D4.3 INCO-TRUST Workshop 2 and Report

2nd FP7 INCO-TRUST Workshop on

INTERNATIONAL COOPERATION IN TRUST AND SECURITY
Workshop topic: International Data Exchange with Security and Privacy: Applications, Policy, Technology, and Use"

4-5th May 2010
Venue: New York, New York, USA

Grant Agreement number: 216867

Project acronym: INCO-TRUST

Project title: International Co-operation in Trustworthy, Secure and Dependable ICT infrastructures

Funding Scheme: ICT Call 1 FP7

Project co-ordinator name, title and organisation: James Clarke, Program Manager, Waterford Institute of Technology

Tel: +353-71-9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

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

Revision: **Workshop held 4-5th May 2010**
Final Report Available ...24...../ ...09...../ .2010.....

Date: ...24...../ ...09...../ .2010.....

Signature of Coordinator: ....

Main Authors: Rebecca WRIGHT, Rutgers University and Jim CLARKE, Waterford Institute of Technology;

Main Contributors: Anupam Datta, *Carnegie Mellon University,* Artur Hecker, *Institute Telecom-ParisTech;* José Fernandez, *École Polytechnique de Montréal;* Aljosa Pasic, *Atos Origin;* Volkmar Lotz, *SAP;* Neeraj Suri, *TU Darmstadt;* and, of course, all Workshop participants.

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	**PUBLIC**	

Table of Contents

I. Executive Summary

Security and privacy are critical to establishing a trustworthy cyber infrastructure. A plenary workshop bringing together key international security/privacy representatives was held on 4-5th May 2010 in New York City, following the first INCO-TRUST workshop in 2009[1]. The workshop was co-organised by the National Science Foundation, Rutgers University, and the European Commission-funded INCO-TRUST project. One of the topics highlighted during the 2009 workshop was there are many problems that need to be solved in order for data to be shared securely, both within a country and internationally. Therefore, an integrated, internationally driven approach towards security information and data gathering and exchange is needed. To this end, the goal of the 2010 workshop was to foster long-lasting international scientific collaborations investigating the scientific foundations, design, and feasibility of a future international cyber architecture. Such an architecture must allow for transnational data repositories and be capable of enforcing both today's and future diverse security and privacy policies.

The workshop included a variety of security researchers from Europe, the United States, and other countries, and specifically addressed issues of privacy, anonymity, provenance, transnational storage and dissemination, and ownership of data. The focus extended beyond technology challenges for trustworthy data exchange to also cover the diversities of transnational policies, legal aspects as well as the diverse cultural and societal considerations of users with information and data. Participants included representatives from academia, industry, and program management.

In addition to keynote speakers and panel sessions, breakout sessions were held on identifying the challenges and opportunities for transnational data repositories and examining the differences and commonalities of international and domestic approaches to a variety of application domains. These are described in more detail in Annex I and II, respectively. The workshop contributed to the growing dialog and call for collaboration regarding international cooperation related to trust and security.

The workshop agenda, slides, and other documents are available at links in the electronic version of this document and from the project web site located at www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/.

The key recommendations and conclusions of the workshop are the following:

- There is a continuing need for research and development of the technical components of secure and private data repositories. These include a number of steps related to representing and structuring data; policy representation and understanding; architectures and enforcement; and development of specific testbeds.
- International collaboration is critical to ensure that solutions can operate across national and cultural boundaries.
- A potential cooperation could take the form of working together on a framework for an International Cyber Data Exchange System. This would not only benefit the US-EU but also expand to support OECD-wide data exchange.
- There is a need for expressing national and local policies in order to enable automated comparison, negotiation, and merging across international borders.
- The international research community must work together on mechanisms that enable policy enforcement or assurance of compliance, enabling accountability.

- Identification and establishment of collaborative, context-specific, automated and non-automated common trust models ("virtual organization") in concrete scenarios are needed in order to:
  - provide better understanding of challenges of international data exchange in general; and
  - support current and future collaborative research efforts in computer security (malware, attack data, etc.),
  - while recognizing constraints on research (e.g. human subjects).
- It is necessary to develop models and mechanisms for information and knowledge exchange, not just data exchange. Among other aspects, this:
  - facilitates certain legal and policy requirements;
  - necessitates research into ways of automatically extracting and reconstructing information from data in a traceable fashion.
- There was considerable support amongst the participating researchers that if the programme mechanisms (funding, infrastructure, facilitations, etc.) could be substantially enhanced, they would significantly help enable the international researchers to meaningfully further their work together between the workshops. Currently, their limited processes or funding mechanisms in place pragmatically constrain the level of interactions making it difficult to carry out the levels of interaction needed for the work described above.

II. Keynote Talks

Three keynote addresses during the workshop served to highlight and introduce some of the research issues, ongoing activities, innovative approaches, and remaining challenges in security and privacy for international data exchange.

Keynote 1. ***Accountability in International Data Exchange***, Joan Feigenbaum, Yale University.

