DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC 2013)

Malaga, Spain, June 6–7, 2013

Organizing Committee

James Clarke, Waterford Institute of Technology - TSSG, (co-chair)
Rebecca Wright, Rutgers University, (co-chair)
Julie Grady, HP Labs Bristol
Aljosa Pasic, ATOS
Siani Pearson, HP Labs Bristol
Keyun Ruan, University College, Dublin (UCD)

Rapporteurs

Session 1 - Lenore Zuck, University of Illinois at Chicago
Session 2 - Nick Papanikolaou, HP Labs, Bristol
Session 3 - James Clarke, Waterford Institute of Technology – TSSG
Session 4 - Karima Boudaoud, Ecole Polytechnique de Nice Sophia Antipolis
Session 5 - Mounib Mekhilef, Ability Europe Ltd.
Overall workshop report – Henning Arendt, @bc; Fernando Kraus Sanchez, ATOS; Michel Riguidel, Telecom Paris-Tech, and significant contributions from the organizers and rapporteurs.
Pre-proceedings publication and local support - M. Carmen Fernandez-Gago, Univ. of Malaga

Cover photo (L-R):

Manmohan Chaturvedi, Ansal University; Mike Burmester, Florida State University; Aggelos Kiayias, University of Connecticut and University of Athens; Deepak Garg, Max Planck Institute for Software Systems.

Executive Summary

Cloud computing has been widely advocated as a "game changer" and an enabler for innovation. European Commission Vice-President Neelie Kroes pledged to work towards increasing the adoption of Cloud at the Davos Summit 2012; however, she also stated that among obstacles currently impeding broader cloud adoption are lack of standards, certification, data protection, interoperability, lock-in, legal certainty, and basic trust[1].

Several EU FP7 projects and other international activities are focussing on solutions to overcome these obstacles. Two of the projects, BIC[2] and A4Cloud[3], joined together with the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS)[4], and the regional UK and Ireland branches of the Cloud Security Alliance (CSA)[5] in organising an international workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC 2013). The international workshop brought together experts from trust and security, cloud computing, forensics and other disciplines to discuss collectively how public and private sectors as well as the research communities can increase the confidence in the use of cloud computing, and how to deploy innovative services for use by citizens and businesses. The TAFC 2013[6] workshop was held in Malaga, Spain on 6-7th June 2013, in conjunction with the 7th IFIP WG 11.11 International Conference on Trust Management[7].

There were sessions related to Accountability in the Cloud; Forensics, Evidence and Accountability; Security and Trust in the Cloud; International Cooperation approaches for Trustworthy ICT including the need for trust, privacy and security models and mechanisms for international Trustworthy ICT projects, and addressing the inter-related programme management, policy and ethics challenges. The workshop was attended by over 40 participants from Australia, South Africa, Brazil, Europe, Japan, India, Canada and the United States. The speakers represented funding agencies, major universities, research organizations and companies with global reach.

The main EU emphasis, as we move from FP7 to H2020, is shifting from *Science and Technological Development* (STD) to *Research and Innovation* (R&I) where 'Innovation' means enablers for new products and methods that can be fed back into the greater good of EU economic development. Therefore, in order to start scoping ideas for the development of international projects for H2020, which is an underlying objective of this workshop, interested partners need to examine and clarify how the new R&I model in H2020 harmonizes with the funding models of the other countries, where there might be more emphasis on the *research* elements only. This is not an easy topic to converge agreement on but it is a very important one that must be discussed on both bi-lateral and multi-lateral planes.

In the US, the Secure and Trustworthy Cyberspace (SaTC) programme at the National Science Foundation (NSF) has around 60 current SaTC-funded awards directly related to cloud security with three main thrusts: 1) Trustworthiness of Cloud Providers, including functional encryption and auditing providers; 2) Protecting cloud providers from threats, including isolation between cloud customers, protecting providers from customers, detecting attacks, and avoiding privacy violations; and 3) Leveraging cloud computing to provide trustworthy applications, including enforcing differing security

1 more recently http://europa.eu/rapid/press-release_MEMO-13-654_en.htm#PR_metaPressRelease_bottom
2 http://www.bic-trust.eu/
3 http://www.a4cloud.eu/
4 http://dimacs.rutgers.edu
5 http://www.linkedin.com/company/cloud-security-alliance---UK-&-Ireland-chapter and https://cloudsecurityalliance.org
6 http://www.bic-trust.eu/events/tafc2013/
7 http://conf2013.ifiptm.org/

policies among collaborating clients and cloud-based health records. International aspects affect all three of these thrust areas, and future collaboration should include these thrusts while also addressing cultural, privacy and legal issues.

The following accountability approaches and mechanisms are identified as areas that would benefit from further international research: model contracts; binding corporate rules (BCRs); privacy management frameworks; technical standards; management standards; and privacy seals.

The panel discussions focussed on the questions: *How can accountability be defined as a concept? Can causality always be assigned? Is accountability always important? How is it possible to deal with and even guarantee against loss of data?* and conversely*, is it possible to guarantee and prove deletion* (forgetting) *of data and its traces?* International cooperation is necessary to further consider harmonisation of data protection measures.

In order to provide forensics-as-a-service and models for forensic brokerage, the different perspectives of cloud forensics need to be considered: law enforcement, security and traditional digital forensic challenges, as all pose significant challenges in organizational, technical and legal dimensions. Evidence gathering for accountable cloud computing services requires development of processes and mechanisms to monitor and audit the terms of a service-level agreement.

Concerning trust and cloud security, it is key to build the chain of trust, where the use of security standards and certification is included in the contractual terms. International cooperation is necessary to leverage the skill bases of international peers, for example for the work on cryptography, a trusted cloud architecture, trusted storage controllers, and development of collaborative threat and incident response.

Regarding the topic of policy, ethics and international cooperation, points raised were that a relevant code of ethics must always evolve to keep up-to-date with the progress in computer technology. In addition, data is being shared across borders and current regulations fail to capture the complexities involved. Ethical, privacy-preserving, accountability-enabled treatment of data requires solutions to numerous technical problems with several challenges. A truly coherent, strategic multi-lateral ICT collaborative model, rather than current disparate, tactical tightly constrained bi-lateral models, is seen as the more effective approach for aspects of international cooperation in cyber and network information security considered here.

Certain aspects of making digital content trustworthy can be achieved by using digital signatures and digital fingerprinting with the following requirements: certainty that any content has not changed since the creation date or since authorised amendment, and automatically detect if content was changed outside permitted channels with threat detection, early alarm for attempted fraud or data corruption, established provenance (who created, who witnessed, is it signed, version history, etc.) and other metadata (data type, how created, where created, relevant identities). Applying this technology to the cloud requires deployment of the technology with multiple points of certification: evidence before upload and immediate evidence provided if content is created in the cloud or externally. However a further challenge is the detection, if not prevention, of unintended access or disclosure in transit, processing, or storage of information and its metadata.

