. This would greatly improve defensive understanding and coordination resulting in biasing the successful work factors for cyber attack and defense in favor of defenders.

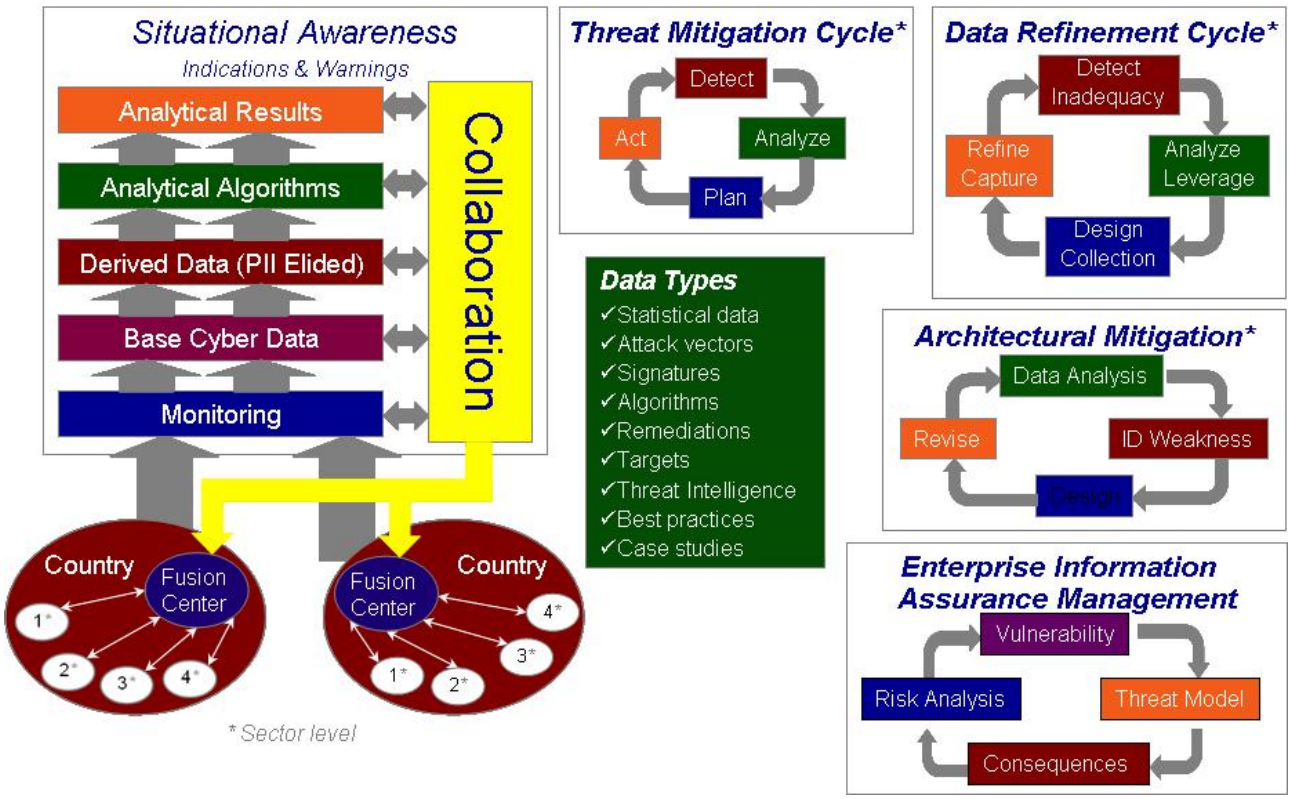

Figure 1 – Straw-man architecture for Int'l data exchange

At the workshop in May 2010, as shown in **Figure 1**, a straw-man architecture was generated and this will be used as a starting point for the session discussions on 6th July 2011. The purpose of the session is to bring this work to the next level and commitment to the research and development coordination, which will enhance the outcomes through tactical planning, leveraging and combining task-relevant national expertise.

Outline of Straw-man Architecture

Malicious actors[2] 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. In this workshop, we will develop and refine visions of such architecture and use these conceptualizations to identify and prioritize what is needed in the medium- and long-term research. For example,

- What kind of data sharing and collaborative analysis architecture could be built with today's technologies and operational knowledge?
- Who are the current actors around the globe and what are their approaches and can these be leveraged and harmonized together?
- What are the gaps?
- What research would be needed to build a better architecture in the 5-10 year time frame?
- Who are the actors needed to carry out this research and where are they from?
- What organizational modes are necessary for this research to proceed most expeditiously?
- What funding sources and mechanisms can be mobilized to support the joint efforts required?
- The rationale for designing and building sophisticated architectures for international cyber data sharing, collaborative analysis, and collective defense are as follows:
- Dramatically improve defensive coordination to move the advantage away from offense in favour of defence;
- Create shared real-time situational awareness;
- Identify cyber data for sharing together with leverage scenarios and collection issues;
- Motivate targeted research to enable effective collection, sharing, analysis and response.