Joan Feigenbaum's keynote talk introduced many of the key concepts for the workshop. She discussed what is meant by "data exchange", which incorporates the establishment of common goals, policies, and procedures; transmission of data; maintenance and updating of databases (and of goals, policies, and procedures); use of data; and auditing and compliance. In addition, the concept of cyber "architecture" was outlined informally as the general structure of a class of systems, not the detailed design of a single system in the class. The cyber architecture refers to the "Internet architecture" comprised of distinct types of system components intended to or forbidden from performing certain actions. There are resources available to each type and the architecture comprises the manner in which different types of components are intended to interact.

The presentation then focused on accountability challenges and the support of an agenda based on accountability within international data exchange based on the contention that most security and privacy policies are preventive in nature and based on authorization before the fact. Less is known about accountability after the fact. Within a cyber architecture for international data exchange, an approach based upon accountability will be more important than prevention due to inadequacies of the latter. The notion of "deterrence"—complementing prevention—was introduced as being more effective in many cyber scenarios, especially when taking economic and legal considerations into account. This assertion was backed up with a large number of references and projects based on accountability via policy awareness and adjudication.

The presentation concluded with a number of research goals for the international community to engage in for mutual benefit. These include enumeration of important policy elements that must be strictly enforced and examination of whether the cyber architecture needed to enforce them would be acceptable to users. If not, can we use economic, legal, and other non-technological mechanisms to enforce them?

Keynote 2. ***Trust in the Internet: Observations on Being Highly Connected***, John Zic, Commonwealth Scientific and Industrial Research Organisation (CSIRO).

John Zic's talk went into great detail about the definitions, requirements and elements of trust, from both the user and the system perspectives. He presented a number of misbehaviours and potential defence mechanisms, as well as the concept of complete characterisation. In complete characterisation, before any transaction between two parties A and B, an exchange of information is made characterising all their possible behaviours to each other. Achieving this requires both secure authentication and secure transfer of information. If the measure is as expected, transaction proceeds; if not, then transaction is cancelled.

A Trust Extension Device (TED), which can be instantiated either in software or in hardware, was presented as one solution to end-point trust. Using a TED, both identity and operational integrity (behaviour) are proven before any transaction or information is exchanged.

Zic concluded that trust interactions rely on three components: identity information; assuring reliable operation despite outside interference or environment; and proofs that the system will behave in a known manner. The amount of interconnectedness, and ease to which information is accessible, offers many research challenges how to do this on a sufficient scale.

Keynote 3. ***The Legal and Cultural Landscape of Privacy and Data Use***, Steve Purser, European Network and Information Security Agency (ENISA).

Steve Purser of the European Network and Information Security Agency (ENISA) made a keynote presentation entitled **The Legal and Cultural Landscape of Privacy and Data Use,** during which he described the overall objective and activities for ENISA activities in the area under the Work Program of 2010 and ENISA's plans for the Work Program of 2011.

To ensure that Europe can effectively manage the introduction of a new services with a high level of security while limiting the threats to civil liberties and privacy, ENISA has several specific goals including: advocating and fostering a Pan-European approach to privacy; study of new models for trust-establishment (i.e., reputation systems, network topology, behavioural biometrics and anomaly detection, etc.); understanding the changing role of authentication in the information society and use and management of multiple identities in online services, including the role of anonymity, and development of guidelines for regulatory review and interpretation.

ENISA's current activities in these area include: studying models of electronic services considering available methods for the user-consented management of personal data; following the development and deployment of technologies enabling privacy-preserving access to data, mechanisms to ascertain minimal disclosure, advanced identity schemes including reputation-based schemes), and aiming towards policy and good practice initiatives that achieve a balance among transparency, accountability, and responsibility, and contributing to the review process of the European data breach notification requirement (Article 4) introduced in the review of the ePrivacy Directive (2002/58/EC).

In the context of the debate for its Work Program for 2011, a number of the activities mentioned above will be continued and extended, with a specific focus on making proposals on the role of ENISA in a European data breach notification scheme, namely in the implementation of Article 4 of the ePrivacy Directive (2002/58/EC), and development of guidelines and recommendations for necessary regulations, for example, in the areas of identity management and minimal identity disclosure.

III. Panel Sessions

Each of three panel sessions covered a specific topic from the perspective of three panelists, with ample time for discussion among the panelists and other workshop participants.

Panel Session 1. ***Data for Network Management and Security.***

Moderator: Sotiris Ioannidis, FORTH.

Panelists:

- *Experiences of DDoS*, Hyuncheol Jeong, Korea Internet & Security Agency.
- *Insights, challenges and techniques related to botnet infiltration,* Christian Kreibich, International Computer Science Institute.
- *Attack attribution,* Marc Dacier, Symantec.

The panel focused on large-scale attacks on computers and networks, including how data can be leveraged to detect, trace, and ultimately prevent such attacks.

Hyuncheol Jeong gave an overview of distributed denial-of-service (DDoS) attacks. Countermeasures employed against DDoS were then presented focussing on information sharing as the most important factor for success of effective prevention and response. He noted that based on their experience in Korea, there is a need for developing further information sharing technology, raising awareness, and improving the legal system. International cooperation is necessary to combat cross-border cyber attacks by developing consensus for monitoring, keeping logs, information sharing, and cooperation against incidents.