Different frameworks were suggested in order to extract cultural behaviours and beliefs, which may lead to the definition and development of culturally specific trust mechanisms and models to address the needs of a cultural group or set of groups. The idea of a multi-lateral approach for collaborating together on Trustworthy ICT research and innovation topics has been emphasised as essential.

Several areas were highlighted for topics for future international cooperation projects at the conclusion of the workshop; these included: trust management for emerging countries; international data exchange architectures for cyber security; cyber forensics; privacy in the cloud; mobile security; and cloud computing interlinking with crypto/trusted storage, trust models and adaptations to culture.

Table of Contents

1 Introduction

As part of their official description of work (DOW), the FP7 BIC Project were committed to holding a workshop dedicated to scoping topics for future projects incorporating both international cooperation and Trustworthy ICT during June 2013. Instead of working in isolation, the project decided to join forces with another large scale FP7 Integrated Project (IP) and one of the largest ICT Trust and Security conferences held in Europe on an annual basis. In parallel with the planning of this workshop, a National Science Foundation (NSF) funded project contacted BIC with the intention of joining together with the EU Trust and Security research community to co-host a large scale workshop, also with the objective of scoping potential topics for future collaboration and building projects.

As a result of this planning and circumstances described above, during 6-7th June, 2013, an International workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC 2013) was co-organised by the EU FP7 BIC project, the DIMACS Center for Discrete Mathematics & Theoretical Computer Science (with support from the National Science Foundation), EU FP7 A4Cloud project, and the regional UK and Ireland branches of the Cloud Security Alliance (CSA).

The TAFC 2013 workshop was held in Malaga, Spain, in conjunction with the 7th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2013). It was jointly organized by the following projects and initiatives:

- **Building International Cooperation for Trustworthy ICT** (BIC) an EU FP7 Coordination Action http://www.bic-trust.eu/ within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security.
- **Center for Discrete Mathematics and Theoretical Computer Science** (DIMACS) a joint collaboration coordinated by Rutgers University, New Jersey, United States of America http://dimacs.rutgers.edu.
- **Accountability for Cloud** (A4Cloud), an EU FP7 Research Project http://www.a4cloud.eu/ within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security.
- **Cloud Security Alliance** (CSA) with their UK and Irish Chapters http://www.linkedin.com/company/cloud-security-alliance---UK-&-Ireland-chapter https://cloudsecurityalliance.org.

In order to prepare for the workshop, the organisers issued a Call for Papers including research topics related to Trustworthiness, Accountability and Forensics in the Cloud, including Interoperability. The papers went through a light peer review process and the accepted papers were published in informal workshop pre-proceedings, which can be found at http://www.bic-trust.eu/events/tafc2013/. Links to the accepted papers can also be found within this workshop report.

The workshop was attended by over 40 participants from Australia, South Africa, Brazil, Europe, India, Canada and the United States. The speakers represented major universities, research organizations and companies with global reach.

The following report presents a detailed summary of the outcomes of the TAFC 2013 workshop.

2 Inaugural and Keynotes Session

The TAFC 2013 Co-Chairs, Jim Clarke and Rebecca Wright, opened the workshop by describing the overall purpose of the event: To generate and stimulate discussions amongst the participating stakeholders in trustworthiness, accountability and forensics in the Cloud environment and to address the general question of the scope and priorities in this research area and the needs for International Cooperation (INCO).

"The emphasis as we move from FP7 to H2020 is shifting from Science and Technological Development (STD) to Research and Innovation (R&I) where 'Innovation' means new products and methods that are being fed back into the greater good of the EU economic development. Therefore, in order to truly start scoping ideas for the development of international projects for H2020, which is an underlying goal of this workshop, we need to examine and clarify how the new Research and Innovation (R&I) model in H2020 gels with the funding models of the other countries, where there might be more emphasis on the 'Research' elements only. This could have a significant impact on the mechanisms available (or not) between the countries in the future," said Mr. Clarke during the opening session.

Mr. Clarke further elaborated the main goals of the workshop and the relation to the BIC project and events of the previous project INCO-TRUST, and how the stakeholders have built upon previous events from as early as 2007. Mr. Clarke then described the agenda, which was broken down under a variety of inter-related topics, including motivation and vision in international research collaboration, cyber security threats and actors, as well as specific technical challenges that have been identified by the working groups of the BIC project at previous events (see http://www.bic-trust.eu/events/).

Sam Weber, Program Director at National Science Foundation (NSF) explained the roles of the NSF and its Secure and Trustworthy Cyberspace (SaTC) programme as well as the importance of on-going activities including international collaboration. Dr. Weber addressed also the important international research issues related to Cloud/Big Data security from the NSF perspective.

"In the NSF Strategic Plan, it has been stated that today's research requires globally-engaged investigators working collaboratively across agencies and international organizations to apply the results of basic research to long-standing global challenges," said Dr. Weber

The Secure and Trustworthy Cyberspace Program (SaTC) has a budget of $69 Million and its main goal is to protect cyber-systems (including host machines, the internet and other cyber-infrastructures) from malicious behaviours, whilst preserving privacy and promoting usability.

In this direction, funding is available for catalysing new international collaborations for supporting initial phases of new international collaboration, such as

- Planning visits;
- Initial data gathering activities;
- Proof-of-concept; and
- Single or multiple research visits. The maximum duration of the funded awards is typically one year, with funding typically ranging between $10k-$100k.

As an example of international collaboration, Dr. Weber outlined the GENI and Fed4Fire collaboration where EU and US research communities wish to perform collaborative research, on the basis of equality and reciprocity, in areas of mutual interest, which may be characterized as

(a) Investigations of the research infrastructures suitable for hosting at-scale experimentation in future Internet architectures, services, and applications, and

(b) Use of such infrastructures for experimental research.

Addressing the topic of cloud security, Dr. Weber mentioned there are around 60 current SaTC-funded awards related to cloud security with three main thrusts (others are welcome):

1. Trustworthiness of Cloud Providers, including Functional encryption, auditing providers;
2. Protecting cloud providers from threats, including isolation between cloud customers, protect provider from customers, detecting attacks, privacy violations;
3. Leveraging cloud to provide trustworthy applications, including enforcing differing security policies among collaborating clients, cloud-based health records.

International aspects affect all three of these thrust areas, and Dr. Weber cited examples of future collaboration should include those addressing cultural, privacy and legal issues.

