BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

EU-South Africa Cooperation Workshop
(co-located with ISSA 2011 [1])

Gauteng, Johannesburg, South Africa
16th August 2011

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

Table of Contents

INTRODUCTION, MOTIVATION AND VISION

The EU Framework Programme 7 ***BIC*** project (Building International Cooperation for Trustworthy ICT*: Security, Privacy and Trust in Global Networks & Services)* [2], within the project portfolio of DG INFSO, Unit F5 ICT Trust and Security Research [3], along with the tremendous assistance of the local organising committee of ISSA 2011 [4], organised and hosted a South Africa – EU Cooperation Workshop in Gauteng, Johannesburg, South Africa on 16th August 2011 with over 80 attendees.

ISSA2011 is the annual conference for the information security community in South Africa, which has been running since 2000 and, from 2010, has been co-sponsored by the IEEE Systems, Man and Cybernetics Society (SMCS) Chapter, a chapter of the IEEE South Africa Section. In addition, ISSA2011 was held under the auspices of the University of Johannesburg Academy for Computer Science and Software Engineering, the University of South Africa School of Computing and the University of Pretoria School of Information Technology.

The setup and preparation of the BIC workshop took place over a number of months and the BIC partners relied heavily on the ISSA 2011 organisers and also on the tremendous local support from the Council for Scientific and Industrial Research (CSIR) Meraka Institute, SAP Research IA&S Africa / SAP Meraka UTD, University of Johannesburg, University of Pretoria and University of South Africa.

The overall theme of the BIC workshop was laying the ground work for building a long term strategy in international research for Trustworthy ICT between South Africa and the EU. The workshop had the following core objectives:

- Understanding the critical issues in trustworthy ICT requiring international cooperation;
- Identifying promising trust and security research directions in each country and the mutual benefit to international collaboration;
- Foster collaboration between the EU and South Africa research teams.

The organising committee of the BIC SA – EU Coordination workshop included:

Jim Clarke,	Waterford Institute of Technology, Ireland
Barend Taute,	CSIR Meraka Institute, Pretoria, South Africa
Neeraj Suri,	Technische Universitat Darmstadt, Germany
Jan Eloff,	SAP Research IA&S Africa/ SAP Meraka UTD, South Africa
Michel Riguidel,	Telecom Paris-Tech, France
Marijke Coetzee	University of Johannesburg, South Africa
Aljosa Pasic,	AtoS, Spain
Marianne Loock	University of South Africa, South Africa
Hein S. Venter	University of Pretoria, South Africa

Further information on the workshop and identified topics for mutual cooperation are contained within the report and on the workshop web site at http://www.bic-trust.eu/events/event/eu-%E2%80%93-south-africa-cooperation-workshop/.

AGENDA

Time	Description	Speakers
08:00– 08:15	Session 1. Building International cooperation between South Africa and EU in Trustworthy ICT.	Session chair: Dr Barend Taute, CSIR Meraka Institute
08:15 – 08:30	Welcome address	Professor Hein S. Venter, University of Pretoria
08:30 – 10:00	Building a long term strategy for International cooperation in Trustworthy ICT between EU and South Africa Trustworthy ICT and Cyber Security Research – Adding value from an African perspective. Trustworthiness in Cloud Computing. A way forward to engender global cooperation Cyberspace – A growing underground economy	James Clarke, Waterford Institute of Technology, Waterford, Ireland Prof Sebastiaan von Solms, University of Johannesburg, South Africa Prof Neeraj Suri, TU Darmstadt, Germany Colonel Beaunard Grobler, South African Police Service (SAPS), South Africa
10:00 – 10:30	Coffee break and networking	
	Session 2. Building International cooperation in Trustworthy ICT.	Session chair: Jim Clarke, Waterford IT, BIC coordinator.
10:30 – 12:00	Future Internet in Europe: an overview of related initiatives and ICT trust and security challenges Enabling services for secure eBanking in South Africa New models of communication and security for the Future Internet Technologies for Emerging Economies – Security?	Aljosa Pasic, AtoS, Spain Dr Buks Louwrens and Mr Gideon Serfontein, SABRIC, South Africa Prof Michel Riguidel, Telecom ParisTech, ENST, Paris, France Prof Jan Eloff, Research Director (SAP Research IA&S Africa / SAP Meraka UTD) and Professor Marijke Coetzee, University of Johannesburg, South Africa
12:00 – 13:00	Lunch and networking	
13:00 – 16:00	Organisers wrap up session • Determining a comprehensive coverage of INCO topics required. • Identifying key themes for an EU – SA workshop to be held at EuroAfrica - ICT- 2011 in November 2011.	Session chair: Jim Clarke, Waterford IT, BIC coordinator. BIC partners and organising committee members and others.