Botnets are a central technical phenomenon playing on the weakness of distributed systems. Christian Kreibich discussed his and his colleagues' efforts to understand botnets by infiltrating them, thereby leading to ways to thwart botnets and the damage they can cause. Since around 2007, they have been a constant presence including Storm, MegaD, Waledac, amongst others. It is a new research experience generating significant interest, but in addition to the technical challenges, dealing with botnets is also fraught with sociological, legal, and ethical challenges that need to be addressed. The following table shows a summary of the insights and challenges presented:

	INSIGHTS	CHALLENGES
TECHNICAL	» Understanding of MO[1] » Spam awareness » Botnet size estimation » C&C rewriting » Offense in depth [1]modus operandi	» Arms race advancement » Invasion resilience » Bot reliability » Malware containment » Colliding experiments
SOCIOLOGICAL	» Victim behaviour » Spammer behaviour » Bot herder behaviour » Market analysis » Volumes » Profits	» Victim privacy » Human subjects » IRB approval » Law enforcement involvement » Ethics » Do no harm

Table 1. Insights and Challenges for Botnet infiltration, Kreibich, C.

Marc Dacier focussed on the need for exchanging data for the purpose of attack attribution, which identify the root causes of observed attacks by linking them together through the use of common, external, contextual "fingerprints". He provided examples and references to what is being done within their WOMBAT and other projects. Cyber criminals often automate various steps of their attack workflow, and this leaves traces that can then be found through various methods, potentially including automated methods. Within the WOMBAT project, they have developed a semi-automated framework, TRIAGE, that includes expert knowledge in order to extract meaningful data sets to reason about the modus operandi of the malicious actors. Application of the approach led to significant contributions in a Symantec Internet Security Threat Report on Rogue Anti-Virus programs.

TRIAGE can help to obtain better insights into how cyber criminals operate, or how and when they change their tactics. Consequently, this will help improving detection or end-user protection systems. It will also automate the identification of networks of attackers, unless they completely change their modus operandi for each campaign. This will speed up the move towards an early warning system and ultimately, support law-enforcement for stopping emerging / ongoing attack phenomena.

A major challenge for this emerging field is that it requires a multidisciplinary approach, with expertise required from computer security, networking, knowledge mining, visualisation, law, sociology, forensics, and more. Another major challenge is that international collaboration is needed for access to stable, representative and diversified sets of data. Symantec owns a very rich amount of threats related datasets and is working to build an infrastructure to provide access by researchers to a sampled set of these data feeds. Doing so will require addressing issues related to privacy and confidentiality of data, noting that simple anonymization is not sufficient. For example, discovered knowledge can be sensitive (from a technical, political, sociological or even business viewpoint).

The panel led to a lively discussion, with particular excitement around the desire for researchers to have access to relevant data. Based partly on conversations initiated at the workshop, NSF later sponsored a workshop, "Cybersecurity Data for Experimentation" on August 27, 2010, bringing together cybersecurity researchers and industry and government representatives with relevant data resources, including Symantec, towards the goal of enabling the use by the academic research community of real-world cybersecurity data.

A summary of conclusions from the session ***Data for Network Management and Security***:

- Data sharing can facilitate the detection, prevention, and attribution of a wide variety of cyber attacks, including denial of service attacks and botnets.
- International cooperation is required to combat cross-border cyber attacks in order to have consensus for monitoring, keeping logs, information sharing, and cooperation against incidents.
- International data sharing will require both technical and legal advances.
- Insights and challenges for combating cyber attacks span across technological and sociological domains.

Panel Session 2. ***Approaches to Risk in a Networked World.***

Moderator: Volkmar Lotz, SAP.

Panelists:

- *Problems with notice and consent,* Helen Nissenbaum, New York University.
- *LinkedOn – concerns about data linkability,* Mireille Hildebrandt, Vrije Universiteit Brussels.
- *Dealing with risks associated to network services*, Kazukuni Kobara, National Institute of Advanced Industrial Science & Technology and Japan Science and Technology Agency Center for Research and Development Strategy.

The panel concentrated on a number of risks to trust and security in a networked world and approaches of mitigating those risks, taking into account not only technical perspectives but also sociological and legal perspectives.

Helen Nissenbaum spoke about challenges related to notice and consent. Notice and consent has been a common approach to dealing with data exchange, but there are problems with scaling it to today's networked world and across international boundaries. Obtaining consent is costly in time and resources, both of providers and users, and requests to users can be confusing and/or ignored. The potential for confusion is even greater when dealing with cross-national requirements. The provision of opt-in or opt-out mechanisms could be a way forward, but that must be built into the technology of the systems and they only partially mitigating the potential for confusion. Nissenbaum proposes that the notion of contextual integrity, or context-relative informational norms, can be a useful framework for considering solutions that give more control to the user.

Mireille Hildebrandt discussed risks related to transnational flows of data including personal data, relational data, and other data. A number of example scenarios were discussed, including information from SWIFT, PNRs, SNS, search engine logs (Google), cloud computing, eCommerce, EIN, travel/transport, ehealth, and mhealth.