The keynote talk from Colin Bennett addressed privacy and accountability issues from the time perspective – addressing the 'newness' of these issues and challenges. Usually, there seems no problem in the beginning, but later facts call for both, privacy and accountability, specifically within the domain of social media. Prof. Bennett illustrated this point while comparing different approaches e.g. Canadian vs. the European country-to-country approaches when dealing with privacy strategy and legislation. Prof. Bennett also illustrated it with the example of his Canadian Access to Social Media Information (CATSMI) Project[8], which operates out of the University of Victoria in Canada and provides researchers and users with valuable insights of informational privacy and its underlying legal and regulatory policies.

When it comes to accountability approaches and mechanisms, the following areas were highlighted by Prof. Bennett as those requiring international research:

- Model contracts;
- Binding Corporate Rules (BCRs);
- Privacy management frameworks;
- Technical standards;
- Management standards;
- Privacy seals.

"Scholars have spilled a lot of ink considering the many meanings of the word accountability," said Professor Colin Bennett.

Prof. Bennett pointed out that there have been considerable numbers of definitions put on the table on accountability. However, there seems to be a consensus that the process must involve being called "to account" by some authority for one's actions. The involvement of an external body is, therefore, indispensable. Accountability implies a process of transparent interaction, in which that body seeks answers and possible rectification. That external agent is presumed to have rights of authority over those who are accountable – including the rights to demand answers and impose sanctions. Thus, if there is no possibility of external compulsion to change practices, there can be no accountability. Furthermore, accountability means more than "responsibility." One can always act "responsibly" without reference to anyone else. Accountability is always directed towards an external agent; responsibility is not. Accountability is also more than "responsiveness." For example, the responsiveness of a company to its customers is a desirable component of accountability, but again does not imply that there is external accountability. Accountability is not present simply because consumers have an option of choosing another company in a

[8] http://www.catsmi.ca/

competitive marketplace. The literature is, Prof. Bennett concluded, far more complex, but these seem to be the central elements. There must be a common understanding of who is accountable, for what, and to whom.

3 Session Reports

This section contains a summary of the presentations and discussions carried out during each of the workshop sessions, including links to full presentations and available papers.

3.1 Session 1: Accountability

As noted by Prof. Bennett's keynote talk, accountability is complex and there are a number of definitions on the table. Similarly, there are many tools that can provide some aspects of accountability, but it is not always clear how the tools can be combined to appropriately provide accountability in any given scenario. In this session, four speakers discussed their views and progress on accountability.

In many practical settings, accountability can be achieved by documenting policies, procedures and practices; assigning the duty to implement privacy policies to specified individuals in the organization; providing suitable training; informing stakeholders about privacy breaches; and effective sanctions and procedures for compensations in case of privacy breaches. It requires transparency and liability for privacy.
http://www.bic-trust.eu/files/2013/06/SBERTHOLD_ET_AL.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_SB.pdf

Deterrence is an important complement to preventive security; however, it requires formalizing accountability and disambiguating various often-conflated concepts related to accountability. One important question is the extent to which accountability requires identifiability. A focus on deterrence via punishment or other consequences may allow a reduced focus on identifiability while still achieving the same end goals as accountability.
http://www.bic-trust.eu/files/2013/06/AJAGGARD.pdf
Project web pages at http://www.dimacs.rutgers.edu/~adj/accountability.

The cloud accountability project (A4Cloud) provides a framework to assist holding service providers accountable for managing personal, sensitive and confidential information in the cloud, consisting of the following steps: operationalise the accountability definitions, capture different abstraction levels of accountability, identify attributes contributing towards accountability, characterize accountable organisations, identify elements of accountability practices and enable accountability practices.
http://www.bic-trust.eu/files/2013/06/SPEARSON.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_SP.pdf

Accountability is a rich and diverse notion with many interpretations in different contexts. A summary of the different interpretations include answerability, liability, responsibility, transparency, attribution capability, ability to provide evidence, compliance, controllability, responsiveness, disclosure, non-repudiation, undeniability, monitorability, auditability, verifiability, assurance and remediation.
http://www.bic-trust.eu/files/2013/06/NPAPANIKOLAOU.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_NP.pdf

The panel discussions focussed on the following questions: when is and isn't accountability well defined? is accountability always important? how to deal with loss of data? how to guarantee data deletion? Further research is needed to find new directions in privacy and accountability in the face of new technical advancements and in teasing apart the new from the old definitions of privacy and accountability that can be used to gauge compliance with enforcement of policies. International cooperation is necessary to enable self regulations of various privacy laws and seamless merging of those

laws for data exchange/sharing/transfer/disclosure. This should lead to the enforcement of policies across borders (including compliance transfers).

3.2 Session 2: Forensics, Evidence and Accountability

In order to provide forensics as a service (FaaS) and models for forensic brokerage, it needs to cover the different perspectives of cloud forensics: law enforcement, security and traditional digital forensic challenges, as all pose significant challenges in organizational, technical and legal dimensions. Based on the definition of cloud forensics, there are opportunities to be leveraged including FaaS, standardization acceleration, a cloud forensic investigative architecture and models for cloud forensic brokerage.
http://www.bic-trust.eu/files/2013/06/KRuan.pdf

Evidence gathering for accountable cloud computing services requires development of processes and mechanisms to monitor and audit the terms of a service level agreement (SLA). Providers must provide evidence and in the cloud, a customer must be allowed to verify that his/her data is being stored and maintained correctly in the cloud, and that his/her policies are adhered to. It is suggested to build an evidence base for collected information to assure accountability and support audits. This is quite a challenge as evidence needs to be collected at many architectural layers in the cloud stack.
http://www.bic-trust.eu/files/2013/06/TRubsamen_ET_AL1.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_TR.pdf

The methods used to combat the increasing amount of high-technology and computer crimes must be improved. The amount of data and sharing of ICT resources through the cloud is so extensive and complex that current methods are incapable to cope. Proactive, ultra-large scale forensic investigations need to be researched and developed. Computational forensics (CF) is an emerging interdisciplinary field of research. It unites expertise from computer science and forensic science. Data-science methods may establish decentralized, collaborative and independent investigation procedures. These require computing algorithms that are context-aware, adaptable and self-organizing. Typical challenges in investigations are about gathering evidence, search, ability to link various evidence and to visualize them. Computational forensics in the cloud require dynamic analysis where malware is executed in a monitored environment to observe its behaviours. To cope with the overwhelming amount of information graphs may be one way of comparing normal and malicious behaviour. However, it requires us to know the normal behaviour of a system to compare with. For the computer scientist, it poses a new frontier where new problems and challenges are to be faced and the challenges of interdisciplinary research, and challenging problems should attract high quality students and researchers. In addition to the technological issues are the social and socio-technical, e.g. when it comes to culture, social behaviour, law and policy rules in different countries. International cyber laws should be further improved so that international cooperation can strengthened. There is great demand to establish a legal framework for ICT (Sunde, 2006), and implement the law into ICT functionality, e.g. programming laws and regulations to automate the enforcement of them (Sunde, 2010). Selected examples of successful methods adopted for data processing, and ongoing research will contribute to the understanding and confidence in the new technology. Examples include digital forensics through the cloud, i.e. (i) detection malicious PDF, (ii) the detection of malware when the malicious program operates, and (iii) automatic linking evidence from multiple computers.
http://www.bic-trust.eu/files/2013/06/KyFranke.pdf