SUMMARY OF DISCUSSIONS

During the afternoon of the BIC workshop, there was a session dedicated to going over the results of the morning sessions and brainstorming further on the potential topics for cooperation between the research communities engaged within trustworthy ICT in both countries. The workshop organisers and some interested others (from the EU and South Africa) held the dedicated session in order to quickly summarise the presentations and discussions from the morning sessions into a skeleton format in order to be elaborated rather quickly into a report version included here. Due to recent developments taking place in EU – Africa cooperation within FP7, it was decided there was a need to quickly highlight the main areas of potential cooperation between the EU and South Africa research communities in order to feed into the planning phases for the conference and a dedicated workshop on Trustworthy ICT to be held during Euro-Africa-ICT 2011 [5] conference being held over 14 – 15th November 2011.

The following topics were elaborated during the workshop and found to be of interest to both countries.

1. Trust Management for techno-socio business ecosystems in the context of Emerging Economies

A techno-socio business ecosystem in the context of Emerging Economies is defined as a collaborative on-line and real time trading environment where large enterprises (LEs) such as suppliers and financial institutions transact with Very Small Enterprises (VSEs) such as small retail stores. In the majority of cases these VSEs are operating from remote and rural areas and have a lack of ICT infrastructure. VSEs use mobile phones to interact with the techno-socio business ecosystem.

Many sociological and cultural differences prevent the trusted interaction amongst VSEs; between LEs and VSEs; and in general between rural communities and mainstream commerce.

As there is a large level of variation in the acceptance of social and other controls that govern trust between the different types of participants in these business ecosystems, this poses a major challenge. In order to support collaboration and interaction, the development of an “indigenous trust model” for such communities is required. An “indigenous trust model” in the context of this proposal is a model that reflects the unique requirements of emerging economies such as the concept of focusing on people's allegiances (Ubuntu). A trust model needs to be defined over the premises that rural participants, such as VSEs, may be more likely to trust an application (technological system) if they experience a sense of normality because their familiar social controls are present in the systems.

As the concept of community and community leaders is of special importance to rural people in the African context, it is suggested that this concept be

incorporated in trust models for deploying technology (applications) in these communities. Consider for example the following:

- The formation of groups and clusters of people in local communities. These groups are formed not only on similar types of participants but also on similar needs. A good example in South Africa is the concept of "Stokvel" whereby a syndicate of people does pooling of financial resources.
- Community leaders as moderators of trust. This is useful where a participant needs to transact with a stranger who is part of a community as the community leader may provide a trusted introduction.

The envisaged trust model for mobile applications in emerging economies will be based on agent technology that collects and stores feedback about participants, build reputation of participants and share reputation information with others.

2. International Cyber security research – added value of the African perspective

A question that was raised a number of occasions during the BIC workshop was: *"Could Africa become the home of the world's largest botnet or an unbridled cyber security pandemic?"* This is at least a possible scenario given the fast pace of increased broadband (and largely wireless) internet penetration in Africa where there is currently very low broadband penetration in many areas, high levels of computer illiteracy, sometimes ineffective legislation, and where anti-virus software may be un-affordable or too technically sophisticated for the low-cost devices that are still used. This heterogeneous continent harbours a large socio-techno digital divide that needs to be accounted for in first-world security solutions since this world is connected to the developed world through the opportunities and challenges of the internet.

International, collaborative research can address these challenges by looking at a variety of approaches that require innovative implementation, including:

- ISPs taking a bigger role / responsibility with the provision of security services so that much less depends critically on the end user (ie creating "thin clients" vs the "thick client" where the ISP only provides the pipeline).
- Bottom-up, community oriented approaches to Critical Information Infrastructure Protection.
- Sector based cyber security alliances (universities, industries, banks) that share information / best practice.
- Opening up international data-exchange architectures for cyber security.
- Models and platforms for national and regional cybersecurity coordination (citizens, industry, security sector, government, regional governments).

3. Financial Infrastructure protection

The financial sector is particularly challenged by their need for providing secure eBanking in the face of a barrage of sophisticated, creative, efficient and persistent phishing attacks. The banks are providing competitive eBanking services for computers and mobile devices but regard reducing and fighting crime as a shared and non-competitive responsibility. This can benefit hugely from public-private-partnerships including the current close cooperation with the Police as well as local and international research collaboration on issues such as:

- Mathematic analysis of normal vs abnormal patterns in banking behaviour.
- Packaging abnormal behaviour (suspicious behaviour, attack vectors).
- Anonymising the shared data and information to effectively address concerns about reputation loss, paramount client privacy and anti-competition laws.
- Establishing a Financial Sector Computer Security Incident Response Team (CSIRT) that meets international standards for reducing risk and responding to incidents. SA has already had collaboration with ENISA, EU CSIRTs, USA and others.
- Leveraging technical developments in the mobile and cellular networks to provide increased trust as well as usability of eBanking solutions.