She noted while addressing such risks are important, one must remember the primacy of connectivity and linkability and the primacy of data science. Specifically, connectivity is what turns data into information and information into knowledge; linkability is what makes devices and infrastructures smart. Data science includes knowledge discovery in data bases and is the combination of software programming, statistics and storytelling/art that "extracts the nuggets of gold hidden under mountains of data" (Economist 27th February 2010). Linkability includes cases where data pertaining to one individual is linked across different contexts (e.g., deanonymising data) and cases where linking personal or other data to computational knowledge (e.g., targeted servicing). Again, linkability provides both valuable knowledge discovery opportunities and risks to privacy.

A number of solutions were presented including Hildebrandt's proposal of ambient law, consisting of: articulations of legal protections into the smart infrastructure; feedback to enable a measure of smart control; transparency enhancing tools; and "piercing the computational veil," or coming to terms with hidden computational complexity.

Kazukuni Kobara focussed on a variety of risks to services operating across networks and countermeasures against these risks. He described several examples including social engineering (phishing, peeping); insecure channels (eavesdropping, man-in-the-middle attacks, impersonation); leakage from server (abuse of privilege, intrusion); leakage from client (loss, theft); and hijacked terminals (malware-infected terminals, fake or physically modified terminals). Countermeasures include the use of independent authentications and terminals for secure e-transactions, enhancement of tamper-resistance, protection against side channel attacks, and making cryptosystems resistant against key leakage.

A summary of conclusions from the session ***Approaches to Risk in a Networked World***:

- Because security and privacy are often after-thoughts to the primary purpose of a transaction or interaction, risks to security and privacy are widespread.
- There are a variety of approaches to dealing with such risks, including giving more control to the user, building articulations of legal protections into smart infrastructures, and cryptographic mechanisms.
- Risk can be viewed differently when taking a technology, legal, or economic viewpoint.

Panel Session 3. ***Technical Challenges and Approaches for Data Sharing***

Moderator: Felix Wu, University of California at Davis.

Panelists:

- *Formal foundations for security architectures*, Ron van der Meyden, University of New South Wales.
- *Getting the information across to the user with Visual Analytics: Challenges and Applications,* Daniel Keim, University of Konstanz.
- *Pinning down "privacy" in statistical databases*, Adam Smith, Penn State University

This panel highlighted some recent and promising technical approaches to cope with difficulties of data sharing.

Ron van der Meyden covered a number of recent attacks in Australia against networks, e.g., hacking attacks against major mining companies, and suggested that this demonstrates the need for military-grade security for enterprises. The design processes and objectives of "multiple independent levels of security" were presented, including the requirements for semantics of architecture designs for this approach and extensions to this work being carried out by the speaker. A number of examples where given showing the feasibility of formally deriving global properties from an abstract level of specification of architecture and properties of trusted components. However, many research challenges remain including: are there classes of architectural specifications that can be implemented using standard patterns? connections to concrete mechanisms, e.g. access control; how to implement such specifications in general? richer semantics of architectures, for example for timing, probability; syntax required for architectural specifications; and efficiently automatable cases of verification.

Daniel Keim discussed the issue that one of the most important challenges of the emerging information age is to effectively utilize the immense wealth of data and information acquired, computed and stored by modern information systems, even without considering the security and privacy of the stored information. Due to the extreme size of the data sets, users, and analysts may get lost in irrelevant or inappropriately processed or presented information, a problem that is generally called the information overload problem. Visual analytics is an emerging research discipline that tries to make the best use of the huge information loads by combining the strengths of intelligent automatic data analysis with the visual perception and analysis capabilities of the human user. Presenting data in an interactive, graphical form often fosters new insights, encouraging the formation and enabling the validation of new hypotheses. Visual analytics has an exciting potential as exemplified by a diverse set of applications but a number of challenges remain, including the eminent problem of data security and privacy.

Adam Smith discussed differential privacy, and approach to privacy in statistical databases. In addition to having large amounts of personal data, statistical databases are now containing larger sets of data and more types of data. As noted in the previous panel, there are two seemingly conflicting goals in the use of data: utility, which extracts important information from the data, and privacy, which protects important information from disclosure. As many recent examples have demonstrated, straightforward anonymization of data is not sufficient to protect individual privacy. In the context of statistical databases, differential privacy provides a solution to the apparent conflict between utility and privacy. Roughly speaking, utility is interpreted to mean that global or aggregate properties can be disclosed, while privacy ensures that individual information stays hidden. Differential privacy is an extremely promising approach, but challenges remain, including understanding when aggregate information may itself reveal information that should be kept privacy and how to reason about privacy and anonymity more generally.

A summary of conclusions from the session ***Technical Challenges and Approaches for Data Sharing***:

- Data sharing has challenges that range across a variety of areas including specification of correct behavior, helping end users make sense of vast amounts of data, and privacy.
- Significant challenges associated with security architectures using formal foundations include: are there classes of architectural specifications that can be implemented using standard patterns? connections to concrete mechanisms, e.g. access control; how to implement such specifications in general? richer semantics of architectures e.g. for timing, probability; syntax required for architectural specifications, efficiently automatable cases of verification.
- The information overload problem can be addressed with intelligent automatic data analysis with the visual perception and analysis capabilities of the human user with visual analytics.
- Straightforward anonymization is frequently subject to linkability and de-anonymization attacks.
- Significant new inroads are being made on privacy in statistical databases via differential privacy.