In order to understand how to use the network to forensically account for and measure service level agreements in a cloud and how to detect or prevent exfiltration of data from private clouds, a Software-defined Network Interface Card (SoNIC) was developed by the Weatherspoon group at Cornell University. It allows the measurement of network inter-packet delays of very fast large-scale networks in real time and provides forensic evidence by using a covert timing channel.
http://www.bic-trust.eu/files/2013/06/HWeatherspoon_ET_AL.pdf

The panel discussions asked for clarification of: which artefacts are useful for investigations across the cloud stack, what patterns need to be looked at in executable traces, what types of analysis can be carried out at the hardware level. Examples were given of covert channels and time synchronization across a network. It was also discussed: what are the right tools in a toolkit for forensics and how often should they be updated, how to build cloud architectures that provide forensic mechanisms, what about digital freedoms as forensic mechanisms have good and bad uses. There was a debate about the need of a chain of custody for legal cases/prosecution, but in practice, most cases are not taken to court, or penalties are not enforceable. More research is needed in the following areas: FaaS, types of evidence and how it can be automatically produced, graph-based matching for malware detection, using network hardware to forensically check compliance to SLAs.

International cooperation is necessary as data centres are located worldwide and, therefore, the need for law enforcement to work transparently across borders. Additionally, interoperability is needed between standards used by different agencies for forensic data.

3.3 Session 3: Trust and Cloud Security

Standardisation, certification and International issues in cloud security were presented by a member of the CIRRUS project team. CIRRUS has three specific actions: cutting through the jungle of standards, guiding to safe and fair contract terms and conditions and establishing a European cloud partnership to drive innovation and growth from the public sector. The key is to build the chain of trust, where the use of security standards and certification is included in the contract terms. However, cloud service providers tend to choose or even impose their standards, certificates and contract terms, supported by legislative environment of their choice. Customers are advised to better negotiate their service level agreement and other contract terms. Researchers should align with market and policy priorities while standardization agencies should synchronize and converge their efforts and recommendations.
http://www.bic-trust.eu/files/2013/06/APasic.pdf

A presentation on securing services running over untrusted clouds analysed the question of the level of certainty that a user can have about the hosts provided by his cloud providers and how much effort/cost is needed to become fully certain, based on a two tier model where some servers are always good (certain) and others might be hijacked (less certain). A new security protocol is proposed that is based under the reasonable system assumptions that there is a way to utilize the good (honest) servers even though it is not known where they are. Corruption resiliency may be obtained by the system if a mathematically defined portion of reliable good servers can be used, assuming server anonymization.
http://www.bic-trust.eu/files/2013/06/AKiayias.pdf

Mobile computing security poses several challenges as the devices have limited processing power, low storage, general less security, unpredictable Internet connectivity and less energy. It is difficult to enforce a standardized credential protection mechanism due to the big variety of mobile devices. Therefore, a Data and Application Security Framework is proposed, which uses the processing power of the cloud (SaaS). Researchers are invited to join together to form a project to contribute with the required semantics, protocol selection, and partitioning of workload between mobile and cloud.
http://www.bic-trust.eu/files/2013/06/MChaturvedi_ET_AL.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_MC.pdf

For a critical infrastructure Trusted Cloud (TC) network, an architecture is proposed with a private cloud deployment and trusted service providers, a trusted cloud monitor, an access control model for computing services that supports need to know and separation of duties policies by using lightweight TC-compliant computing services and compliant client service endpoints.
http://www.bic-trust.eu/files/2013/06/MBurmester1.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_MB.pdf

Finally, a trusted storage development is proposed, where trusted storage controllers are built into the storage devices to handle all policies and cryptography related with the stored objects. It enables the building of end to end secure channels between the user and his data and can attest verifiable the state of stored data.
http://www.bic-trust.eu/files/2013/06/DGarg_ET_AL.pdf

The panel discussion covered mainly trusted storage controllers questions, for example discussion about how a language for trusted storage controllers maps to standards, its own interpreter, policy checking on both sides (user and the controller), scalability, potential cooperation between the controller and the proposed data and application security framework. Among the areas identified for future international research are: crypto protocols for distributing trust, semantic data for security parameters for mobile and cloud security attributes under different security requirements; platform independent security architecture, including legal requirements in the cloud. International cooperation is necessary to leverage the skill bases of international peers, specifically for the work on cryptography, a trusted cloud architecture and a trusted storage controller.

3.4 Session 4: Policy, Ethics and International Cooperation

Computer technology is ever evolving and so should be relevant code of ethics. Data is being shared across borders and current regulations fail to capture the complexity involved. Ethical, privacy-preserving, accountability enabled, treatment of data requires solutions to numerous technical problems with several challenges.
http://www.bic-trust.eu/files/2013/06/LZuck.pdf

The deepening world-wide cyber insecurity crisis is destabilizing traditional international security architectures. Funding by government research agencies can shift the balance from offense towards defence dominance by raising assurance globally across the information and communication technology fabric. Such a strategy can be implemented via research programs to create open-source high assurance reference platforms for host computers and networking components that will accelerate research, education, and adoption by industry.

Therefore, trustworthy host platforms are needed for accelerated research and education. It is evident that strategic cyber threat reduction can only be achieved through international research cooperation. A Verifiable System Programming Language is proposed as an expressive dynamic language designed to support parallelism, verification, and suitable for system programming.

As the cyber insecurity crisis is deepening, cyber arms control needs to make offensive techniques obsolete by enhancing resilience of military and civilian systems. Beyond capacity building and research productivity, an important objective is to spread lower risk technologies around the world in order to raise the difficulty for malicious actors to engage in cybercrime, espionage and attacks. This approach implements cyber arms control not by unverifiable and unlikely international treaties but rather by raising the assurance level of systems globally and pervasively so as to eliminate lower difficulty penetration vectors and privilege escalation techniques, and thereby, constrain cyber offense.