4. South African Law Enforcement approaches to deal with cybercrime

The SA Law Enforcement agencies have to deal with a variety of cyber crimes with significant criminal intent including increasingly sophisticated social engineering, customised Trojans and commercial spyware, computers and information for sale, “ransomware” (the next level “scareware”), attacks on mobile devices and even signs of attacks on automobile computer systems. There are strong signs of this being organised cyber crime with the criminals operating directly or by proxy from just about anywhere in the world.

This is already addressed through closely intertwined and good relations between law enforcement and technology providers e.g. ISPs on a national basis, adopting a mutually supportive strategy. These relationships assist with the capturing and justly punishing of the cybercriminal which is necessary in order to impact their business models. However, there is still a large gap between sentencing for physical crime vs cybercrime.

International, collaborative research should give direction to the serious challenges with the prevention/combating, investigation and prosecution of cross border cyber crime. This requires adaption of everything from policy to legislation to technology strategy.

Better coordination of the country’s cross border cyber crime detection and prevention is not currently prioritised. How can this effectively be elevated to the highest authority? What is the national “business case” for increased attention, coordination and funding?

5. EU approach towards trust and security in the Future Internet

South Africa does not currently have an active debate regarding the Future Internet, as is the case in Europe and elsewhere. This crucial debate is shaping the creation of the next generation of the Internet with an increase of Internet based services. The physical and virtual worlds are converging. There is a revolution in data networks such as LTE. Open delivery platforms are becoming the norm.

While the developing world including South Africa is catching up and mobilising the current Internet, and wrestling with the trust, security and privacy issues that it brings, it also needs to be ready for the Future Internet. This is as true for governments as it is for industry, and it is clear that any Future Internet will require significant public-private-partnerships.

The EU can assist through collaborative international research enabled by the ongoing Future Internet activities and these were discussed during the workshop. Examples include the FI-PPP and the Future Internet Assembly in which a number of the participants are key members.

CONCLUSIONS

A successful workshop was held in order to begin the process of identifying topics of cooperation that would be of mutual benefit to the EU and South Africa in the research fields of ICT Trust and Security.

A number of follow up activities were identified that would benefit and increase collaboration between the EU and South Africa research teams:

- 4th EuroAfrica-ICT Cooperation Forum on ICT Research, 14-15 November 2011, Cape Town, South Africa: Session 1d will be on Building International Collaboration on Trustworthy ICT, including presentations from the BIC project team members. With the broader African / European attendance, this session will be used to convey the outcomes of the BIC Workshop at the ISSA2011 conference and add further value and clarity to joint EU/Africa research priorities in Trustworthy ICT.
- South African Trust and Security Research Database: Establishing such a database will be taken up with the ISSA conference organisers as a way of supporting international collaboration and access to knowledge and research skills. This will also be cross - correlated with the work being done in BIC in building the trust and security research community.
- The University of Johannesburg is driving the establishment of a South African Academic Cybersecurity Alliance that will, among other things, arrange a yearly Cybersecurity Awareness Day that could link with international awareness efforts.

ACKNOWLEDGEMENTS

The BIC project [1] is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research [2].

The BIC project would like to acknowledge the support of the organizing committee members of ISSA 2011 [4], most especially to those that took part in the organizing committee of the BIC workshop.

The BIC project would also like to acknowledge the tremendous support of Dr. Barend Taute of CSIR Meraka Institute in Pretoria for all of his extra efforts and assistance in the organisation and running of the BIC workshop.

Finally, the BIC project would like to thank all of the speakers and participants. The slides for the workshop are available at http://www.bic-trust.eu/events/event/eu-%E2%80%93-south-africa-cooperation-workshop/.

REFERENCES

[1] ISSA2011 web site http://www.infosecsa.co.za/intro.html

[2] BIC web site http://www.bic-trust.eu

[3] DG INFSO Unit F5 web site http://cordis.europa.eu/fp7/ict/security/

[4] ISSA 2011 organising committee members http://www.infosecsa.co.za/committee.html

[5] Euro-Africa-ICT web site http://euroafrica-ict.org/events/cooperation-forums/2011-cooperation-forum/agenda_at_a_glance/