IV. Breakout Sessions

The workshop included two breakout sessions in order to allow for the entire group to focus on two aspects of security and privacy in international data exchange. The topics were: ***technical challenges and opportunities for transnational data repositories*****,** which included addressing ways to represent, reason about, and enforce diverse security, privacy, and retention policies, and ***differences and commonalities: international vs. domestic, different application domains***, which examined whether and how the challenges of international exchanges are different from domestic data exchanges, as well as differences that arise across different application domains. We describe each in more detail below.

Breakout group on technical challenges and opportunities for transnational data repositories:

Co-leaders:
Anupam Datta, *Carnegie Mellon University*
Artur Hecker, *Institut Telecom-ParisTech*

This breakout group explored the technical challenges, and associated technical opportunities, for data repositories that a transnational in nature—i.e., those that are physically spread across different countries, or that include data from different countries, or that make data available to different countries. For example, as was highlighted earlier in the workshop, active collaboration of the international community on the exchange of technology/user experiences, global honey pots, test beds, and attack pattern data would significantly help develop both synergy and cohesive handling of global scale security/privacy attacks.

The participants discussed the need for an international system for data exchange related to cyber crime, attack patterns and best practices. With a reasonable characterization of the target and development of data exchange scenarios in this context, it was felt that the result would help motivate the required enabling and supporting technical research and development opportunities for international collaboration. This concept is very difficult for countries to address, even though an inability to effectively coordinate such a system leaves communities engaged in protection against cyber attacks at a severe disadvantage. Therefore, it is clearly important to work out how exchanging and collaboration could work across multiple countries, and work out the technologies that could make this approach safe for all concerned as they increase its feasibility. Such a sharing and collaboration framework could be very relevant in the EU-US context, but could also support OECD-wide data exchange with other countries. The benefits gained from such an international framework would be significant. It would clearly result in improvements to coordination of protection activities across countries, enhance data available to understand cyber trends, and provide an empirical foundation for securing systems.

In addition to focusing on a number of important questions related to the technical and policy challenges and opportunities for transnational data repositories, the session focused specifically on actions that could be taken by the international trust and security communities in the short term. The discussion that took place at the workshop served to highlight the need for further research and international collaboration in these areas.

A number of questions help frame the discussion:

What is the purpose of data exchange? Before delving into technical challenges, it is important to understand what the actual goals of a transnational data repository might be.

In particular, what can we do with transnational data repositories that we could not do otherwise?

What are typical applications? Some examples that lend themselves to benefiting from international collaboration include critical infrastructure protection, enterprise IT security improvement, and law enforcement.

What are examples of scenarios for international data exchange? Some examples include network attack signatures, e-finance, health records, and electrical grid faults.

What incentives promote/deter data exchange? Some benefits to be gained by sharing data are the ability to obtain a broader view, and the ability for defenders to collaborate. However, it is recognised there is difficulty in collecting and evaluating data from diverse sources, which could deter data exchange. There are also different privacy concerns and rules, which must be adhered to and addressed for all participants engaged in the exchanges.

What are acceptable policies governing such exchanges? A framework for considering questions of acceptable policies is “contextual integrity” (as put forth by workshop participant Helen Nissenbaum from New York University).

How do we express and enforce such policies? Some aspects of policy enforcement have been well studied by the security community for years. Three primary mechanisms for providing security and privacy for data are: (1) preventive policy enforcement, e.g., access control; (2) privacy through accountability (e.g., enforced through incentives or audit); (3) privacy-preserving transfer of and computation over aggregate information rather than data about individuals.

International data exchange is particularly relevant when there is a need that crosses national boundaries, such as data needed to determine compliance with international regulations (emissions etc.), cyber-crime (attack and defense patterns), global pandemics, financial data sharing, and rapid incident-response. Some specific examples include: tracking trends on cyber statistics across the OECD; anti-crime measures related to cyber crime targets, vectors, methods, counter-measures; early warnings could be enhanced with integrated detection capabilities, signatures and anomaly recognition for analysis; closing defensive gaps enabled with comparison of defensive coordination and best practices; IP Protection enabled with detection and prevention of industrial espionage; expertise integration possible with a focus of collective expertise on important cyber data and analysis tasks.

As compared with domestic data exchange, some challenges that arise with international data exchange arise from dealing with differences across countries, such as different cultural norms, different legal regimes e.g., data retention, related to privacy, etc., and different authorization and credential mechanisms. Suggested directions for addressing these differences include the development of international technology platforms, the use of incentive-based enforcement, standardization of formats (semantic web etc.) and of best practices for data exchange. Although even domestic data exchanges must be able to cross administrative domains, there is a larger distance between administrative domains in the international setting and co-operation and input across countries in standardization efforts is critical.