The need for international collaboration encompasses both areas, requiring science, engineering, and policy to leverage complementary expertise, achieve higher total funding, speed development and adoption, benefit from diverse perspectives, educate and train more computer security professionals, create momentum for higher assurance, open source catalysing defensive virtuous cycles, spread tools to resist malicious cyber actors and incentivize private sector to adopt superior architectures for their security needs. To further incentivize adoption, the proposed research program emphasizes high agility tool chains designed for verifiability, modularity, collaboration, and evolution as a means to lower development costs through higher productivity.
http://www.bic-trust.eu/files/2013/06/JCMallery.pdf

A member of the BIC International Advisory Group from India, Mr. Abhishek Sharma, presented an international cooperation multi-lateral strategic model for trustworthy ICT based on the extension of the original BIC model and the inclusion of an Extended Working Group in each country. In this proposed structure, as shown at the Figure 1, Extended Working Groups (EWGs) are defined as the country specific arms of the Core Working Group (CWG) of BIC. India has spearheaded this model already and held a kick off meeting of their EWG in New Delhi with the support of the India government and the European Commission delegate in New Delhi. Further details on that meeting can be found at http://www.bic-trust.eu/2013/05/22/bic-extended-working-group-ewg-launched-in-india-22nd-may-2013/

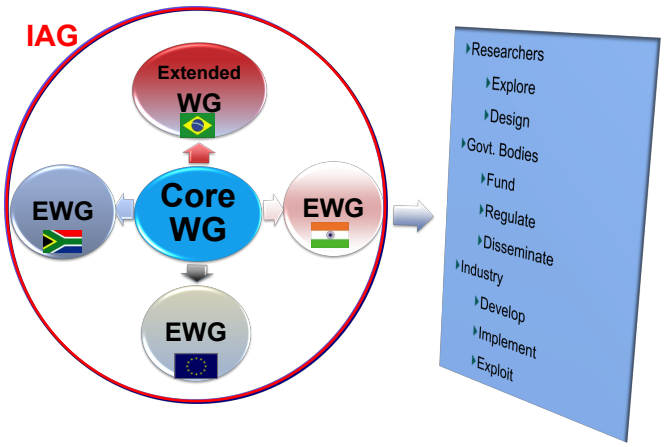

Figure 1: International Advisory Group and Working Groups structure

"In a world of multi-lateral ICT, the bi-lateral cooperation models in use today are not logically suitable for international cooperation in cyber security. Therefore, a multi-lateral strategic cooperation model, as proposed in BIC, is essential as we move forward to Horizon 2020," said Mr. Sharma

Mr. Sharma re-iterated that while this concept of EWG was not envisaged in the original BIC project, the research domain "Trustworthy ICT" is an area of continuous work as new threats will come up with the passage of time so there would always be the need for international cooperation in this area. The work done under BIC, therefore, needs to be essentially carried forward in a seamless manner to the next level of the project bands. On completion of the present term of BIC, the project needs to be continued in some avenue under H2020 for sustained INCO and collaboration, which is critical for all such global research programmes for the "Trustworthy ICT". The early formation of these groups can start this process making it coherent, meaningful and effective as the contacts within the extended working groups can already be forming strong relationships, work on consolidating position papers on key areas of BIC, scope areas of research and innovation for Horizon 2020 and begin to mobilise consortiums on these research topics.
http://www.bic-trust.eu/files/2013/06/ABSharma.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_ABS.pdf

International Cooperation from the South African and Industrial perspective was presented and calls for more joint cooperation, as it is a smaller market, closer to clients with an openness to change and a willingness to take calculated risks. As a working group member of BIC project, the contact base is continually growing. In the first years, working groups focussed on technical aspects of network information & cyber security and human oriented approaches for trust, privacy and security and continue to work on these (aligning research topics between the countries and providing guidance to the European

Commission for further joint international projects (and other programme management in other BIC countries). In parallel, now a working group (WG3) in BIC is focussing on a longer term strategy including logistical aspects, necessary models, mechanisms and processes required for the enablement of international cooperation. The key will be the continuing effort to develop cyber security expertise and building long term international collaborations.
http://www.bic-trust.eu/files/2013/06/AHutchison2.pdf

3.5 Session 5: Trust and International Cooperation

Making digital content trustworthy can be achieved by using digital signatures and digital fingerprinting with the following requirements: certainty that any content has not changed since creation date, since authorised amendment (must include version history) and automatically detect if content changed outside permitted channels with threat detection, early alarm for attempted fraud or data corruption, established provenance (who created, who witnessed, is it signed or contains signatures, version history) and other meta data (data type, how created, where created - location, identity). Applying this technology to the cloud requires deployment of this technology with multiple points of certification: evidence before upload and immediate "evidentiation" if content is created in the cloud or externally. All content presentation needs local verification.
http://www.bic-trust.eu/files/2013/06/CKinsella.pdf

Trust management in emerging countries has to deal with both a very varied population (from young to elderly) and a trust culture, which is based on loyalty to extended families rather than to an established legal system. The international research community needs to gain an understanding of existing cultural frameworks to determine the most suitable framework to use in order to extract cultural behaviours and beliefs, which may lead to the definition and development of culturally specific trust mechanisms and models to address the needs of a cultural group or set of groups. The expected outcome of this work would be a generic framework that supports the ability to adapt trust models to culture, in a very generic manner, thereby complementing other research conducted in the ICT trust research communities.
http://www.bic-trust.eu/files/2013/06/MCoetzee_ET_AL1.pdf
Full paper at http://www.bic-trust.eu/files/2013/06/Paper_MC_etal.pdf

In the panel discussions, further details were discussed about how to classify the cultural aspects of trust, which is currently more heavily favoured towards a more formalised version of trust in the West. The various frameworks to describe cultures were differentiated as individualism vs. collectivism. 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. The research challenges entail:

- A study of existing cultural frameworks to determine the most suitable to use;
- Extraction of relevant cultural behaviours and beliefs that are applicable to consumer trust;
- A study of trust models to identify the most applicable to use for business ecosystems in India, Africa and possibly Brazil;
- The enhancement of trust models with cultural norms;
- The implementation and evaluation of a prototype system to determine if the culturally adapted trust model can be used in rural communities.

On the topic of trust management for emerging countries, it was agreed that the international research community should investigate the effects of culture on trust models in order to determine the most suitable cultural framework and how the individualist cultures models could influence the development of trust management.

Other areas covered during the panel discussions included how the current policies do not capture complexity and the panel discussed some examples and causes and possible solutions including the dream of using natural language processing, which needs domain knowledge and interdisciplinary collaboration, e.g., Computer science and sociology. This is accentuated by issues related to un-decidability, unpredictability, errors, intrinsic to the complexity nature of the problem Some routes suggests a discussion on whether we would be happy with an 80% solution with a 20% effort. Others suggest exploring whether approaches using deontic logic should be considered to handle the complexity. Moreover, there are other natural routes to approach the problem coming from System Theory (as suggested by Jean-Louis Lemoigne & others) or system engineering approaches. All these methodologies and others that multi-disciplinarily can bring deserve attention and in-depth analysis under a joint research program to ensure understandability, acceptance and feasibility.