A strong focus of the session will be on starting answering key research questions, for example:

1. **Data:** What cyber data should be shared?
2. **Analysis:** How can data be effectively analysed?
3. **Impact:** How will it help participating countries?
4. **Synergies:** What synergies arise from integrating data across national boundaries?
5. **Incentives:** What are the incentives for providing data?
6. **Quality:** How can the integrity and quality of data be assured?

[2] cyber criminals, adversarial national intelligence agencies, hacktivists, and cyber terrorists for starters

7. **Availability:** How can data be made available in useful formats and in time to be relevant?
8. **Collaboration:** How can relevant expertise be focused on priority issues to achieve synergistic outcomes?
9. **Threat Mitigation:** How can the entire infrastructure support rapid or proactive response to emerging threats?
10. **Risk:** How should data sharing risks be managed?
    - What risks are involved in assembling and sharing data?
    - How can data be sliced, compartmentalized or aggregated to reduce risks?
    - How can access be controlled with incremental revelation to reduce risks while enabling benefits?
    - How can different levels of trust be managed over time?
    - What computer and storage architectures will be needed?
    - What network architectures can enable high availability and secure communications?
    - What cryptographic support is required?
    - What kinds of authentication and authorization systems will be needed?
    - How can sharing systems protect against insider and supply chain risks?
11. **Legal Enablers:** How to manage legal and regulatory issues including privacy, corporate responsibility in order to improve coordinated defence?
12. **Learning:** How can learning at all levels be enhanced and cross-pollinated to outpace adaptations by malicious actors?

References

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

[2] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

[3] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

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

[5] 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

[6] Mallery, John., CSAIL, MIT, http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/position.html

Annex I BIC[3] Session Terms of Reference

To capitalise on the presence of a large group of system security research communities, the BIC session is held within the SysSec workshop[4] on 6th July, 2011. **Note: there are a number of co-located events of interest-** EffectsPlus Clusters Workshop[5] on 4/5th July and DIMVA 2011[6], one of Europe's leading security events.

The session will focus on the mid term (present – 2013) to longer term (2014 – 2020) strategies for sharing skills, common tools and techniques for the development of an **International data exchange and collaboration architecture for the scalable cyber-defense coordination.** Within this topic, a number of relevant sub-topics can be covered, including:

- Development of an architecture for International sharing of data and expert collaboration relevant to cybersecurity;
- High leverage cyber data to help track threats in real-time and mitigate them with short term manoeuvres or longer term feedback into architectures;
- Enabling technologies such as crypto to support sharing, secure systems to manage data, authorization frameworks to control access, and analytical techniques to understand threats;
- Cooperative frameworks to register, analyse, anticipate and mitigate emerging ICT threats within sectors and across countries;
- Aligning of data protection and privacy governance;
- Enabling legal frameworks for sectoral and international data sharing and collaboration;
- Developing a global ICT security policy based on cooperative engagement around cyber defence issues and ostracism of malicious action.
- Highlight other potential collaboration subjects that are mutually beneficial and require international collaboration in ICT Trust and Security.
- Share information about international projects already underway and generate ideas for new ones.
- Decide next steps for the collaborations.

Session Date and Location

6th July 2011, afternoon of the SysSec workshop Venue: Vrije Universiteit, Amsterdam– see http://www.cs.vu.nl/dimva2011/venue.shtml. You are welcome also to attend the 4/5th July 2011 Effectplus workshop where it is expected some initial discussions will take occur prior to the BIC session. In order to ensure space for the 4/5th July Effectplus event, please let us know ahead of time if you can attend by email to jclarke@tssg.org.

Organising Committee

Jim Clarke, Waterford Institute of Technology, Coordinator of the BIC Project
Evangelos Markatos, FORTH, Greece, SysSeC project
John C. Mallery, Massachusetts Institute of Technology, USA
Aljosa Pasic, ATOS Origin, Spain
Karl Levitt, The University of California, Davis, USA
Neeraj Suri, Technische Universitat Darmstadt, Germany
Michel Riguidel, Telecom Paris-Tech
Rebecca Wright, Rutgers University, USA

---

[3] FP7 Coordination and Support Action BIC: Building International Cooperation for Trustworthy ICT http://www.bic-trust.eu/

[4] http://www.syssec-project.eu/events/1st-syssec-workshop/

[5] http://www.effectsplus.eu/files/2011/05/Effectsplus-July-eventcall-for-contributions1.pdf

[6] http://www.cs.vu.nl/dimva2011/