For making progress on technical challenges in international data exchange, it is desirable to focus on specific domains and use those experiences to identify some general abstractions and technology goals that cut across these domains. Within specific domains, common issues to be addressed include: data, policies, mechanisms, architectures; use and purpose of data; what are the representative abstractions? are there useful “meta-formalisms” by which different formalisms used by different countries

can be integrated?; what specific policies do people care about in the real world?; and are these policies in conflict? Can we develop formalisms and tools that help manage inconsistencies?

The participants specifically discussed the possibility of working together on an architecture or framework for an **International Cyber Data Exchange System**[1]. International collaboration and coordination could reduce defensive gaps across the OECD and build crisis-response capacity. Research and development coordination will be enhanced through leveraging and combining task-relevant national expertise. Such an international system would improve defensive understanding and coordination resulting in biasing the successful work factors for cyber attack and defence in favour of defenders. The international system could be used for data exchange related to cyber crime, attack patterns and best defence practices. In addition, bringing together of the trust and security communities could motivate relevant research and international collaboration opportunities via the technical needs in a data exchange scenario. There would be added benefits to this approach rather than forward chaining from current cyber research alone (deduce scenario from security capabilities). A backward chain approach where the data exchange scenarios would lead to enabling research and development would be more appropriate for determining the relevant technical challenges and opportunities. This approach could also lead to a much better understanding of the data itself: what data makes sense to exchange, what are impacts, what are the collection issues, and what sequence of data domains might be used to ramp up?

The participants discussed some specific challenges that would need to be met in order to develop the technical components of secure and private data repositories. These include: (1) representing and structuring data (including standards for structured text); (2) policy representation and understanding (including understanding the law and social norms, expressive policy languages, policy analysis and conflict detection, formalization and semi-automated enforcement, and usability); (3) architectures and enforcement (including cryptography, private data analysis, and watermarking, identifying anomalous behaviour, audit and accountability, managing risks and economic analysis, access control and other preventive techniques, issues regarding integrity of data, undo decisions, provenance, retraction, and update, process-centric vs. data-centric architectures, usability, and compositional enforcement of policies under constraints, and working in legal requirements and social norms into different points of the architecture; and (4) development of specific testbeds to use as testing ground for ideas in all of the above areas.

As specific direction for considering specific testbeds, cloud platforms in which data moves around and associated policies change can allow effective exploration of how to design such a system to support enforcement of policies across boundaries. A platform can provide an interface for people to contribute data to a data repository that can be used as a testbed (e.g., network attack data, DHS, clinical studies data, vulnerability data). Such a platform could be used to explore types of data and data ontologies. Cloud computing platforms offer generality and are international by default. They can also be specialized to different application domains including DRM and health care.

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

Breakout group on differences and commonalities: international vs. domestic, different application domains.

Co-leaders:
José Fernandez, *École Polytechnique de Montréal*
Aljosa Pasic, *Atos Origin*

The session examined where international cooperation is critical to this topic and to what extent can the same technical tools be useful across different application domains, and where do differences arise. A number of research challenges for the international trust and security communities were identified. In order to progress towards international data exchange, there is a need to first be able to express national and local policies in order to enable automated comparison/negotiation/merging of data across borders.

Providing trust and confidence in global data exchange schemes requires also the compatibility of national legislations and acknowledgement of international challenges, including infrastructures offering the required mechanisms. International data exchange requirements, as opposed to national requirements, will correspond to an interest from stakeholders as well as the convergence in policies, strategies etc. National legislation and cultural differences may both require "reconciliation," or at least some level of compatibility. Investigation should be oriented towards devising a global view of the relation between actors in data exchange, encompassing not only the technological aspects (related to dependability, resilience, survivability, security, privacy, etc.) but also inter- and multi-disciplinary fields that span over usability, education, sociology, law, and government. Interpretation of the national can be subjective; especially if this is to be translated into "executable" policies (rules encoded in data exchange components). These "semantic gaps" can cause further divergence between rules applied in individual countries: "policy decomposition" and "policy expression" have been mentioned as a major issues that must be addressed in order to reach the goal of mechanisms that enable policy enforcement or assurance of compliance (enabling accountability and authorization).

Data exchange processes should be adequately supported by flexible policy composition and integration frameworks, capable of harmonizing heterogeneous policies across multiple trust and/or administrative domains, and resolving conflicts effectively on a large scale. A challenge is managing very large policy-driven systems, where conflicts and inconsistencies are likely to arise. The ability of composing specifications formulated with an open class of heterogeneous languages and ontology model is essential for evolvable and long lasting data exchange policy systems and schemes. Standards and protocols for authorization, access policy, and audit should follow after these major concerns have been established. Related investigation areas encompass security configuration management, policy management (including fuzzy policies), policy-based access controls, and inventory management. Competing policy regimes at different levels (routing, network, federated identity, etc.) might result in emergence of small (restricted or constrained) circles of trust that limit international dimension of data exchange.

Governance and engagement of various stakeholders in decisions will increase strategic alignment of data exchange schemes and processes with security research community. Pre-defined trust relationships in data exchange system environments will no longer be taken for granted. Dealing with dynamicity will have to address research in issues such as distributed monitoring and data collection or harmonisation and dynamic policy management.