Another discussion point during the panel was on the current public perceptions of trust in the cloud, which seems to imply inherently delegating our decision making processes to the providers, thus causing the potential situation that all kinds of private personal data is floating around unencrypted. As an example, European companies are generally hesitant to outsource to some cloud providers that are located elsewhere. This situation is certainly undermining levels of trust in the cloud, which must be addressed by the community.

In the panel discussions, it was also highlighted and discussed that in addition to the technical topics related to trustworthy ICT and security, a number of other less technical (but equally as important) research areas were identified, including: philosophy, mathematics (computer science, information theory, graph theory, decision theory, optimization, simulation/predictability), Human Sciences (sociology, industrial anthropology, psychology), legal (privacy regulations, IPR, laws/regulation, standardisation), business (model building, operations, information logistics, best practices, lessons learned low investment, international trading), policy (education, strategy building, risk and conflict management, economic and other incentives, and design (user oriented, co/eco-design, design for X).

4 Conclusions and Wrap Up

During the workshop, it became very clear that further international cooperation is key to the success of the research, development and innovation activities of the participants. Specifically, the idea of a strategic multi-lateral approach for collaborating together on Trustworthy ICT research and innovation topics has been highlighted as essential, whether it is related to cyber security, or the more human oriented aspects such as trust management and privacy in the cloud. Such an approach is needed to both build communications channels and trust among international partners and to establish a common understanding of how to develop and exchange research and technological information further in order to foster common Trustworthy ICT network and services infrastructures. The multi-lateral approach is specifically needed for smaller countries or groups of countries, as otherwise, it will be difficult to cooperate with some of the larger countries. Conversely, it is also essential for the larger countries to learn from and cater for the different cultures in their future trust models in order to maximise their levels of future innovations.

The following areas were recommended for international cooperation projects at the conclusion of the workshop:

Recommended areas for international cooperation at the conclusion

R1. The need for international cooperation in projects related to accountability was highlighted time and again. Both the need for, and the nature of, accountability is culturally dependent, yet cloud computing and other Internet technology crosses geographic and cultural boundaries. Additionally, the ability to carry through accountability measures to actually hold a person or entity accountable relies on relevant local laws and practices. International collaboration is needed to understand the technical and the political aspects of accountability and to develop and promote workable accountability frameworks and solutions.

R2. Trust management for emerging countries is an idea of a future project that has gained considerable momentum, where some organisations in the EU, India, South Africa, and Brazil have already started working together and welcome other participants going forward. Research work involving the mix of technology and taking into account cultural differences with regard to trust would benefit multi-cultural societies, and inform development of trust models and their adaptation to culture (can we learn from similar problems that arise in different cross-cultural settings?). For example, addressing differences in Problem 1 between Cultures A and B may guide the response to differences in Problem 2 between Cultures C and D. Technology providers need input from culture as there is a significant international component to mix of technologies, users, and providers, e.g., hardware, software, service provider, content generator, content aggregator, and users all in different countries. The participants felt there is a need for a strong push to bring the cultural perspectives all the way through to implementation will require significant international collaborations in the future!

R3. International data exchange architectures for cyber security, including the incentivising the inherent benefits of data exchange / sharing for cyber security, cyber forensics, mobile security and cloud computing interlinking with crypto/trusted storage etc. cover several new project ideas, based on existing bi- or multi-lateral cooperation (BIC).

R4. Currently, there may be greater user-trust in academics than in commercial enterprises; can we try to harmonise and bring these together as this endorsement could help good companies succeeding in terms of innovations. This would include how to foster greater interest in spreading high assurance; raise capacity and familiarity through international co-operations, using technology as a leveller and we should look at models to incentivise where commercial adversaries are collaborating internationally for a common purpose. It clearly is not a purely technical problem and requires significant multi-disciplinary and international collaboration,

R5. An international project incorporating the views of many stakeholders looking at a number of important socio-technical aspects should be convened, including looking at context (protectionism, global market, lawless lands, different priorities, including non-western world concepts, H2020); threats (co-design as a context, values, needs vs. time, cultural differences, clock speed, sophistication growing); opportunities (countries as “field trials”, small markets, closeness to clients, open-ness to change, growing market, lack of framework, lack of roadmap, lack of bodies tying it all ‘together’, lack of coordination); and detailed examination of the coming needs (impacts on large networks, continuity of actions, missing common objective, future building, funding planning, sharing experiences).

The discussions in the panel sessions consistently turned towards the need for an approach based on multi-cultural/multi-disciplinary approach for research and innovation in H2020. Examples of topics raised during the workshop that accentuated the strong need for a more integrated research and innovation approach include those of data and information privacy in the cloud and trust management models across cultures. Trust, privacy, and security are evolving, and in some places are characterized by the rise of protectionism facing established global markets as well as lawless lands. These three kinds of dogmas lay on the same network where the life cycle assessment of data, information & knowledge is inscrolled. The panellists in this session acknowledged the fact that no joint framework is yet set, and no roadmap is drawn because of the lack of a common understanding of the real concept of trust, privacy, and security.

While from the technical standpoint, several initiatives exist at different levels, they don't handle the threats from the entire range of perspectives (including technological, economic, legal, social, and cultural). In fact, this is a situation in which multi-disciplinary, multi-cultural approaches are needed. It is of crucial importance that the researchers both at the academic and industrial levels consider inputs from industrial anthropology, sociology, psychology, ergonomics and likely more sciences that can translate not only the user needs but also the cultural acceptability.

The workshop recommended that parallel international research teams should be formed to propose a framework able to integrate a diversity of cultural and economic considerations.

Recommended (initial) considerations for an integrated framework

R6. The **cultural differences** as any solution coming from any side of the world wouldn't be sustainable. Co-creation is a key.
R7. The **understanding of values** as while the values are universal, their relative importance in various countries and context may differ slightly.
R8. The **multi-disciplinarily** as all possible viewpoints/sciences/interests should be considered.
R9. The **market value**: as an integrated framework needs to be the host of new business models. The participants agreed there could be considered a market value placed on privacy and security.

From a paradigmatic perspective, the framework needs to be translated into a new generation roadmap. This roadmap should take the form of an extended and integrated set of *user* requirements translated into *functional* requirements. Although it was recognised that this kind of work is probably outside the scope of BIC itself, in future workshops or even within proposed projects being built by the community, some principles are recommended here, and should be extended.

Recommended principles for roadmap considerations

R10. Use **collaborative design** as a context;
R11. The roadmap should be a **live document** as the evolution of the network, applications, attacks, and, therefore, needs are changing continuously;
R12. The roadmap should be **dynamic** as different countries or regions expect different level of protection and management however will follow the path of other, more experienced users;
R13. **Inclusive design** as a paradigm to provide ad-hoc solutions for any kind of disabled or minorities;
R14. **Extend and develop** these principles.

The attendees agreed that the international cooperation taking place through BIC is a good starting point; however, the project, acting alone, lacks adequate resources to consider all of this activity. Conversely, the attendees recognised the strong need to take advantage of the international community to form a cluster or project(s) addressing a range of key multi-cultural, multi-disciplinary, and multi-interest partners and expand it as a philosophy to get the best out of it. Some approaches were recommended:

R15. Participating countries could be used easily as "field trials" for the technology acceptance and efficiency testing, especially in light of their particular points of strength;
R16. Participating countries could be considered as a market-test without investing too much and indeed have a potential for quicker large scale innovation and return on investments;
R17. Participating countries could offer the possibility to be closer to the clients to better understand their needs but also to understand how the technology is used daily (feeding into the "*Research and Innovation*" objectives of H2020);
R18. Some of the participating countries are much more ready for change than others; therefore, the programme can be designed to leverage this and a strong momentum is easy to reach;
R19. Some of the participating countries are considered as highly growing markets, which allows rapid scalability.

In conclusion, the participants at the TAFC 2013 workshop felt that in order to adequately address the key research topics related to International Cooperation and Trustworthy ICT, there is a need for multi-lateral (by this we truly mean "multiple countries TO multiple countries")/multi-cultural/multi-discipline/multi-interest approaches. Therefore, this action initiated within the BIC project should be considered as the way to progress in the future beyond the current obligations of the project itself and as a way to continue building that framework, roadmap and requirements.

However, the participants saw that there are obstacles facing the international research community that should be considered carefully by the designers and decision makers and implementers of future policies and later programmes and projects.

Identified Challenges:

C1. **Lack of coordination:** It is important to set a coordination body to assemble all the key stakeholders to catalyse the activities, make the best out of the current resources, avoid duplications and create an international roadmap with momentum and acceptability; This is something that projects like BIC have been carrying out – but what happens after?

C2. **Lack of appropriate mechanisms for effective INCO:** The BIC project is promoting a longer term, multi-lateral cooperation model for topics like Trustworthy ICT while at the same time integrating with the tactical, bi-lateral approaches used today. Although the current discussions around H2020 and INCO are espousing a more strategic planning approach, it still is not clear whether this will include adequate mechanisms for enabling this type of interaction between multiple countries.

C3. **Flexibility to deal with coming needs:** The clock-speeds of the research actions, policy and decision makers are obviously different. It was recommended that there is a need for setting a general policy that considers this discrepancy and allows the coordination body to handle emerging needs. Challenges related to different countries' priorities, addressing different areas (e.g. focus on research only instead of research and innovation) need to be addressed with urgency.

C4. **Impacts on large networks (e.g. Future Internet):** need also to be considered as the Internet is growing daily and more than this the quantity of data generated is growing even faster, causing a much greater need for INCO research and innovation in topics related to trustworthy ICT.

C5. **Continuity of action is required.** Horizon 2020 gives a time frame of 7 years which is appreciated; however, it does not create confidence long enough into the future. There is a need to guarantee the continuity of action at the international level on a long term strategic perspective and avoid very short term projects, and hence, avoiding short terms visions.

Finally, two relevant events / initiatives were announced at the end of the workshop:

IFIPTM 2014, the 8th International Conference on Trust Management will be held in Tel Aviv, Israel in May 2014. More information will be given to the participants at a later date.

A European *Network and Information Security* (NIS) Public-Private Platform is being set up by the European Commission; call for expression of interest at http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=10289.

Appendix 1. Workshop Program

Thursday, June 6, 2013

08:45 - 09:00 Welcome and Overview from the Co-Chairs
Jim Clarke, *Waterford Institute of Technology* and Rebecca Wright, *Rutgers University*

09:00 - 09:45 International Research Issues in Cloud Security and NSF
Sam Weber, *National Science Foundation*

9:45 - 10:30 Keynote talk: Accountability for Privacy in Cloud Computing: Is This a New Problem
Colin Bennett, *University of Victoria*

11:00 - 12:30 **SESSION 1 – ACCOUNTABILITY**

11:00 - 11:15 Crime and Punishment in the Cloud: Accountability, Transparency, and Privacy
Stefan Berthold, Simone Fischer-Hübner, Leonardo Martucci, and Tobais Pulls, *Karlstad University*

11:15 - 11:30 Accountability, Deterrence, and Identifiability
Joan Feigenbaum, *Yale*, Aaron Jaggard, *US Naval Research Laboratory*, and Rebecca Wright, *Rutgers*

11:30 - 11:45 A Conceptual Framework for Accountability
Siani Pearson, *HP Labs*

11:45 - 12:00 Perspectives on Accountability
Nick Papanikolaou, *HP Labs*

12:00 - 12:30 Panel Discussion (all session speakers).
Moderator: Rebecca Wright, *Rutgers University*

14:00 - 15:45 **SESSION 2 – FORENSICS, EVIDENCE, AND ACCOUNTABILITY**

14:00 - 14:30 Forensics as a Service
Keyun Ruan, *University College Dublin*

14:30 – 14:45 Evidence for Accountable Cloud Computing Services
Thomas Rübsamen, *Hochschule Furtwangen University*

14:45 - 15:00 Forensic Investigations in Cyberspace: what about big data?
Katrin Franke, *Gjøvik University College*

15:00 - 15:15 Forensics in the SoNIC project on Precise Realtime Software Access and Control of Wired Networks
Hakim Weatherspoon, *Cornell University*

15:15 - 15:45 Panel Discussion (all session speakers).
Moderator: Siani Pearson, *HP Labs*

16:15 - 17:45 **SESSION 3 – TRUST AND CLOUD SECURITY**

16:15 - 16:30 Standardization and International Convergence Issues in Cloud Security
Aljosa Pasic, *Atos Certification*

16:30 - 16:45 Securing Services Running over Untrusted Clouds: the Two-Tiered Trust Model
Aggelos Kiayias, *University of Connecticut* and *University of Athens*

16:45 - 17:00 Privacy & Security of Mobile Cloud Computing
Manmohan Chaturvedi, *Ansal University*

17:00 - 17:15 Trusted Clouds
Mike Burmester, *Florida State University*

17:15 - 17:30 Data Protection and Accounting with Trusted Storage
Anjo Vahldiek, Eslam Elnikety, Aastha Mehta, Deepak Garg, and Peter Druschel, *Max Planck Institute for Software Systems*

17:30 - 17:45 Panel Discussion (all session speakers) Moderator: Sam Weber, National Science Foundation