Economic factors and cost metrics in different countries are another factor to take into account. Information security economics, risk assessment, best practices, and information security management standards are some of the available metrics and measurement that might be useful in data exchange. Some important issues to consider are: mediating authority in relation to cost and consequences, such as for the security of the personal data, and detection of “fake” offices or offices with doubtful reputation. Incentives are also crucial, and they can be different in international setting, as opposed to a single sector or single country. A comparison can be made with security controls: in the beginning these have been seen as a burden, but the organisation that has security controls in place now sees these as a competitive advantage.

While many sectors have been mentioned as possible areas where international data exchange is needed, most of the discussion in this session focused on cybersecurity data exchange. It seems easy to start research in this sector as collaboration and data exchange already exists, although not always through “official” channels. However, these cybersecurity data exchanges are often limited to a circle of trust that provides a virtual organisation. There are clear incentives for all participants. Whatever the sector, end-to-end scenarios are needed in order to understand the privacy and security requirements involved. A major challenge here is dealing with cases of noncompliance through the complete chain of stakeholders in data exchange schemes. A major research challenge is the necessary assurance of compliance, especially for rules such as mandatory data breach notifications, minimum statutory damages for data subjects, etc. Compliance with transparency rules, and its feasibility at technical level, was discussed as a possible approach. It is possible that visual analytics could help with a solution.

Finally, there was also a discussion on the nature of data itself within international data exchange. A number of important topics that should be addressed in the future were raised including:

- the nuances of the exchange of social network data;
- Coordinated scoping and enforcement of policies;
- shifting from data exchange to information and knowledge exchange; and
- data forensics.

V. Next Steps

The organisation of the workshop ran very smoothly due to the extra efforts put in by the overall chairs, keynote speakers, panel session chairs, panelists, breakout session leaders, and all other attendees. The organisers were very thankful for the support received by all, especially from the National Science Foundation and the European Commission. INCO-TRUST would like to give special thanks to Rebecca Wright and Rutgers University for the local organisation aspects, which were considered excellent.

It is expected that there will be more discussions amongst the programme management regarding the need for more pro-active and "researcher-friendly" mechanisms for enabling international project teams to work together fruitfully, perhaps on some of the research challenges highlighted in this workshop. Examples of such mechanisms could be supplemental work programs similar to Objective 9.2[2] recently available in calls 4 and 5 of the European Framework 7 ICT program, which enabled add-ons to existing projects for International Cooperation specifically within Trust and Security. In addition, more medium-term to long-term mechanisms should be discussed also in parallel, such as alignment of joint research programs and one country funding both countries in truly international consortia.

For the research communities, they can examine how these topics are being addressed within their own research projects and if there is a benefit to working together (as expressed during the workshop), they should undertake this as it will be further evidence for program management to make these funding mechanisms available to the research communities. The INCO-TRUST project will promote and make this information available to the EU research communities within ICT Trust and Security and, conversely, the program management from the other countries should perform the same function. In addition, the workshop participants should disseminate and promote to other collaborators who were not in attendance at the workshop.

Regarding the selection of the topic for the workshop and future such workshops, there was considerable feedback from the participants that clearly focussing on international data exchange was an excellent decision instead of focussing more broadly on a range of trust and security topics. This strategy will be kept in mind for future workshops.

Programme management of the EU and the US announced at the conclusion of the workshop that they 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 programme management 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.

[2] http://www.inco-trust.eu/incotrust/latest-news/info-pack-for-ict-2009-9-2-inco.html

ANNEX 1. Agenda

Tuesday, May 4, 2010 at New York Academy of Sciences

9:00 - 9:30am

Welcome and Introduction:

- Rebecca Wright, Rutgers University
- Neeraj Suri, Technische Universitaet Darmstadt. Slides
- Gustav Kalbe, Acting Head of Unit — Trust and Security, DG-INFSO, European Commission
- Lenore Zuck, Program Officer, Trustworthy Computing, National Science Foundation

9:30 - 10:30am *Keynote Talk: Accountability in International Data Exchange.* Joan Feigenbaum, Yale University.

10:30 - 11:00am *Break*

11:00am - 12:15pm *Panel: Data for Network Management and Security.* (Moderator: Sotiris Ioannidis, FORTH)

- *Experiences with DDoS*, Hyuncheol Jeong, Korea Internet & Security Agency
- *Botnet infiltration*, Christian Kreibich, International Computer Science Institute
- *Attack attribution*, Marc Dacier, Symantec

12:15 - 1:30pm *Lunch*

1:30 - 2:45pm *Panel: Approaches to Risk in a Networked World.* (Moderator: Volkmar Lotz, SAP)

- *Problems with notice and consent?*, Helen Nissenbaum, New York University
- *LinkedOn: concerns about data linkability*, Mireille Hildebrandt, Vrije Universiteit Brussel
- *How to deal with risks associated to network services*, Kazukuni Kobara, National Institute of Advanced Industrial Science and Technology

2:45 - 3:45pm *Keynote Talk: Trust in the Internet: Observations on Being Highly Connected.* John Zic, Commonwealth Scientific and Industrial Research Organisation.