Friday, June 7, 2013

09:00 - 10:30 **SESSION 4 – POLICY, ETHICS, and INTERNATIONAL COLLABORATION**

09:00 - 09:30 Privacy, Ethics, and Accountability
Lenore Zuck, *University of Illinois at Chicago*

09:30 - 10:00 Trustworthy Host Platforms For Accelerated Research And Education:
Strategic Cyber Threat Reduction Through International Research Cooperation:
John Mallery, *MIT*

10:00 - 10:30 Strategy for Coordination of the Cross Domain Activities & Multi-Lateral Approach in International Cooperation:
Abhishek Sharma, *Beyond Evolution TechSolutions*, and James Clarke, *WIT* (both of BIC International Advisory Group), Andrew Hutchison, *T - Systems, South Africa& Adj. Professor, University of Cape Town*

11:00 - 12:15 **SESSION 5 – TRUST AND INTERNATIONAL COLLABORATION**

11:00 - 11:15 Can You Trust It? Digital content in the Cloud
Cian Kinsella, *Digiprove*

11:15 - 11:30 Trust Management in Emerging Countries: International Cooperation Research Challenges for Horizon 2020
Marijke Coetzee, *University of Johannesburg*, Jan Eloff, *SAP Meraka UTD, CSIR, Pretoria, South Africa; Department of Computer Science, University of Pretoria*, Donovan Isherwood, *University of Johannesburg*, James Clarke, *Waterford IT*, Manmohan Chaturvedi, *Ansal University*, Abhishek Sharma, *Beyond Evolution Tech Solutions Pvt. Ltd*, Karima Boudaoud, *I3S Laboratory - University of Nice Sophia Antipolis/CNRS,* Mounib Mekhilef, *Ability Europe Ltd.*

11:30 - 11:45 Strategy for Coordination of the Cross Domain Activities & Multi-Lateral Approach in International Cooperation
Abhishek Sharma, *Beyond Evolution Tech Solutions* and James Clarke, *Waterford IT*

11:45 - 12:15 Panel Discussion (all Friday session speakers).
Moderator: Rebecca Wright, *Rutgers University*

12:15 - 12:45 Next steps and Wrap-up,
Lenore Zuck, *University of Illinois at Chicago and* Sam Weber, *National Science Foundation*

12:45 - 13:00 Workshop Closing from the Co-Chairs
James Clarke, *Waterford Institute of Technology* and Rebecca Wright, *Rutgers University*

Appendix 2. Participants

Hans Henning Arendt, @BC, Germany
Lynn Batten, Deakin University, Australia
Colin Bennett, University of Victoria, Canada
Stefan Berthold, Karlstad University, Sweden
Karima Boudaoud, Ecole Polytechnique de Nice Sophia Antipolis, France
Michael Burmester, Florida State University, USA
David Chadwick, University of Kent, United Kingdom
Manmohan Chaturvedi, Ansal University, India
Jim Clarke, Waterford Institute of Technology – TSSG, Ireland
Marijke Coetzee, University of Johannesburg, South Africa
Jan Eloff, University of Pretoria, South Africa
Mariki Eloff, University of South Africa, South Africa
M. Carmen Fernandez Gago, University of Malaga, Spain
Katrin Franke, Gjøvik University College, Norway
Deepak Garg, Max Planck Instotute For Software Systems, Germany
Ehud Gudes, Ben Gurion University, Israel
Andrew Hutchison, University of Cape Town, South Africa
Aaron D. Jaggard, US Naval Research Laboratory, USA
Aggelos Kiayias, University of Athens, Greece
Javier Lopez, University of Malaga, Spain
Di Ma, University of Michigan Dearborn, USA
John Mallery, Massachusetts Institute of Technology, USA
Fabio Martinelli, National Research Council, Italy
Mounib Mekhilef, Ability Europe Ltd., France
Yuko Murayama, Iwate Prefectural University, Japan
Nicholas Papanikolaos, HP Labs, United Kingdom
Manish Parashar, Rutgers University, USA
Aljosa Pasic, Atos, Spain
Saini Pearson, HP Labs, United Kingdom
Rene Peralta, National Institute of Standards and Technology, USA
Michel Riguidel, Telecom Paristech, France
Keyun Ruan, University College Dublin, Ireland
Thomas Rubsamen, Hochschule Furtwangen University, Germany
Abhishek Sharma, Beyond Evolution TechSolutions, India
Kalpana Singh, Deakin University, Australia
Priscilla Solis Barretto, University of Brazil, Brazil
Norihiko Takeuchi, Waseda University, Japan
Tokio Takeuchi Aichi, University of Education, Japan
Tomokazu Takeuchi, Gakushuin University, Japan
Hakim Weatherspoon, Cornell University, USA
Samuel Weber, National Science Foundation, USA
Rebecca Wright, Rutgers University, USA
Lenore Zuck, University of Illinois – Chicago, USA

Appendix 3. About the Organizers

BIC, which stands for Building International Cooperation for Trustworthy ICT is an EU FP7 Coordination Action project bringing together researchers from around the globe to scope mutually beneficial research topics in the areas related to Trustworthy ICT. The topics of this workshop were among the many research topics recommended for international research by the working groups of BIC leading to the proposition for this workshop and have been the subject of a number of working papers, which can be found in the project impact section of the web at http://www.bic-trust.eu/project-impact/. The BIC project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4 Trust and Security. More in depth information on BIC can be found at http://www.bic-trust.eu/.

DIMACS, the Center for Discrete Mathematics and Theoretical Computer Science, was founded in 1989 as a National Science Foundation Science and Technology Center. DIMACS catalyzes and conducts research and education in mathematical, computational, and statistical methods, algorithms, modelling, analysis, and applications. DIMACS is a joint collaboration coordinated by Rutgers University, New Jersey, United States of America. More information can be found at http://dimacs.rutgers.edu. DIMACS's role in the workshop was supported by the National Science Foundation under Grant No. CNS-1040356. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and the workshop participants and do not necessarily reflect the views of the National Science Foundation.

A4Cloud is an Integrated Project on Accountability for Cloud, an EU FP7 Research Project started in October 2012, coordinated by HP Labs and funded within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security. Additional information can be found at http://www.a4cloud.eu/.

UK and Irish Chapters of the Cloud Security Alliance (CSA): The CSA is a global not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The UK and Irish Chapters facilitate project work, share news and organise events for UK and Irish Chapter members. In terms of research direction, the UK chapter is focusing on guidance about cloud security for SMBs and the Irish chapter is looking at incident response and Ireland's strategic role in the EU cloud ecosystem by hosting most of the major US provider data centers. Additional information can be found at http://www.linkedin.com/company/cloud-security-alliance---UK-&-Ireland-chapter and https://cloudsecurityalliance.org