3:45 - 4:15pm *Break*

4:15 - 5:30pm *Panel: Technical Challenges and Approaches for Data Sharing.* (Moderator: Felix Wu, University of California at Davis)

- *Formal foundations for security architectures*, Ron van der Meyden, University of New South Wales
- *Getting the information across to the user*, Daniel Keim, University of Konstanz
- *Pinning down "privacy" in statistical databases*, Adam Smith, Penn State University

Wednesday, May 5, 2010 New York Academy of Sciences

9:00 - 10:00am *Keynote Talk: The Legal and Cultural Landscape of Privacy and Data Use*. Steve Purser, European Network and Information Security Agency (ENISA).

10:00am - 10:30am *Breakout Groups*

- *Breakout group 1*. Co-leaders: Anupam Datta, Carnegie Mellon University, and Artur Hecker, ENST. *Technical challenges and opportunities for transnational data repositories*: how to represent, reason about, and enforce diverse security, privacy, and retention policies?

- *Breakout group 2*. Co-leaders: José Fernandez, École Polytechnique de Montréal, and Aljosa Pasic, Atos Origin. *Differences and commonalities: international vs. domestic, different application domains*. In what ways are the challenges of international exchanges different from, and the same as, domestic data exchanges? Where is international cooperation critical? To what extent can the same technical tools be useful across different application domains, and where do differences arise?

10:30 - 11:00am *Break*

11:00am - 12:00 *Breakout groups continued*

12:00 - 12:30pm *Breakout groups reports and discussion*

12:30 - 1:00pm *Further steps and wrap-up*

- Jim Clarke, INCO-TRUST project coordinator, Waterford Institute of Technology
- Gustav Kalbe, Acting Head of Unit — Trust and Security, DG-INFSO, European Commission
- Lenore Zuck, Program Officer, Trustworthy Computing, National Science Foundation

1:00pm *Lunch, Workshop Adjourned*

ANNEX 2. List of Attendees

Organizers

Rebecca Wright (US Chair)	Rutgers University, USA
James Clarke (EU Chair)	Waterford Institute of Technology, Ireland
Lenore Zuck	National Science Foundation, USA
Gustav Kalbe	European Commission, Belgium

Chairs and Speakers

Marc Dacier	Symantec, France
Anupam Datta	Carnegie Mellon University, USA
Joan Feigenbaum	Yale University, USA
José M. Fernandez	École Polytechnique de Montréal, Canada
Artur Hecker	Institut Telecom-ParisTech, France
Mireille Hildebrandt	Vrije Universiteit Brussels, Belgium
Sotiris Ioannidis	FORTH, Greece
Hyuncheol Jeong	Korea Internet & Security Agency, Korea
Daniel Keim	University of Konstanz, Germany
Kazukuni Kobara	National Institute of Advanced Industrial Science and Technology, Japan
Christian Kreibich	International Computer Science Institute, USA
Volkmar Lotz	SAP Research Labs, France
Helen Nissenbaum	New York University, USA
Aljosa Pasic	ATOS Origin, Spain
Steve Purser	European Network and Information Security Agency, Greece
Adam Smith	Penn State University, USA
Neeraj Suri	Technische Universitaet Darmstadt, Germany
Ron van der Meyden	University of New South Wales, Australia
Felix Wu	University of California at Davis, USA
John Zic	Commonwealth Scientific and Industrial Research Organisation, Australia

Other Participants

Priscila Solis Barreto	University of Brasilia, Brazil
Jacir Luiz Bordim	University of Brasilia, Brazil
Lujo Bauer	Carnegie Mellon University, USA
Kyungho Chung	Korea Communications Commission, Korea
Jan Eloff	SAP and SAP Meraka Unit, South Africa
Vinod Ganapathy	Rutgers University, USA
Jose Manuel Gomez-Perez	iSOCO, Spain
William Horne	Hewlett Packard Labs, USA
Sorin Huss	Technische Universitaet Darmstadt, Germany
Souhwan Jung	Korea Evaluation Institute of Industrial Technology / Ministry Knowledge Economy, Korea
Erin Kenneally	University of California at San Diego, USA
Angelos Keromytis	Columbia University, USA
Carl Landwehr	National Science Foundation, USA
Lucy Lynch	ISOC, USA
John Mallery	Massachusetts Institute of Technology, USA
Fabio Martinelli	National Research Council CNR, Italy
Patrick McDaniel	Penn State University, USA
Joel Reidenberg	Fordham University, USA
Xiaoyang (Sean) Wang	National Science Foundation, USA
Sam Weber	National Science Foundation, USA
Heung Youl Youm	Soonchunhyang University, Korea

ANNEX 3. Position Papers

A number of the workshop participants provided additional positions statements and other materials before, during, and after the workshop:

Jim Clarke and Neeraj Suri
Jan Eloff
Daniel Keim
Jose Manuel Gomez, also this presentation
Artur Hecker and Michel Riguidel
Mireille Hildebrandt
Bill Horne
Sorin Huss, also this presentation
Volkmar Lotz
John Mallery
Fabio Martinelli
Aljosa Pasic
Steve Purser

Note: there are hyperlinks within the names of the papers here. The programme, slides, and position papers can also be found at the workshop web site:
http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/program.html